DETAILED DESCRIPTION OF THE INVENTION

[0020] By way of introduction to one preferred inventive implementation, **FIG. 1** illustrates a known prior art network layer stack **10** defined to include the internet connection protocol ("IP") as discussed below. At the top of stack **10** is an application layer **12**, which typically represents one or more programs that are commonly used by consumers for various reasons, including personal and business computing. Beneath application layer **12** are located two protocol layers, namely, a transmission control protocol ("TCP") layer **14** and a user datagram protocol ("UDP") layer **16**. TCP layer **14** is a connection-oriented layer, that is, once a connection is established from a source to a destination and through that layer, then traffic through that connection is confirmed so that if a packet is lost before it is confirmed by its destination then the source re-transmits the packet. In contrast, UDP layer **16** is connectionless and, thus, no confirmation is made as between a packet passing from a source to its destination; accordingly, if a packet is lost in a UDP communication then there is no re-transmission of that packet. Comparing then the TCP and UDP layers **14** and **16**, TCP assures greater integrity of communications yet it requires greater overhead than UDP.

[0021] Below layers **14** and **16** is an IP layer **18**, using IP as introduced above. Thus, both TCP and UDP network packets along a given network pass through the IP layer **18** and therefore also must comply with the requirements of the IP protocol. IP layer **18** is also a connectionless layer, although for TCP packets passing through the layer the connection-oriented nature of TCP layer **14** may be relied upon to provide additional data integrity. Due to the connectionless nature of IP layer **18**, there is a trend in the networking art to provide measures of so-called quality of service ("QoS") in order to give priority or otherwise provide guidance to the flow of connectionless IP packets. In any event, and importantly for one example of the preferred embodiment as detailed in this document, each TCP (as opposed to UDP) network packet passing from a single source to a single destination and through IP layer **18** includes a unique TCP sequence number that thereby distinguishes that packet from all other TCP packets communicated from the source to the destination in a given flow session. This TCP sequence number is required as a TCP parameter and may be used for various purposes as known in the art, while the preferred embodiments further monitor the number to evaluate network performance as detailed below. Before reaching that discussion and completing the discussion of **FIG. 1**, located below IP layer **18** is a physical layer **20**. Physical layer **20** is commonly associated with the physical hardware at a source or destination, as typically represented by a network interface having a media access control ("MAC") address.

[0022] As further explored below, the preferred embodiments evaluate network performance, preferably as it is reflected in communications between specified nodes such as in specified sub-networks in the network, in response to a real-time evaluation of the progression of TCP packet sequence numbers. In this regard, in part the evaluation by the preferred embodiments includes consideration of three prior art observations made by the NLANR as relating to TCP sequence numbers. These three observations are explored below in connection with **FIGS. 2 through 4**.

[0023] **FIG. 2** illustrates a plot of the evolution of TCP sequence numbers over time when a TCP session, including the source, destination, and network, behave normally. In **FIG. 2**, the horizontal axis represents the passage of time since the beginning of the TCP session observation, while the vertical axis represents the sequence number of the last byte of each data packet. Note that the sequence numbers are shown for simplicity of illustration to start from zero, whereas in reality they typically commence from a non-zero, and likely random, number, and then increase from that point. In any event, the sequence numbers will increase monotonically unless there are reordered or retransmitted packets. While intuitively one might expect a linear relationship for normal behavior, instead note that the plot provides a number of upward curves each ending with a peak, such as shown by ways of example with a curve prior to a point P_1 at time t_1 and a point P_2 at a time t_2. Note that these curves, followed by respective peaks, occur under ideal network operation because the source transmission rate will tend to increase toward and reach the normal upper limit of the traffic rate for the destination (or the network). In other words, under TCP protocol, transmission occurs in a TCP control window, where the source starts transmitting at a certain rate, and hence with a corresponding steady increase in TCP sequence numbers, followed by an attempt within the window over time to increase the transmission rate and hence with a change in the rate of the ascension of the TCP sequence numbers. The source's periodic attempts during the TCP control window to increase the TCP sequence number frequency continues until the limit of the destination (or network) to accurately communicate packets is reached. As this limit is reached, the source will reduce its transmission rate for a time and thereafter again continue to increase it until the limit is again reached later in time.

[0024] **FIG. 3** illustrates a plot of the evolution of TCP sequence numbers over time, when during a TCP session the network operates normally but either the source or destination is limiting the bandwidth on communication. Here again, the horizontal axis represents the passage of time while the vertical axis represents the increase in sequence numbers. However, the plot of TCP sequence numbers reflects a straight line. Typically such a result is anticipated because it represents that the source is not reaching the maximum bandwidth limitation of the network or destination. Thus, while the TCP sequence numbers increase, the increase of the sequence numbers from one to the next is in a constant fashion across the entire illustrated plot, as opposed to an acceleration of those numbers that increases over time as shown in **FIG. 2** and that also peaks from time to time as a normal limit is reached.

[0025] **FIG. 4** illustrates a plot of the evolution of TCP sequence numbers over time, when during a TCP session the network is limiting the bandwidth of communication between the source and destination and, thus, it is presumed during such time that the source and destination are otherwise capable of communicating at their respective maximum bandwidths. However, the plot of TCP sequence numbers illustrates curves with discontinuities between the curves. For example, at time ti, the TCP sequence numbers are at a point P_{10}, but transmission is interrupted until a time t_2. At time t_2, however, note that a slight drop occurs in the TCP sequence number as shown at point P_{11}. This type of pattern repeats later at time t_3 where a sequence number shown as point P_{12} is reached, but an interruption then occurs until

BNSDOCID: <US____20040073655A1_I_>

communication through to the destination from the source is achieved at time t_4 and having a sequence number at point P_{13}. The behavior illustrated by these discontinuities occurs due to packet losses along the network as resulting from network irregularities. In other words, recalling that TCP communications are connection-oriented, when a network irregularity occurs one or more TCP packets will be lost, and those packets will be required to be re-transmitted by the source. As a result, the source, which receives the indication of the failure at a time when it was prepared to transmit a new packet having a certain TCP sequence number, is instead required to backtrack to re-transmit a previous packet with a lower TCP sequence number, followed by all packets following the re-transmitted packet. The beginning of such a re-transmission, therefore, is shown by way of example at point P_{11} (and various other points in **FIG. 4**), where a drop is shown in TCP sequence number as compared to point P_{10}, where the drop occurs due to the backtrack and re-transmission by the source of a previously-transmitted packet(s).

[0026] **FIG. 5** illustrates a block diagram of a system **60** into which the preferred embodiments are implemented. System **60** generally includes a number of stations ST_1 through ST_4, each coupled to a network **70** via a router, and each operable to send packets as a source or receive packets as a destination. By way of example, network **70** is an internet protocol ("IP") network such as the global internet or other IP-using network, where each station and IP networks in general are well known in the art. However, one skilled in the art should appreciate that the use of the IP protocol is by way of illustration, and many of the various inventive teachings herein may apply to numerous other protocols, including by way of examples asynchronous transfer mode ("ATM"), token ring, Novell, Apple Talk, and still others. In any event, returning to network **70** as in IP network, and also by way of an example, each station ST_x may be constructed and function as one of various different types of computing devices, all capable of communicating according to the IP and to include the TCP protocol. Lastly and also by way of example, only four stations ST_x are shown so as to simplify the illustration and example, where in reality each such station may be proximate other stations (not shown) and at a geography located at a considerable distance from the other illustrated stations. For example, station ST_1 might be located in Montana while station ST_2 is located in California, and station ST_3 might be located in New York while station ST_4 is located in Florida.

[0027] Continuing with **FIG. 5**, along the outer periphery of network **70** are shown a number of edge routers ER_1 through ER_{11}, while within network **70** are shown a number of core routers CR_1 through CR_4. The terms edge router and core router are known in the art and generally relate to the function and relative network location of a router. Typically, edge routers connect to remotely located networks and handle considerably less traffic than core routers. In addition and due in part to the relative amount of traffic handled by core routers, they tend to perform less complex operations on data and instead serve primarily a switching function; in other words, because of the tremendous amount of throughput expected of the core routers, they are typically hardware bound as switching machines and not given the capability to provide operations based on the specific data passing through the router. Indeed, core routers typically do not include much in the way of control mechanism as there could be 10,000 or more connections in a single trunk. Further, typically core routers do not involve their operations with TCP related items and instead deal at the IP level and below. In contrast, edge routers are able to monitor various parameters within data packets encountered by the respective router. In any event, the various routers in **FIG. 5** are shown merely by way of example, where one skilled in the art will recognize that a typical network may include quite a different number of both types of routers. Finally, note that each core router CR_x also generally may be constructed and function according to the art, with the exception that preferably the core routers may include additional functionality for purposes of traffic irregularity detection based on TCP sequence number evaluation as described below. In addition, each edge router ER_x also generally may be constructed and function according to the art, with the exception that preferably the edge routers are responsive to the traffic irregularity detection of the core routers, as also described below.

[0028] Completing the discussion of **FIG. 5**, note that the various stations, edge routers, and core routers therein are shown connected to one another in various fashions and also by way of example. Such connections are intended to illustrate an example for later discussion of the preferred operation and also to reflect a general depiction of how networks are generally established. Thus, each station ST_x is shown connected to a single edge router ER_x, where that edge router ER_x is connected to one or more core routers CR_x. The core routers CR_x, also by way of example, are shown connected to multiple ones of the other core routers CR_x. By way of reference, the following Table 1 identifies each station and router shown in **FIG. 5** as well as the other device(s) to which each is connected.

TABLE 1

station or router	connected nodes
ST_1	ER_1
ST_2	ER_{10}
ST_3	ER_5
ST_4	ER_7
ER_1	ST_1; CR_1
ER_2	CR_3; CR_2
ER_3	CR_2
ER_4	CR_2
ER_5	ST_3; CR2; CR_3
ER_6	CR_3; CR_4
ER_7	ST_4; CR_4
ER_8	CR_4
ER_9	CR_4
ER_{10}	ST_2; CR_1
ER_{11}	CR_4
CR_1	ER_1; ER_{11}; ER_{10}; ER_2; CR_2; CR_3; CR_4
CR_2	ER_2; ER_3; ER_4; CR_1, CR_3; CR_4; ER_5
CR_3	ER_5; ER_6; CR_2, CR_1; CR_4
CR_4	ER_7; ER_8; ER_9, CR_1, CR_2; CR_3; ER_6

[0029] Given the various illustrated connections as also set forth in Table 1, in general IP packets flow along the various illustrated paths of network **70**, and in groups or in their entirety such packets are often referred to as network traffic. In this regard and as developed below, the preferred embodiments operate to identify any irregularities in such network traffic. Finally, note that **FIG. 5** may represent a simplified

version of a network or the internet in that only a few stations and routers are shown, while one skilled in the art will readily appreciate that the inventive concepts in this document may be applied to a larger number of stations, routers, and the network interconnectivity between those devices.

[0030] **FIG. 5** also illustrates a number of network monitors NM_1 through NM_5, where the choice of five such network monitors is only by way of example given the limited amount of other hardware that is shown for network **70**. As detailed below, each network monitor NM_x is operable to sample, and possibly respond to, irregularities in the TCP sequence number in an IP packet that passes along the conductor(s) to which the network monitor is connected. Further, the components of each network monitor NM_x are described below, but at this point the connections of each such monitor are noted in the following Table 2:

TABLE 2

network monitor	connected nodes
NM_1	CR_1; CR_2
NM_2	CR_2; CR_3
NM_3	CR_1; CR_3
NM_4	CR_3; CR_4
NM_5	CR_1; CR_2; CR_3; ER_7; ER_8; ER_9

[0031] **FIG. 5** and Table 2 demonstrate that each of network monitors NM_1 through NM_4 is connected to sample packets passing along the conductor(s) between a pair of core routers. However, network monitor NM_5 is by way of an alternative example incorporated into core router CR_4. As a result, network monitor NM_5 is able to sample packets communicated with any of the nodes to which core router CR_4 is connected, namely, core routers CR_1, CR_2, CR_3, and edge routers ER_7, ER_8, and ER_9. Thus, the contrast of network monitor NM_5 to the other illustrated network monitors NM_1 through NM_4 is shown to demonstrate that in the preferred embodiment each network monitor NM_x may sample packets as a stand alone entity or may be combined with the hardware and software of an existing router; indeed, in the preferred embodiments a network monitor NM_x also may be combined with network or element management systems. In any event and by way of introduction to details provided later, in the preferred embodiments the sampling functionality of each network monitor NM_x permits real-time monitoring of the TCP sequence numbers in network packets, and in response determinations may be made, and actions may be taken, based on detecting network traffic irregularities based on the behavior of the TCP sequence numbers.

[0032] **FIG. 6** illustrates a block diagram of each network monitor NM_1 through NM_4 of **FIG. 1**, with the further understanding that functionally the following description also may be applied to network monitor NM_5 with the addition that certain functionality may be provided by the hardware and software already available from core router CR_4. Turning then to **FIG. 6**, first note that a console **30** is associated with network monitor NM_x, where in the preferred embodiment a single such console **30** communicates with multiple network monitors NM_x. For example, returning briefly to **FIG. 5**, preferably each of network monitors NM_1 through NM_5 communicates with a single console **30**, where such communications also may be by way of packets between console **30** and the network monitors NM_x. Console **30** may be constructed by one skilled in the art using various forms of hardware and software, where the selection is a matter of implementation choice in order to achieve the functionality described in this document. Turning to that functionality, console **30** preferably provides an administration (configuration) function and a characterization (reporting) function. To permit a user to perform these functions, various interfaces may be used such as a graphical Web-based configuration tool or a command line tool, where one preferable approach implements console **30**, by way of example, using the Apache Web server with the PHP server-side scripting language to provide a dynamic interface to a flow store **32**. In any event, the user interface preferably provides different screens for each of the administration and characterization functions. The actual interface and screens, however, may be implemented in various forms, where it is desirable for any form that a user can properly control console **30** to perform its administration and characterization function with respect to its flow store **32**. Preferably, a network administrator or the like uses the administration functionality of console **30** to create a set of rules and to provide those rules along with a predictor methodology to an RTFM meter **36** described later, where those rules cause meter **36** to retrieve TCP sequence numbers and the predictor methodology is later used to evaluate the history of the TCP sequence numbers for a flow, as also discussed later. Also, once the system is configured and left to collect TCP sequence number information from or about the monitored packets, the network administrator can use the characterization screen to query the information so as to generate network status reports based on the collected information and to thereby detect any network irregularities.

[0033] As introduced above, console **30** is connected to a flow store **32**, which preferably represents a storage medium that stores a flow database relating to monitored TCP sequence numbers. In the preferred embodiment, each network monitor NM_x includes its own flow database, although alternative embodiments may be created where more than one network monitor NM_x shares a common flow database. In the preferred embodiment the flow database in flow store **32** is an SQL-compatible database using the PostgreSQL relational database management system, and console **30** communicates with this database through the Web server's PHP link to the SQL database. Thus, any administration and configuration changes made via console **30** are passed directly to flow store **32**. Given the preceding, one skilled in the art should appreciate that access to flow store **32** can be achieved by SQL queries, enabling network administrators to automate the configuration process or integrate report generation. In the preferred embodiment, flow store **32** stores what is referred to in this document as a "rule set" (or "rule sets" when plural), which is initially provided to the flow store **32** from console **30** as part of the administration function and which is also conveyed to meter **36**. Additionally, flow store **32** stores the progression of TCP sequence numbers from a monitored flow between a source and destination node, as further detailed below. Moreover and as also discussed below, flow store **32** may store numerous different progressions of TCP sequence numbers, each corresponding to a monitored flow between sets of corresponding source and corresponding destination nodes. Still fur-

BNSDOCID: <US____20040073655A1_I_>

ther, flow store **32** preferably stores packet time of arrival data, as also detailed later. Lastly, recall that an RTFM meter **36**, described below, stores a predictor methodology. From this predictor methodology, analyses are preferably made on the TCP sequence number progression(s) and times of arrival as stored in flow store **32**, and those analyses may be reported to console **30** and are also used as a basis to respond to network irregularities.

[0034] Continuing with **FIG. 6**, recorder layer **34** provides an interface between flow store **32** and a meter **36** (or meters) in use and coupled to the network, and meter **36** copies TCP sequence numbers from respective selected network packets passing through the meter. Specifically, as each network packet is identified as between a particular same source and destination node, meter **36**, in response to a predictor methodology, provides the TCP sequence number from the packet to recorder layer **34**, which in turn communicates that information to flow store **32**. In the preferred embodiment, the monitored source and destination node can be determined randomly, or it can be identified from one or more rules in a rule set in flow store **32**. Thus, the applications of recorder layer **34** can be separated into two categories: manager applications and meter reading applications. Manager applications configure meter **36**, based on information, including rules in one or more rule sets, in flow store **32**. Meter reading applications permit the TCP sequence number data collected by meter **36** to be provided in a data format usable by flow store **32** and, indeed, recorder layer **34** facilitates the passage of that data into the flow database of flow store **32**. Recorder layer **34** applications may pass information between flow store **32** and the network probes of meter **36** either synchronously or asynchronously. This gives network administrators the flexibility of either using real-time network flow meters (i.e. NeTraMet) or importing data from other network analysis tools that are not able to provide real-time data (e.g. Cisco NetFlow data).

[0035] In the preferred embodiment, meter **36** is a Real-Time Traffic Flow Measurement ("RTFM") meter which is a concept from the Internet Engineering Task Force ("IETF"). As known in the RTFM art, RTFM meters are previously known to be used in systems for determining the service requested by IP packets that are passing through a network for purposes of collecting revenue, where such a service is identifiable by the transport port number specified in each IP packet. For example, RTFM meters are currently being considered for use in systems whereby an internet user is charged based on the service he or she is using on the internet; for example, a different fee may be charged to the user for each different internet service, including mail, video, phone calls, and web browsing. However, as detailed in this document, the preferred embodiment implements the RTFM meter instead to analyze each IP packet and to determine if the packet is a TCP packet between a given source and destination and, if so, to copy its TCP sequence number for storage so that the copied numbers can be interpreted for purposes of monitoring network activity so as to evaluate network performance and, hence, identify any irregularities with such performance. More specifically, meter **36** physically probes the underlying network traffic and each time meter **36** detects an IP packet on the network, it determines whether the packet is a TCP packet and is between a given (i.e., either randomly or specifically identified) source and destination. Accordingly, during the real-time passage of numerous IP packets by the evaluating meter **36**, that meter **36** does not always copy a fixed portion of each such packet into a database such as the entire packet or the entire packet header; instead, each meter **36** evaluates the source and destination address of each TCP packet and, if a given source and destination are matched, then meter **36** communicates the TCP sequence number for the packet to recorder layer **34**. In response, recorder layer **34** inserts the captured TCP sequence number into flow store **32**. Accordingly, that stored information is then available for analysis and reporting to console **30**, as detailed below.

[0036] **FIG. 7** illustrates a flow chart of an overall method **40** of operation for each network monitor NM_x of **FIGS. 5 and 6**, where method **40** is now described and additional preferred details are provided later with respect to **FIG. 8**. Additionally, while method **40** is described below with respect to a single network monitor NM_x, preferably each network monitor NM_x performs a comparable method at its respective location in network **70**. As a result, distributed operations occur at different network locations, where by way of example the results of each individual network monitor NM_x may be accumulated by a common resource, such as at a single console **30**. From this accumulated information, greater accuracy may be achieved in identifying network irregularities and their causes.

[0037] Turning to method **40**, in step **42** a network monitor NM_x according to the preferred embodiment first detects and stores the TCP sequence numbers for each of a number n TCP packets between a first set of source and destination nodes. In the preferred embodiment, the first set of source and destination nodes can be selected randomly or may be specified by a rule in flow store **32** that is conveyed to meter **36**. By way of one example, preferably such a first set includes only a single source and a single destination. Also by way of example, each of the single source and single destination is likely in a different physical sub-network, where each such sub-network is identifiable in that nodes in each sub-network share a same portion of their address as directed to the sub-network, where typically such an address portion is that following the subnet mask in the packet address. By way of an illustrative example, assume that the source is the **FIG. 5** station ST_1 in a first physical sub-network in Montana and the destination is station ST_3 in a second physical sub-network in New York. Thus, for step **42**, the RTFM meter **36** of the given network monitor NM_x evaluates each packet passing through the meter to determine if the packet is a TCP packet from the certain source to the certain destination in the two respective sub-networks. If so, then the TCP sequence number for that packet is stored. Once n such TCP sequence numbers are stored (i.e., corresponding to n packets between the same source and destination along the logical sub-network of interest), then step **42** also processes those sequence numbers so that the regularity of subsequently received packets may be predicted, but a discussion of such processing is deferred until later. In any event, note that at the initial completion of step **42**, a first window of n packets will have been detected and processed; this window is updated to maintain a total of n packets by later processing subsequent selected packets, where for each such subsequent packet its information is processed and added to the overall information while at the same time the information for the then-oldest packet is removed from the processed information. These details are

BNSDOCID: <US____20040073655A1_I_>

better understood below. In any event, once step **42** is complete, method **40** continues to step **44**.

[0038] In step **44**, the network monitor NM_x continues to monitor IP packets until it detects another TCP packet between the step **42** source and destination, and then step **44** determines whether an irregularity exists in the TCP sequence number of the additionally-detected packet. Specifically, from the plots of **FIGS. 2 through 4**, once a sufficient number n of TCP sequence numbers are collected in step **42**, a plot of those numbers and the TCP sequence number from the additional packet in step **44** may be compared as against the trends represented by the plots of **FIGS. 2 through 4**, where the case of **FIG. 4** is of particular interest in the preferred embodiments. However, in practice, such an approach may require a considerably large value set for the value n of step **42** or it may involve a considerable delay in either collection or analysis time. Accordingly, in the preferred embodiment, step **44** collects one TCP sequence number from a next TCP packet in the first set. Additionally and as detailed below, through the use of the predictor methodology in meter **36**, as also introduced with respect to the processing of n packets in step **42** so that the regularity of future packets may be predicted, step **44** determines whether the actual TCP sequence number of the newly-collected TCP packet is within a range as predicted from the n previously-collected TCP sequence numbers of step **42**; further, step **44** also preferably determines whether the newly-collected TCP packet arrives within a time as expected based on the time of reception of one or more of the n previously-collected sequence numbers of step **42**. Additional details for this predictor methodology are described below. For sake of continuing with **FIG. 7** at this point, however, step **44** generally determines, such as through the use of the predictor methodology, whether an irregularity in the TCP sequence number of the newly-detected packet exists, such as may be indicated if the TCP sequence number of the newly-detected packet, and/or the time of arrival of the newly-detected packet, deviates beyond a threshold. Such an irregularity may reflect the conditions of **FIG. 4**. If no such irregularity is detected, then the flow returns to step **44** to detect another TCP packet in the first set and to repeat the same analysis with respect to its time of arrival and TCP sequence number. If an irregularity is detected, then flow continues from step **44** to step **46**.

[0039] Before discussing step **46**, note also in step **44** that regardless of whether an irregularity is detected, step **44** also indicates that the newly-detected packet is processed to update the data based on n packets. Specifically, recall that step **42** detects a first group of n packets in the first set and processes the sequence numbers of packets so that the regularity of future packets may be predicted. Looking now to step **44**, the latter indication of processing in that step **44** is intended to demonstrate that step **44** also updates the previous data based on the n packets of the preceding step **42**. In the preferred embodiment, this updating is such that the packet detected in step **44** becomes one of the n packets, whereas the oldest first set packet received by step **42** is now removed from the n packets. In other words, preferably the data relating to n packets is updated in a sliding window type manner, where at any given time after step **42**, the data and the predictions derived from that data as detailed below, relate only to the most recently received n packets in the first set. Once updated in this manner, the flow continues from step **44** either to step **46** or to return to step **44**, as discussed earlier.

[0040] In step **46**, having been reached due to a detected TCP sequence number irregularity between a source and destination in the first set from step **44**, the network monitor NM_x detects a TCP sequence number from one or more additional TCP packets communicated in the first set (e.g., as between the single source and single destination mentioned in the example of step **42**). For each of these additionally-detected packets in the first set, step **46** determines whether the TCP sequence number (and arrival time) also indicates an irregularity as compared to previous TCP sequence numbers and times of arrival of packets between the same source and destination. If an irregularity is not detected, then the preferred embodiment operates under the assumption that the irregularity detected in the preceding step **44** was either an isolated incident, a relatively minor irregularity, or otherwise not reason to make a network response or adjustment, and the flow of method **40** returns from step **46** to step **44**. On the other hand, if an irregularity is detected in step **46**, then the preferred method flow continues to step **48**. As detailed below, preferably an irregularity is considered as detected if the TCP sequence number and/or time of arrival of the TCP sequence packet deviates beyond a threshold, where the deviation relative to the threshold is measured based on an predicted TCP sequence number and time of arrival as provided by the predictor methodology. This threshold may be selected by one skilled in the art, and by way of example may be on the order of five percent from the predicted value.

[0041] Before discussing step **48**, note that step **46** also indicates at its conclusion, and in the same manner as discussed above with respect to step **44**, that regardless of whether an irregularity is detected, step **46** also processes the newly-detected packet to update the data based on n packets. Once more, therefore, this indication is intended to represent the update operation achieved by the sliding window, to again encompass information based on a total of n packets. Accordingly, in step **46** the updating is such that the packet (or packets) detected in step **46** becomes one of the n packets, whereas the oldest first set packet received by step **42** or step **44** is now removed from the n packets. Again, therefore, the data after step **46**, and the predictions derived from that data as detailed below, relate only to the most recently received n packets in the first set. Once updated in this manner, the flow continues from step **46** either to step **48** or to return to step **44**, as discussed earlier.

[0042] In step **48**, the network monitor NM_x continues to monitor IP packets and now collects IP sequence numbers and time of arrival data for packets in a second set of source and destination nodes, where the second set is preferably related in some rational sense to the first set (e.g., the single source and single destination) of steps **42**, **44**, and **46** and the second set is also defined by a rule or rules conveyed from flow store **32** to meter **36**. For example, recall earlier that step **44** was demonstrated by monitoring packets to detect those between source station ST_1 in a first sub-network in Montana and destination station ST_3 in a second sub-network in New York. Further, for step **48**, and since the second set is preferably related to the first set, then as a first example of step **48** consider that the second set includes any source node in the same physical sub-network as station ST_1 in

BNSDOCID: <US____20040073655A1_I_>

Montana and any destination node in the same physical sub-network as station ST_3 in New York. As a second example of step **48**, the second set may include any source node in a different physical Montana sub-network (i.e., not including the sub-network of station ST_1) and any destination node in a different physical New York sub-network (i.e., not including the sub-network of station ST_3). As a third example of step **48**, the second set may include any source node in the same physical sub-network as station ST_1 in Montana, but any destination node in a specified physical sub-network as station ST_4 in Florida; this latter example may prove beneficial where again this second set relates in some sense to the first set, such as may be the case where the destination sub-network of the first set (i.e., in New York) communicates packages received from Montana onward to Florida. In any event, the relationship between the first and second set is preferably stated or implied in the rule set(s) stored in flow store **32**. In this manner, one skilled in the art may establish different rules to thereby encompass different relationships between the first and second monitored steps, and to thereby draw corresponding conclusions based on any irregularities in the traffic flow between the nodes of the two different sets. Also in this regard, in one preferred embodiment the second set may includes the first set, and it also preferably includes a greater number of nodes than the first set. For example, step **44** (and **46**) may be directed to a single source node and a single destination node, while step **48** is directed to multiple source nodes and multiple destination nodes. In any event, therefore, in step **48** and for each packet passing through the network monitor NM_x, if it is a TCP packet of the second set, then the network monitor NM_x preferably copies the TCP sequence number, source address, destination address, and time of arrival for each of n packets between a same source and destination in the second set. In other words, if the second set has three sources, each communicating with three respective destinations (in addition to the first set source and destination), then step **48** endeavors to collect packet data for each these three pairs of source/destination nodes, thereby accumulating data for a total of three times n packets. Thereafter, method **40** continues from step **48** to step **50**.

[0043] In step **50**, the network monitor NM_x generally operates in the same fashion as described above with respect to step **46**, that is, another packet is detected and processed; however, step **50** performs its analysis with respect to the packet information obtained from step **48** in view of a next received second set packet. In other words, while step **46** analyzed packets from the first set, step **50** analyses the TCP sequence numbers and times of arrival for packets from the second set, again determining whether those two parameters deviate beyond a certain percent relative to a predicted value provided by a predictor methodology. In the preferred embodiment, the threshold of step **50** may be the same or different than the threshold used by step **46**. In any event, if the deviation, if any, is less than or equal to the step **50** threshold, then method **40** proceeds under the assumption that the earlier-detected irregularity from steps **44** and **46** were limited to the nodes in the first set, and the method returns to step **44**; optionally, however, as also shown in **FIG. 7**, before returning to step **44**, the flow can pass through a step **50***a* wherein an alarm is issued relating solely to the first set of packets. In other words, if no irregularity is found in the second set packet as examined by step **50**, then there is still the observation from the affirmative findings in steps **44** and **46** that there was an irregularity in at least two first set packets. Thus, if the level of granularity at interest is such that irregularities solely within the first set are of interest, then step **50***a* represents an indication, such as an alarm, relating to the first set so that future examination or action may be taken with respect to the cause of the first set irregularity. Continuing with step **50**, however, if the second set packet deviation exceeds the step **50** threshold, then method **40** continues to step **51**.

[0044] Before discussing step **51**, note that step **50**, in the same manner as steps **44** and **46** discussed above, also indicates at its conclusion the operation of processing the newly-detected packet to update the data based on n packets. Here, note that the packet at issue is a second set packet (as monitored from step **48**). Accordingly, the data based on a sliding window of n packets continues to be updated, but now that data is reflective of packets in the second set, which recall preferably reflects a larger number of source and/or destinations as compared to the first set. Further, the updated data is only that relative to the specific source and destination between which the step **50** packet was communicated. Lastly, as this update occurs for a packet, the data from the oldest packet of the previously-processed n packets is preferably no longer maintained.

[0045] In step **51**, having been reached due to a detected TCP sequence number irregularity between a source and destination in the second set from step **50**, the network monitor NM_x detects one or more additional TCP packets communicated in the second set. For each of these additionally-detected packets in the second set, step **51** determines whether the TCP sequence number (and arrival time) also indicates an irregularity. If an irregularity is not detected, then the preferred embodiment operates under the assumption that the irregularity detected in the preceding step **50** was either an isolated incident, a relatively minor irregularity, or otherwise not reason to make a network response or adjustment, and the flow of method **40** returns from step **51** to step **44**, again with the option as shown in step **50***a* of indicating an alarm relating to the irregularities detected earlier with respect to the first set packets. On the other hand, if an irregularity is detected in step **51**, then the preferred method flow continues to step **52**. Lastly, as with steps **44**, **46**, and **50**, for a given packet between a specific source and destination, step **51** also concludes by updating the data from the sliding window of the most recent n packets in the second set as between that specific source and destination, as updated for each packet (or packets) as detected by step **51**.

[0046] From the preceding, one skilled in the art will appreciate that step **52** is reached when method **40** has detected irregularities in the TCP sequence numbers and/or TCP packet times of arrival in both the first and second sets of source and destination nodes. Thus, irregularities have been detected in communications between a plural number of source and destination nodes having a relationship to one another, where that relationship is implied by the rule(s) that define the first and second sets. Note that the actual irregularity may be for various reasons. Moreover, the specific reason(s) causing the irregularity may be inferred based on the amount of the deviation between the actual and predicted values. For example, if the predicted and real values differ by a figure of approximately 50 percent, then the preferred embodiment concludes that a packet (or more than one packet) was lost. This might occur because the source TCP

BNSDOCID: <US____20040073655A1_I_>

control window was halved or the destination may have dropped a packet. Still other examples may be ascertained by one skilled in the art. In any event, in step **52**, method **40** attempts a corrective action to improve traffic flow in view of the irregularity. Preferably, such a corrective action is taken by the network meter issuing an event report, such as via a network packet, to the edge routers ER_x on the logical sub-network having the detected irregularity(ies). The edge router, in response, may take various actions. For example, one or more alarms may be set off to indicate to a user or network manager that an irregularity or irregularities have been detected. As another example, traffic queuing at the edge routers ER_x relating to the logical sub-network at issue may be adjusted. As still another example which is likely a rare case, there may be an observation that 90% of the flows are losing packets independently of their source and destination; in this case there is likely a considerable issue with the link where the abnormal behavior has been observed.

[0047] Two additional observations are also noteworthy with respect to method **40**. As a first observation, note that method **40** only generally illustrates the use of two sets of packets, where by way of example the first set is reflected in steps **42** through **46** and in one instance may be packets between only a single source and single destination of two respective physical sub-networks, where the second set is reflected in steps **48** through **51** and in one instance may be all packets between any source and any destination of the same two respective physical sub-networks. However, the present inventive teachings contemplate different divisions for each set, where there may be additional iterations for number, where preferably each additional set encompasses all packets in a lesser analyzed set. In this manner, the analysis of method **40** effectively continues to expand its scope to consider a greater amount of network traffic, each time including the traffic as considered during the lesser scope of analysis. In operating in this fashion, a greater amount of data may be collected to determine the magnitude of a potential irregularity in network traffic. As a second observation, note that each of steps **46** and **51** states that it evaluates one or more additional packets. This is intended to demonstrate that the irregularity detection for a given set can be based on any number of packets; thus, by looking only at **FIG. 7**, steps **44** and **46** may appear to represent the analysis of only two first set packets, but the earlier statement that step **46** may include multiple packets is intended to indicate that the inventive scope includes a variation where more than two first set packets are processed, that is, for each of those packets, they are analyzed to determine if an irregularity exists, and the data from those packets is also used to update the sliding window of n packets. Similarly, from **FIG. 7** alone, steps **50** and **51** may appear to represent the analysis of only two second set packets, but the earlier statement that step **51** may include multiple packets is intended to indicate that the inventive scope includes a variation where more than two second set packets are processed, that is, for each of those packets, they are analyzed to determine if an irregularity exists, and the data from those packets is also used to update the sliding window of n packets corresponding to each source and destination between which each packet is communicated.

[0048] **FIG. 8** illustrates a flow chart of the predictor methodology introduced above and which is therefore preferably used in connection with method **40** of **FIG. 7**. Indeed, for sake of cross-reference between **FIGS. 8 and 7**, the predictor steps of **FIG. 8** may be considered to occur as part of various steps from method **40** of **FIG. 7**. Thus, by way of example, **FIG. 8** illustrates steps **40** and **42** from **FIG. 7** and which are shown generally with an elaboration of various sub-steps as described below. Further, while the illustration of **FIG. 8** is directed to steps **42** and **44**, one skilled in the art should appreciate that the discussion below with respect to newly-received and processed as described above, also receives an additional packet(s) and updates the corresponding sliding window of n packet data, where from the following it will become apparent that from each update additional parameters are predicted and those predictions form the basis for detecting irregularities in each of steps **44**, **46**, **50**, and **51**. This processing is now further explored below in the various sub-steps of step **42**.

[0049] In sub-step **42***a*, the network monitor NM_x detects a network packet of the first set, that is, a packet having a source and destination address matching the source and destination (or multiple sources and destinations) that are specified, by a rule(s), to be monitored. In sub-step **42***b*, the TCP sequence number ("SN") and the time of arrival ("TOA") of the detected TCP packet are stored, such as in a buffer located in flow store **32**. In sub-step **42***c*, a difference, or offset, is determined and stored for the TCP SN parameter of sub-step **42***b* relative to the immediately-preceding packet that was received for the same source and destination. In other words, a TCP SN offset is determined by subtracting from the TCP SN of the presently-detected packet the TCP SN of the immediately-preceding packet that was received for the same source and destination. For the sake of reference, this offset value is hereafter referred to as Δ(TCP SN), and in the preferred embodiment it is stored in flow store **32**. Further, because sub-step **42***c* is repeated for each of the n packets, then in the preferred embodiment the TCP SN is stored and the value Δ(TCP SN) is computed for each of the n packets (although the first packet in the n packets may not provide a value of Δ(TCP SN) because there is no immediately-preceding packet from which to make the determination of the then-present packet relative to the immediately-preceding packet).

[0050] In sub-step **42***d*, a difference, or offset, is determined for the TOA parameter of sub-step **42***b* relative to the immediately-preceding packet that was received for the same source and destination. However, unlike the operation with respect to Δ(TCP SN), preferably there is no storage of multiple offset values of TOA for the multiple ones of the n packets. Instead, in the preferred embodiment and in order to reduce complexity and storage requirements, for each packet received, first the difference between the actual TOA of the received packet and the stored value of the immediately-previous packet (of the same set) is determined, and that difference, hereafter referred to as Δ(TOA), is stored to a single location. Once that value of Δ(TOA) is stored, then the actual TOA of the present packet is also stored to single storage location, thereby overwriting the actual TOA of any previous packet. Thus, when a next packet in the n packets is received, sub-step **42***d* again operates in this manner, thereby determining the Δ(TOA) as between that packet and the immediately-preceding packet, and then overwriting the previous value of Δ(TOA) with a new value of Δ(TOA) and also overwriting the previously-stored actual TOA of the immediately-preceding packet with the actual TOA value of the then-processed packet.

BNSDOCID: <US____20040073655A1_I_>

[0051] Sub-steps **42***a* through **42***d* continue for a total of n packets in the first set, where such a repetition is shown by the condition sub-step **42***e*. In other words, until n packets are processed through sub-steps **42***a* through **42***d*, then those sub-steps are repeated, thereby storing the value Δ(TCP SN) for each of the n packets relative to the packet that preceded it. However, with respect to the TOA, only the TOA of the immediately-preceding packet is saved and it is overwritten once another packet is detected and the value of Δ(TOA) with respect to that packet is determined and stored. Once n packets are processed in this manner, step **42***e* causes the flow to continue to sub-step **42***f*.

[0052] Sub-step **42***f* predicts an offset to the TCP SN for a future packet having the same source and destination as the n packets already detected. In the preferred embodiment, in order to provide the prediction of the offset with respect to the next TCP SN, first step **42***f* reviews the n stored values of Δ(TCP SN) and chooses the most common stored value as the predicted TCP SN offset value for future packets. For sake of reference, the predicted offset value is hereafter referred to as PO_{Δ}(TCP SN). Note also that one skilled in the art may implement alternative manners of processing the n stored values of Δ(TCP SN) in order to provide the predicted value of PO_{Δ}(TCP SN). In any event, once PO_{Δ}(TCP SN) is determined, method **40** continues to step **44**.

[0053] Looking to step **44** in **FIG. 8**, recall first from **FIG. 7** that step **44** detects another TCP packet between the step **42** source and destination, and then step **44** determines whether an irregularity exists in the TCP sequence number of the new packet as compared to past TCP sequence number history. According to the preferred predictor methodology, the determination of an irregularity is made using the predicted offset value PO_{Δ}(TCP SN) and the last-determined offset time of arrival value, Δ(TOA), from sub-step **42***d* by determining predicted values with respect to the newly-detected packet. Specifically, the offset value of PO_{Δ}(TCP SN) is added to the TCP SN of the immediately-preceding received packet in the first set, that is, the previous TCP SN is increased by the offset value it is predicted to change based on step **42***f*. Also, the value of Δ(TOA) is added to the TOA of the immediately-preceding received packet in the first set, that is, the TOA of the immediately-previous first set packet is increased by the amount of time that occurred between that previous packet and the packet that preceded it. These two totals, therefore, represent what are a predicted values for the TCP SN and TOA of the packet detected in step **44**. Given these expected values, the actual detected values of the packet detected in step **44** are compared to the predicted values, and a measure of deviation may be determined between the two. If the deviation, for either TCP SN or TOA, between the actual value and the predicted value is beyond a threshold, then an irregularity is deemed to occur and, as described above with respect to **FIG. 7**, method **40** continues to step **46**. To the contrary, if the deviation is equal to or less than the threshold, then no irregularity is deemed to occur and, as described above with respect to **FIG. 7**, method **40** returns to step **44** to detect a next TCP packet in the first set and to process that step as just described. Note also now that the threshold may be adjusted by one skilled in the art based on various considerations, including the observations made in **FIGS. 2 through 4**.

[0054] Before proceeding recall also that step **44** in **FIG. 7** concludes with an update of the data based on n packets. Given the sub-steps shown in **FIG. 8**, one skilled in the art should now appreciate that this update operates in the same general manner as for the first n packets in step **42**, but for step **44** the packet at issue is the step **44** detected packet. Thus, for step **44**, the offset value Δ(TCP SN) is determined with respect to the step **44** packet and in view of the immediately-preceding packet from step **42**; particularly, Δ(TCP SN) is determined by subtracting from the TCP SN of the presently-detected step **44** packet the TCP SN of the immediately-preceding packet that was received for the same source and destination in step **42**. Also, the step **44** value Δ(TCP SN) is stored while the oldest value of the n stored values of Δ(TCP SN), as corresponding to the oldest received first set packet in a group of n packets, is discarded (e.g., overwritten). As a result, the determination of the predicted offset value, PO_{Δ}(TCP SN), also may be updated given the newest value of Δ(TCP SN) and the removal of the oldest value of Δ(TCP SN). Also as part of the step **44** update, a new value of Δ(TOA) is determined, here by comparing the TOA of the step **44** packet with the last received packet in step **42**. Again, the new value of Δ(TOA) is stored, thereby overwriting the actual TOA of any previous packet. Lastly, note that these same update principles, as applying to Δ(TCP SN) and Δ(TOA), also apply to steps **46**, **50**, and **51**, that is, each indicated update is preferably achieved in the same manner with respect to these two parameters, where in each instance the most recently detected packet, for either the corresponding first or second set, is used to adjust Δ(TCP SN) so that is reflective of the last n received packets as between the same source and destination as the previous packets, and similarly Δ(TOA) is adjusted as a comparison between the presently received packet and its immediate predecessor of the same set.

[0055] Having described the application of the preferred predictor methodology with respect to step **44**, as mentioned above note that a comparable analysis is also preferably performed with respect to steps **46**, **50**, and **51** in **FIG. 7**. For example, recall from FIG. **7** that step **46** detects whether an irregularity occurs for an additional packet in the first set only once step **44** detects a first TCP packet in the first set with an irregular deviation in its throughput (e.g., as detected based on TCP SN and TOA). In the case where step **46** detects multiple packets, then it updates and uses the most current value of PO_{Δ}(TCP SN) as relating to the immediately-preceding n packets in the first set. Thus, for each received packet its actual TCP SN is compared to the sum of the TCP SN of the immediately-preceding packet plus the then-updated value of PO_{Δ}(TCP SN). Additionally, a time of arrival analysis is made for each packet, where the time of arrival of the then-detected packet is compared to the predicted time of arrival based on the Δ(TOA) value from the immediately-preceding packet. Thus, the value of Δ(TOA) is also changed for each successive packet. In other words, each time a first set packet is detected, the TOA of the immediately-preceding first set packet is subtracted from the TOA of the then-received first set packet, and the difference is stored as Δ(TOA); that difference is then added to the TOA of the then-received first set packet to predict the TOA of the next received first set packet, and when that next received first set packet is received, its TOA is compared to the immediately-previous predicted TOA. Again, a deviation beyond a threshold gives rise to some type of corrective/

warning response. Further, the preceding as applied to step **46** will also be readily applied by one skilled in the art to steps **50** and **51**.

[0056] An additional observation is also contemplated with respect to the TOA and Δ(TOA) values included within the present inventive scope. Particularly, the preceding describes the use of only two successive packets to determine those two values with respect to any of steps **42**, **44**, **46**, **50**, and **51**. However, note that the changing of Δ(TOA) immediately after an irregular packet is received may cause difficulty in detecting further TOA irregularities. Specifically, if the TOA of the irregular packet is used to overwrite a previous TOA and also to determine the next Δ(TOA), then that next value of Δ(TOA) may itself be irregular because it is based on an irregular packet. As such, the next packet may arrive at a regular timing, but its timing may be misconstrued as irregular because it will be compared to Δ(TOA) as derived from the previously-received irregular packet. Accordingly, further contemplated within the present inventive scope are other manners of determining Δ(TOA). As one example, rather than using only the TOA from two successive packets, the TOA of a number of packets greater than two may be compared against one another to determine a Δ(TOA), such as via the average of the difference between the TOAs of each of the previously-received packets.

[0057] Having described the application of the preferred predictor methodology with respect to steps **44** and **46**, note that a comparable analysis is also preferably performed with respect to steps **50** and **51**, but as relating to the second set. Therefore, when a new second set packet is detected, the value of PO_{Δ}(TCP SN) comparable to that from sub-step **42***f* is added to the TCP SN of the immediately-preceding second set packet and the result is compared to the actual TCP SN of the new second set packet. Similarly, when the new second set packet is detected, its actual TOA is compared to the sum of the TOA of the immediately-preceding second set packet with the difference in TOA between that immediately-preceding second packet and the second set packet which preceded it. The comparisons provide an indication of a deviation, if any, between the predicted TCP SN and TOA values and the actual values, and for the sake of step **50** or **51** those deviations are compared to the step **50** or **51** threshold as described above, with a response taken based on how the deviations, if any, compare to the step **50** threshold.

[0058] From the above illustrations and description, one skilled in the art should appreciate that the preferred embodiments provide a manner of monitoring the flow of network packets, with a particular benefit having been shown for monitoring TCP packets based on their TCP sequence numbers as well as their times of arrival. By the preferential analysis of flows in terms of TCP sequence numbers and times of arrival, a measure of throughput is realized, which as evidenced in **FIGS. 2 through 4** depicts the change of TCP sequence numbers as it relates to the times of arrival. The embodiments provide numerous benefits over the prior art. As one example of a benefit, unlike the prior art active systems, the preferred embodiments do not send special test packets (e.g., PING) and do not introduce additional test traffic onto the route of the regular data packets. Thus, in this sense the preferred embodiments do not impact the network performance. As another example of a benefit, as compared to the traditional passive measurement mechanisms in which the IP packets (or portions thereof) are routinely stored and then later studied using an off-line analysis of historical data, the preferred embodiments use real-time RTFM meters to retrieve packet information from packets as they are incurred during actual real-time traffic flow and to store portions of those packets; this stored data is also preferably used in a real-time or near real-time manner, such as on the order of less than one second of when the packet sequence numbers and times of arrival are collected, to evaluate the regularity of the underlying network and to take corrective action(s), if necessary. As still another example of a benefit, prior art MIBs provide single point analysis directed to the traffic flow at the location of the MIB. In contrast, the preferred embodiments contemplate analyzing real-time collected packet information from multiple points in the network and they are not constrained to the hardware type or manufacturer of each router. Still further, the preferred embodiments also provide numerous benefits inherited from the following intrinsic advantages of RTFM meter architecture: (1) all data on the IP network is recordable; (2) functional even when the given network elements are incapable of flow monitoring; (3) independence from physical and data layer technologies; and (4) good performance even during fault conditions. In all events, the preceding as well as other benefits should be appreciated by one skilled in the art. As another benefit, while the preferred embodiments are implemented with respect to TCP sequence numbers, the inventive teachings likewise may apply to another selected field(s) in a packet that readily distinguishes that packet from past and future packets in the sequence, where based on past packets the future packets can be monitored given an expectation of the value of the selected field for each of the future packets. As a final benefit, while the preferred embodiments are particularly advantageous in IP networks, they also may be applied to numerous other networks as well. In addition, while the present embodiments have been described in detail, various substitutions, modifications or alterations could be made to the descriptions set forth above without departing from the inventive scope which is defined by the following claims.

1. A network monitoring system, comprising:

storage circuitry for storing network packet information, wherein the network packet information includes a predicted identifier; and

at least one monitoring circuit coupled to a network along which network traffic flows in a form of packets, the at least one monitoring circuit programmed to perform the steps of:

receiving a packet communicated along the network;

determining whether the received packet is communicated between a source and destination in a first set of network nodes, wherein each packet in a sequence of communications between the source and the destination comprises a packet identifier that uniquely identifies the packet from all other communications in a flow between the source and the destination; and

responsive to determining the received packet is communicated between a source and destination in the first set of network nodes, comparing the packet identifier of the received packet to the predicted identifier to determine an identifier deviation

BNSDOCID: <US____20040073655A1_I_>

between the packet identifier and the predicted identifier for identifying an irregularity in the network traffic.

2. The system of claim 1 wherein the at least one monitoring circuit is programmed to further perform the steps of:

comparing the identifier deviation to a threshold; and

responsive to the identifier deviation exceeding a threshold, indicating an alarm.

3. The system of claim 1 wherein the at least one monitoring circuit is programmed to further perform the steps of:

comparing the identifier deviation to a threshold; and

responsive to the identifier deviation exceeding a threshold, adjusting packet communications between the source and the destination.

4. The system of claim 3:

wherein the at least one monitoring circuit monitors packets between core routers; and

wherein the adjusting step adjusts packet communications at an edge router.

5. The system of claim 1 wherein the packet identifier comprises a sequence number.

6. The system of claim 1:

wherein the packet comprises a TCP packet; and

wherein the packet identifier comprises a TCP sequence number.

7. The system of claim 1 wherein the at least one monitoring circuit is programmed to further perform, prior to the comparing step, the steps of:

receiving a plurality of packets communicated along the network;

for each packet in the plurality of packets:

determining whether the received packet is communicated between a source and destination in the first set of network nodes; and

responsive to determining the received packet is communicated between a source and destination in the first set of network nodes, storing in the storage circuitry the packet identifier of the received packet.

8. The system of claim 7 wherein the at least one monitoring circuit is programmed to further perform the step of determining the predicted identifier in response to a plurality of packet identifiers stored by the storing step corresponding to a plurality of packets in the first set.

9. The system of claim 8 wherein the at least one monitoring circuit is programmed to further perform the step of determining the predicted identifier as a most common one of the plurality of packet identifiers.

10. The system of claim 1 wherein the at least one monitoring circuit is programmed to further perform the step of, responsive to determining the received packet is communicated between a source and destination in the first set of network nodes, comparing a time of arrival of the received packet to a predicted time of arrival to determine a time deviation between the time of arrival and the predicted time of arrival.

11. The system of claim 10 wherein the at least one monitoring circuit is programmed to further perform the steps of:

comparing the time deviation to a threshold; and

responsive to the time deviation exceeding a threshold, indicating an alarm.

12. The system of claim 10 wherein the at least one monitoring circuit is programmed to further perform the steps of:

comparing the time deviation to a threshold; and

responsive to the time deviation exceeding a threshold, adjusting packet communications between the source and the destination.

13. The system of claim 10 wherein the at least one monitoring circuit is programmed to further perform, prior to the step of comparing a time of arrival, the step of determining the predicted time of arrival in response to a difference in time between two successively-received packets between the source and the destination in the first set of network nodes.

14. The system of claim 1 wherein the first set consists of a single source and a single destination node.

15. The system of claim 1 wherein the first set comprises a plurality of source nodes in a first physical sub-network and a plurality of destination nodes in a second physical sub-network that differs from the first physical sub-network.

16. The system of claim 1 wherein the at least one monitoring circuit is programmed to further perform the steps of, responsive to determining that the identifier deviation exceeds a threshold:

receiving an additional packet communicated along the network;

determining whether the additional packet is communicated between the source and the destination in the first set of network nodes; and

responsive to determining the additional packet is communicated between a source and destination in the first set of network nodes, comparing the packet identifier of the additional packet to a predicted identifier to determine an identifier deviation between the packet identifier of the additional packet and a predicted identifier.

17. The system of claim 16 wherein the at least one monitoring circuit is programmed to further perform, responsive to determining that the identifier deviation between the packet identifier of the additional packet to a predicted identifier exceeds a threshold, the steps of:

receiving a plurality of packets communicated along the network; and

determining whether each packet in the plurality of packets is communicated between a source and destination in a second set of network nodes, wherein the second set of network nodes comprises the first set of network nodes.

18. The system of claim 17:

wherein the first set consists of a first number of nodes; and

wherein the second set consists of a second number of nodes greater than the first set of nodes.

19. The system of claim 18 wherein the first set consists of a single source and a single destination node.

20. The system of claim 18:

wherein the single source node corresponds to a first physical sub-network and the single destination node corresponds to a second physical sub-network; and

wherein the second set comprises a plurality of source nodes corresponding to the first physical sub-network and a plurality of destination nodes corresponding to the second physical network.

21. The system of claim 17 wherein the at least one monitoring circuit is programmed to further perform, relative to each packet in the plurality of packets and determined to be communicated between a source and destination in the second set of network nodes, the step of comparing the packet identifier of each respective received packet to a predicted identifier to determine a respective identifier deviation between the packet identifier of the respective received packet and the predicted identifier.

22. The system of claim 21 wherein the at least one monitoring circuit is programmed to further perform, relative to each packet in the plurality of packets and determined to be communicated between a source and destination in a second set of network nodes, the steps of:

comparing the respective identifier deviation to a threshold; and

responsive to the respective identifier deviation exceeding a threshold, adjusting packet communications along the second set of network nodes.

23. The system of claim 22 wherein the step of adjusting packet communications along the second set of network nodes comprises adjusting packet communications at least one an edge router.

24. The system of claim 21 wherein the at least one monitoring circuit is programmed to further perform, relative to each packet in the plurality of packets and determined to be communicated between a source and destination in a second set of network nodes, the steps of:

comparing the respective identifier deviation to a threshold; and

responsive to the respective deviation exceeding a threshold, indicating an alarm.

25. The system of claim 16 wherein the at least one monitoring circuit is programmed to further perform the step of, responsive to determining the additional packet is communicated between a source and destination in the first set of network nodes, comparing a time of arrival of the additional packet to a first predicted time of arrival to determine a time deviation between the time of arrival of the additional packet and the first predicted time of arrival.

26. The system of claim 25 wherein the at least one monitoring circuit is programmed to further perform, responsive to determining that the time deviation exceeds a threshold, the steps of:

receiving a plurality of packets communicated along the network; and

determining whether each packet in the plurality of packets is communicated between a source and destination in a second set of network nodes, wherein the second set of network nodes comprises the first set of network nodes.

27. The system of claim 26 wherein the at least one monitoring circuit is programmed to further perform, relative to each packet in the plurality of packets and determined to be communicated between a source and destination in a second set of network nodes, the step of comparing a time of arrival of the packet to a corresponding predicted time of arrival to determine a corresponding time deviation between the time of arrival of the packet and the corresponding predicted time of arrival.

28. The system of claim 27 wherein the at least one monitoring circuit is programmed to further perform the steps of:

comparing the corresponding time deviation to a threshold; and

responsive to the corresponding time deviation exceeding a threshold, indicating an alarm.

29. The system of claim 27 wherein the at least one monitoring circuit is programmed to further perform the steps of:

comparing the corresponding time deviation to a threshold; and

responsive to the corresponding time deviation exceeding a threshold, adjusting packet communications between at least some of the second set of nodes.

30. The system of claim 1 wherein the network comprises an internet protocol network.

31. The system of claim 1 wherein the internet protocol network comprises the global internet.

32. The system of claim 1 and further comprising a plurality of monitoring circuit, each coupled to the network, and each programmed to perform the steps of:

receiving a packet communicated along the network;

determining whether the received packet is communicated between a source and destination in a first set of network nodes, wherein each packet in a sequence of communications between the source and the destination comprises a packet identifier that uniquely identifies the packet from all other communications in a flow between the source and the destination; and

responsive to determining the received packet is communicated between a source and destination in the first set of network nodes, comparing the packet identifier of the received packet to the predicted identifier to determine an identifier deviation between the packet identifier and the predicted identifier for identifying an irregularity in the network traffic.

33. A method of monitoring a network along which network traffic flows in a form of packets, the method comprising:

storing network packet information in storing circuitry, wherein the network packet information includes a predicted identifier and wherein the storing circuitry is accessible to the network; and

BNSDOCID: <US____20040073655A1_I_>

operating at least one monitoring circuit coupled to the network along which network traffic flows in a form of packets, the operating step comprising the steps of:

receiving a packet communicated along the network;

determining whether the received packet is communicated between a source and destination in a first set of network nodes, wherein each packet in a sequence of communications between the source and the destination comprises a packet identifier that uniquely identifies the packet from all other communications in a flow between the source and the destination; and

responsive to determining the received packet is communicated between a source and destination in the first set of network nodes, comparing the packet identifier of the received packet to the predicted identifier to determine an identifier deviation between the packet identifier and the predicted identifier for identifying an irregularity in the network traffic.

34. The method of claim 33, wherein the operating step further comprises:

comparing the identifier deviation to a threshold; and

responsive to the identifier deviation exceeding a threshold, one of the steps from the group consisting of indicating an alarm and adjusting packet communications between the source and the destination.

35. The method of claim 33 wherein the packet identifier comprises a sequence number.

36. The method of claim 33, wherein the operating step further comprises, responsive to determining the received packet is communicated between a source and destination in the first set of network nodes, comparing a time of arrival of the received packet to a predicted time of arrival to determine a time deviation between the time of arrival and the predicted time of arrival.

37. The method of claim 36 wherein the operating step further comprises:

comparing the time deviation to a threshold; and

responsive to the time deviation exceeding a threshold, one of the steps from the group consisting of indicating an alarm and adjusting packet communications between the source and the destination.

38. The method of claim 33 wherein the operating step further comprises, after determining that the identifier deviation between the packet identifier of the packet to a predicted identifier exceeds a threshold, the steps of:

receiving a plurality of packets communicated along the network; and

determining whether each packet in the plurality of packets is communicated between a source and destination in a second set of network nodes.

39. The method of claim 38 wherein the second set of network nodes comprises the first set of network nodes and wherein the second set consists of a number of nodes greater a number of nodes in the first set of nodes.

40. The method of claim 38 wherein the operating step further comprises, relative to each packet in the plurality of packets and determined to be communicated between a source and destination in the second set of network nodes, the steps of:

comparing the packet identifier of each respective received packet to a predicted identifier to determine a respective identifier deviation between the packet identifier of the respective received packet and the predicted identifier;

comparing the respective identifier deviation to a threshold; and

responsive to the respective identifier deviation exceeding a threshold, one of the steps from the group consisting of indicating an alarm and adjusting packet communications between the network.

* * * * *

BNSDOCID: <US____20040073655A1_I_>

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2012 (01.11.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/146265 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 12/26* (2006.01)
H04L 12/24 (2006.01)

(21) International Application Number:
PCT/EP2011/002145

(22) International Filing Date:
28 April 2011 (28.04.2011)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **VOIPFUTURE GMBH** [DE/DE]; Wendenstrasse 4, 20097 Hamburg (DE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SCHOLZ, Hendrik** [DE/DE]; C/o Voipfuture Gmbh, Wendenstrasse 4, 20097 Hamburg (DE). **WALLBAUM, Michael** [DE/DE]; C/o Voipfuture Gmbh, Wendenstrasse 4, 20097 Hamburg (DE). **KRUEGER, Michael** [DE/DE]; C/o Voipfuture Gmbh, Wendenstrasse 4, 20097 Hamburg (DE). **BASTIAN, Jan** [DE/DE]; C/o Voipfuture Gmbh, Wendenstrasse 4, 20097 Hamburg (DE).

(74) Agent: **BOEHMERT & BOEHMERT**; Felix Hermann, Hollerallee 32, 28209 Bremen (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: CORRELATION OF MEDIA PLANE AND SIGNALING PLANE OF MEDIA SERVICES IN A PACKET-SWITCHED NETWORK

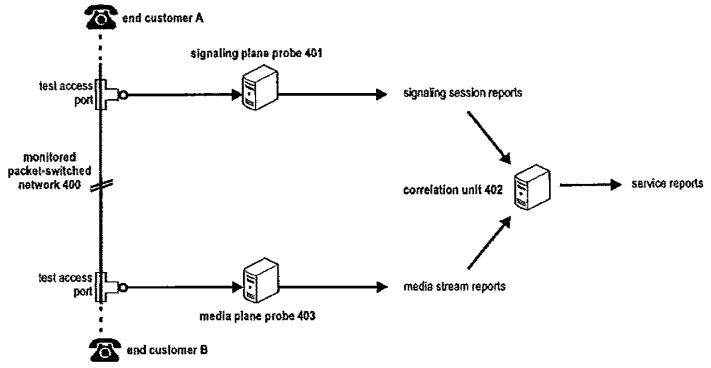


Fig. 4

(57) **Abstract**: This invention relates to methods for correlating media streams and signaling sessions of services, for example, in a passive monitoring system of a packet-switched network. Furthermore, the invention also relates to an implementation of these methods in hardware and software, and provides a signaling plane probe, a media plane probe and a correlation unit. Moreover, a passive monitoring system comprising one or more of these hardware devices is provided. To correlate media streams and signaling sessions of services, the invention proposes to independently generate correlation keys in a media plane probe for monitored media streams and correlation keys for signaling sessions that are monitored by a signaling plane probe in a fashion that matching correlation keys are generated for a respective service. By identifying reports on the media streams and reports on the signaling session that contain matching correlation keys respectively, the media streams and the signaling streams are correlated in a correlation unit.

WO 2012/146265 A1

BNSDOCID: <WO_____2012146265A1_I_>

Correlation of Media Plane and Signaling Plane of Media Services in a Packet-Switched Network

FIELD OF THE INVENTION

This invention relates to methods for correlating media streams and signaling sessions of services, for example, in a passive monitoring system of a packet-switched network. Furthermore, the invention also relates to an implementation of these methods in hardware and software, and provides a signaling plane probe, a media plane probe and a correlation unit. Moreover, a passive monitoring system comprising one or more of these hardware devices is provided.

TECHNICAL BACKGROUND

VoIP Services

VoIP ("Voice over IP" – IP denoting the Internet Protocol) services may be considered to consist of a signaling plane and a media plane. On the signaling plane various protocols describe the session (call) flow in terms of involved parties, intermediary VoIP entities (i.e. VoIP proxies, routers) and the characteristics of the VoIP service (call).The media plane typically carries the media information (i.e. audio and/or video data) between the involved parties. Neither the media plane nor the signaling plane alone is sufficient to carry a VoIP service. On the signaling plane protocols like SIP (see IETF RFC 3261, "SIP: Session Initiation Protocol", available at http://www.ietf.org) or ITU-T recommendation H.323 (see H.323, "Packet-based multimedia communications systems", Edition 7, 2009, available at http://www.itu.int) are commonly used, whereas protocols like RTP (Real-time Transport Protocol, see IETF RFC 3550, "RTP: A Transport Protocol for Real-Time Applications", available at http://www.ietf.org), MSRP (see IETF RFC 4975, "The Message Session Relay Protocol (MSRP)", available at http://www.ietf.org) or ITU recommendation T.38 (see T.38, "Procedures for real-time Group 3 facsimile communication over IP networks", Edition 5 (2007) or Edition 6 (2010), available at http://www.itu.int) may be present on the media plane.

BNSDOCID: <WO_____2012146265A1_I_>

In contrast to the traditional PSTN (Public Switched Telephone Network) network both planes may be on different infrastructure using different protocols and even take different routes through a network.

Correlation Information

The property of disjunct signaling stream(s) and media stream(s) of a VoIP service within packet-switched networks may necessitate a correlation mechanism. This correlation may only be based on the common parameters carried on both planes of the session. Monitoring equipment used in VoIP networks may be limited to either the signaling or media plane due to the network structure. A correlation of signaling stream(s) and media stream(s) is thus needed outside the VoIP network in between the monitoring components.

In RTP-based VoIP networks the data basis is rather limited as defined by the RTP protocol and the underlying transport and Internet layer protocols. An RTP stream which typically carries voice or video information from one party to another of a VoIP service is made up of plural RTP packets. The header of each RTP packet does not contain an identifier which can be used to distinctively associate single RTP packets or the entire RTP stream to a VoIP service (defined by the VoIP signaling). The same way the VoIP signaling protocol does not carry information to relate a signaling session (signaling plane of the VoIP service) to RTP protocol header information.

The parties originating or receiving a VoIP service actively dictate the transport and Internet layer address (IP address and port) on which they want to receive media streams. This configuration is done on the signaling plane. Using SIP as a signaling protocol, the address tuple(s) to be used on the media plane is/are defined in a so-called SDP body (see IETF RFC 3264, "An Offer/Answer Model with the Session Description Protocol (SDP)", available at http://www.ietf.org). The address tuple(s) - usually consisting of an IP address and port – is/are the sole information to correlate media plane of a VoIP service with the signaling plane of the VoIP service, and vice versa.

Challenges in Correlation of Signaling Plane and Media Plane

Beside the limited information available for correlation, the correlation of the signaling plane and media plane imposes also numerous further challenges, especially in passive mid-point monitoring scenarios. While an address tuple (IP address and port) may be enough information to identify a single RTP stream at a given point in time, multiple streams

identified by different address tuples may exist in a regular VoIP call. In fact at least two media streams are needed to allow two-way communication between the caller and callee.

It will be outlined in further detail in the following how multiple media streams may occur in a single VoIP service and how they are communicated between the parties involved (which may not always be the case).

Mid-point monitoring equipment (i.e. the signaling and media probes) is introduced into the network path which active components (e.g. VoIP phones and servers) use to communicate with each other. This passive equipment is not involved in the communication itself and has to derive all information from the network packets it observes on said network path. The correlation challenge increases as the passive equipment lacks information the active components internally have. A VoIP phone may internally assign a media port to a signaling session but never send out this information combined so that a mid-point monitoring probe could benefit from this information.

Time Constraints due to Port Reuse

The IP address and port combination transmitted inside the signaling plane of a VoIP service as well as the IP address and port observed on the media plane of the VoIP service may be reused. For exemplary purposes it can be assumed that each VoIP device has a single IP address. The port range from which the client can draw is limited to roughly 65000 ports by the underlying transport layer protocol UDP (see RFC 768, "User Datagram Protocol", available at http://www.ietf.org). In practice additional specifications and configuration parameters significantly further limit this port range. RFC 3550 which defines the Real-Time Transport Protocol mandates that only even port numbers may be used to transport media streams. The odd ports are reserved for Real-Time Transport Control Protocol (RTCP) packets. This standardization alone effectively halves the number of ports available for VoIP communication.

As a result a VoIP device has to re-use a certain IP address and port combination, thus eliminating a unique identification criterion. Essentially the IP address and port combination can only be assumed to be unique for a limited amount of time. The time-frame depends on the utilization of the VoIP device as well as the number of IP addresses required in an Internet Service Provider's network. If a correlation of the signaling and media plane takes place without a time criteria, it would therefore produce so-called false positives: Multiple media streams would match the requested IP address and port combination, since the signaling plane may have caused re-use of the very same IP address and/or port for another VoIP service.

EX1002
CISCO SYSTEMS, INC. / Page 980 of 1453

Media Streams

Multiple streams may exist per direction of each VoIP service. The caller sends data to the callee and vice versa resulting in at least one media stream per direction. Desirable features, such as for example codec changes, may trigger additional streams. On the network multiple streams may use the same IP address and port tuple depending on the media protocol. For example, each RTP stream is additionally identified by a unique identifier - the Sender Synchronization Source (SSRC) – which is used to distinguish between multiple streams.

Fig. 1 shows exemplary situations where multiple media streams may be triggered. The focus is on the media plane traffic and its timing. The x-axis denotes the time basis, starting on the left side. The vertical lines in Fig. 1 denote signaling events and the bold horizontal lines are RTP streams present in the respective exemplified VoIP service example (please note that the different VoIP service examples are separated by broken horizontal lines). Only the RTP stream direction from the callee to the caller is shown per VoIP service example. The RTP stream from the caller to the callee can be assumed to be less complex (e.g. as shown in the "normal" VoIP service example).

The three vertical lines denote important events in the phase of a call. The leftmost line denotes the start timestamp. This is the time at which the caller submitted the call setup request to the network. The connected point is the timestamp at which a callee or his endpoint/handset picked up and moved the service into a fully established state. The service ends when one of the parties sends a termination request.

The most common VoIP services will be the trivial session examples where there is only one RTP stream per direction (see "normal" or "early media"). In a "normal" VoIP service flow both parties only start sending once the session is fully established on the signaling plane. More often the callee would start sending early media, i.e. when sending ring-tones or (pre-call) announcements. In "session forking" VoIP service example there may be multiple concurrent or sequential RTP streams at the beginning of a service e.g. due ring-tones being sent to multiple VoIP devices of the callee, while one is answered at the connect event

During a service media codecs may be changed (see "code change" VOIP service example) which is commonly resulting in a new media stream. Another service scenario may be the VoIP call being put on hold and picked up at a later time essentially generating multiple media streams (see "call on hold" VoIP service example). Silence suppression and other RTP features may cause multiple streams sporadically during a service (see "silence suppression" VoIP service example). Also retransmissions on the signaling plane may

EX1002
CISCO SYSTEMS, INC. / Page 981 of 1453

desynchronize the signaling plane and media plane (see "SIP retransmissions" VoIP service examples).

Geographic Distribution or Media Plane and Signaling Plane

As indicated above, signaling plane data and media plane data of VoIP services may take different routes. In examples, where SIP is used for session setup, this is indeed the case as those sessions usually contain signaling-only components (i.e. SIP proxies, REGISTRARs). As a result passive mid-point monitoring solutions may be split geographically along the routes of the VoIP traffic.

An exemplary passive mid-point monitoring scenario for this case is shown in Fig. 2. Fig. 2 shows three geographically distributed POPs (Point of Presence) which are linked over the carrier's internal network. The signaling data flows on the signaling plane between POP A and B via the signaling-only POP C. POP C would typically host a centralized routing entity which reduces the complexity in the POPs A and B. To prevent back-hauling traffic from POP A to POP C before sending it to POP B the VoIP system is configured in a way that would allow the media to flow directly on the media plane between POPs A and B.

Typical mid-point monitoring locations would be inside each POP. Due to the layout of the network no media traffic would be visible in POP C. To allow for successful correlation of signaling and media streams by the correlation mechanism it is therefore desirable to support distributed networks. If the same session traverses multiple POPs it would be desirable for the correlation mechanism to identify this and support correlation of the session legs across multiple sites.

Limitations/Challenges in Correlation of Signaling Plane and Media Plane

The correlation may be solely based on the IP address and port used on the transport and Internet layer. On the media plane each RTP stream is destined to exactly one IP address and port on the transport layer. On the signaling plane one IP address and port is typically exchanged inside the Session Description Body of the SDP protocol during the VoIP service setup. However this IP address and port combination may not be the combination used throughout the VoIP service. In this case the above mentioned correlation mechanism fails: It fails upon searching a media stream for a specific signaling session of the VoIP service. The same way it fails to locate a signaling session of the VoIP service for a specific media stream on the media plane. The reasons for using another IP address port combination than advertised upon session setup are manifold.

EX1002
CISCO SYSTEMS, INC. / Page 982 of 1453

Network Address Translation (NAT)

Network Address Translation (NAT, RFC 1631) was developed to solve Internet address space depletion and routing problems. In today's Internet one may distinguish between internal addresses which are often only unique locally (i.e. typically used inside company or home networks), and external addresses of global validity and uniqueness as used on the public Internet.

Fig. 3 shows an exemplary network using internal and external addresses. The internal network on the left side uses IP addresses from the so-called private space, as for example defined in IETF RFC 1918, "Address Allocation for Private Internets", available at http://www.ietf.org. The external network on the right side is the public Internet with globally reachable addresses. A router with embedded Network Address Translation (NAT) functionality is located in between the two networks. The router does not directly route packets in between the two connected networks, but "translates" (i.e. replaces) IP source and destination addresses within the routed IP packets on demand.

Essentially, the NAT functionality of the router hides the entire internal network (10.0.0.0/8 in this example) behind one public IP address (192.0.2.1). Every IP connection from within the internal network to the Internet will seem to originate from the sole public IP address (192.0.2.1) of the entire network.

For each node inside the internal network this imposes some limitations. Although Internet access works in general, a node in the internal network may not be reachable from the outside. This is due to the fact that IP traffic from an outside node (i.e. a node in the external network) would be destined to the public IP address (192.0.2.1), but the router with this IP address does not know at this point in time where to forward the traffic to on the internal network, given that there was no prior communication from an node inside of the internal network and the external node.

Additionally the internal node may not be aware that it is behind a router which performs the NAT. As required by the transport protocols, the internal node will use the internal IP address for communication purposes. On the VoIP signaling and media layer (i.e. session layer or application layer), the application will also use the internal IP address (i.e. 10.0.0.123) instead of the public IP address. VoIP signaling protocols (e.g. SIP or H.323) contain various IP addresses on the application layer. An intermediary NAT device (i.e. the router in Fig. 3) will not perform translation of the addresses on the session layer or application layer, but only translates IP addresses in the network layer. The internal IP addresses inside the VoIP

EX1002
CISCO SYSTEMS, INC. / Page 983 of 1453

signaling (i.e. SIP or H.323 messages) impose a problem to the application as internal IP addresses are most likely not reachable from the public Internet.

VoIP devices involved in the processing of a certain call may detect this problem by comparing the IP addresses seen on the Internet and transport layers with the IP addresses set on the application layer. The following message is an exemplary SIP message as seen on the network and transport layer, which means that both the Internet and transport layer information (IP addresses and ports) are visible:

```
U 2010/09/09 13:57:31.925226 192.0.2.99:37682 -> 10.0.0.1:5060
```

The Internet and transport layers show that the UDP packet (U) was received from the external address 192.0.2.99 (port 37682).

The following message represents the same exemplary SIP message as seen on the application layer, which means that both the Internet and transport layer information (IP addresses and ports) as well as the application layer (SIP message contents) are visible:

```
INVITE sip:echo@example.com SIP/2.0
Via: SIP/2.0/UDP
192.168.1.216;branch=z9hG4bK3BB64874;rport=37682;received=192.0
.2.99
CSeq: 7726 INVITE
To: <sip:echo@example.com>
Content-Type: application/sdp
From: "John Doe" <sip:jdoe@example.com>;tag=693C7725
Call-ID: 1341723561@192.168.1.216
Subject: sip:jdoe@example.com
Content-Length: 230
User-Agent: kphone/4.2
Contact: "John Doe" <sip:jdoe@192.168.1.216;transport=udp>
v=0
o=username 0 0 IN IP4 192.168.1.216
s=The Funky Flow
c=IN IP4 192.168.1.216
t=0 0
m=audio 60942 RTP/AVP 0 97 8 3
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:97 iLBC/8000
a=fmtp:97 mode=30
```

In contrast to the information available at the network and transport layers claiming that the message was received from the external address 192.0.2.99 (port 37682), the application claims that the source was the internal address 192.168.1.216 (port 5060 - the port 5060 is not viewed for the source address as it is the default port).

In general the translation of the network (IP) address also applies to the port numbers which are used on the transport layer. This feature is named Port Address Translation (PAT). NAT and PAT commonly happen at the same time in the same device.

PAT becomes necessary if multiple devices attempt to use the same port. Since different devices have different IP addresses their IP address and port tuple is unique. If packet streams from both devices traverse the same NAT device, the NAT device has to translate the port of one of the two packet streams. Otherwise there would be two distinct packet streams sharing the same external IP address of the NAT device and the same port. While this may not be a problem if the destination IP address and port tuple of the destination device are different for the two packet streams, it adds overhead which the NAT device wants to prevent. By rewriting the source port of one of the packet streams the address tuples of the external IP address and ports become unique again.

However, in networks where NAT (and PAT) is performed to for example hide private networks from the outside Internet, the correlation of signaling sessions of VoIP services and the associated media plane streams is becoming complex.

Multiple Communication Paths

Numerous solutions have been developed to allow traffic of VoIP services to operate in networks with Network Address Translation (NAT). These mechanisms require the involved caller and callee to exchange information, for instance on additional transport protocols or addresses which can be used to reach the remote party. These include – but are not limited to - IPv6 (Internet Protocol Version 6, see IETF RFC 2460, "Internet Protocol, Version 6 (IPv6), Specification"), TURN (Traversal Using Relays around NAT, see IETF RFC 5766, "Traversal Using Relays around NAT (TURN):Relay Extensions to Session Traversal Utilities for NAT (STUN)") addresses or ICE (Interactive Connection Establishment, see IETF RFC 5245, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols") candidates (all RFCs available at http://www.ietf.org).

These additional tuples of IP addresses and ports communicated in these solutions establish different data paths in media plane and signaling plane of a VoIP service and thereby break

EX1002
CISCO SYSTEMS, INC. / Page 985 of 1453

up the previous one-to-one relation of signaling session to media stream to a given VoIP device. Previously one media stream to the given VoIP device could be distinctively identified by exactly one IP address and port. In the new scenario on the signaling plane a list of IP address and port tuples is transported on which the VoIP device may receive media thereby increasing the complexity of correlation between media plane and signaling plane of a VoIP service.

SUMMARY OF THE INVENTION

One object of the invention is to suggest correlation mechanisms that allow overcoming one or more of the limitations and challenges on the correlation of signaling plane and media plane of services.

The object is solved by the subject matter of the independent claims. Advantageous embodiments of the invention are subject to the dependent claims.

One of the various aspects of the invention is to suggest a definition of correlation keys that allow the correlation of media streams of services and the associated signaling session of the respective services based on data records (reports) that provide information on the media plane and signaling plane of the respective services. These correlation keys may be for example provided in form of hash keys. A correlation key may be associated to a given direction of the media data paths of the media streams belonging to a given service (e.g. caller-to-callee or callee-to-caller for a simple bi-directional service, e.g. VoIP call). Hence, assuming that the service comprises at least two media streams of different directions, at least two correlation keys are provided on the signaling plane for later correlation of the media plane and signaling plane of the service. On the media plane one correlation key is provided per media stream.

The correlation keys for use in correlation are generated by a media plane probe and a signaling plane probe independently from each other, but the two probes generate matching correlation keys for a given media service (i.e. the signaling plane probe and the media plane probe independently each generate the same correlation key for a given direction/media data path of the media service, given that there are not any exceptional situations preventing the match of the correlation keys).

In response to the detection of the end of a signaling session, the signaling plane probe generates for this signaling session at least one correlation key for each "direction" of the service to which the signaling session belongs. Each correlation key (e.g. hash key) is generated by the signaling plane probe based on a timestamp indicative of the point in time

EX1002
CISCO SYSTEMS, INC. / Page 986 of 1453

at which the end of the respective signaling session has been detected by the signaling plane probe and using information on respective direction of the media plane data flow (e.g. caller-to-callee or callee-to-caller for a simple bi-directional service, e.g. VoIP call). The correlation keys generated for the different directions of the service corresponding to the signaling session the end of which has been detected are then collated in a signaling session report, which may be for example stored in a database or a flat file.

For the media plane, the media plane probe generates a correlation key (e.g. hash key) for each media stream. The correlation keys for the media steams are generated upon the media plane probe detecting the end of the respective media stream. The correlation key for a respective terminated media stream is generated by the media plane probe based on the direction of the respective media stream, e.g. based on the media data path of a media stream, and on a timestamp indicative of the point in time at which the respective media stream has ended. The timestamp at which the respective media stream has ended is for example the time at which the last packet of the media stream has been received by the media plane probe. The media plane probe stores the correlation key (e.g. hash key) for the media stream in a media stream report, which may be for example stored in a database or exported as a flat file.

Another aspect of the invention is the use of the correlation keys comprised in the signaling session reports and the media stream reports to identify the media streams and signaling session belonging to a single media service. As indicated above, the correlation keys generated by the signaling plane probe and the media plane probe should be matching each other (i.e. the correlation keys of a given signaling session report should be found in the media stream reports, respectively, the correlation key of a media stream report should be found in one of the signaling session reports), provided that signaling session and related media streams are terminated nearly at the same point in time, i.e. within a given timeframe. Hence, a correlation unit can identify which media streams belong to which signaling session (or vice versa) and may therefore generate a service record that summarizes a service based on information contained in the media stream reports and information contained in the signaling session report of the respective service.

According to one exemplary embodiment of the invention, a method for correlating media streams and signaling sessions of services in a passive monitoring system of a packet-switched network is provided. It is assumed for exemplary purposes that one service has one signaling session.

In this method a signaling plane probe generates at least one correlation key for each direction of a service based on the information of the signaling session of the respective

service monitored at the signaling plane probe. As noted above the direction may be equivalent to a respective media data path of a media stream belonging to a given service. The correlation keys for a respective service may be generated using a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the signaling plane probe and using information on the direction of the respective service. Furthermore, the signaling plane probe stores a signaling session report for each signaling session in a database. Each of the signaling session reports comprises at least two correlation keys generated for the respective directions of the service.

Moreover, in this method a media plane probe also generates a correlation key for each media stream monitored by the media plane probe. The media plane probe generates the correlation key using a timestamp indicative of the point in time of the end of the respective media stream as detected by the media plane probe and using information on the media data path of the respective media stream. The media plane probe stores a media stream report for each media stream in a database, wherein each media stream report comprises at least the correlation key generated for the respective media.

A correlation unit further correlates the media streams and the signaling sessions based on the correlation keys comprised within media stream reports and signaling session reports.

In a more detailed exemplary embodiment of the invention, the generation of the respective correlation keys for the respective media streams by the media plane probe is based on the media data path information of the respective media stream and the timestamp indicative of the point in time at which the respective media stream ended.

According to another exemplary embodiment of the invention, information on the direction of the respective service – based on which the correlation keys are generated by signaling plane probe for a respective service – is information on one or more media data paths of media streams of the service learned from messages of the signaling session of the service. In other words, the direction of the service may be for example given by the media data path which is yielding a given direction. For example in a simple VoIP call between two peer devices, there are two directions: caller-to-callee and callee-to-caller as noted above.

In a further embodiment of the invention, the signaling plane probe monitors signaling messages of the respective signaling sessions of the services, and detects media streams belonging to each service associated to a respective monitored signaling session based on the signaling messages of the respective signaling sessions. The correlation keys for a respective one of the signaling sessions may be generated by the signaling plane probe

based on information on the media data path of the media streams belonging to the service associated to the respective one of the signaling sessions and the timestamp indicative of the point in time at which the end of the respective signaling session has been detected by the signaling plane probe. For example, in one possible implementation information on a media data path of a media stream is a destination IP address and port number of the media stream.

In another embodiment, the timestamps used for the generation of the correlation keys by the signaling plane probe and the media plane probe could be for example rounded (e.g. in a configurable or fixed interval) before the generation of the correlation keys, in order to ensure that timing differences in the events monitored in the media plane and signaling plane of the services do not lead to generation of non-matching correlation keys for a given service. Alternatively, in another exemplary implementation, the timestamps – by default – have a granularity that is higher than one second, e.g. a granularity in the range of one to ten seconds.

In a further embodiment, instead of storing a single correlation key per direction of a signaling session or per media stream, additional correlation keys may be generated and stored. The input for these additional correlation keys are the same IP address and port information, but a different timestamp. For example, the signaling plane probe could calculate an additional correlation key using a timestamp earlier than the timestamp indicative of the end of the respective signaling session.

In case of using a rounded timestamp this earlier timestamp may be the next earlier rounded timestamp before the rounded timestamp indicative of the end of the respective signaling session. In one exemplary implementation, the signaling plane probe could generate two timestamps from a (non-rounded) timestamp indicative of the end of the respective signaling session which are each used together with the same IP address and port information to generate two respective correlation keys for a given direction: One of these two generated timestamps used for calculation of the correlation keys may be the timestamp indicative of the end of the respective signaling session rounded to the nearest lower value according to the rounding interval, while the other of these two generated timestamps may be the timestamp indicative of the end of the respective signaling session rounded to the nearest higher value according to the rounding interval.

All correlation keys that are generated by the signaling plane probe for a given direction may be stored as part of the signaling session records.

EX1002
CISCO SYSTEMS, INC. / Page 989 of 1453

In a similar fashion as described above for the signaling plane probe and the directions indicated in the signaling, also the media plane probe may optionally generate more than one correlation key for a given media data path/media stream. In case of using rounded timestamps also the media plane probe could generate two timestamps from a (non-rounded) timestamp indicative of the end of the respective media stream which are each used together with the same IP address and port information of the media stream to generate two respective correlation keys. One of the two timestamps generated by the media plane probe may be the timestamp indicative of the end of the respective media stream rounded to the nearest lower value according to the rounding interval, while the other of these two generated timestamps may be the timestamp indicative of the end of the respective media stream rounded to the nearest higher value according to the rounding interval. All correlation keys that are generated by the media plane probe for a given media stream may be stored as part of the media stream records.

In case of rounding timestamps in the media plane probe and the signaling plane probe, the rounding interval in both probes should be identical. The gain of having both probes generating additional correlation keys and correlating a multitude of correlation keys may not reflect in the increased processing needs.

In a further exemplary embodiment of the invention, the correlation of the media streams and the signaling session of the respective services is performed by a correlation unit periodically or in response to a query.

Another exemplary embodiment of the invention is related to a method for correlating media streams and signaling sessions of services. According to this method a correlation unit correlates the media streams and the signaling sessions of one or more services based on the correlation keys comprised within media stream reports of the media streams and signaling session reports of the signaling sessions to thereby identify the media stream reports and signaling session report belonging to a respective one of said one or more services. For correlating media streams and the signaling sessions, the correlation unit identifies one or more media streams of a respective service and the corresponding signaling session of the respective service based on the correlation keys comprised in the media stream reports and signaling session reports. Further, the correlation unit generates a service record for a respective one of said at least one service based on information contained in the media stream reports and information contained in the signaling session report of said at least one service.

EX1002
CISCO SYSTEMS, INC. / Page 990 of 1453

In one exemplary implementation, these steps are performed by a correlation unit periodically for all signaling session reports and media stream reports generated within a configurable time interval, or in response to a request.

In case the correlation unit is unable to match one or more media streams to said signaling session report, the correlation unit may optionally generate a service record without quality information of the media streams of the service or may optionally generate a corresponding indication of the user/operator of the correlation unit.

A service report generated for a service by the correlation unit may comprise – according to one exemplary implementation – information on the service and the quality information of the media streams of the service.

In one exemplary implementation, the correlation keys provided in a respective signaling session report may have been generated using a timestamp indicative of the point in time at which the end of the respective signaling session of the corresponding service has been detected and using information on the media streams of the service. Similarly, the correlation keys provided in a respective media stream report may have been generated using a timestamp indicative of the point in time at which the respective media stream ended and using information on the media data path of the media stream.

In one further exemplary implementation, the correlation unit first attempts a correlation of media stream reports and signaling session reports using the correlation keys that have been generated based on the timestamps indicative of the end of the signaling session, respectively, the end of the media stream(s). In case the correlation is unsuccessful, the correlation unit may further use optionally available additional correlation keys contained in the signaling session reports and/or media plane reports which are based on other timestamps, e.g. before and after the actual end of the respective signaling session or media stream(s), respectively. This layered approach allows to first conduct the correlation using the correlation keys which are more likely to yield a result and as a fallback conduct the correlation using a wider timeframe.

According to a more detailed exemplary embodiment of the invention, the correlation of the media streams and the signaling sessions of one or more services based on the correlation keys comprised within media stream reports of the media streams and signaling session reports of the signaling sessions by the correlation unit comprises matching the respective correlation keys of the media stream reports of media streams are to the respective correlation keys of the signaling session reports, or vice versa. A match of the correlation keys of a one of the media stream reports and one of the signaling session reports (i.e. the

EX1002
CISCO SYSTEMS, INC. / Page 991 of 1453

two correlation keys are identical) yields that the media stream of said one media stream report belongs to the same (media) service to which the signaling session of said one signaling session report belongs.

In another exemplary embodiment of the invention, for correlating the media streams and the signaling sessions of one or more services by the correlation unit, same may obtain from a signaling session report correlation keys identifying the media streams belonging to the same service as the signaling session. Further the correlation unit could then identify those media stream reports which include one of the correlation keys obtained from the signaling session report.

Alternatively, in another exemplary embodiment, the correlation of the media streams and the signaling sessions of one or more services could also be implemented by the correlation unit obtaining from a media stream report a correlation key identifying the media stream, and further the correlation unit identifying a signaling session report among the signaling session reports which includes the same correlation key obtained from the signaling session report.

According to one exemplary embodiment of the invention, a method for correlating media streams and signaling sessions of services in a passive monitoring system of a packet-switched network is provided. It is assumed for exemplary purposes that one service has one signaling session.

Another embodiment of the invention is related to a passive monitoring system for correlating media streams and signaling sessions of services in a packet-switched network. The passive monitoring system comprises a signaling plane probe that generates at least one correlation key for each direction of a service based on the information of the signaling session of the respective service monitored at the signaling plane probe. As noted above, there may be one or more correlation keys for each direction of the service. The correlation keys for a respective service are generated by the signaling plane probe using a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the signaling plane probe and further using information on the direction of the respective service (e.g. information on the media data path of the given direction, such as a destination IP address and UDP port number). The signaling plane probe stores a signaling session report for each signaling session in a database, wherein each signaling session report comprises the at least two correlation keys generated for the respective directions of the service.

Furthermore, the passive monitoring system also comprises a media plane probe for generating a correlation key for each media stream monitored by the media plane probe. The

EX1002
CISCO SYSTEMS, INC. / Page 992 of 1453

correlation key is generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream. The media plane probe stores a media stream report for each media stream in a database. Each media stream report comprises at least the correlation key generated for the respective media.

The passive monitoring system further comprises a correlation unit for correlating the media streams and the signaling sessions based on the correlation keys comprised within media stream reports and signaling session reports. The correlation unit may for example use one of the different correlation methods described herein for this purpose.

Another embodiment of the invention is related to the design of the signaling plane probe. According to this embodiment of the invention, the signaling plane probe comprises a network interface card for receiving packets of signaling sessions of multiple media services and a monitoring unit for monitoring the signaling sessions based on the packets of the signaling sessions received by the signaling plane probe to thereby obtain information on a respective one of the signaling sessions. The monitoring unit of the signaling plane probe is further capable of detecting the point in time at which a respective signaling session of the respective service terminates.

The signaling plane probe also comprises a processing unit for generating at least one correlation key for each direction of a service based on a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the monitoring unit and based on information on the direction of the respective service. Moreover, the monitoring unit stores a signaling session report for each signaling session in a database, wherein each signaling session report comprises at least two correlation keys generated for the respective directions of the service.

Another embodiment of the invention is related to a media plane probe which comprises a network interface card for receiving packets of media streams of multiple media services, and a monitoring unit for monitoring the media streams based on the packets of the media streams received by the media plane probe. Thereby the media plane probe obtains information on a media data path a respective one of the media stream. Further, the monitoring unit detects the point in time at which a respective media stream of the respective service terminates, and a processing unit of the media plane probe generates a correlation key for each media stream monitored by the monitoring unit. This correlation key may be for example generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream.

EX1002
CISCO SYSTEMS, INC. / Page 993 of 1453

The media plane probe's monitoring unit further stores a media stream report for each media stream in a database, wherein each media stream report comprises at least the correlation key generated for the respective media.

The invention according to another embodiment is related to a correlation unit capable of correlating media streams and signaling sessions of services in a passive monitoring system of a packet-switched network. The correlation unit comprises a database access unit for accessing a database comprising signaling session reports for signaling sessions of services and a database comprising media stream reports of media streams of the services. The signaling session reports each comprise at least one correlation key for each direction of a respective service, and the media stream reports each comprise one correlation key indicating the direction of the media stream. A processing unit of the correlation unit is used to correlate the media streams and the signaling sessions of the services based on the correlation keys comprised within media stream reports and signaling session reports to thereby identify the media stream reports and signaling session report belonging to a respective one of said one or more services. The processing unit identifies one or more media streams of a respective service and the corresponding signaling session of the respective service based on the correlation keys comprised in the media stream reports and signaling session reports. The correlation unit may further comprise a service record generation unit (e.g. implemented by a processing unit) for generating a service record for a respective service based on information comprised in the media stream reports and information comprised the signaling session report of said at least one service.

In a further embodiment of the invention, the correlation unit is further adapted, e.g. by comprised respective configured means, to perform the steps of the correlation methods according to one of the different embodiments described herein. Furthermore, also the signaling plane probe and the media plane probe may be adapted, e.g. by comprised respective configured means, to implement the different functions thereof as described herein.

Further embodiments of the invention relate to the implementation of the different functions of media plane probe, signaling plane probe and correlation unit in software. In this context, another embodiment of the invention provides a computer-readable medium storing instructions that, when executed by a processor of a signaling plane probe, cause the signaling plane probe to receive packets of signaling sessions of multiple media services, and to monitor the signaling sessions based on the packets of the signaling sessions received by the signaling plane probe to thereby obtain information on a respective one of the signaling sessions. The execution of the instructions further cause the signaling plane probe to detect the point in time at which a respective signaling session of the respective

EX1002
CISCO SYSTEMS, INC. / Page 994 of 1453

service terminates, and to generate at least one correlation key for each direction of a service based a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected and based on information on the direction of the respective service. Moreover, the executed instructions may further cause the signaling plane probe to store a signaling session report for each signaling session in a database, wherein each signaling session report comprises the at least two correlation keys generated for the respective directions of the service.

Another exemplary embodiment of the invention is providing a computer-readable medium storing instructions that, when executed by a processor of a media plane probe, cause the media plane probe to receive packets of media streams of multiple media services, and to monitor the media streams based on the packets of the media streams received by the media plane probe to thereby obtain information on a media data path a respective one of the media streams. Moreover, the execution of the instructions cause the media plane probe to detect the point in time at which a respective media stream of the respective service terminates, and to generate a correlation key for each media stream monitored by the monitoring unit, wherein the correlation key is generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream. Furthermore, the execution of the instructions may further cause the media plane probe to store a media stream report for each media stream in a database, wherein each media stream report comprises at least the correlation key generated for the respective media.

Another embodiment of the invention is providing a computer-readable medium storing instructions that, when executed by a correlation unit, cause the correlation unit to correlate media streams and signaling sessions of services in a passive monitoring system of a packet-switched network. The execution of the instructions cause the correlation unit to access a database comprising signaling session reports for signaling sessions of services and a database comprising media stream reports of media streams of the services. The signaling session reports each comprise at least one correlation key for each direction of a respective service, and the media stream reports each comprise one correlation key indication the direction of the media stream. The execution of the instructions further cause the correlation unit to correlate the media streams and the signaling sessions of the services based on the correlation keys comprised within media stream reports and signaling session reports to thereby identify the media stream reports and signaling session report belonging to a respective one of said one or more services and to identify one or more media streams of a respective service and the corresponding signaling session of the respective service based on the correlation keys comprised in the media stream reports and signaling session reports.

EX1002
CISCO SYSTEMS, INC. / Page 995 of 1453

The execution of the instructions also cause the correlation unit to generate a service record for a respective one of said at least one service based on information comprised in the media stream reports and information comprised the signaling session report of said at least one service.

Another embodiment is providing a computer readable medium storing instruction that, when executed by the processor of the correlation unit, cause the correlation unit to perform the steps of the method for correlating media streams and signaling sessions of services according to one of the different embodiments described herein.

BRIEF DESCRIPTION OF THE FIGURES

In the following the invention is described in more detail in reference to the attached figures and drawings. Similar or corresponding details in the figures are marked with the same reference numerals.

Fig. 1 shows exemplary situations where multiple media streams may be triggered in a media service,

Fig. 2 shows three geographically distributed POPs (Point of Presence) which are linked over the carrier's internal network,

Fig. 3 shows an exemplary network using internal and external addresses,

Fig. 4 shows an exemplary overview on a system according to an embodiment of the invention comprising signaling plane probe, a correlation unit and a media plane probe in a packet-switched network,

Fig. 5 shows a flow chart of the operation of the correlation unit according to an exemplary embodiment of the invention,

Fig. 6 shows the structure of a correlation unit according to an exemplary embodiment of the invention,

Figs. 7 & 8 shows two exemplary flow charts of the operation of a signaling plane probe according to different exemplary embodiments of the invention,

Fig. 9 shows the structure of a signaling plane probe according to an embodiment of the invention,

EX1002
CISCO SYSTEMS, INC. / Page 996 of 1453

Fig 10 shows the structure of a media plane probe according to an embodiment of the invention,

Fig. 11 shows a flow chart of the operation of a media plane probe according to an embodiment of the invention,

Fig. 12 shows a network in which locations are indicated, where signaling and media plane probes of the invention may be advantageously located according to an embodiment of the invention,

Fig. 13 illustrates the use of rounded timestamps within a signaling plane probe and a media plane probe to highlight potential sources of error in correlation, and

Fig. 14 illustrates the use of two rounded timestamps for generating respective correlation keys according to an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following paragraphs will describe various embodiments of the invention. For exemplary purposes only, most of the embodiments are outlined in relation mainly to VoIP services as an example for a media service, but the invention is not limited to VoIP services. For example, the invention may also be used for other types of media services provided in packet-switched networks. The invention may be advantageously used in media services which have signaling plane and media plane separated and/or taking different routes through the packet-switched network.

The explanations given in the Technical Background section above are intended to better understand the often VoIP call-related exemplary embodiments described herein and should not be understood as limiting the invention to the described specific implementations of processes and functions in a packet-switched communication network.

As indicated above, the invention generally relates to methods for correlating at least one media data path and a signaling session of a service in a passive monitoring system that is monitoring a packet-switched network. Furthermore, the invention also relates to an implementation of these methods in hardware and software, and provides a signaling plane probe, a media plane probe and a correlation unit, as well as passive monitoring system comprising same. Based on the assumption of disjunctive signaling and media components of a service, the correlation mechanism suggested herein supports correlation across

multiple hosts connected via a network (e.g. a Local Area Network (LAN), Wide Area Network (WAN) or the Internet).

One of the various aspects of the invention is to suggest a definition of correlation keys that allow the correlation of media streams of services and the associated signaling session of the respective services based on data records (reports) that provide information on the media plane and signaling plane of the respective services. In the following these correlation keys are implemented as in form of hash keys for exemplary purposes. The correlation keys may be used to query database(s) to correlate media stream reports for media streams monitored by a media plane probe and a signaling session report on the signaling session provided by a signaling plane probe that belongs to the same service – it should be noted that for the proper functioning of the invention, it is not decisive whether media stream reports and signaling session reports are stored in the same or different databases, or whether there are even multiple database partitions provided. The media stream reports and signaling session reports may even be stored in files.

The correlation keys are generated by one or more media plane probes and one or more signaling plane probes that monitor a packet-switched network independently from each other. This independent calculation of the correlation keys facilitates distributed correlation spanning across multiple geographically distributed components or even across multiple vendors of software components. Furthermore, as will become more apparent from the following, for a given media data path – respectively a corresponding given direction –, the parameters that are used for generating correlation keys at the signaling plane probe(s) and the media plane probe(s) ensure that the identical correlation keys are generated for the given media data path by the signaling plane probe(s) and the media plane probe(s) to facilitate correlation. A respective correlation key may be associated to a given direction of the media data paths of the media streams belonging to a given service. For example, assuming for exemplary purposes a simple bi-directional service, e.g. VoIP call, there are two directions: caller-to-callee and callee-to-caller.

The signaling plane probe may generate a correlation key for each direction of the service. For example, the signaling plane probe generates one correlation key for the caller-to-callee direction and another correlation key for the callee-to-caller direction. However, the signaling plane probe may also generate multiple correlation keys per direction, as will be outlined below in further detail. Consequently, in case it is assumed that a service comprises at least two media streams of different directions, then at least two correlation keys are calculated by the signaling plane probe for later correlation of the media plane and signaling plane of the service. The correlation key for a given direction or media data path may be generated based on information on the direction or media data path, such as for example a tuple comprising

EX1002
CISCO SYSTEMS, INC. / Page 998 of 1453

the destination IP address and UDP port for a media stream in the service's media plane corresponding to the given direction or media data path. In addition, the generation of the correlation key is further based on a timestamp. With respect to the generation of the correlation key by the signaling plane probe, the timestamp may for example indicate the point in time at which the signaling plane probe has detected the end of the signaling session (and thus the service). In another exemplary implementation, the timestamp used in the generation of a correlation key for a media data path of a media stream in the media plane of the service could also be the point in time of the termination (end) of the media stream in the media plane detected by the signaling plane probe.

The signaling plane probe may generate the correlation keys for the different endpoints (the endpoint indicate a direction of the related media data flow) of a service upon detection of the end of a signaling session and additionally or alternatively, upon detection of the end of a media stream in the service's media plane. Typically but not limited thereto, there is one endpoint per direction, e.g. the caller and callee. The callee may be represented by multiple endpoints in case of more complex media service scenarios, e.g. when session forking is used (see Fig. 1).

The end of a signaling session may be for example detected in the signaling plane probe by detecting a signaling protocol specific hang-up message, a terminal failure to connect the involved endpoints or a session timeout. Each correlation key (e.g. hash key) is then generated by the signaling plane probe based on a timestamp indicative of the point in time at which the end of the respective signaling session has been detected by the signaling plane probe and using information on respective direction of the media plane data flow (e.g. caller-to-callee or callee-to-caller for a simple bi-directional service, e.g. VoIP call).

The direction may be for example given by a media data path of a media stream of the respective service. A media data path could be for example indicated by a tuple comprising the destination IP address and UDP port number for transmitting the media packets of a media stream of the service. The signaling plane probe may thereby generate only one single correlation key per direction or multiple correlation keys per direction. In one exemplary embodiment of the invention, the signaling plane probe generates one correlation key per direction, where the correlation key for a respective direction is based on a media data path of a media stream. This media stream of which the media data path information is used to generate the correlation key should be existent at the end of the signaling session (according to the session signaling monitored by the signaling plane probe), in order to be able to match the correlation key to a corresponding correlation key in a media stream report generated by a media plane probe. The media data path(s) of a service and optionally their

EX1002
CISCO SYSTEMS, INC. / Page 999 of 1453

existence (e.g. start time and termination time) could be for example learned by the signaling plane probe from the messages of the signaling session of the service.

The correlation keys generated for the different directions of the service corresponding to the signaling session the end of which has been detected are then comprised in a signaling session report, which may be for example stored in a database or (flat) file.

Alternatively, the signaling plane probe may also generate a correlation key for each media stream in the media plane of the service. In this case it may be assumed that the signaling plane traffic, i.e. the packets of the signaling protocol of the signaling plane, allow the signaling plane probe to detect the termination (i.e. end) of respective media streams in the media plane. In this case, the detection of the end of a media stream could trigger the generation of a correlation key for the respective media stream based on information on its media data path and a timestamp indicating the point in time at which the signaling plane probe detected the termination of the media stream.

Further, in another alternative implementation, the detection of the end of a signaling session, respectively, service as well as the end of a media stream as detected by a signaling plane probe could be used to trigger the generation of correlation keys in the signaling plane probe. For example, during the ongoing service the detection of the termination of a media stream in the media plane as learned from the signaling plane traffic could trigger the signaling plane probe to generate and include respective correlation keys for the media streams terminated during the ongoing session into the signaling session report of the service, while the detection of the end of the signaling session, and thus the service, could be used as a trigger for generating correlation keys for the respective media streams being "alive" in the media plane of the service at the signaling plane probe and their inclusion into the signaling session report of the service.

In the media plane, the media plane probe generates a correlation key (e.g. hash key) for each media stream. The correlation keys for the media steams are generated upon the media plane probe detecting the end of the respective media stream. The correlation key for a respective terminated media stream is calculated by the media plane probe based on the direction of the respective media stream, e.g. based on the media data path of a media stream, and on a timestamp indicative of the point in time at which the respective media stream ended. This point in time is for example the point in time at which the last packet of the media stream has been received at the media plane probe. In this latter case, the media plane probe may thus maintain a timestamp indicating the time of reception of the last packet of the media stream at the media plane probe.

The timestamp used for the generation of the correlation key may indicate another point in time than the point in time at which the media plane probe detects the end of the media stream. For example, in a packet switched network, there may be interruption in the packet stream of the media stream so that there may be a timer that measures the time since the last reception of a packet of the media stream. In case the time since the last reception of a packet of the media stream is exceeding a threshold (e.g. the timer "expires") – for example after 15 or 30 seconds, or the like – then the media plane probe detects the end of the media stream. The timestamp used in the correlation key generation may nevertheless be the point in time at which the last packet of the media stream has been received. The media plane probe stores the correlation key (e.g. hash key) for the media stream in a media stream report, which may be for example stored in a database or exported as a flat file.

Furthermore the timestamp used for the generation of a correlation key may be rounded. This counters differences in the time basis (local time) of multiple signaling and media probes as slightly different timestamps still yield the same rounded timestamp. Additional correlation keys may be generated with different timestamps, e.g. indicative of the – optionally rounded – end of a respective signaling session and/or media stream or a timeframe before or thereafter. These additional correlation keys may be stored in the respective signaling session reports and/or media session reports.

A media stream may also be interrupted due to codec features such as Voice Activity Detection (VAD). If a sender of a media stream is mute the codec may not encode any data resulting in an interruption of the media stream. This is typically indicated in the packet stream transporting the media and should not be considered by the media plane probe as an indication of the end of the media stream itself. In case a timer mechanism is used to detect terminated media streams, the timer should be configured such that codec features that lead to a temporary interruption of the media stream are not triggering the termination of the media stream (according to the detection mechanism for detecting terminated media streams in the media plane probe).

Furthermore, in another exemplary embodiment, the correlation of media streams of services and the signaling sessions of the services may also be based on a compound keys used as a correlation keys. This exemplary alternative implementation may however require a more complex database structure of the media stream reports and signaling session reports, as will be outlined below.

Another further aspect of the invention is the use of the correlation keys comprised in the signaling session reports and the media stream reports to identify the media streams and signaling session belonging to the respective services. This correlation of media streams and

EX1002
CISCO SYSTEMS, INC. / Page 1001 of 1453

signaling session could be done for example periodically or on request. The correlation keys generated by the signaling plane probe and the media plane probe should be matching each other (i.e. the correlation keys of a given signaling session report should be found in the media stream reports, respectively, the correlation key of a media stream report should be found in one of the signaling session reports). Hence, a correlation unit can identify which media streams belong to which signaling session (or vice versa) based on the correlation keys contained in the media stream reports and the signaling session reports and may therefore generate a service record for a respective service based on information contained in the media stream reports and information contained the signaling session report of the service.

The correlation methods according to the different embodiments of the invention proposed herein are based on a probe monitoring the signaling plane traffic of services (i.e. the signaling plane probe) identifying new services and associated media data paths of the media plane by detecting their corresponding signaling sessions and determining for each service correlation keys allowing to identify at least the media streams of the media plane existent upon termination of the service. It should be noted that "at least the media streams" means that it is optionally possible to generate a correlation key for each media data path of the media plane learned from the signaling plane traffic of the service, in case it is possible to detect the termination of the media data paths of the media plane in the signaling plane traffic. In this case the correlation key for a respective media stream may be based on the information on the media data path of the respective media stream visible in the signaling plane of the service and the point in time at which the signaling plane probe detects the termination of the media stream in the signaling plane.

Regarding the use of the point in time of the termination of the signaling session (e.g. a signaling message in the signaling plane indicating "hang up") for the generation of correlation keys it should be noted that the termination of the signaling session also means that all existent media data paths, respectively, the corresponding media streams of the media plane are terminated. Hence, in case it is not possible to detect the termination of the media data paths of the media plane in the signaling plane traffic, it is assumed to be possible to detect at least the end of the signaling session and to thereby conclude on the termination of the respective media data paths of the media plane and to thereby facilitate correlation of the media streams that have been "alive" at the end of the service and the corresponding signaling session of the service.

As noted above, another possibility may be to use compound keys as correlation keys. A compound key is defining a set of information comprised e.g. in a given set of fields of a database entry of a signaling session report and media stream report that – together with

additional criteria on the point in time of the termination of a media stream or the service – allows to correlate media streams and signaling sessions of the services. In one exemplary embodiment, the one or more databases that are used to store the signaling session reports and the media stream reports are partitioned into partitions covering only a given amount of time (i.e. time interval) of signaling session reports and/or media stream reports, respectively. The "size", i.e. the time interval covered by the partitions may be for example determined based on the average time interval in which port reuse occurs in the target monitored packet-switched network (e.g. the partition could cover ½ of the average time interval in which port reuse occurs). In the given partitions it may thus be assumed that the media data path information, such as destination IP address and UDP port number are unique. In this case, the signaling session reports and media stream reports may not include separate correlation keys, but the correlation key can be generated on-demand as a compound key from the information on the media data paths contained in the signaling session reports and media stream reports.

Hence, it would be sufficient that the signaling session reports and media stream reports store information on the media data paths of the service (e.g. destination IP address and UDP port number) and a timestamp that indicates the point in time of termination of the respective media data path in the media plane, as detected by the signaling plane probe from the monitored signaling sessions and the media plane probe from the monitored media streams. As noted above, the signaling plane probe can also detect the point in time of termination of the media data path(s) in the media plane by detecting the point in time of termination of the signaling session, which is – in most practical cases – coinciding with the termination of all media streams of the service in the media plane as well.

In this case, the correlation could be realized by first selecting the database partition of the media plane reports according to a timestamp of the termination of a media data path/signaling session within a given signaling session report, and by then determining the media stream reports that comprise media stream information matching those indicated in the given signaling session report.

Fig. 4 shows a packet switched network 400 according to an exemplary embodiment of the invention that comprises a signaling plane probe 401, a correlation unit 402 and a media plane probe 403. Please note that more than one signaling plane probe 401 and media plane probe 403 may be provided. Optionally, there may be multiple correlation units 402 present, working independent of each other and not impacting the performance or correlation accuracy of any other component.

The signaling monitoring probe 401 and the media plane probe 402 are monitoring the traffic on a packet-switched network 400, which may be for example an IP based packet switched network. It is assumed for exemplary purposes that the signaling plane probe 401 and the media plane probe 403 monitor the traffic of the packet-switched network 400 at different locations of the packet-switched network 400, but observe the same network traffic.

In one exemplary implementation, the signaling plane probe 401 and the media plane probe 403 are probes of a minimal non-intrusive, passive monitoring system. The respective monitoring probes 401, 403 are connected to the packet-switched network 400 via respective test access ports (TAPs). A TAP is a passive network device that mirrors network traffic of the packet-switched network without interference of the original network traffic. It provides a copy of every packet sent or received on the network, by duplicating the data packets observed on the physical layer of the network. Instead of a TAP a Switch Port Analyzer (SPAN) port may be used to monitor the traffic of the packet-switched network.

In packet-switched environments, the signaling data of the signaling plane and media data of the media plane is packaged into packets on the transmitter side. Packets are transported over the packet-switched network independent of each other. The receiver of the packets – identified by the destination IP address and port – may have to regroup and sometimes reorder packets in order to compile streams from single packets.

On the signaling plane multiple packets belong to one signaling session. The first packet of a signaling session – usually containing a "call setup" message – starts a new signaling session (respectively a new service). At this point, the signaling plane probe 401 generates a session entry along with auxiliary data, i.e. a unique correlation key identifying the session internally (signaling session identifier). Packets following the initial signaling packet are matched to one of the currently ongoing signaling sessions (respectively services) and signaling sessions managed by the signaling plane probe. Packets which do not start a new signaling session and do not belong to existing sessions may be discarded.

Matching single signaling packets to existing signaling sessions is specified in the standards which define the signaling protocol itself. Transport layer information like IP addresses and protocol-specific information (e.g. SIP Call-IDs and tags) may be used.

A signaling session may be torn down upon reception of a special packet – a "call hang-up" message. This message again is specific to the signaling protocol used. Upon reception of this message the signaling plane probe 401 can conclude on the termination (end) of the signaling session and generates the correlation keys for use in correlation of media plane and signaling plane of the services. Furthermore, the signaling session may be removed

EX1002
CISCO SYSTEMS, INC. / Page 1004 of 1453

from its internal storage. Additionally the signaling monitoring component may remove sessions from its internal storage, if it identifies stale sessions.

The media plane 403 of the service may for example identify the media plane data in form of RTP streams. RTP streams are – analog to the signaling sessions – made up from individual RTP packets. The transmitter of an RTP stream generates RTP packets by splitting the media data into smaller pieces. In general these packets are relatively small to reduce the delay between sender and receiver. As a result many packets are created and form a single RTP stream – typically 50 packets per second. Single RTP packets can be grouped into an RTP stream by media plane probe 403. When using RTP, the media plane probe 403 has transport layer information as well as the RTP protocol header which contains a so called Synchronization source (SSRC). The SSRC is a 32-bit numeric identifier which is contained in every single packet and deemed mandatory by the RTP. When media plane probe 403 first receives a packet which does not match an existing RTP stream in its internal storage it creates an RTP stream. Consecutive RTP packets can then be matched to the existing streams by comparing the transport layer information and SSRC value. If no packets are received for a single RTP stream for a certain time the stream is considered ended and can be removed from the internal storage. A short interruption in the packet stream should not trigger the media plane probe 403 to mark an RTP stream as ended, thus the time before a media plane probe 403 can consider an RTP stream as ended is multiple seconds and has to take features like voice activity detection into account.

The signaling plane probe 401 and the media plane probe 403 generate information about the signaling session and media streams, respectively. This generated information is comprised in signaling session reports and media stream reports, respectively. In order to track running sessions and media streams the entities 401, 403 store information internally while the signaling sessions and media streams are in progress. When a signaling session or media stream is terminated the respective monitoring component 401, 403 may generate a signaling session report with signaling information, respectively media stream report with information on the media stream. As will be outlined below in further detail, the signaling session report provides a summary of the signaling session (service) and includes the correlation keys (e.g. hash keys) for correlation. Similarly, the media stream reports summarize the media stream and also include a respective correlation key (e.g. hash key) to facilitate correlation.

Each signaling session report for a signaling session may be for example written by the signaling plane probe 401 upon completion of a signaling session and contains data which describes the signaling session it monitored. For example, in one embodiment of the invention, the data stored in the signaling session report and describing the signaling session

EX1002
CISCO SYSTEMS, INC. / Page 1005 of 1453

include – but are not limited to – a set of caller and callee specific properties which will be available per endpoint (caller or callee). These endpoint-specific properties may for example include at least one of the following:

- endpoint address/name (e.g. SIP URI),
- phone number,
- User-Agent (endpoint software and version),
- capabilities/features,
- supported media types,
- IP addresses and ports for signaling and media streams (from SDP body), and
- hash key of the media path (for example described by the destination IP address and UDP port of the expected media stream)
- signaling routing information.

Additionally, one or more of the following signaling session properties which are not endpoint-specific may also be included in the signaling plane report:

- timestamps: e.g. session start, Post-Dial-Delay (PDD), connect time, session end;
- information on the session flow (e.g. signaling message(s) with timestamps),
- session state (e.g. successful, unsuccessful, timed out, reason for failure), and
- events during session (media on hold, codec renegotiation, session forking, authentication)

In one exemplary embodiment of the invention, the signaling session report comprises all of the above noted endpoint-specific properties, and – optionally – all signaling session properties listed above, as far as they are available from the signaling protocol messages.

Depending on the specific implementation and capabilities of the signaling plane probe, the signaling session reports may contain information about multiple endpoints and/or multiple media streams per endpoint. In this case the session end timestamp may be available per involved endpoint, and not per session.

EX1002
CISCO SYSTEMS, INC. / Page 1006 of 1453

For example, the most trivial VoIP service is a phone call between two parties (including two media streams, one in each direction). In this case, the signaling session report could store each party as one endpoint with the above mentioned information and the media stream's destination IP address and port information. If the VoIP service would contain a video call (i.e. one audio and video stream per direction) the endpoint information may be extended to contain the destination IP address(es) and port numbers of the two media streams per direction (one IP address & port tuple for audio, one IP address & port tuple pair for video). Considering a VoIP service, the respective tuples of destination IP address and UDP port number of the media streams of the session may be for example learned by the signaling plane probe from the SDP body of SIP signaling.

Likewise, the signaling plane probe may extend the signaling session report to include additional endpoints, if multiple endpoints were part of the VoIP service. Multiple endpoints could be for example involved in a VoIP service, in case a caller tries to reach a callee which has call forwarding configured. The caller may then hear a ring-tone from the callee's landline, followed by a ring-tone from the callee's mobile phone. Finally a voicemail box picks up the session generating a third endpoint on the callee's side.

The media plane probe 403 monitors the media traffic, i.e. the individual media streams that convey the media information of the different services. The media plane probe 403 identifies a new media stream of a media service based on the network traffic it observes on the monitored packet switched network 400. The identification of a new media stream for a given service may happen shortly after this service is set up on the signaling plane. Throughout the duration of the media stream information on the media stream may be stored in an internal data record on the media steam. The media plane probe 403 may note for each stream the last RTP packet received for the respective media stream in an internal data record on the media stream in order to allow detecting the media stream's termination.

The media plane probe 403 may optionally perform a real-time analysis of the media streams monitored on the packet switched network and may generate a fine-grained media stream quality report with media stream related information. Fine-grained media stream quality reports could be for example written in predetermined time intervals, e.g. every five seconds, and could provide a summary of the media stream in the respective interval as well as quality information of the media stream in the respective interval. The information of the fine-grained media stream quality reports of a media stream could be used by the media plane probe 403 to generate a single media stream report on the media stream upon the end of the media stream is detected by the media plane probe 403. The media stream report and optionally also the fine-grained media stream quality reports of a media stream may be stored in individual databases.

EX1002
CISCO SYSTEMS, INC. / Page 1007 of 1453

The media stream report generated by the media plane probe 403 upon detecting the end of the media stream may contain data which describes the unidirectional media stream it monitored as well as correlation key that can be for example generated based on the destination IP address and UDP port number of the media stream and a timestamp that indicates the point in time at which the media stream ended/terminated. The media plane probe 403 could for example learn the destination IP address and UDP port number from the IP header encapsulating the RTP packets on the network layer. The characteristics of each media stream can be grouped into two categories. The transport and RTP header information characterize the media stream, e.g. for correlation purposes, whereas the quality information enable quality related processing of the media stream. In general the transport information is the same for all media packets processed as part of a single media stream. The stream quality information includes information covering all media packets and may be aggregated or stored on a per-packet basis.

In one exemplary embodiment of the invention, the media stream report generated by the media plane probe 403 for a given media stream may for example include one or more of the following transport media information:

- source and destination IP address,
- source and destination UDP port,
- RTP header Synchronization source (SSRC) value,
- RTP payload type, and
- correlation key(s) (e.g. hash value(s)) calculated based on destination IP address, destination UDP port and a timestamp indicating the point in time at which the of the media stream terminated (e.g. the timestamp of the last packet received for the media stream) or timestamp indicative of the timeframe before or after the termination timestamp.

The stream quality information that may be added to the media stream report by the media plane probe 403 may for example include/indicate one or more of the following:

- timestamp information (e.g. start and/or end time),
- RTP format violations,
- protocol conformance (e.g. sequence errors and/or DSCP errors),

- transport information (e.g. packet interval and jitter statistics, information on packet loss, information on duplicate packets, etc.), and

- MOS values (e.g. per time-slice (e.g. every 5 seconds), minimum/average/maximum value for entire stream duration, etc.),

- events (e.g. comfort noise, silence suppression, DTMF tones, codec changes, marker bits).

In one exemplary embodiment of the invention, the media stream report comprises all of the above noted transport media information and optionally further all stream quality information listed above, as far as they are available to the media plane probe from the packets of the media streams.

In addition to "measured values" (e.g. jitter between multiple media packets) the media stream report may also contain calculated information like MOS (Mean Opinion Score) values and information about impairments experienced by the receiver of the stream.

As further shown in Fig. 4, a correlation unit 402 correlates the media stream reports and signaling session reports generated by the signaling plane probe 401 and the media plane probe 403 in order to identify the media streams and the signaling session that belong to a respective service. It should be noted that each service is assumed to have one signaling session, but may have one or more media streams.

Generation of Correlation Key

The correlation key that is used for correlation may be built from:

- the timestamp that indicates the end of the signaling session, respectively the end of a given media stream, and

- information on a media stream, such as for example the destination IP address and UDP port of the media stream.

The correlation of signaling plane and media plane by the correlation unit 402 is based on this compound correlation key.

As noted earlier, the correlation key may be for example a hash key generated based on the before-mentioned parameters. The hash function to calculate the hash key (sometimes also called hash value) from the given data should be known to all parties involved (i.e. signaling plane probe 401, and media plane probe 403 and optionally also correlation unit 402) so that

EX1002
CISCO SYSTEMS, INC. / Page 1009 of 1453

the result for a given input is the same for all parties. Therefore, the hash keys are determined by the signaling plane probe 401 and media plane probe 403 using media data path information in addition to a timestamp that indicates point in time when the signaling session, respectively, the media stream ended/terminated. The correlation unit 402 may generate additional correlation keys based on the timestamps indicative of the timeframe before or after the timestamp that indicates the point in time when the respective session ended.

The hash function to determine the hash key may be a simple concatenation of one or more of the input parameters. For example, a concatenation of a destination IP address, destination UDP port number and a timestamp may (optionally including a delimiter character in between the parameters) be used for defining the hash keys. Of course more complex mechanisms may also be used to calculate a hash key representing the signaling session identifiers and/or the media path identifiers. For example the MD5 message digest function (see IETF RFC 1321, "The MD5 Message-Digest Algorithm", 1992, available at http://www.ietf.org) could be used to create a valid hash key. The MD5 message digest function may be fed with a concatenation of a destination IP address, destination UDP port number and the timestamp indicating the time of termination of the signaling session, respectively, the media stream and the resulting string can be used as a correlation key. Another hash function that could be used may be selected from the SHA cryptographic hash function family (see FIPS PUB-180, "Secure Hash Standard (SHS)", 2008 available at http://www.itl.nist.gov/fipspubs/). Furthermore, in another embodiment, a linear hash function may be used.

As outlined with respect to Fig. 1 earlier herein, ephemeral media streams may exist at any point during a service, such as a VoIP service. The ephemeral media streams may be generated by early media streams, service forking and codec changes. As a result the start and end timestamps of media streams may not necessarily concur with the start and end time of the VoIP service itself. Yet the timestamps of the start or end of a signaling session or media stream are an important piece of information for a successful correlation, as it significantly reduces the search window and amount of data to search. In typical scenarios, it can be expected that the start time of signaling and media streams deviate significantly and are thus not ideal candidates for a correlation mechanism.

At the end of a VoIP service both caller and callee have an established signaling session and send each other media on the media plane. Once a party hangs up the session a hang-up signal is send on the signaling plane and at the same time stops sending media packets. Once the remote party receives the hang-up signal it also stops transmitting media. The timestamps of the end of the signaling session of a service and the end of the corresponding

media streams in the media plane of the service are commonly very close to each other compared to the start of a media service in signaling plane and media plane. All these events will be subject to the same network- and application-imposed delays. Still the time-frame in which these happen is typically in the few milliseconds range or in the sub-second-range on long-distance or low bandwidth networks. This makes the timestamps of the end of the signaling session and the end of the media streams a good choice for calculating a correlation key.

Nevertheless, since signaling plane probe 401 and media plane probe 403 independently determine the correlation keys based on timestamps (and even minor deviations of the timestamps in the millisecond-range could lead non-matching correlation keys), the granularity of the timestamps used for the generation of the correlation keys may be chosen to account for those deviations of events in signaling plane and media plane events (i.e. deviations in the end of the signaling session in the signaling plane and the end of the corresponding media streams in the media plane of a service). Therefore the timestamps could have a granularity for example in the range of one or more seconds or at least 250 milliseconds or 500 milliseconds. In one exemplary embodiment, UNIX timestamps (which is indicating the seconds passed since January 1, 1970, 00:00:00) are used for the calculation of the correlation keys. Alternatively, also timestamps with a high resolution (e.g. resolution of one or ten or hundred milliseconds) could be used, but the timestamps may be rounded for the calculation of the correlation keys. It should be noted that the choice of the granularity or rounding interval may also impact the performance of a database or databases storing the media stream reports and signaling session reports for correlation. The larger the granularity, respectively the rounding interval and thus the search window the more data have to be processed to match signaling sessions and media streams.

Rounding timestamps could be for example implemented by rounding the timestamp to the nearest n second interval. Assuming for example that the interval is 5 seconds the following UNIX timestamps would be rounded as exemplified in Table 1.

Unix timestamp value	rounded value (5 sec)	description
1283936131	1283936130	rounded down
1283936133	1283936135	rounded up
1283936135	1283936135	unchanged
1283936136	1283936135	rounded down
1283936139	1283936140	rounded up

Table 1

The rounding interval can be any time interval in seconds or even milliseconds whereas the specific value is a trade-off between speed and accuracy. As noted above, the larger the interval the more data may have to be processed to match signaling sessions and media streams. The smaller the search window is the more likely it is to miss a match due to misaligned timestamps or derivations due to the delays outlined above.

The best rounding interval depends on the network monitored. Reasons for increased time differences are possible derivations from a shared time source (NTP) or differences seen in signaling and media events, i.e. the delay between a call being terminated and the endpoints stopping to send media.

For a smaller search window of three seconds the rounded values are different, as for example shown in Table 2.

Unix timestamp value	rounded value (3 sec)	description
1283936131	1283936130	rounded down
1283936133	1283936133	unchanged
1283936135	1283936136	rounded up
1283936136	1283936136	unchanged
1283936139	1283936139	unchanged

Table 2

Using normalized "session end" timestamp (i.e. timestamps of low granularity or timestamps that have been rounded) may be advantageous to counter the effects (e.g. false positive hash key matches) of the re-used port numbers. Since the end of a service (and/or end of media streams) becomes part of the correlation criteria only the port numbers that are used and valid at this point in time are considered in the correlation.

Another issue that could complicate the correlation processing is that deviations in detecting the end of a media stream, respectively a signaling session at the media plane probe 403 and the signaling plane probe 401 leads to the two entities rounding the timestamps to different values. For example, the signaling plane probe 401 could round the timestamp up, while the media plane probe 403 rounds the timestamp down to the next rounding interval value due to (minor) deviations in the timestamps at the signaling plane probe 401 and media plane probe 403. In another exemplary embodiment, additional correlation keys may be therefore generated by either one or both, the signaling plane probe 401 and media plane probe 403.

The signaling plane probe 401 and/or media plane probe 403 may use timestamps indicative of the rounding intervals before or after the timestamp indicative of the point in time where a

particular signaling session or media steam ended. For example a session ended at a point in time identified by the Unix timestamp value 1283936135. The correlation unit applies the rounding mechanism based on 3 second intervals. The rounded value thus is 1283936136. The correlation unit may generate additional keys with the timeframes before or after the mentioned rounded value. In this case the timestamps used for generation of the additional keys are 1283936133 (1283936136 – 3 seconds) and 1283936139 (1283936136 + 3 seconds). Of course, especially in cases where the rounding interval is short, it may also be desirable to more rounded timestamps rounded to the next and subsequent rounding interval(s) based on which correlation keys are calculated.

As noted above, the inclusion of multiple correlation keys calculated based on different timestamps for a given direction of a signaling session and/or media stream may for example be useful to counter correlation failures due to applying different rounding of timestamps in the signaling plane probe 401 and media plane probe 403 as will be outlined in further detail based on Fig. 13 and Fig. 14 in the following. The end of the signaling session $t_{signaling}$ of a service as observed by the signaling plane probe 401 and the end of the one or more media streams t_{stream} of the service as observed in the media plane probe 403 may not perfectly match each other as shown in Fig. 13. Even in case signaling plane probe 401 and media plane probe 403 calculate correlation keys based on the same IP address and UDP port tuple, the use of different timestamps $t_{signaling}$ and t_{stream} for the calculation of the correlation key will result in the correlation keys generated by signaling plane probe 401 and media plane probe 403 not matching each other. Additionally the use of rounded timestamps may not necessarily resolve this problem, as it cannot always be assured that the timestamps $t_{signaling}$ and t_{stream} are rounded to the same value. As also highlighted in Fig. 13 it could well happen that signaling plane probe 401 rounds the timestamp $t_{signaling}$ to the next lower rounded value T_1 in accordance with the rounding interval R, while the media plane probe 403 rounds the timestamp t_{stream} to the next higher rounded value T_2 in accordance with the rounding interval R. Again, correlation keys calculated on the different rounded timestamps T_1 and T_2 would not match each other.

As noted above, one possible solution to this problem is to include additional correlation keys at least to one of the signaling session reports and media stream reports. For example, in one exemplary embodiment, the media plane probe 403 could include two correlation keys per direction to the signaling session report. For a given media data path of a media stream (e.g. IP address and UDP port tuple) observed by the signaling plane probe, the signaling

plane probe could calculate one correlation key $C_{stream,1}$ on the media data path information and a rounded timestamp T_1, i.e. using the timestamp indicative of the end of the signaling session $t_{signaling}$ rounded to the next lower value according to the rounding interval, and the signaling plane probe could further calculate one correlation key $C_{stream,2}$ on the media data path information and a rounded timestamp T_2, i.e. using the timestamp indicative of the end of the signaling session $t_{signaling}$ rounded to the next higher value according to the rounding interval. Both correlation keys could then be included for the direction/media data path to the signaling session report.

A further implementation may include even further correlation keys, e.g. a third correlation key that is based on the rounded timestamp T_0, indicative of the next lower timestamp to T_1 according to the rounding interval.

The media plane probe 403 may calculate only one correlation key C_{stream} based on a rounded timestamp T_1 or T_2, i.e. based on the timestamp indicative of the end of the media stream (media data path) t_{stream} rounded to the next lower or higher value according to the rounding interval (and rounding rules). This correlation key for the media stream would then be included to the media stream report.

The correlation of the signaling session to the media stream(s) of the service would be successful in this embodiment, since either the correlation key $C_{stream,1}$ or the correlation key $C_{stream,2}$ within the signaling session report for the given direction/media stream would correspond to the correlation key C_{stream} included in the media stream's media stream report.

Optionally, in another embodiment of the invention, also the media plane probe 403 may calculate two or more correlation keys for each media stream, one correlation key based on the rounded timestamp T_1, i.e. based on the timestamp indicative of the end of the media stream (media data path) t_{stream} rounded to the next lower value according to the rounding interval, and the other correlation key based on the rounded timestamp T_2, i.e. based on the timestamp indicative of the end of the media stream (media data path) t_{stream} rounded to the next higher value according to the rounding interval. Both timestamps would then be included in the media stream report for the media stream by the media plane probe. In this exemplary implementation, the correlation may check whether the two correlation keys of the service's signaling session report for the direction/media stream match the two correlation keys within

the media stream report of the service's media stream to confirm the signaling session report and media stream report belonging to the same service.

Please note that instead of or in addition to the media plane probe 403 including two or more correlation keys to the media stream reports, also the signaling plane probe 401 could calculate two or more correlation keys per direction/media data path that is to be indicated in the signaling session report. Including multiple correlation keys per direction/media data path in the signaling session reports may be advantageous as it reduces the overhead information, since there are commonly less signaling session reports than media stream reports generated in the passive monitoring system.

Furthermore, in another exemplary implementation, the database(s) for signaling session reports and media stream reports may be further partitioned to reduce the search space for correlation. For example, the (respective) database could be partitioned in chunks of multiple hours, e.g. 4 or 6 hours or the like. The signaling session reports and media stream reports may further include as a separate element the timestamps of the end of the signaling session, respectively, the end of the media streams, based on which the database(s) can be partitioned and based on which the correct partition could be chosen for correlation later. Hence, in a more advanced implementation, besides the correlation keys a service end timestamp can be used as a search criteria to limit the amount of data that are to be searched in a database significantly.

In another exemplary implementation, the signaling plane probe may also generate a respective correlation key for all media streams of a service, in case the end of media streams is detectable within the session signaling, as noted previously. In this case the signaling session reports could further include a timestamp that indicates the end of each media stream, in order to allow choosing the correct partition of media stream reports in the database for correlation.

Correlation Mechanisms

For correlation of the media streams and the signaling sessions, different possibilities exist how the correlation by the correlation unit can be implemented. For example, according to exemplary embodiments of the invention, the correlation unit may correlate the media streams and the signaling session of the respective services periodically (or proactive) or in response to a query (i.e. on demand).

For example, a proactive correlation process could be utilized by a third party entity which has access to both signaling session reports and media stream reports. Their data may be

present in one or more databases to ease access to the raw data. As noted above, the correlation aims at correlating signaling and media information of the services and at merging them into combined service reports that may be then accessed by a third party, e.g. for evaluation of the services.

The proactive correlation process periodically takes all new signaling session reports which outline – but not fully describe – the media services, e.g. the monitored VoIP sessions. For each signaling session report the correlation process draws the calculated correlation keys from the signaling session report. There are at least two correlation keys in each signaling session report, at least one per direction. Additional correlation keys may optionally exist in the signaling session report, for instance if it describes a video call or a session with multiple endpoints. For each correlation key contained in a respective signaling session report the correlation process searches the media stream report database for the media streams with the same correlation key. If the correlation keys in the signaling session report are generated based on a timestamp indicating the end of the signaling session, every media stream of the service that existed at the end of the service in the media plane should have the same correlation key and will be in the result set of the search. If the correlation keys in the signaling session report also contain correlation keys for media streams that have been terminated during the ongoing service, the search may also further detect those media streams in the media stream report database based on the correlation key.

If a search returned two or more media stream reports, the correlation process encountered one of two scenarios. Either both media streams belong to the signaling session (i.e. service) or one of them was returned due to a correlation key collision. Both cases may be recovered by comparing the contents of the media stream report against the signaling session report. If a media stream in the result set starts before or ends after a signaling session, it was added to the result set due to a correlation key collision. Due to time information it cannot match the signaling session and is deleted from the result set by the correlation unit. If the media stream result set still contains multiple entries after the previous correlation key collision check, all remaining media streams (i.e. their media stream reports) belong to the media service (e.g. the VoIP session).

If a search returned no usable entry, i.e. no signaling session reports and media stream reports comprising matching correlation keys have been found, the correlation unit may optionally use additional correlation keys contained in either the signaling session reports and/or media stream reports to run another search, as explained with respect to Fig. 13 and Fig. 14 above.

The correlation process may optionally select only the most significant media stream for each direction for inclusion to the service report on the media service. The parameters to define the significance of the media streams may be for example configurable by the user/administrator. One parameter for deciding the significance of a media stream in the result set could be the duration of a media stream. For example, the service report generated for a given media service by the correlation unit could include the media stream with the longest duration, in case multiple media stream reports match a correlation key of a signaling session report. Another option would be to include in the service report the last media stream that has been alive in the media service, in case multiple media stream reports match a correlation key of a signaling session report. The correlation process may optionally add information from multiple media streams to the service report, e.g. when the service consisted of an audio and video part.

For a given signaling session (i.e. service), the correlation process may run at least twice, one time for each correlation key in a signaling session report. For example, in case the media service is a VoIP service, the correlation process may be for example performed by the correlation unit once for the caller's media stream and once for the callee's media stream, both identified by their respective correlation keys in the signaling session report.

The correlation unit combines the information contained in the media stream reports that are correlated to a respective signaling session report and the information contained in the signaling session report to provide a service report, providing an outline of the service. The content of this combined service report may be for example the sum or a subset of information of the signaling and media stream reports of a given service. Furthermore, the content of the service reports for the respective services may be configurable and/or depending on the application.

In another exemplary embodiment of the invention, the correlation unit may perform the correlation based on the media stream reports as starting points which are matched to their corresponding signaling session report. Ideally, each media stream of a media stream report should match to one signaling session report based on its correlation key. This implementation may optimize the search time in the correlation processing. The above correlation mechanism starting from the signaling session reports searches the rather large media stream report database at least twice for each signaling session. If the correlation process is based on the correlation keys within the media stream reports entries as starting point, the correlation would periodically take all new media stream reports, obtain the correlation keys thereof and search the signaling session reports for matching signaling sessions. At this point the same steps are taken as outlined above.

EX1002
CISCO SYSTEMS, INC. / Page 1017 of 1453

Another option may be to correlate media stream reports and signaling session reports on demand. An on-demand correlation employs the same mechanism as the proactive correlation mechanism described above, but instead of running periodically, e.g. when introducing new signaling session reports or media stream reports into the database(s), the on-demand correlation process runs when a user requests particular data.

In an exemplary implementation, the database may contain independent sets of signaling session reports and media stream reports. An operator could request service reports of services linked to some given search criteria, e.g. a specific user, a specific source and/destination IP address, a certain service type, services using a particular software application, codec, etc. The user could be for example specified by providing a username, phone number, the user's SIP URI, etc. or another identifier of the user that can be found in a signaling session report. The correlation unit would then search for the signaling session reports for all signaling sessions matching the particular search criteria. The search criteria may be for example provided to the correlation unit through a web application running on a browser.

For each signaling session report matching the search criteria, the correlation unit subsequently searches for the matching media stream reports as described above for the proactive correlation process. The input for this on-demand correlation is a set of signaling session reports matching the search criteria and not all signaling session reports as in the proactive correlation procedure described above. The on-demand correlation process generates for each signaling session report matching the search criteria a service report, for example by enriching the information of the signaling session report with the matching media stream report information and returns the service report for each matching signaling session report. The returned data may be for example viewed by the web application as individual service reports. Optionally the on-demand correlation process may also store the generated service reports in a database. This would save the on-demand correlation processing time in case an operator requests the same information multiple times.

Correlation Unit

Next, the correlation unit 402 as shown in Fig. 4 is discussed in further detail with respect to Fig. 5 and Fig. 6. Fig. 6 shows the structure of a correlation unit 402 according to an exemplary embodiment of the invention.

The correlation unit 402 may be reachable via the packet-switched network, e.g. through a web based application. For this purpose, the correlation unit 402 may comprise one or more network interface cards 601. The correlation unit 402 has a receiving unit 602 and a

EX1002
CISCO SYSTEMS, INC. / Page 1018 of 1453

transmitter unit 603, for example for receiving correlation related messages, such as for example on-demand correlation requests, and for responding thereto. Furthermore, the receiving unit 602 and a transmitter unit 603 may transmit and receive messages for accessing remote database(s) that contain(s) the signaling session reports and the media stream reports. The receiving unit 602 and transmitter unit 603 may receive and transmit the correlation related messages from its network interface card(s) 601.

The correlation unit 402 may also have a processing unit 604. The processing unit 604 may be used to determine correlation respective signaling sessions to their corresponding media streams. Furthermore, the processing unit 604 may be used to generate services reports. The service reports may for example comprise information on the respective services and the quality information of the media streams of the respective services. This information may be obtained from the signaling session report and media stream reports belonging to a given service. For correlation, it may be necessary to query one or more databases that comprise the signaling session reports and the media stream reports as provided by one or more signaling plane probes 401 and media plane probes 403. The correlation unit 402 may therefore comprise a database access unit 605 which provides functionality to access these one or more databases. In one exemplary implementation, the database(s) may be located remote from the correlation unit 403.

The correlation unit 402 may also have a storage unit 606, e.g. a RAM, for (temporarily) storing information and data related to the correlation processing. For example, the result set of media stream reports for correlation process, the data of the signaling session reports, and the service report generated for a respective service may be stored in the storage unit 606.

Fig. 5 shows a flow chart of the operation of the correlation unit 402 according to an exemplary embodiment of the invention. Exemplarily, the correlation processing for determining the media streams belonging to one given signaling session report is illustrated in Fig. 5. In case a correlation should be performed for more than one signaling session (report), the procedure of Fig. 5 is repeated for each signaling session report. For example, when using a proactive correlation mechanism, the correlation unit 402 could obtain all signaling session reports that have been generated since the previous correlation process from a signaling session database and process each of the signaling session reports according to Fig. 5. In another embodiment related to an on-demand correlation process, the correlation unit 402 could also receive a correlation request that is indicating one or more search criteria, and may first – not shown in Fig. 5 – query a signaling session database for all signaling session reports that match the search criteria. The signaling session reports matching the search one or more criteria may then be each processed according to Fig. 5 and the service report(s) are returned to the querying party.

The correlation unit 402 obtains 501 a signaling session report to be processed and generates 502 a service report for the service corresponding to the given signaling session. This service report may include information contained in the signaling session report and will be further supplemented with additional information as described below. Furthermore, the correlation unit 402 obtains 503 a correlation key contained in the signaling session report – as noted previously there should be at least two correlation keys contained in the signaling session report. Using the obtained correlation key, the correlation unit 402 queries 504 a media report database to receive all media stream reports that match the correlation key i.e. that contain the same correlation key.

As noted above, it may happen that the query results in the database returning more than one media stream report for the given correlation key, for example due to a hash collision of the correlation key. Therefore, the correlation unit 402 checks 505 whether the returned result set of the database query comprises more than one media stream report. If not (no), the correlation unit 402 can immediately enrich 508 the service report with information on the media stream as contained in the one media stream report returned from the media stream database.

In case the result set returned by the database comprises multiple media stream reports, the correlation unit 402 may try to detect 506 and resolve a hash collision. For example, the hash collision could be resolved by checking further information in the media stream reports of the result set for parameters that identify the media stream (report) that belongs to the correlation key that has been queried. For example, in case the media stream reports contain timestamps of the beginning and/or end of the media stream, same could be compared to respective timestamps contained in the signaling session report, which yield the beginning and/or end of the signaling session. The media stream report(s) of media stream(s) that start before or end after the signaling session may be obtained from the database due to a hash collision. Accordingly, the correlation unit 402 may select 507 only the most relevant media stream report, i.e. the media stream report that is most likely corresponding to the service of the signaling session report from the result set and may add 508 at least a part of its information to the service report. Further, the correlation unit checks 509 whether there is a further correlation key contained in the signaling session report and, if so (yes), repeats steps 503 to 508. These steps are repeated for each further correlation key(s) comprised in the signaling session report.

Once all correlation keys contained in the signaling session report have been processed, the service report for the signaling session is complete, and may be optionally stored 510 by the correlation unit 402 in a service report database.

Depending on the correlation type or application, the procedure of Fig. 5 could be supplemented with additional steps. For example, in case of a proactive/periodic correlation, the correlation unit 402 may check whether there is another signaling session report to be matched to its corresponding media stream reports, and if so the procedure of Fig. 5 would be executed for each signaling session report to be processed. In case of performing a correlation on demand, the correlation unit 402 may likewise check whether there is another signaling session report to be matched to its corresponding media stream reports, and if so the procedure of Fig. 5 would be executed for each signaling session report to be processed. Once all signaling session reports have been processed the correlation unit 402 may generate a correlation response message comprising the service reports generated by the correlation unit 402 in response to the search criteria provided in a correlation request, and returns the correlation response message to the querying entity, e.g. another device/computer.

Signaling Plane Probe

Fig. 9 shows an exemplary implementation of a signaling plane probe 401 and Figs. 7 and 8 show two exemplary flow charts of the operation of same according to different embodiments of the invention. In general, the signaling plane probe 401 observes one or more network links to obtain a copy of all packets passing these network links/interfaces. For this purpose, the signaling plane probe 401 comprises a monitoring unit 901 that receives 701 packets of a service on the packet-switched network 400. For example, this monitoring unit 901 may receive the packets from a one or more specialized packet capture cards 906 (network interface card - NIC) which is capable of receiving and processing packets on the physical interface and to provide them to the application layer, nearly without requiring CPU processing time and operation system functionality. An optional filter in each packet capture card of the signaling plane probe 401 may be used to prevent unwanted packets from being copied from the network interfaces to the processing processes. These filters may be for example implemented as stateless or stateful Internet Protocol (IP) or payload filters. For example, this filter may check 702, whether the currently processed packet is a signaling packet or not. If the packet does not belong to a signaling session, i.e. is not packet of a signaling related protocol, the next packet may be processed.

Each signaling packet received at the signaling plane probe 401 will be processed by a detection unit 902 which analyzes the contents of the packets provided by the monitoring unit 901 so as to identify and process packets as signaling packets. Specifically, the detection unit 902 detects signaling packets and matches these to signaling sessions of the media service, and is capable of identifying one or more media data paths of a media plane of the

service based on signaling information of the service comprised in the received packets. Optionally, the detection unit 902 may be provided in one or more specialized packet capture cards.

For example, the detection unit 902 identifies packets containing signaling information (signaling packets) in a parsing process based on their header information. If parsed successfully as a signaling packet, the signaling packet is forwarded to a state engine. The state engine is designed to identify 703 and form signaling sessions from individual signaling packets.

The state engine (which may be considered an internal database with correlation related information maintained in the storage unit 903) of the detection unit 902 has a processing facility and a state table which holds information about signaling sessions (signaling session records). Based on the protocol-specific identifiers in the signaling packets the detection unit 902 can identify the start and end of a signaling session, respectively media service, or "append" a respective processed signaling packet to an existing signaling session. Signaling packets may also contain information on the start and termination of media streams in the media plane of the media service, which are events that may be tracked by the detection unit 902. Depending on whether the identified signaling session is already registered in the signaling plane probe 401 (step 704), the detection unit 902 registers 705 the new signaling session in the state table, including the generation of a new signaling session record for the signaling session.

The signaling session record may be supplemented with information on the signaling session while same is running to account – for example – for endpoint address/name (e.g. SIP URI); the phone number of the user; the user-agent (endpoint software and version); capabilities/features; supported media types; IP addresses and ports for signaling and media streams (from SDP body); signaling routing information; timestamps: e.g. session start, Post-Dial-Delay (PDD), connect time, session end; information on the session flow (e.g. signaling message(s) with timestamps); session state (e.g. successful, unsuccessful, timed out, reason for failure), and/or events during session (media on hold, codec renegotiation, session forking, authentication), etc.

Furthermore, by analyzing 706 the contents of the signaling packets, e.g. a SDP body of a SIP messages comprised in signaling packets, the detection unit 902 may further learn one or more media data paths of the media plane of the service belonging to the media service that is associated to a given signaling session. The signaling plane probe 401 may further comprise a storage unit 903, e.g. a volatile memory, to store the information describing the state of the respective signaling sessions in the state table. In case the signaling packet

indicates the start of a new media stream (step 706: yes), the detection unit 902 may add 707 information on the media data path (e.g. IP address and port number of the destination, and optionally the source of the media stream) of this media stream to the signaling session record. Likewise, in case the signaling packet indicates the end/termination of a new media stream (step 708: yes), the detection unit 902 may remove the information on the respective media stream from the signaling session record maintained in storage unit 903. In case the signaling packet indicates the termination of the signaling session (step 710: yes), the detection unit 902 may either itself or trigger the processing unit 904 to generate 711 a respective correlation key for each media data path indicated in the signaling session record. The correlation key for a respective media data path of a media stream may be generated for example based on information on the directivity of the media stream (e.g. as given by the tuple of destination IP address and UDP port number) and a timestamp indicating the point in time at which the signaling session was terminated. For example, this timestamp may indicate the point in time of reception of the signaling packet indicating the event of the termination of the signaling session at the signaling plane probe 401. For example, the network interface card(s) 906 of the signaling plane probe could generate a timestamp indicating the time of reception of the respective signaling plane packet and could make same available to the other components of the signaling plane probe 401. Furthermore, the detection unit 902 or the processing unit 904 may further generate 912 a signaling session report based on the information on the signaling session gathered in the signaling session record. Further, the signaling session report also included the correlation keys for the media data paths of the service that exist at the end of the service according to the signaling plane information. The signaling session report may then be stored in a signaling session report database, for example using the database access unit 907 of the signaling plane probe 401. Moreover, the signaling session is deregistered 713 from the state table.

Once a given signaling packet has been processed, it may be discarded. It should be also noted that the order of the checks in steps 706, 708 and 710 and the respective actions to be taken is only exemplary. It is only important that the information on the media streams of the service that exist in the media plane are tracked by the signaling plane probe 401, and that the signaling plane probe 401 is able to detect the termination of the signaling session.

Optionally (not shown in Fig. 7), in another exemplary embodiment, the detection unit 902 of the signaling plane probe 401 periodically (e.g. every 5, 10 or 15 seconds) traverses all entries in the state table in order to find and clean up stale signaling sessions. For this purpose, the signaling plane probe 401 may add a timestamp to each signaling session record in the state table that is updated each time a new signaling packet/message of the respective signaling session is received. Based on this timestamp allows to identify stale

EX1002
CISCO SYSTEMS, INC. / Page 1023 of 1453

signaling session by simply checking based on the signaling sessions' timestamps whether the last signaling packet/message for a given signaling session has been received longer than a threshold time period ago. For example, stale sessions might be those which did not receive new signaling packets/messages for 86400 seconds or signaling sessions may be defined stale and are terminated after a certain time. This clean-up removes unnecessary information from the state.

Fig. 8 shows another flow chart of the operation of a signaling plane probe 401 according to another embodiment of the invention. In the example discussed with respect to Fig. 7, the signaling plane probe 401 keeps track of the media streams currently existing in the media plane of the service, eliminating those media streams from the signaling session record that are terminated during the ongoing signaling session/service. In the flow chart of Fig. 8, which is corresponding to Fig. 7 to a large extent, the termination of one or more media streams in the media plane, as detected in step 708, causes the detection unit 902 or the processing unit 904 (triggered by the detection unit 902) to generate 801 a correlation key for each terminated media stream. Similar to the other correlation keys, the correlation key for a terminated media stream may be generated based on its media data path information (e.g. destination IP address and UDP port number) and a timestamp that indicates the point in time the media stream was terminated. This timestamp may indicate the point in time of reception of the signaling packet indicating the event of the termination of the media stream at the signaling plane probe 401. The correlation key generated is then added 802 to the signaling session record of the signaling session by the detection unit 902 or the processing unit 904 and is later then also stored in the signaling session report in step 712 together with the other correlation keys either generated in step 801 or step 711.

Media Plane Probe

Next, the media plane probe 403 according to an exemplary embodiment of the invention is described with respect to Fig. 10 and Fig. 11. Fig 10 shows an exemplary embodiment of a media plane probe 403, while Fig. 11 shows a flow chart of its exemplary operation according to an embodiment of the invention.

Similar to the signaling plane probe 401, the media plane probe 403 observes one or more network links to obtain a copy of all packets passing these interfaces. The media plane probe 403 may observe one or more network links to obtain a copy of all packets passing these interfaces. The media plane probe 403 comprises a monitoring unit 1001 that receives 1101 packets of a service on the packet-switched network 401. For example, this monitoring unit 1001 received the packets from one or more specialized packet capture cards 1006 (network interface card - NIC) which are capable of receiving and processing packets on the physical

EX1002
CISCO SYSTEMS, INC. / Page 1024 of 1453

interface and to provide them to the application layer, nearly without requiring CPU processing time and operation system functionality. An optional filter in the packet capture card of the media plane probe 403 may be used to prevent unwanted packets from being copied from the network interfaces to the processing processes. This filter may be for example implemented as stateless or stateful Internet Protocol (IP) or payload filter. For example, this filter may check 1102, whether the currently processed packet is a media plane packet (media packet) or is some other packet. If the packet does not belong to the media plane, i.e. is not packet of a media related protocol, such as for example RTP, the next packet may be processed.

Each media packet received will be processed by the media plane probe 403. The detection unit 1002 of the media plane probe 403 is designed to detect and form media streams from single media packets. The media plane probe 403 may further comprise a processing unit 1002 that may hold a state table which stores information about the media streams monitored by the media plane probe 403 in a local storage unit 1003, e.g. a volatile memory. Based on the protocol-specific identifiers in the media streams the media plane probe 403 (e.g. based on header information in the RTP packets and/or lower layer headers) the detection unit 1002 identifies 1103 the media data path, i.e. the media stream, the media packet belongs to. If the media data path has not been yet registered (step 1104: no), i.e. the processed media packet starts a new media stream (with the given media data path) the detection unit 1002 generates a new media data record in the state table to account for the new media data path observed by the media plane probe 403. This media stream record may contain information on the media stream such as for example the destination (and optionally the source) IP address and port combination of the media stream, the SSRC in the packet header (in case RTP is used for media transport), etc. If the media data path is already known (step 1104: yes), the media stream record already exists. In any case, the detection unit 1002 updates a timestamp 1106 in the media stream record to indicate the point in time at which the last media packet of the media stream has been received. This timestamp may be used for calculating the correlation key for the media stream. Furthermore, the detection unit 1002 may (re)start a timer 1108 for the media stream record, which when timing out is indicating the termination of the media stream as will be outlined below. Alternatively, no timer is used, but the media plane probe 403 periodically checks for media streams the last media packet of which was received more than a threshold time period ago, in order to determine terminated media streams.

The media stream records of the media streams may for example indicate the respective media data paths thereof by an IP address and port tuple of the destination device, i.e. the receiving device of the media stream. The media plane probe's detection unit 1002 stores

information describing the state of the detected media streams in the media stream records maintained in the state table. Optionally, the individual media streams (i.e. their media data paths) may be identified by a media path identifier (e.g. stream hash key) as unique key. Further optionally, upon detecting a new media stream, respectively media path (step 1104: no), the processing unit 1004 could generate 1105 a media path identifier (e.g. a media path identifier (e.g. stream hash key)) for the media stream, respectively media path and stores 1106 the media stream record in the state table as outlined above.

Optionally, the processing unit 1004 could analyze every received packet for quality information 1107 and – further optionally – store them in the storage unit 1003 for a given time period. Periodically the processing unit 1004 may aggregate or compress the quality information to form fine-grained media stream quality reports with media stream related information. Fine-grained media stream quality reports could be for example written in predetermined time intervals, e.g. every five seconds, and could provide a summary of the media stream in the respective interval and the aggregated quality information of the media stream in the respective interval. Upon generation of a respective fine-grained media stream quality report, the packets used for the generation of this fine-grained media stream quality report can be removed from the storage unit 1003.

The processing unit 1004 of the media plane probe may for example periodically check 1109 (e.g. every 5, 10 or 15 seconds); whether a timer set of a media stream (record) in step 1108 has expired. Alternatively, as noted above, the media plane probe 403 may also check timestamps indicating the last update (i.e. last reception of a media packet) of the respective media stream reports in the state table. A media stream may be for example considered terminated, if no new media packets have been received by the monitoring unit 1001 for the existing media stream for a given amount of time (e.g. 60 seconds). Accordingly, if using a timer to monitor the termination, the timer value could be set to this given amount of time. Further alternatively, instead of periodically checking the media stream records or expiry of their timers, the expiry of a timer for a media stream (record) could cause an interrupt invoking the processing unit 1004 to perform steps 1110 to 1112 as outlined below.

Upon detecting the termination of a media stream, the processing unit 1004 processes the respective information in the media stream record of this media stream the state table. The processing unit 1004 generates 1110 a correlation key for the media stream based on its media data path information (e.g. the destination IP address and UDP port number) and the timestamp in the media stream record that is indicating the point in time of receiving the last media packet of the media stream (see step 1106). Furthermore, the processing unit 1004 generates 1111 a media stream report for the media data path, respectively media stream, which includes the generated correlation key and further information on the media stream.

This further information may be for example transport media information and optionally stream quality information. For example, in case RTP is used for media transport, the transport media information could include the source and destination IP address of the RTP stream, the source and destination UDP port of the RTP stream, the RTP header Synchronization source (SSRC) value and the RTP payload type. Furthermore, the processing unit 1004 may also generate information on the media stream quality that is included to the media stream report as stream quality information. This stream quality information could for example include timestamp information (e.g. start and/or end time of the media stream), an indication of RTP format violations (e.g. the number thereof), information on the protocol conformance (e.g. sequence errors and/or DSCP errors), and transport information (e.g. packet interval and jitter statistics, information on packet loss, information on duplicate packets, etc.), MOS values (e.g. per time-slice (e.g. every 5 seconds), minimum/average/maximum value for entire stream duration, etc.), and/or events (e.g. comfort noise, silence suppression, DTMF tones, codec changes, marker bits). The contents of the media stream reports may be configurable by an operator and may be adapted to customers' needs.

The media stream record may be further stored in a media stream report database using the database access unit 1007 of the media plane probe 403. Finally, the processing unit 1004 of the media plane probe 403 deregisters 1112 the media data path from the state table, e.g. by deleting the corresponding media stream record.

Steps 1110 to 1112 are performed for every media stream that is considered terminated by the media plane probe.

Optimizations may be used to speed up processing of entries in the state tables inside the signaling plane probe 401, the correlation unit 402 and the media plane probe 403. A simple list would be sufficient to implement the features as outlined above. Add, modify, delete and search operations on simple lists may however be too slow. These operations may be implemented utilizing more complex but faster data structures, e.g. hash tables or data structures heavily dependent on CPU and Operating System specific behavior and functionality. The Intel Thread Building Block (TBB) library for instance can be used to implement in-memory databases used for the state tables in the signaling plane probe 401, the correlation unit 402 and the media plane probe 403. The Intel Thread Building Block (TBB) library may also be used to aid implementation of the processing queues inside and in between the components outlined above.

Please note that in case the signaling plane probe 401 and the media plane probe 403 should perform passive non-intrusive monitoring of the signaling plane traffic, respectively

media plane traffic, a separate network interface card is employed for the transmission of correlation related messages (i.e. the network interface card(s) for monitoring the traffic are only employed for packet reception but not for packet transmission).

Please also note that in the procedures described above the detection unit 902, 1002 and the processing unit 904, 1004 may use the database access unit 907, 1007 to access the database/state table in the storage unit 903, 1003.

Application

The correlation mechanism for signaling plane and media plane of a service may be used in manifold applications. For example, the correlation mechanism is useful in small networks but is more important in larger scale networks where the various signaling and media components are decomposed and present on different, sometimes geographically split, network entities. This is the case in IP Multimedia Subsystem (IMS) or Next Generation Network (NGN) setups.

Fig. 12 shows a simplified network in which locations are indicated where correlation may be desired and can be implemented using the correlation mechanism according to one of the various embodiments described herein. Possible monitoring locations are for example (and not limited thereto):

- The Access Session Border Controller (SBC) network interfaces with end customers (shown of the left side of Fig. 12),
- a decomposed gateways system, e.g. to the PSTN, is shown as Media Gateway (MGW) and a Media Gateway Controller (MGC) – see In the top right section of Fig. 12, and
- an Interconnection SBC interfaces to one or more interconnection or transit partners (see the lower right side of Fig. 12.

It should be noted that the location of the monitoring probes for signaling plane and media plane may also be subject to requirements on the monitoring solution.

In some cases, signaling plane and media plane may originate and/or terminate at the same endpoint (device). In case of an end customer this endpoint most likely uses the same IP address on the signaling and media plane. These streams may be for example observed, if the signaling plane probes 401 and the media plane probes 403 are placed close to the end customer devices. The Access Session Border Controller may be considered to be close to the carrier internal network's "border" towards end customer devices and to therefore receive

EX1002
CISCO SYSTEMS, INC. / Page 1028 of 1453

traffic from the end customers on one side and transmits this traffic on the other side towards the carrier internal network. Most commonly these Session Border Controllers (SBC) are used to separate the devices outside the own trust domain from the inside network. Although the traffic is in one geographic location the SBC may use different IP addresses to load balance traffic. In this case a simple IP address based correlation mechanism not using the principles and ideas outlined herein would already fail whereas the correlation mechanism described herein would succeed. The signaling plane probes 401 and media plane probes 403 may be for example placed in a way that they observe the signaling streams and media streams respectively.

In the upper right corner of the diagram shown in Fig. 12, a decomposed gateway is shown which uses different physical entities as media and signaling components (MGC and MGW, respectively). In between those devices a third party protocol may be used to synchronize the devices. For the sake of a minimum size network diagram only one of each component types is shown but in real life scenarios multiple media components are controlled by one signaling component (as it is the case in IMS, NGN). The media components may be co-located in the same location with the signaling component or spread across the internal network of the carrier. In either case the correlation task is rather complex as it involves multiple IP addresses on different physical network links and thus may require multiple signaling plane probes 401 as well as media plane probes 403.

In a third exemplary scenario the correlation has to correlate signaling and media streams from different locations. A media plane probe 403 component on the internal side of the interconnection point (lower right corner of the diagram – Interconnection SBC) observes a media stream from the Access SBC (middle left). The corresponding signaling session is observed next to the aforementioned Access SBC by a separate signaling plane probe 401.

The location of the correlation unit 402 does not impact what signaling sessions or media streams can be correlated. The correlation unit 402 should have access to the signaling session reports and media stream reports of the signaling plane probes 401 and media plane probes 403 and can be implemented as distinct physical machine or co-located on an existing signaling plane probe 401 or media plane probe 403.

The terms probe and correlation unit used herein can be considered to refer to dedicated hardware, a software program or a combination thereof to implement the desired functionality of the respective probe, respectively, correlation unit. Accordingly, another embodiment of the invention relates to the implementation of the above described various embodiments using hardware and software. It is recognized that probes and correlation unit of the invention may be implemented by having computing devices (processors) execute a software

EX1002
CISCO SYSTEMS, INC. / Page 1029 of 1453

program that causes the desired functionality being executed. A computing device or processor may for example be general purpose processors, digital signal processors (DSP), application specific integrated circuits (ASIC), field programmable gate arrays (FPGA) or other programmable logic devices, etc. Some of the computing devices may store the software program internally.

The various embodiments of the invention may also be performed or embodied by a combination of computing devices and software programs providing the desired functionality stored on any kind of computer readable storage media, for example RAM, EPROM, EEPROM, flash memory, registers, hard disks, CD-ROM, DVD, etc.

It should be further noted that the individual features of the different embodiments of the invention may individually or in arbitrary combination be subject matter to another invention.

It would be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

EX1002
CISCO SYSTEMS, INC. / Page 1030 of 1453

CLAIMS

1. A method for correlating media streams and signaling sessions of services in a passive monitoring system of a packet-switched network, the method comprising:

a) generating at least one correlation key for each direction of a service based on the information of the signaling session of the respective service monitored at the signaling plane probe, wherein the correlation keys for a respective service are generated using a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the signaling plane probe and using information on the direction of the respective service,

b) storing, by the signaling plane probe, a signaling session report for each signaling session in a database, wherein each signaling session report comprises the at least two correlation keys generated for the respective directions of the service,

c) generating a correlation key for each media stream monitored by the media plane probe, wherein the correlation key is generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream,

d) storing, by the media plane probe, a media stream report for each media stream in a database, wherein each media stream report comprises at least the correlation key generated for the respective media, and

e) correlating the media streams and the signaling sessions based on the correlation keys comprised within media stream reports and signaling session reports.

2. The method according to claim 1, wherein the generation of the respective correlation keys for the respective media streams by the media plane probe is based on the media data path information of the respective media stream and the timestamp indicative of the point in time at which the respective media stream ended.

3. The method according to claim 1 or 2, wherein information on the direction of the respective service, based on which the correlation keys are generated by

EX1002
CISCO SYSTEMS, INC. / Page 1031 of 1453

signaling plane probe for a respective service, is information on one or more media data paths of media streams of the service learned from messages of the signaling session of the service.

4. The method according to one of claims 1 to 3, further comprising the steps of:

f) monitoring, by the signaling plane probe, signaling messages of the respective signaling sessions of the services, and

g) detecting, by the signaling plane probe, media streams belonging to each service associated to a respective monitored signaling session based on the signaling messages of the respective signaling sessions,

wherein the correlation keys for a respective one of the signaling sessions are generated based on information on the media data path of the media streams belonging to the service associated to the respective one of the signaling sessions and the timestamp indicative of the point in time at which the end of the respective signaling session has been detected by the signaling plane probe.

5. The method according to one of claims 1 to 4, wherein information on a media data path of a media stream is a destination IP address and port number of the media stream.

6. The method according to one of claims 1 to 5, wherein the timestamps used for the generation of the correlation keys by the signaling plane probe and the media plane probe are rounded before the generation of the correlation keys or have a granularity in the range of one to ten seconds.

7. The method according to one of claims 1 to 6, wherein the signaling plane probe generates for each direction of the service at least one correlation key using a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the signaling plane probe and being rounded to the next lower timestamp value according to a rounding interval, and at least another correlation key using the timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the signaling plane probe and being rounded to the next higher timestamp value according to the rounding interval.

8. The method according to one of claims 1 to 7, wherein the media plane probe generates for each media stream at least one correlation key using a timestamp indicative of the point in time at which the respective media ended and being rounded to the next lower timestamp value according to a rounding interval, and at least another correlation key using the timestamp indicative of the point in time at which the respective media stream ended and being rounded to the next higher timestamp value according to the rounding interval.

9. The method according to one of claims 1 to 8, wherein the correlation of the media streams and the signaling session of the respective services is performed by a correlation unit periodically or in response to a query.

10. A method for correlating media streams and signaling sessions of services, the method comprising the steps of:

a) correlating the media streams and the signaling sessions of one or more services based on the correlation keys comprised within media stream reports of the media streams and signaling session reports of the signaling sessions to thereby identify the media stream reports and signaling session report belonging to a respective one of said one or more services, wherein correlating the media streams and the signaling sessions comprises identifying one or more media streams of a respective service and the corresponding signaling session of the respective service based on the correlation keys contained in the media stream reports and signaling session reports, and

b) generating a service record for a respective one of said at least one service based on information contained in the media stream reports and information contained the signaling session report of said at least one service.

11. The method according to claim 10, wherein correlation keys provided in a respective signaling session report have been generated using a timestamp indicative of the point in time at which the end of the respective signaling session of the corresponding service has been detected and using information on the media streams of the service.

12. The method according to claim 10 or 11, wherein correlation key provided in a respective media stream report has been generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the media stream.

EX1002
CISCO SYSTEMS, INC. / Page 1033 of 1453

13. The method according to one of claims 10 to 12, wherein correlating the media streams and the signaling sessions of one or more services based on the correlation keys comprised within media stream reports of the media streams and signaling session reports of the signaling sessions comprises:

matching the respective correlation keys of the media stream reports of media streams are to the respective correlation keys of the signaling session reports, or vice versa,

wherein a match of the correlation keys of a one of the media stream reports and one of the signaling session reports yields the media stream of said one media stream report belonging to the same service to which the signaling session of said one signaling session report belongs.

14. The method according to one of claims 10 to 13, wherein the service report comprises information on the service and the quality information of the media streams of the service.

15. The method according to one of claims 10 to 13, wherein correlating the media streams and the signaling sessions of one or more services based on the correlation keys comprised within media stream reports of the media streams and signaling session reports of the signaling sessions comprises:

obtaining from a signaling session report correlation keys identifying the media streams belonging to the same service as the signaling session, and

identifying those media stream reports which include one of the correlation keys obtained from the signaling session report.

16. The method according to one of claims 10 to 13, wherein correlating the media streams and the signaling sessions of one or more services based on the correlation keys comprised within media stream reports of the media streams and signaling session reports of the signaling sessions comprises:

obtaining from a media stream report a correlation key identifying the media stream, and

identifying a signaling session report among the signaling session reports which includes the same correlation key obtained from the signaling session report.

EX1002
CISCO SYSTEMS, INC. / Page 1034 of 1453

17. The method according to one of claims 10 to 16, wherein steps a) and b) are performed by a correlation unit periodically for all signaling session reports and media stream reports generated within a configurable time interval, or in response to a request.

18. The method according to one of claims 10 to 17, further comprising steps a) to d) of claim 1 or the steps of the method according to one of claims 2 to 9.

19. A passive monitoring system for correlating media streams and signaling sessions of services in a packet-switched network, the passive monitoring system comprising:

a signaling plane probe for generating at least one correlation key for each direction of a service based on the information of the signaling session of the respective service monitored at the signaling plane probe, wherein the correlation keys for a respective service are generated using a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the signaling plane probe and using information on the direction of the respective service,

wherein the signaling plane probe is further adapted to store a signaling session report for each signaling session in a database, wherein each signaling session report comprises the at least two correlation keys generated for the respective directions of the service,

a media plane probe for generating a correlation key for each media stream monitored by the media plane probe, wherein the correlation key is generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream,

wherein the media plane probe is adapted to store a media stream report for each media stream in a database, wherein each media stream report comprises at least the correlation key generated for the respective media, and

a correlation unit for correlating the media streams and the signaling sessions based on the correlation keys comprised within media stream reports and signaling session reports.

20. A signaling plane probe comprising:

EX1002
CISCO SYSTEMS, INC. / Page 1035 of 1453

a network interface card for receiving packets of signaling sessions of multiple media services,

monitoring unit for monitoring the signaling sessions based on the packets of the signaling sessions received by the signaling plane probe to thereby obtain information on a respective one of the signaling sessions, wherein the monitoring unit is further adapted to detect the point in time at which a respective signaling session of the respective service terminates, and

a processing unit for generating at least one correlation key for each direction of a service based on a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected by the monitoring unit and based on information on the direction of the respective service,

wherein the monitoring unit is adapted to store a signaling session report for each signaling session in a database, wherein each signaling session report comprises at least two correlation keys generated for the respective directions of the service.

21. A media plane probe comprising:

a network interface card for receiving packets of media streams of multiple media services,

monitoring unit for monitoring the media streams based on the packets of the media streams received by the media plane probe to thereby obtain information on a media data path a respective one of the media streams, wherein the monitoring unit is further adapted to detect the point in time at which a respective media stream of the respective service terminates, and

a processing unit for generating a correlation key for each media stream monitored by the monitoring unit, wherein the correlation key is generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream,

wherein the monitoring unit is adapted to store a media stream report for each media stream in a database, wherein each media stream report comprises at least the correlation key generated for the respective media.

22. A correlation unit for correlating media streams and signaling sessions of services in a passive monitoring system of a packet-switched network, the correlation unit comprising:

a database access unit for accessing a database containing signaling session reports for signaling sessions of services and a database comprising media stream reports of media streams of the services, wherein the signaling session reports each contain at least one correlation key for each direction of a respective service, and the media stream reports each contain one correlation key indication the direction of the media stream,

a processing unit for correlating the media streams and the signaling sessions of the services based on the correlation keys comprised within media stream reports and signaling session reports to thereby identify the media stream reports and signaling session report belonging to a respective one of said one or more services, wherein the processing unit is adapted to identify one or more media streams of a respective service and the corresponding signaling session of the respective service based on the correlation keys contained in the media stream reports and signaling session reports, and

a service record generation unit for generating a service record for a respective one of said at least one service based on information contained in the media stream reports and information contained the signaling session report of said at least one service.

23. The correlation unit according to claim 22, further comprising means to perform the steps of the method according to one of claims 10 to 17.

24. A computer-readable medium storing instructions that, when executed by a processor of a signaling plane probe, cause the signaling plane probe:

to receive packets of signaling sessions of multiple media services,

to monitor the signaling sessions based on the packets of the signaling sessions received by the signaling plane probe to thereby obtain information on a respective one of the signaling sessions,

to detect the point in time at which a respective signaling session of the respective service terminates,

EX1002
CISCO SYSTEMS, INC. / Page 1037 of 1453

to generate at least one correlation key for each direction of a service based a timestamp indicative of the point in time at which the end of the respective signaling session of the respective service has been detected and based on information on the direction of the respective service, and

to store a signaling session report for each signaling session in a database, wherein each signaling session report comprises the at least two correlation keys generated for the respective directions of the service.

25. A computer-readable medium storing instructions that, when executed by a processor of a media plane probe, cause the media plane probe:

to receive packets of media streams of multiple media services,

to monitor the media streams based on the packets of the media streams received by the signaling plane probe to thereby obtain information on a media data path a respective one of the media streams,

to detect the point in time at which a respective media stream of the respective service terminates, and

to generate a correlation key for each media stream monitored by the monitoring unit, wherein the correlation key is generated using a timestamp indicative of the point in time at which the respective media stream has ended and using information on the media data path of the respective media stream,

to store a media stream report for each media stream in a database, wherein each media stream report contains at least the correlation key generated for the respective media.

26. A computer-readable medium storing instructions that, when executed by a correlation unit, cause the correlation unit to correlate media streams and signaling sessions of services in a passive monitoring system of a packet-switched network, by:

accessing a database containing signaling session reports for signaling sessions of services and a database containing media stream reports of media streams of the services, wherein the signaling session reports each contain at least one correlation key for each direction of a respective service, and the media stream reports each contain one correlation key indication the direction of the media stream,

EX1002
CISCO SYSTEMS, INC. / Page 1038 of 1453

correlating the media streams and the signaling sessions of the services based on the correlation keys comprised within media stream reports and signaling session reports to thereby identify the media stream reports and signaling session report belonging to a respective one of said one or more services,

identifying one or more media streams of a respective service and the corresponding signaling session of the respective service based on the correlation keys comprised in the media stream reports and signaling session reports, and

generating a service record for a respective one of said at least one service based on information contained in the media stream reports and information contained the signaling session report of said at least one service.

27. The computer-readable medium according to claim 26, further storing instruction that, when executed by the processor of the correlation unit, cause the correlation unit to perform the steps of the method according to one of claims 10 to 17.

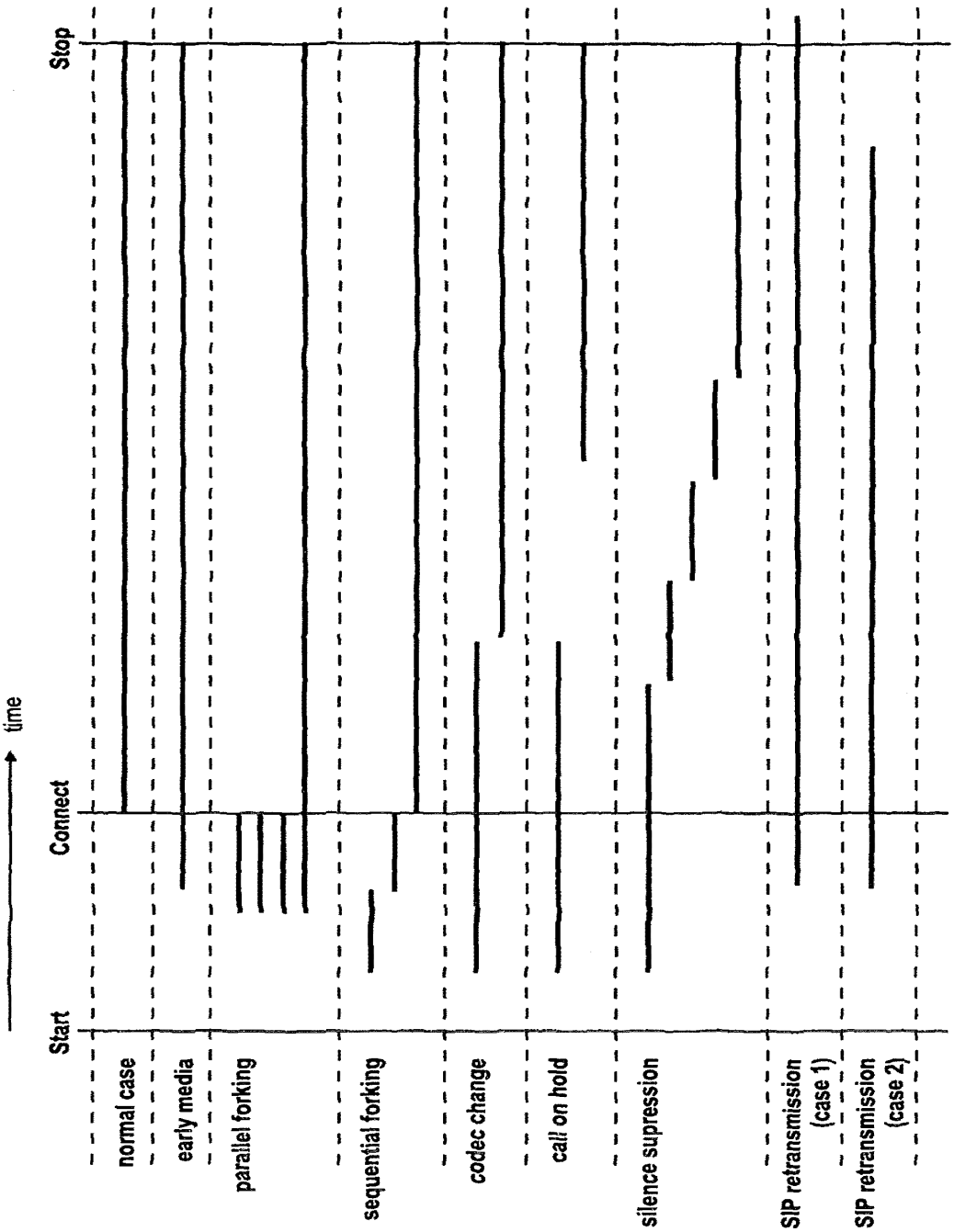


Fig. 1

BNSDOCID: <WO_____2012146265A1_I_>

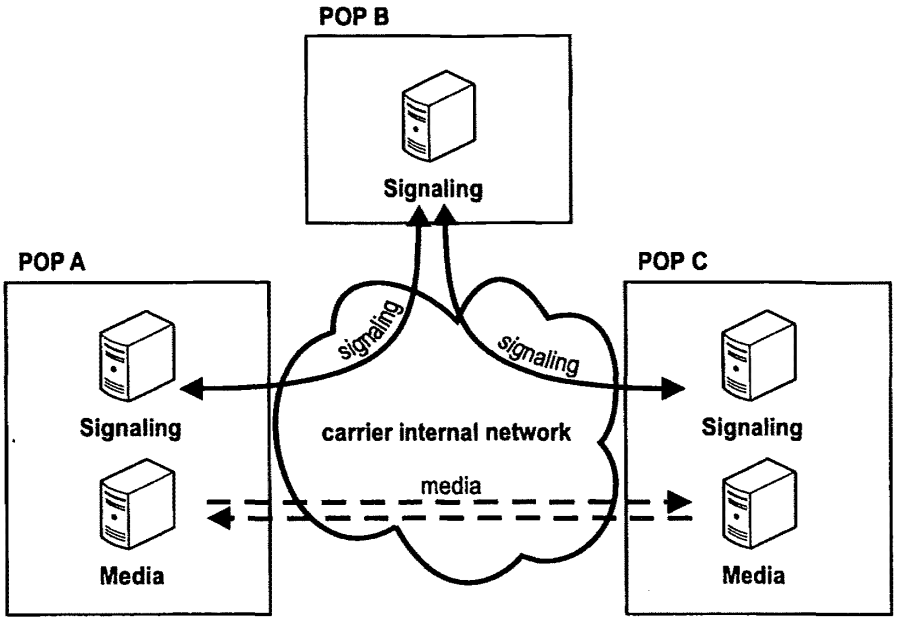

POP B
Signaling
POP A
POP C
signaling
signaling
Signaling
carrier internal network
Signaling
media
Media
Media

Fig. 2

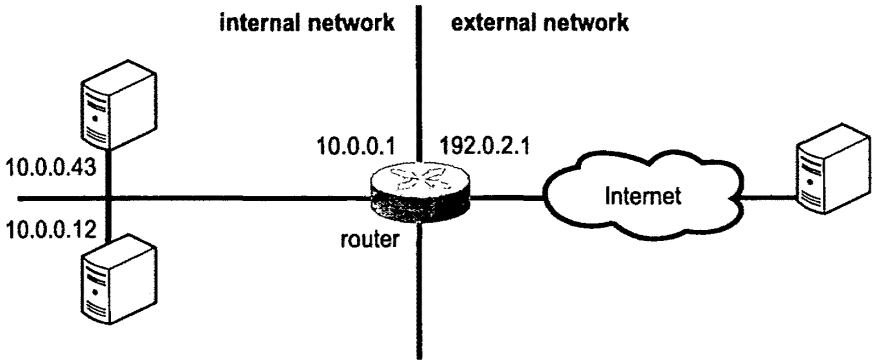

internal network
external network
10.0.0.1
192.0.2.1
10.0.0.43
10.0.0.12
router
Internet

Fig. 3

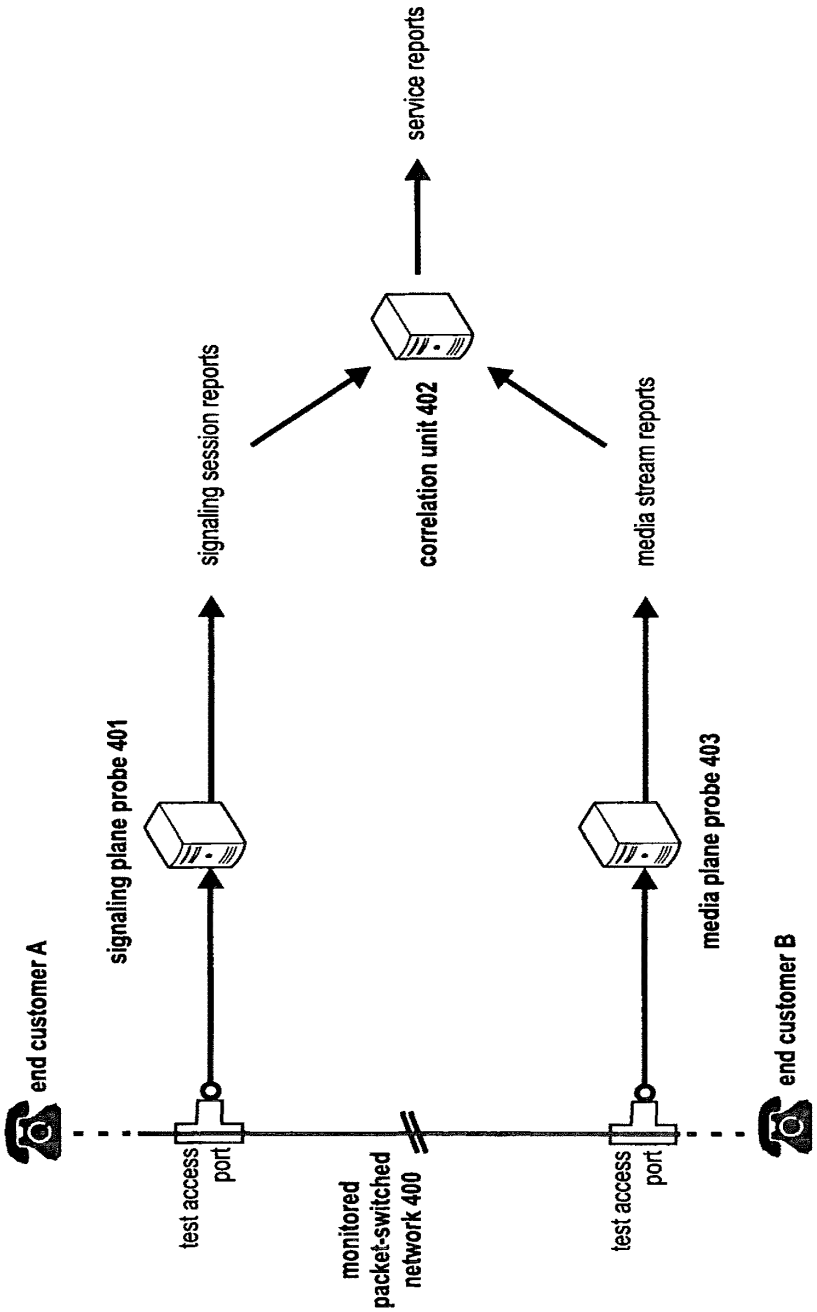

service reports
signaling session reports
correlation unit 402
media stream reports
signaling plane probe 401
media plane probe 403
end customer A
end customer B
test access port
test access port
monitored packet-switched network 400

Fig. 4

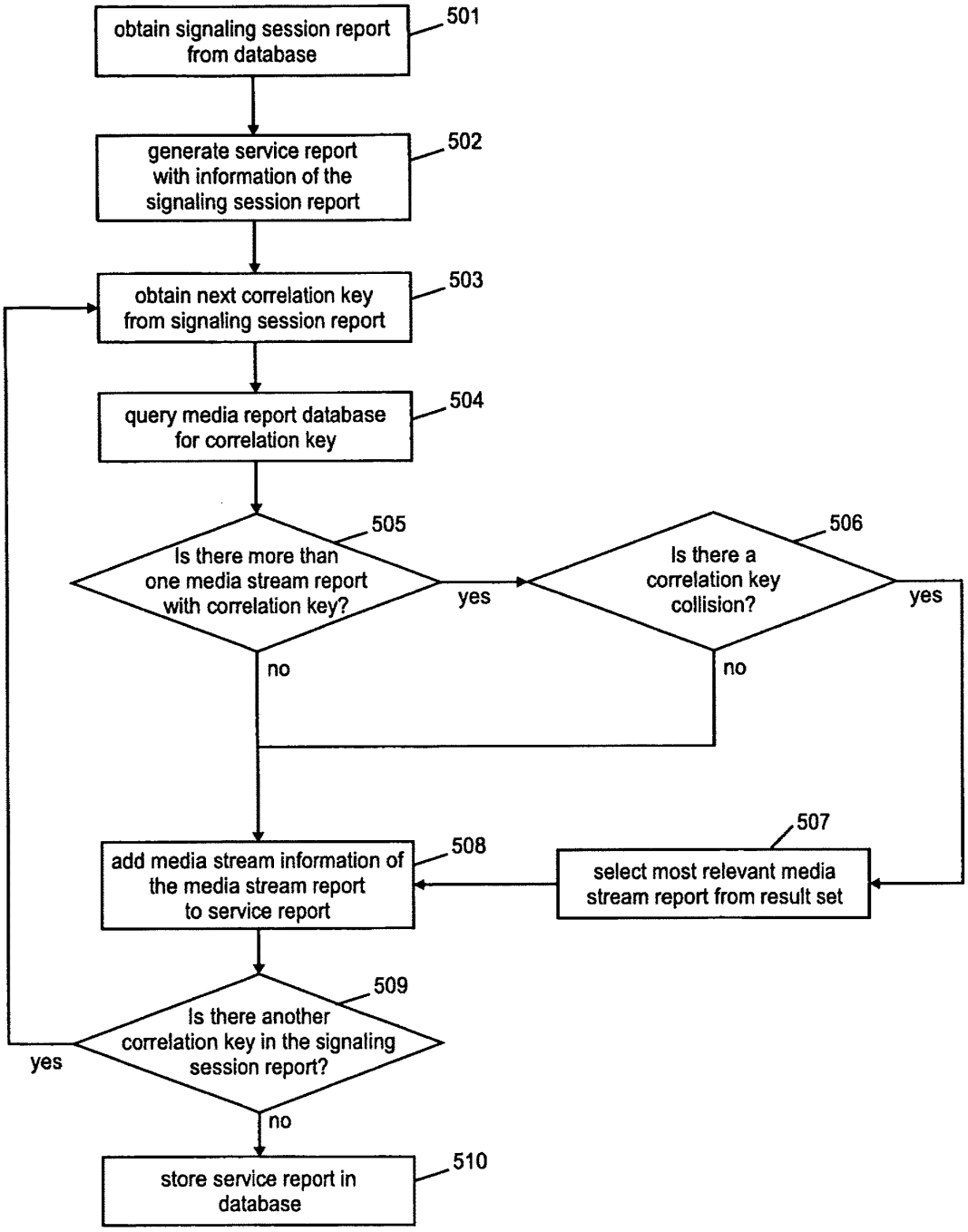


Fig. 5

BNSDOCID: <WO_____2012146265A1_I_>

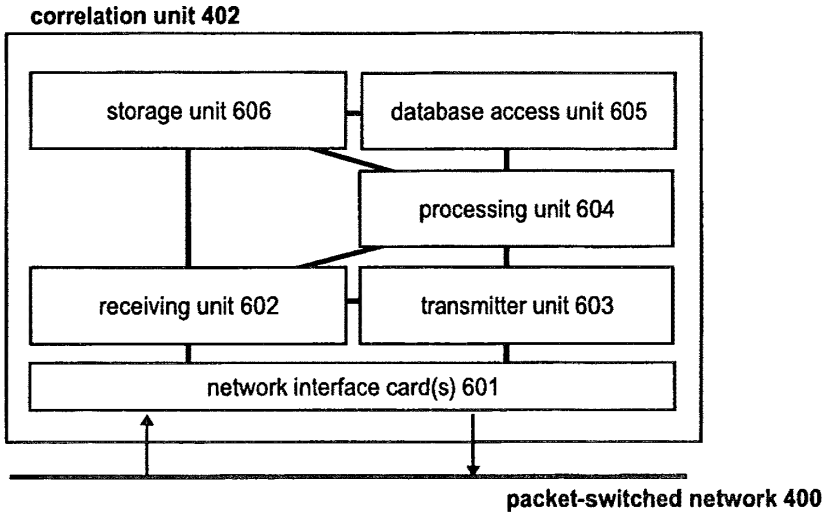
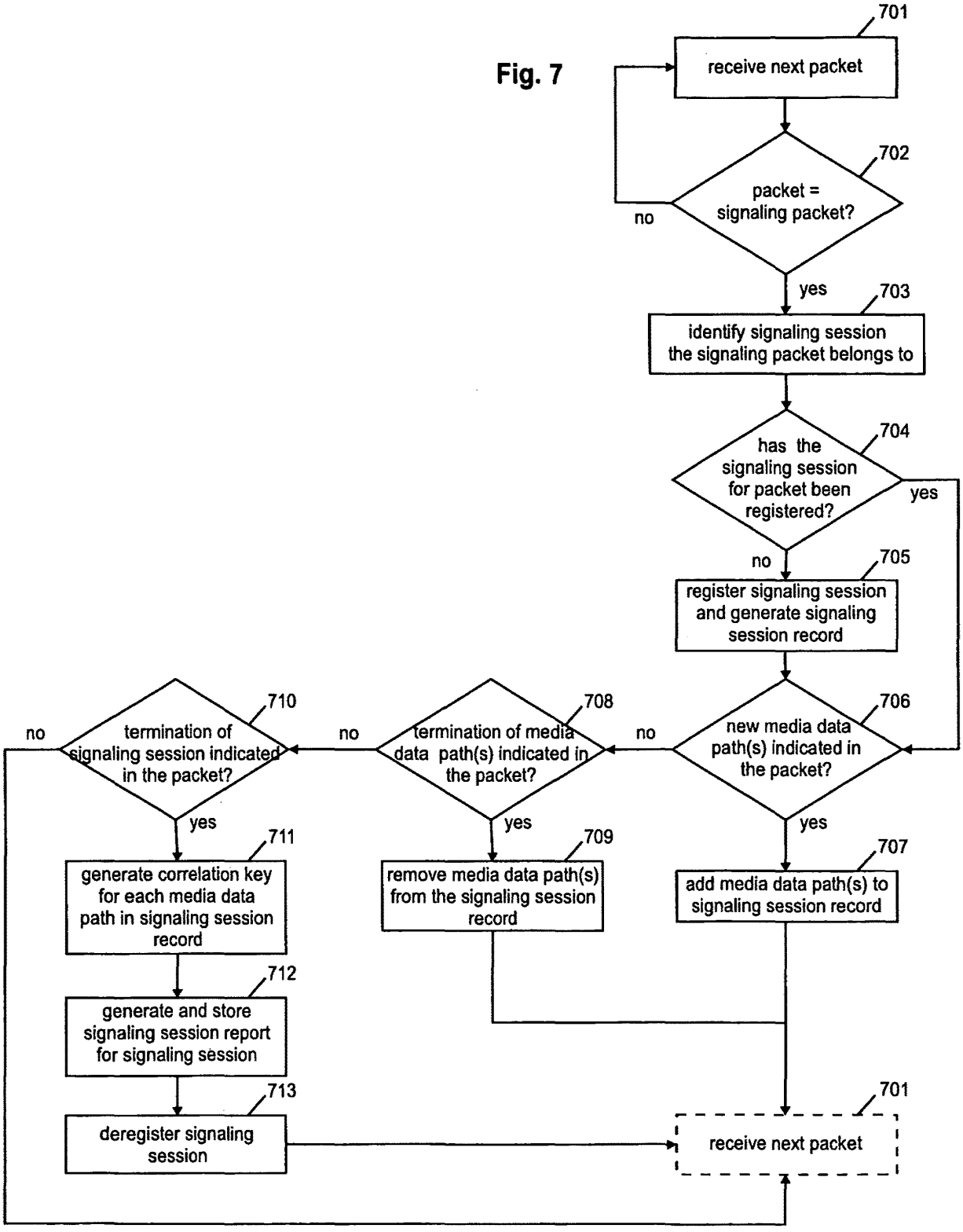

correlation unit 402
storage unit 606
database access unit 605
processing unit 604
receiving unit 602
transmitter unit 603
network interface card(s) 601
packet-switched network 400

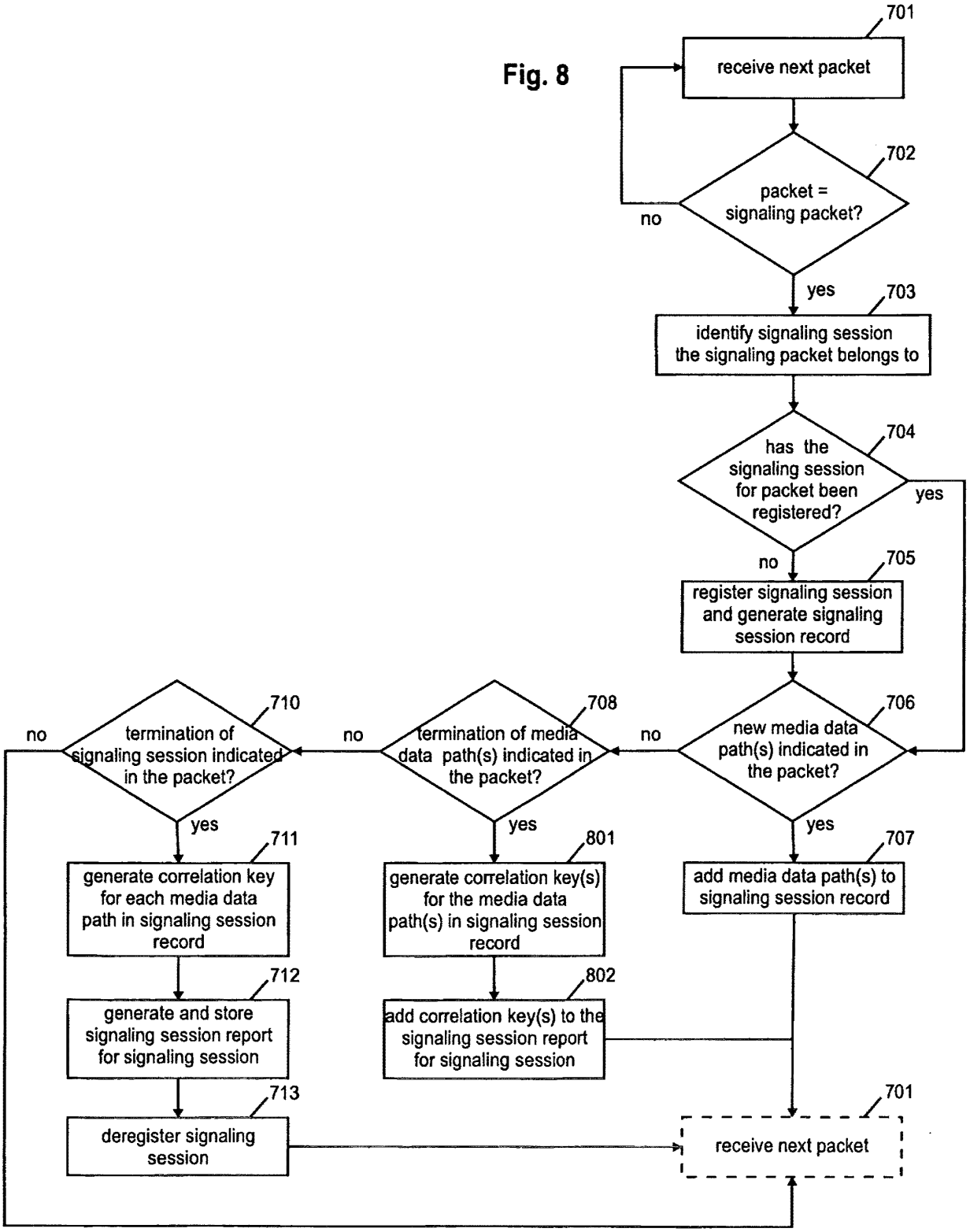
Fig. 6

Fig. 7



BNSDOCID: <WO_____2012146265A1_I_>

Fig. 8


701
receive next packet
702
packet = signaling packet?
no
yes
703
identify signaling session the signaling packet belongs to
704
has the signaling session for packet been registered?
yes
no
705
register signaling session and generate signaling session record
706
new media data path(s) indicated in the packet?
no
yes
707
add media data path(s) to signaling session record
708
termination of media data path(s) indicated in the packet?
no
yes
801
generate correlation key(s) for the media data path(s) in signaling session record
802
add correlation key(s) to the signaling session report for signaling session
710
termination of signaling session indicated in the packet?
no
yes
711
generate correlation key for each media data path in signaling session record
712
generate and store signaling session report for signaling session
713
deregister signaling session
701
receive next packet

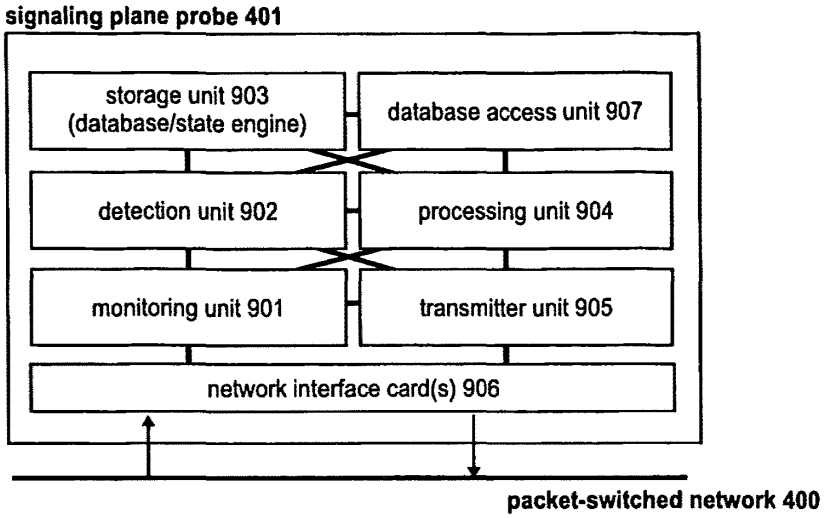

signaling plane probe 401
storage unit 903 (database/state engine)
database access unit 907
detection unit 902
processing unit 904
monitoring unit 901
transmitter unit 905
network interface card(s) 906
packet-switched network 400

Fig. 9

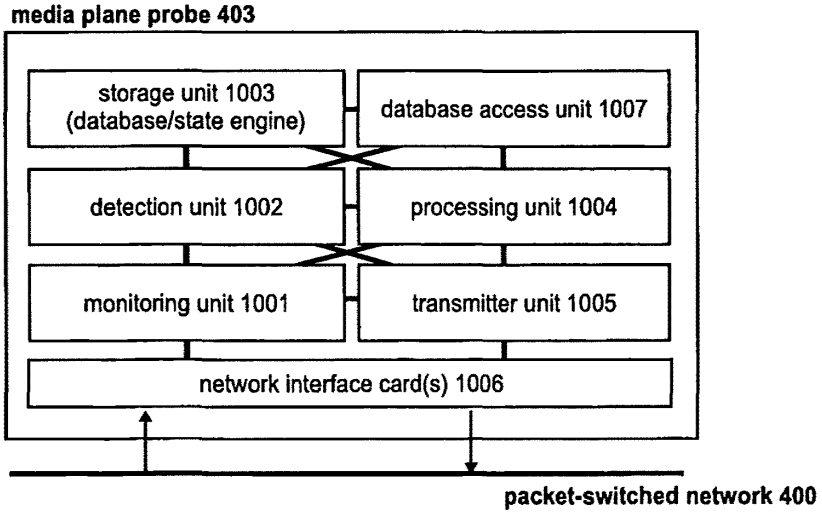

media plane probe 403
storage unit 1003 (database/state engine)
database access unit 1007
detection unit 1002
processing unit 1004
monitoring unit 1001
transmitter unit 1005
network interface card(s) 1006
packet-switched network 400

Fig. 10

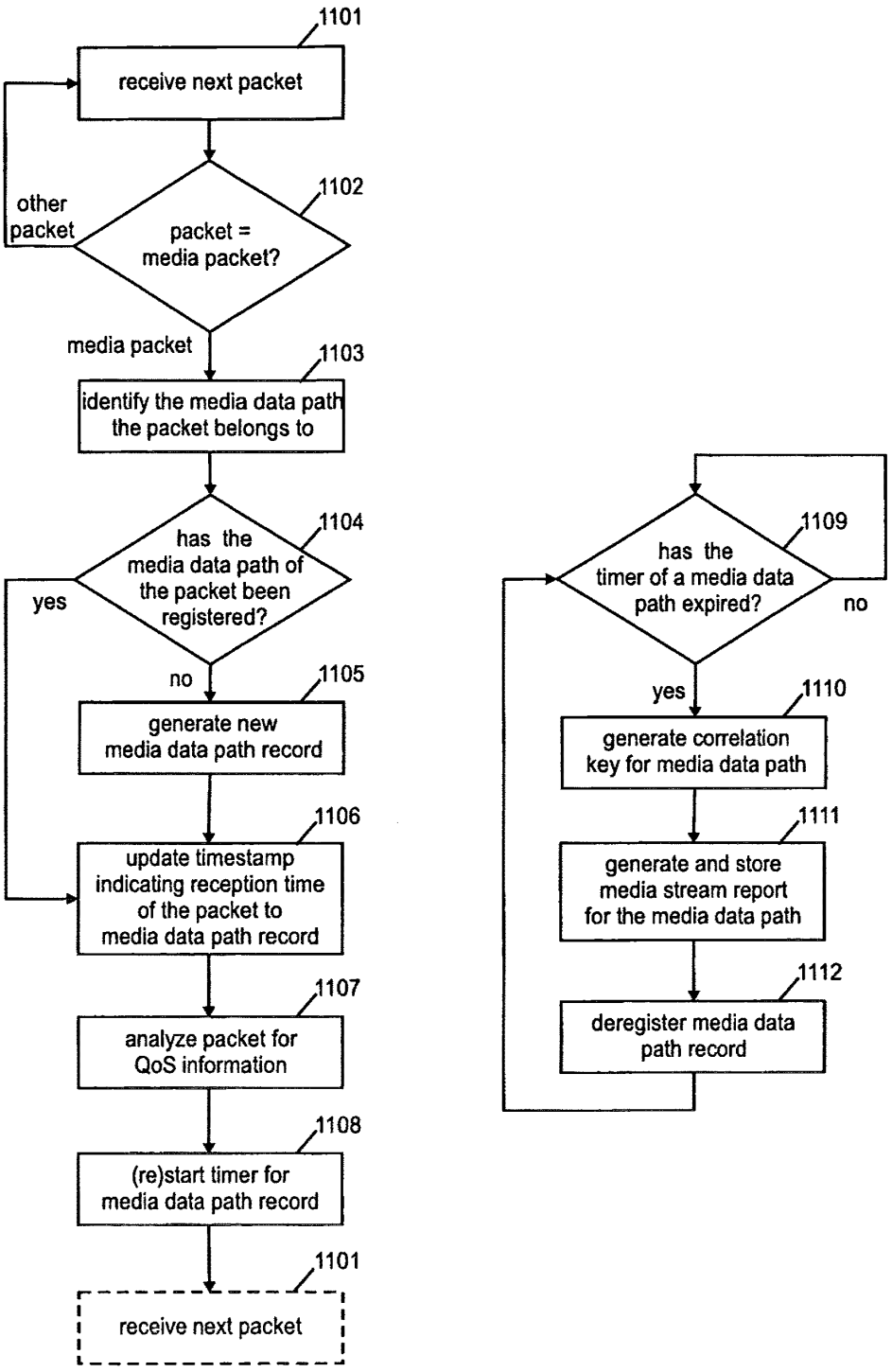


Fig. 11

BNSDOCID: <WO_____2012146265A1_I_>

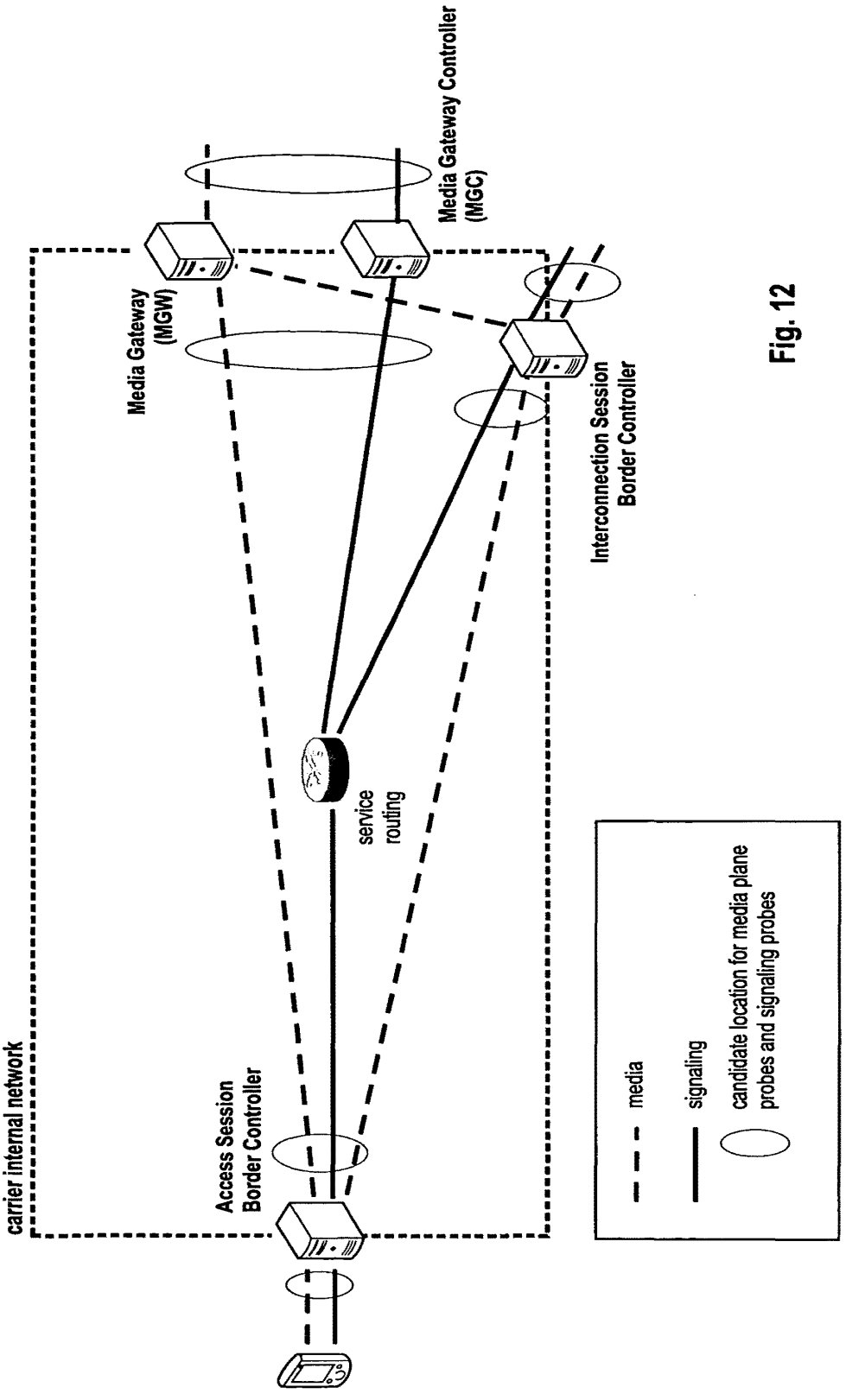

Media Gateway Controller (MGC)
Media Gateway (MGW)
Interconnection Session Border Controller
service routing
carrier internal network
Access Session Border Controller
media
signaling
candidate location for media plane probes and signaling probes

Fig. 12

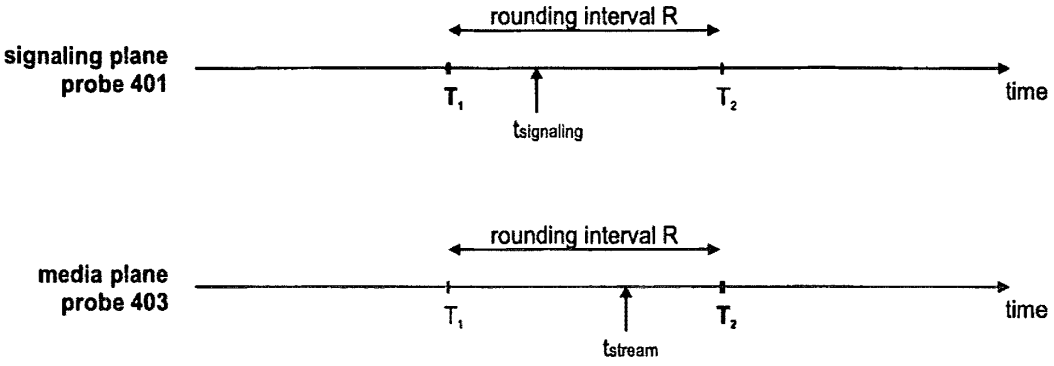

rounding interval R
signaling plane
probe 401
T1
tsignaling
T2
time
rounding interval R
media plane
probe 403
T1
tstream
T2
time

Fig. 13

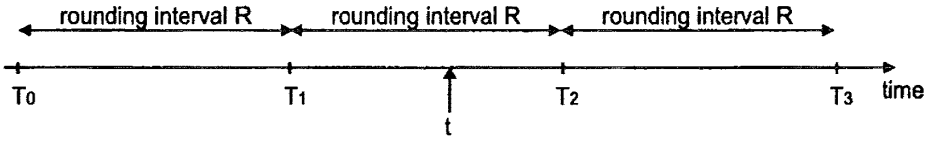

rounding interval R
rounding interval R
rounding interval R
T0
T1
t
T2
T3
time

Fig. 14

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/002145

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/24
ADD. H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, COMPENDEX, INSPEC, IBM-TDB, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ATSUSHI KOBAYASHI ET AL: "VoIP Measurement Architecture Using Data Mediation", 29 October 2009 (2009-10-29), IP OPERATIONS AND MANAGEMENT, SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 15 - 26, XP019133039, ISBN: 978-3-642-04967-5 page 18, line 5 - page 20, line 35	1-27
A	US 2008/151918 A1 (FOTI GEORGE [CA]) 26 June 2008 (2008-06-26) the whole document	1-27
A	WO 2010/106075 A1 (KONINKL KPN NV [NL]; TNO [NL]; STOKKING HANS MAARTEN [NL]; WALRAVEN FA) 23 September 2010 (2010-09-23) page 4, line 16 - page 8, line 26	1-27

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2012	17/01/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Aura Marcos, F

3

Form PCT/ISA/210 (second sheet) (April 2005)

BNSDOCID: <WO_____2012146265A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/002145

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008151918 A1	26-06-2008	US 2008151918 A1	26-06-2008
		WO 2008078209 A2	03-07-2008
WO 2010106075 A1	23-09-2010	EP 2409432 A1	25-01-2012
		KR 20110125674 A	21-11-2011
		WO 2010106075 A1	23-09-2010

Form PCT/ISA/210 (patent family annex) (April 2005)

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7215637	B1	2007-05-08	Ferguson et al.	
	2	8176561	B1	2012-05-08	Hurst et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010039579	A1	2001-11-08	TRCKA et al.	
	2	20030105976	A1	2003-06-05	Copeland	
	3	20030154399	A1	2003-08-14	Zuk et al.	
	4	20040250124	A1	2004-12-09	Chesla et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	5	20060053491	A1	2006-03-09	Khuti et al.	
	6	20060137009	A1	2006-06-22	Chesla	
	7	20070211644	A1	2007-09-13	Ottamalika et al.	
	8	20100095367	A1	2010-04-15	Narayanaswamy	
	9	20130117852	A1	2013-05-09	Stute	
	10	20140075510	A1	2014-03-13	Sonoda et al.	
	11	20150334125	A1	2015-11-19	BARTOS et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	2016 Apr 15 - (US) Notice of Allowance - App 14/855,374	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Bradley C. Wright/	Date (YYYY-MM-DD)	2016-04-21
Name/Print	Bradley C. Wright	Registration Number	38061

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	25560461
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Bradley C. Wright/Holly Parker
Filer Authorized By:	Bradley C. Wright
Attorney Docket Number:	007742.00059
Receipt Date:	21-APR-2016
Filing Date:	23-DEC-2015
Time Stamp:	15:28:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__INTVSUM_17820023.pdf	1978709 4d4e3f669e324489b5cc5e9526926f72d6499efd	no	50
Warnings:					
Information:					

2	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_17829699.pdf	1035410 23b8687c21901d6507a5e0e8fd7cf1591195fb6d	no	5
Warnings:					
Information:					
			Total Files Size (in bytes):	3014119	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/757,638	12/23/2015	David K. Ahn	007742.00059

CONFIRMATION NO. 9492

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

NEW OR REVISED PPD NOTICE

OC000000087452666

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 06/29/2017. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently http://pair.uspto.gov. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Data Management, Application Assistance Unit at (571) 272-4000, or (571) 272-4200, or 1-888-786-0101.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/757,638	12/23/2015	David K. Ahn	007742.00059	9492

22907 7590 04/12/2017

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
04/12/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@bannerwitcoff.com
GPD@bannerwitcoff.com

Office Action Summary	Application No. 14/757,638	Applicant(s) AHN ET AL.	
	Examiner JASON LEE	Art Unit 2438	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/23/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-25* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-25* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *12/23/15* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *03/30/2016, and 4/21/2016*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

4) ☐ Other: _____.

DETAILED ACTION

1. The present application, filed on 12/23/2015 which is after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. The original application is filed on 12/23/2015 with Claim 1-25. Therefore, claim 1-25 are pending and presented for examination.

Drawings

2. The drawings filed on 12/23/2015 are accepted.

Oath/Declaration

3. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 02/12/2016 has been accepted.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 03/30/2016, and 4/21/2016 have been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Claim Objections

5. Claims 24 and 25 are objected to because of the following informalities:

The Examiner notes the claim limitation of claim 24 recites “a **processor”** where “processor” can be as “hardware processor” or “software processor”**.** According to the instant Specification, there is no clear recitation the processor is "hardware processor". (See instant Specification page 40 lines 4-13 “Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types when executed by one or more

processors in a computer or other data-processing device. The computer-executable instructions may be stored on a computer-readable medium such as a hard disk, optical disk, removable storage media, solid-state memory, RAM, etc. As will be appreciated, the functionality of the program modules may be combined or distributed as desired. In addition, the functionality may be embodied in whole or in part in firmware or hardware equivalents, such as integrated circuits, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGA), and the like.”). Therefore, the phrase “processor” can be interpreted as “hardware processor” or “software processor” as to one of ordinary skill in the art to understand. Therefore, to make claim clearly recited, The Examiner suggests adding a "hardware" word in front of the "processor" in order to make the claim limitation clear. Similarly, claim 25 also has “processor”. Appropriate correction is suggested for claims 24 and 25.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1, 24 and 25 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

Claim 1 is directed to "receiving data indicating a plurality of network-threat indicators"; "configuring a plurality of packet-filtering rules"; “identify packets comprising

unencrypted data"; “identify packets comprising encrypted data” and “determine that the packets comprising encrypted data correspond to the one or more network-threat indicators. These steps are similar in concepts and ideas that have been identified as abstract by the courts as organizing human activity (e.g. filtering content (BASCOM)). The claim does not include additional elements that are sufficient to amount to significantly more than the judicial exception because the steps are simply a generic computer performing generic functions. Viewing the limitations as a combination does not add anything further than looking at the limitations individually. Claims 24 and 25 recite substantially similar to claim 1 except including "processor" and "memory" which are components to generic computer and do not include additional elements that are sufficient to amount to significantly more than the judicial exception. Therefore, independent claims 1, 24 and 25 fail to recite statutory subject matter under 35 U.S.C. 101. Accordingly, Claims 1, 24 and 25 fail to recite statutory subject matter and are rejected under 35 U.S.C. 101.

Analysis

The Examiner applies the framework as set forth by the Court in Mayo and reaffirmed by the Court in Alice for determining whether claim 1 is directed to patent-eligible subject matter.

Step one: Are the claims at issue directed to process, machine, manufacture or composition of matter?

Claim 1 recites a method with a packet-filtering system configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-

threat indicators; and configuring the plurality of packet-filtering rules by the packet-filtering system and, therefore, is a process, which is a statutory category of invention (*Step 1: YES*).

Step 2A: Are the claims at issue directed to law of nature, a natural phenomenon, or an abstract idea (judicial recognized exception)?

The claim is then analyzed to determine if the claim is directed to a judicial exception. The claim recites a packet-filtering system for steps of "receiving data indicating a plurality of network-threat indicators"; "configuring a plurality of packet-filtering rules"; “identify packets comprising unencrypted data"; “identify packets comprising encrypted data” and “determine that the packets comprising encrypted data correspond to the one or more network-threat indicators.”

The underlying invention merely employs abstract ideas of steps and are not necessary computer implemented and **could be** performed mentally, verbally or without a machine nor is any transformation apparent. The invention is a generic “receiving”, “configuring”, “identifying” and “determining” that does not need a computing device. Further, the claim does not recite an improvement to another technology or technical field, an improvement to the functioning of the computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment. These steps merely “receiving”, “configuring”, “identifying” and “determining” that are not necessary computer implemented and **could be** performed mentally, verbally or without a machine nor is any transformation apparent. Therefore, the claim is directed to an abstract idea. Therefore, it is reasonable to conclude based on the similarity of the idea

described in this claim to several abstract ideas that claim 1 is directed to an abstract idea (*Step 2A: Yes*).

Step 2B: Is there something else in the claim that ensures that they are directed to significantly more than a patent-ineligible concept?

Under Step 2B, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. As the Federal Circuit determined, these limitations do not amount to significantly more when “taken individually, [because they] recite generic computer, network and Internet components, none of which is inventive by itself.” (See Federal Circuit in BASCOM Global Internet v. AT&T Mobility LLC, 119 USPQ2d 1236 (Fed. Cir. 2016) (BASCOM).

The claim does not include additional elements beyond the abstract idea of receiving, configuring, identifying and determining. Therefore, the claim does not amount to more than the abstract idea itself. (E.g. Step 2B: No. based on the 2014 interim eligibility guidance) The claim amount to nothing significantly more than steps to apply the abstract idea of identify packets comprising unencrypted data"; “identify packets comprising encrypted data” and “determine that the packets comprising encrypted data correspond to the one or more network-threat indicators.” As such, there is no inventive concept sufficient to transform the claimed subject matter into a patent-eligible application. Accordingly, the claim is not patent eligible.

To overcome the above rejection and include additional elements that are sufficient to amount to significantly more than the judicial exception, the Examiner recommends amending claim 1 to include configuring the packet-filtering system to determine that a DNS (domain name system) query with network addresses in the packet header in the unencrypted data (as found in the Specification, page 6). These amendments would add unconventional steps that confine the claim to a particular useful application.

Claim Rejections - 35 USC § 112

8. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1, 8, 24 and 25 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

10. Independent claim 1 recites: “identify packets comprising unencrypted data; identify packets comprising encrypted data; and determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, that the packets comprising **encrypted data** correspond to the one or more network-threat indicators” (See claim listing page 42 lines 8-13). There is a lack antecedent basis error for the later recited “encrypted data”. Therefore, claim 1 is rendered unclear and is rejected under 35 U.S.C 112(b). Similarly, claims 24 and 25

have same errors. Thus, Claim 24 and 25 are unclear and rejected under 35 U.S.C 112(b).

11. Claim 8 recites “one or more network addresses for which encrypted communications should be established via the proxy system, and one or more network addresses for which encrypted communications should not be established via the proxy system; and…. for which encrypted communications should be established via the proxy system” (See claim listing page 44 lines 5-13). The phrase of “should be” is unclear because “should be” give the reader a certain uncertainty whether the communications have been done. Therefore, claim 8 renders unclear and rejected under 35 U.S.C 112(b).

To overcome, the Examiner suggests amend the phrase of "should be “to "are to be" for clarity.

12. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person

> having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 1-13, 16-23, 24 and 25 are rejected under 35 U.S.C. 103 as being unpatentable over Spies et al (U.S. Patent Publication US 2005/0138353 A1; hereafter "Spies") in view of Sorensen et al (U.S. Patent Publication US 2012/0023576 A1; hereafter "Sorensen").

As for claims 1, 24 and 25:

Spies discloses an identity-based-encryption (IBE) techniques for directing data (message) and applying cryptography for managing threat detection for encrypted communication. The IBE technique/scheme can be implemented in an engine or system. In one of the embodiment the IBE is an email system with the IBE technique/scheme. The IBE technique/scheme including steps of receiving a message (i.e. email) based on the rules (See Spies [0008] [0015], FIG 3 element 44 "message processing" [0143] with FIG 8 element 90 and 94, FIG 10, element 122).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to implement Spies' technique for claimed limitation of **a method comprising: receiving, by a packet-filtering system configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators;** (See Spies FIG 6 , FIG 10, FIG 11 element 132, 138 "filtering process") **and configuring, by the packet-filtering system, the plurality of packet-filtering rules to cause the packet-filtering system to:** (See Spies [0143] for "a system administrator may direct the message processing applications 32 to reject all incoming email from a particular sending address. As another example, the system

administrator may instruct the message processing application 32 to require that all message sent to a particular destination address or containing particular types of content in the attachments 116 or body 118 be encrypted using IBE. Policies 122 may include policies on how to detect and treat viruses, policies related to blocking spam, security or encryption enforcement policies, policies related to content filtering, etc. These policy rules 122 determine what types of processed messages are produced during message processing...the message is to be edited or archived, which messages are to be encrypted") **identify packets comprising unencrypted data; identify packets comprising encrypted data;** (See Spies [0143] FIG 12 element 146 "receive IBE-encrypted message") **and determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, that the packets comprising encrypted data correspond to the one or more network-threat indicators.** (See Spies [0106] embodiment of a particular content or message send to a particular domain"; [0114] embodiment of a domain name that identifies the service on which the IBE located)

The Examiner's note: the claimed "network –threat indicator" can be "domain names (e.g., fully qualified domain names (FQDNs)), URIs, network addresses, or the like" (See instant Specification page 6 lines 3-4). Thus, Spies' IBE disclosure of the embodiments with above (e.g. network addresses or domain name) read into the claimed limitations.

Spies does not explicitly disclose the "indicator" as claimed. However, Sorensen

discloses the ”indicator” (See Sorensen [0073] “A [further] indicator that may be implemented at block 310 or any other process may be whether the user account has an exception to a security policy.in certain embodiments, an indicator may consider whether a recipient address of a targeted communication meets certain criteria, such as being associated with a webmail account and/or appears to be personal address of a user associated with the user account....Further indicators may include factors that suggest suspicious communication activity, either through an intranet or the internet”) Sorensen, like Spies, is in the same field of endeavor of application with detection of secure threat in the network, discloses the “indicator” (e.g. address in email) associated with the encrypted communication with security policy.

Therefore, it would have been obvious for one of the ordinary skill in the art before the effective filing date of the claimed invention to modify the invention of Spies to include the teaching of Sorensen with threat indicator for closely monitor the risk for disclosure of information (e.g. data/message) (See Sorensen [0073])

Claims 24 and 25 recite substantially similar limitations to claim 1, mutatis mutandis, the subject matter of claims 24 and 25 which are therefore also considered to be taught by the combination of Spies and Sorensen as above.

As for claim 2:

The combination of Spies and Sorensen discloses **the method of claim 1, wherein: the one or more network-threat indicators comprise a domain name; the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query; and the**

configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the at least one of the DNS query or the reply to the DNS query comprises the domain name. (See Spies [0091], [0166])

As for claim 3:

The combination of Spies and Sorensen discloses **the method of claim 2, wherein: the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.** (See Spies [0143] "content filtering and encrypted using IBE policy) and [0084-0085])

As for claim 4:

The combination of Spies and Sorensen discloses **the method of claim 2, wherein: the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the at least one of the DNS query or the reply to the DNS query; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.** (See Spies [0084-0085] and [0101-0102])

As for claim 5:

The combination of Spies and Sorensen discloses **the method of claim 4, wherein: the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify one or more packets comprising the request.** (See Spies [0082-0083] "web browser" suggests the web proxy limitation and [0148-0150])

As for claim 6:

The combination of Spies and Sorensen discloses **the method of claim 1, wherein: one or more packets of the packets comprising unencrypted data comprise data configured to establish an encrypted communication session between a first host and a second host; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route the one or more of the packets to a proxy system.** (See Spies [0137] gateway 48 work as a proxy for recipient. And [0102] reroute the message)

As for claim 7:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the one or more network-threat indicators comprise a domain name; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route the one or more of the packets to the proxy**

system based on a determination that at least one of the first host or the second host corresponds to the domain name. (See Spies [0101-0102])

As for claim 8:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the plurality of packet-filtering rules indicate: one or more network addresses for which encrypted communications should be established via the proxy system, and one or more network addresses for which encrypted communications should not be established via the proxy system; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route the one or more of the packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications should be established via the proxy system.** (See Spies [0082-0085], [0101-0102] and [0148-0150])

As for claim 9:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the packet-filtering system comprises: one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and one or more interfaces interfacing the packet-filtering system with the proxy system; and the configuring the packet-filtering system to route the one or more of the packets to the proxy system comprises configuring the packet-filtering system to redirect packets received via the one or**

more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system. (See Spies [0012], [0091] and [0131])

As for claim 10:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the packet-filtering system comprises: one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and one or more interfaces interfacing the packet-filtering system with the proxy system; and the configuring the packet-filtering system to route the one or more of the packets to the proxy system comprises configuring the packet-filtering system to forward copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.** (See Spies [0056], [0091], [0106], [0122] and [0132])

As for claims 11 and 12:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to: identify, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and identify,**

via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data. (See Spies [0105], [0141]; Sorensen [0064] also discloses identifying information with address relating to the third party entity with DNS address)

Claim 12 recites "**the method of claim 11, wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data**" is therefore also considered to be taught by the combination of Spies and Sorensen as above.

As for claim 13:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to, responsive to determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of: drop the one or more packets generated by the proxy system; log the one or more packets generated by the proxy system; drop one or more other packets generated by the proxy system; log one or more other packets generated by the proxy system; drop one or more other packets of the packets comprising encrypted data; or log one or more other packets of the**

packets comprising encrypted data. (See Sorensen [0048] for rule of authorize access and log into specific device)

Examiner supplies the same rationale for the combination of the references as in claim 1 above.

As for claim 16:

The combination of Spies and Sorensen discloses **the method of claim 6, wherein: the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.** (See Spies [0082-0084] and [0089]) Examiner's note: Spies discloses "a content filter for a web browser may be used to prevent access to web pages containing undesirable content in the environment such as in the Internet"; therefore, Spies suggests the claimed limitation of ICAP protocol as claimed above.

As for claim 17:

The combination of Spies and Sorensen discloses **the method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the method comprising configuring the plurality of packet-filtering rules to cause the packet-filtering system to at least one of drop or log packets other than the packets comprising encrypted data based on a**

determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host. (See Spies [0015], [0056] and [0083-0084])

As for claim 18, 19, 20 and 21:

The combination of Spies and Sorensen discloses **the method of claim 1, wherein the one or more network-threat indicators comprise a domain name; the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine that the one or more handshake messages comprise the domain name.** (See Spies [0043] "information may be conveyed securely over a secure communications path such as a communications path that uses the secure sockets layer protocol (SSL) or other suitable secure protocol (e.g., TLS), a communications path may be trusted because it is under the control of a trusted party (e.g., because the communications path is physically under the control of a trusted party), and information may be conveyed securely by encrypting the information (e.g., in a message) before sending it over an insecure (or secure) link.') Examiner's notes: Spies discloses using secured protocol such as SSL, TLS for packet communications, therefore, Spies suggests establish encrypted communications session between client and server and the handshake messages in the domain name.

Claim 19, 20 and 21 all recite similar limitations such as handshake message and encrypted data, are therefore also considered to be taught by the combination of Spies and Sorensen as above.

As for claim 22:

The combination of Spies and Sorensen discloses **the method of claim 21, wherein: the one or more network addresses comprise a network address of the server and a network address of a web proxy; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to: identify one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and determine that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.** (See Spies [0143] "content filtering and encrypted using IBE policy), [0084-0085] and [0101-0102])

As for claim 23:

The combination of Spies and Sorensen discloses **the method of claim 1, wherein: the packets comprising unencrypted data comprise a certificate message for an encrypted communication session; and the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to at least one of drop or log one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one**

of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules. (See Spies [0042-0044] a user may provide credentials in the form of a pre-established user name and password. Certificate authorities may create digital certificates that help to verify the identities of certain parties. Digital signatures (e.g., signatures from a certificate authority or other entity that use PKE private keys and that can be verified using matching PKE public keys) may be used to ensure that a message or other signed information is associated with a particular party."), and [0083-0084])

15. Claims 14 and 15 are rejected under 35 U.S.C. 103 as being unpatentable over Spies and Sorensen as applied to claim 13 above, further in view of Bomer et al (US 2004/0199629 A1), hereinafter Bomer.

As for claim 14:

The combination of Spies and Sorensen discloses **the method of claim 13** as above, neither Spies nor Sorensen discloses "**wherein the determining comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the**

plurality of packet-filtering rules." However, Bomer discloses the claimed limitations (See Bomer [0026] "client 302 sends all HTTP requests to the configured proxy server rather than directly to an IP address associated with a URL (Uniform Resource Locator), or more generally, a URI (Uniform Resource Locator), in the HTTP requests after a DNS (Domain Name System) lookup operation. After receiving an HTTP request; an HTTP proxy server would forward the HTTP request in an appropriate manner after performing some type of processing. In the example shown in FIG. 3, proxy server 310 incorporates proxy-based debugging utility 312, which comprises trace unit 314 that allows message traffic to be traced to a log file and request filtering unit 316 that allows request messages to be filtered with reference to configurable filtering rules.")

Bomer, like Spies and Sorensen, is in the same field of endeavor of application with proxy communication in the network, discloses the URI with proxy based application with filtering rules.

Therefore, it would have been obvious for one of the ordinary skill in the art before the effective filing date of the claimed invention to modify the modified-invention of Spies to include the teaching of Bomer with URI for further identifying the threat detection.

As for claim 15:

The combination of Spies and Sorensen discloses **the method of claim 13** as above, **wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI)" meeting a threshold size specified by the plurality of packet-filtering rules.** (See Sorensen [0044], [0050], [0060] and [0074-75] for threshold)

Neither Spies nor Sorensen discloses **"a uniform resource identifier (URI)"** as claimed. However, Bomer discloses the claimed limitations (See Bomer [0026] "client 302 sends all HTTP requests to the configured proxy server rather than directly to an IP address associated with a URL (Uniform Resource Locator), or more generally, a URI (Uniform Resource Locator), in the HTTP requests after a DNS (Domain Name System) lookup operation. After receiving an HTTP request; an HTTP proxy server would forward the HTTP request in an appropriate manner after performing some type of processing. In the example shown in FIG. 3, proxy server 310 incorporates proxy-based debugging utility 312, which comprises trace unit 314 that allows message traffic to be traced to a log file and request filtering unit 316 that allows request messages to be filtered with reference to configurable filtering rules.")

Bomer, like Spies and Sorensen, is in the same field of endeavor of application with proxy communication in the network, discloses the URI with proxy based application with filtering rules.

Therefore, it would have been obvious for one of the ordinary skill in the art before the effective filing date of the claimed invention to modify the modified-invention of Spies to include the teaching of Bomer with URI for further identifying the threat detection with threshold specified with the rules.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9 AM to 5 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JASON LEE/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/757,638	Applicant(s)/Patent Under Reexamination AHN ET AL.	
	Examiner JASON LEE	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2005/0138353 A1	06-2005	Spies, Terence	H04L63/0442	713/153
*	B	US-2012/0023576 A1	01-2012	Sorensen; Amanda	G06F21/577	726/22
*	C	US-2004/0199629 A1	10-2004	Bomer, Staton Thomas	G06F11/362	709/224
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9492

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/757,638	12/23/2015 RULE	713	2438	007742.00059

APPLICANTS

Centripetal Networks, Inc., Herndon, VA;

INVENTORS

David K. Ahn, Winston-Salem, NC;
Sean Moore, Hollis, NH;
Douglas M. DiSabello, Leesburg, VA;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /JASON T LEE/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		NC	13	25	3

ADDRESS

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051
UNITED STATES

TITLE

Rule-based network-threat detection for encrypted communications

FILING FEE RECEIVED		
1305	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.T.L/	1	7215637	B1	2007-05-08	Ferguson et al.	
/J.T.L/	2	8176561	B1	2012-05-08	Hurst et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.T.L/	1	20010039579	A1	2001-11-08	TRCKA et al.	
/J.T.L/	2	20030105976	A1	2003-06-05	Copeland	
/J.T.L/	3	20030154399	A1	2003-08-14	Zuk et al.	
/J.T.L/	4	20040250124	A1	2004-12-09	Chesla et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	5	20060053491	A1	2006-03-09	Khuti et al.		
/J.T.L/	6	20060137009	A1	2006-06-22	Chesla		
/J.T.L/	7	20070211644	A1	2007-09-13	Ottamalika et al.		
/J.T.L/	8	20100095367	A1	2010-04-15	Narayanaswamy		
/J.T.L/	9	20130117852	A1	2013-05-09	Stute		
/J.T.L/	10	20140075510	A1	2014-03-13	Sonoda et al.		
/J.T.L/	11	20150334125	A1	2015-11-19	BARTOS et al.		

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
/J.T.L/	1	2016 Apr 15 - (US) Notice of Allowance - App 14/855,374	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/JASON T LEE/	Date Considered	03/08/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Bradley C. Wright/	Date (YYYY-MM-DD)	2016-04-21
Name/Print	Bradley C. Wright	Registration Number	38061

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /. m ./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" ' ' ' '

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.T.L/	1	6226372		2001-05-01	Beebe et al.	
/J.T.L/	2	7721084		2010-05-18	Salminen et al.	
/J.T.L/	3	7684400		2010-03-23	Govindarajan et al.	
/J.T.L/	4	7539186		2009-05-26	Aerrabotu et al.	
/J.T.L/	5	7710885		2010-05-04	Ilnicki et al.	
/J.T.L/	6	8856926		2014-10-07	Narayanaswamy et al.	
/J.T.L/	7	6611875		2003-08-26	Chopra et al.	
/J.T.L/	8	8806638		2014-08-12	Mani	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	9	8004994		2011-08-23	Darisi et al.	
/J.T.L/	10	6098172		2000-08-01	Coss et al.	
/J.T.L/	11	7331061	B1	2008-02-12	Ramsey et al.	
/J.T.L/	12	7299353	B2	2007-11-20	Le Pennec et al.	
/J.T.L/	13	7227842	B1	2007-06-05	Ji et al.	
/J.T.L/	14	7107613	B1	2006-09-12	Chen et al.	
/J.T.L/	15	7263099	B1	2007-08-28	Woo et al.	
/J.T.L/	16	7237267	B2	2007-06-26	Rayes et al.	
/J.T.L/	17	7089581	B1	2006-08-08	Nagai et al.	
/J.T.L/	18	6662235	B1	2003-12-09	Callis et al.	
/J.T.L/	19	6484261	B1	2002-11-19	Wiegel	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	20	8042167	B2	2011-10-18	Fulp et al.	
/J.T.L/	21	8037517	B2	2011-10-11	Fulp et al.	
/J.T.L/	22	7954143	B2	2011-05-31	Aaron	
/J.T.L/	23	8495725	B2	2013-07-23	Ahn	
/J.T.L/	24	8935785	B2	2015-01-13	Pandrangi	
/J.T.L/	25	8726379	B1	2014-05-13	Stiansen et al.	
/J.T.L/	26	8306994	B2	2012-11-06	Kenworthy	
/J.T.L/	27	7818794	B2	2010-10-19	Wittman	
/J.T.L/	28	7478429	B2	2009-01-13	Lyon	
/J.T.L/	29	6317837	B1	2001-11-13	Kenworthy	
/J.T.L/	30	9124552	B2	2015-09-01	Moore	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	31	9160713	B2	2015-10-13	Moore	
/J.T.L/	32	9094445	B2	2015-07-28	Moore et al.	
/J.T.L/	33	9137205	B2	2015-09-15	Rogers et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.T.L/	1	20030123456	A1	2003-07-03	Denz et al.	
/J.T.L/	2	20070083924	A1	2007-04-12	Lu	
/J.T.L/	3	20060195896		2006-08-31	Fulp et al.	
/J.T.L/	4	20060248580		2006-11-02	Fulp et al.	
/J.T.L/	5	20060048142		2006-03-02	Roese et al.	
/J.T.L/	6	20100011434		2010-01-14	Kay	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	7	20120113987	A1	2012-05-10	Riddoch et al.		
/J.T.L/	8	20110270956	A1	2011-11-03	McDysan et al.		
/J.T.L/	9	20100211678	A1	2010-08-19	McDysan et al.		
/J.T.L/	10	20050117576		2005-06-02	McDysan et al.		
/J.T.L/	11	20040151155	A1	2004-08-05	Jouppi		
/J.T.L/	12	20030212900	A1	2003-11-13	Liu et al.		
/J.T.L/	13	20030188192	A1	2003-10-02	Tang et al.		
/J.T.L/	14	20120264443	A1	2012-10-18	Ng et al.		
/J.T.L/	15	20130059527	A1	2013-03-07	HASESAKA et al.		
/J.T.L/	16	20010039624		2001-11-08	Kellum		
/J.T.L/	17	20030035370	A1	2003-02-20	Brustoloni, Jose		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	18	20030142681		2003-07-31	Chen et al.	
/J.T.L/	19	20030145225		2003-07-31	Bruton et al.	
/J.T.L/	20	20050138204		2005-06-23	Iyer et al.	
/J.T.L/	21	20050141537		2005-06-30	Kumar et al.	
/J.T.L/	22	20060212572		2006-09-21	Afek et al.	
/J.T.L/	23	20080072307		2008-03-20	Maes	
/J.T.L/	24	20100082811		2010-04-01	Van Der Merwe et al.	
/J.T.L/	25	20100296441		2010-11-25	Barkan	
/J.T.L/	26	20110088092		2011-04-14	Nguyen et al.	
/J.T.L/	27	20080005795	A1	2008-01-03	Acharya et al.	
/J.T.L/	28	20090172800	A1	2009-07-02	WOOL	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L./	29	20030097590	A1	2003-05-22	Syvanne	
/J.T.L./	30	20090328219	A1	2009-12-31	Narayanaswamy	
/J.T.L./	31	20120240135	A1	2012-09-20	Risbood et al.	
/J.T.L./	32	20120314617	A1	2012-12-13	Erichsen et al.	
/J.T.L./	33	20040088542	A1	2004-05-06	Daude et al.	
/J.T.L./	34	20080235755	A1	2008-09-25	Blaisdell et al.	
/J.T.L./	35	20100132027	A1	2010-05-27	Ou	
/J.T.L./	36	20110055916	A1	2011-03-03	Ahn	
/J.T.L./	37	20020016858	A1	2002-02-07	Sawada et al.	
/J.T.L./	38	20060262798	A1	2006-11-23	Joshi et al.	
/J.T.L./	39	20080043739	A1	2008-02-21	SUH et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	40	20080279196	A1	2008-11-13	Friskney et al.		
/J.T.L/	41	20130254766	A1	2013-09-26	Zuo et al.		
/J.T.L/	42	20030154297	A1	2003-08-14	Suzuki et al.		
/J.T.L/	43	20060114899	A1	2006-06-01	Toumura et al.		
/J.T.L/	44	20120331543	A1	2012-12-27	Bostrom et al.		
/J.T.L/	45	20110185055	A1	2011-07-28	NAPPIER et al.		
/J.T.L/	46	20060070122	A1	2006-03-30	Bellovin		
/J.T.L/	47	20050010765	A1	2005-01-13	Swander et al.		
/J.T.L/	48	20020198981	A1	2002-12-26	Corl et al.		
/J.T.L/	49	20090138938	A1	2009-05-28	Harrison et al.		
/J.T.L/	50	20060104202	A1	2006-05-18	Reiner		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	51	20050229246	A1	2005-10-13	Rajagopal et al.	
/J.T.L/	52	20040177139	A1	2004-09-09	Schuba et al.	
/J.T.L/	53	20040010712	A1	2004-01-15	Hui et al.	
/J.T.L/	54	20030120622	A1	2003-06-26	Nurmela et al.	
/J.T.L/	55	20080301765	A1	2008-12-04	Nicol et al.	
/J.T.L/	56	20050251570	A1	2005-11-10	Heasman et al.	
/J.T.L/	57	20050183140	A1	2005-08-18	Goddard	
/J.T.L/	58	20050125697	A1	2005-06-09	Tahara	
/J.T.L/	59	20040193943	A1	2004-09-30	Angelino et al.	
/J.T.L/	60	20020165949	A1	2002-11-07	Na et al.	
/J.T.L/	61	20020038339	A1	2002-03-28	Xu	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	62	20050114704	A1	2005-05-26	Swander	
/J.T.L/	63	20100268799	A1	2010-10-21	Maestas	
/J.T.L/	64	20110055923	A1	2011-03-03	Thomas	
/J.T.L/	65	20100303240	A1	2010-12-02	Beachem et al.	
/J.T.L/	66	20100199346	A1	2010-08-05	Ling et al.	
/J.T.L/	67	20100011433	A1	2010-01-14	HARRISON et al.	
/J.T.L/	68	20080077705	A1	2008-03-27	Li et al.	
/J.T.L/	69	20050286522	A1	2005-12-29	Paddon et al.	
/J.T.L/	70	20040205360	A1	2004-10-14	Norton et al.	
/J.T.L/	71	20140366132	A1	2014-12-11	Stiansen et al.	
/J.T.L/	72	20130061294	A1	2013-03-07	Kenworthy	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	73	20100242098	A1	2010-09-23	Kenworthy	
/J.T.L/	74	20070240208	A1	2007-10-11	Yu et al.	
/J.T.L/	75	20060146879	A1	2006-07-06	Anthias et al.	
/J.T.L/	76	20060136987	A1	2006-06-22	Okuda	
/J.T.L/	77	20020049899	A1	2002-04-25	Kenworthy	
/J.T.L/	78	20140281030	A1	2014-09-18	Cui et al.	
/J.T.L/	79	20040073655	A1	2004-04-15	Kan et al.	
/J.T.L/	80	20150237012	A1	2015-08-20	Moore	
/J.T.L/	81	20150304354	A1	2015-10-22	Rogers et al.	
/J.T.L/	82	20140115654	A1	2014-04-24	Rogers et al.	
/J.T.L/	83	20140201123	A1	2014-07-17	Ahn et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	84	20140283004	A1	2014-09-18	Moore		
/J.T.L/	85	20140283030	A1	2014-09-18	Moore et al.		
/J.T.L/	86	20080229415	A1	2008-09-18	Kapoor et al.		
/J.T.L/	87	20140215574	A1	2014-07-31	Erb et al.		

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/J.T.L/	1	1677484	EP	A2	2006-07-05	Microsoft Corp		
/J.T.L/	2	1313290	EP	A1	2003-05-21	Stonesoft Corp		
/J.T.L/	3	2005046145	WO	A1	2005-05-19	Ericsson Telefon Ab L M		
/J.T.L/	4	2385676	EP	A1	2011-11-09	Alcatel Lucent		
/J.T.L/	5	2498442	EP	A1	2012-09-12	Openet Telecom Ltd		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

/J.T.L/	6	20010079361	KR	A	2001-08-22	Kim, Sang Wook		
/J.T.L/	7	1006701	EP	A2	2000-06-07	Lucent Technologies Inc		
/J.T.L/	8	2006105093	WO	A2	2006-10-05	Univ Wake Forest		
/J.T.L/	9	2006093557	WO	A2	2006-09-08	Univ Wake Forest		
/J.T.L/	10	2005328336	AU	B2	2011-09-15	Univ Wake Forest		
/J.T.L/	11	2011038420	WO	A2	2011-03-31	Great Wall Systems		
/J.T.L/	12	1484884	EP	A2	2004-12-08	Microsoft Corp		
/J.T.L/	13	2006230171	AU	B2	2012-06-21	Univ Wake Forest		
/J.T.L/	14	1864226	EP	B1	2013-05-15	Univ Wake Forest		
/J.T.L/	15	2600236	CA	A1	2006-10-05	Univ Wake Forest		
/J.T.L/	16	2012146265	WO	A1	2012-11-01	Voipfuture Gmbh		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

If you wish to add additional Foreign Patent Document citation information please click the Add button [Add]

NON-PATENT LITERATURE DOCUMENTS [Remove]

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
/J.T.L/	1	Copy of ISR for PCT/US2013/057502, dated November 7, 2013.	
/J.T.L/	2	International Search Report off International Application No. PCT/US2014/023286, dated June 24, 2014.	
/J.T.L/	3	ISR off International Application No. PCT/US2013/072566, dated March 24, 2014.	
/J.T.L/	4	ISR off International Application No. PCT/US2014/027723, dated June 26, 2014.	
/J.T.L/	5	"Control Plane Policing Implementation Best Practices"; Cisco Systems; March 13, 2013; <https://web.archive.org/web/20130313135143/http:www.cisco.com/web/about/security/intelligence/coppwp_gs.html>	
/J.T.L/	6	Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI	
/J.T.L/	7	Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.	
/J.T.L/	8	Mizuno et al., A New Remote Configurable Firewall System for Home-use Gateways, January 2005. Second IEEE Consumer Communications and Networking Conference, pp. 599-601.	
/J.T.L/	9	"SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Division 2012 Principal Investigators' Meeting"; Sean Moore, October 10, 2014.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	10	John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc.; Novermber 5, 2010, pps: 1-26.	
/J.T.L/	11	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	
/J.T.L/	12	2016 Jan 11 - (US) Non Final Rejection - App 14/698,560	
/J.T.L/	13	2011 Apr 27 - (WO) International Search Report and Written Opinion - App PCT/US2010/054520	
/J.T.L/	14	2011 Mar 04 - (US) Notice of Allowance - App 11/316,331	
/J.T.L/	15	2011 Mar 03 - (EP) Communication Pursuant to Rules 70(2) and 70a(2) - App 06758213.0	
/J.T.L/	16	2011 Feb 14 - (EP) Search Report - App 06758213.0	
/J.T.L/	17	Fulp, Errin: "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pgs. 1-5 (Copyright 2010)	
/J.T.L/	18	2010 Sept 30 - (US) Office Action - App 11/390,976	
/J.T.L/	19	2010 Sept 10 - (AU) Office Action - App 2006230171	
/J.T.L/	20	2010 Aug 20 - (AU) Office Action - App 2005328336	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	21	2010 Jun 23 - (US) Final Rejection - App 11/316,331	
/J.T.L/	22	2010 Apr 29 - (US) Interview Summary - App 11/390,976	
/J.T.L/	23	2010 Mar 26 - (US) Final Rejection - App 11/390,976	
/J.T.L/	24	2009 Sept 14 (US) Office Action - App 11/316,331	
/J.T.L/	25	2009 Jun 24 - (US) Office Action - App 11/390,976	
/J.T.L/	26	2008 Jul 03 - (WO) Written Opinion of the International Searching Authority - App PCT/US06/11291	
/J.T.L/	27	2007 Aug 31 - (EP) Communication Pursuant to Rules 109 and 110 - App 05857614.1	
/J.T.L/	28	Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pgs. 1-11 (2007)	
/J.T.L/	29	2006 Sept 11 - (WO) Written Opinion of the International Searching Authority - App PCT/US05/47008	
/J.T.L/	30	Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pgs. 1-6 (2006)	
/J.T.L/	31	Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	32	E. Fulp, "Optimization of Network Firewall Policies Using Ordered Sets and Directed Acyclical Graphs", Technical Report, Computer Scient Department, Wake Forest University, January 2004	
/J.T.L/	33	E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004	
/J.T.L/	34	E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004	
/J.T.L/	35	E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded September 2003	
/J.T.L/	36	E. Al-Shaer et al., "Firewall Policy Advisor for Anomaly Discovery and Rule Editing", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, 2003	
/J.T.L/	37	V.P. Ranganath, "A Set-Based Approach to Packet Classification", Proceedings of the IASTED International Conference on Parallel and Distributed Computing and Systems, 889-894, 2003	
/J.T.L/	38	M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS, October 2002	
/J.T.L/	39	Lee et al., "Development Framework for Firewall Processors," IEEE, pgs. 352-355 (2002)	
/J.T.L/	40	L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, June 2001	
/J.T.L/	41	D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001	
/J.T.L/	42	E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	43	S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001	
/J.T.L/	44	G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001	
/J.T.L/	45	P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001	
/J.T.L/	46	D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): February 2000	
/J.T.L/	47	A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000	
/J.T.L/	48	X. Gan et al., "LSMAC vs. LSNAT: Scalable Cluster-based Web servers", Journal of Networks, Software Tools, and Applications, 3(3): 175-185, 2000	
/J.T.L/	49	A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000	
/J.T.L/	50	O. Paul et al., "A full Bandwidth ATM Firewall", Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/JASON T LEE/	Date Considered	03/08/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Bradley C. Wright/	Date (YYYY-MM-DD)	2016-03-30
Name/Print	Bradley C. Wright	Registration Number	38061

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /. m ./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" ' ' ' '

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	Art Unit
	JASON LEE	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
h04l63/1425.cpc.;h04l61/1511.cpc.;h04l63/0263.cpc.;h04l63/0281.cpc.;h04l63/1416.cpc.;	4/3/17	JL

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	153	4/3/17	JL

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searched	4/2/17	JL
inventor name searched	4/3/17	JL
Rule-based network-threat detection searched on topic	4/2/17	JL
(((filter$3 with rule) with treat) same (encrypt$3)); (((filter$3 with rule) with treat) same (encrypt$3)) and (address or session);	4/2/17	JL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	Art Unit
	JASON LEE	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/05/2017								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	3	(((filter$3 with rule) with proxy) same ((URI) or "uniform resource identifier")) and (log or drop)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/04/05 12:09
L8	3	7 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/04/05 12:10
S1	6	"9413722".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:26
S2	2	"20160308894".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:50
S3	3	"9124552".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:51
S4	2	"9264370".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:52
S5	4	"Rule-based network-threat detection".ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:49
S6	6	"2004093513".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:58
S7	3	"20040093513".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:58
S8	0	"20129923576".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:58
S9	3	"20120023576".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:59
S10	2	"20080163333".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:59

S11	1	(S7 or S9 or S10) and indicator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:00
S12	3	"20110055916".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:07
S13	7294	h04l63/1425.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:25
S14	13021	h04l61/1511.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S15	5447	h04l63/0263.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S16	6650	h04l63/0281.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S17	12955	h04l63/1416.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S18	2796	S13 and (S14 or S15 or S16 or S17)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:32
S19	2795	S18 and @ad <"29151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:32
S20	2458	S18 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:33
S21	149	S13 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:34
S22	129	S21 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:34
S23	7306	h04l63/1425.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S24	13031	h04l61/1511.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S25	149	S23 and S24	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	ADJ	ON	2017/03/07 15:29

			IBM_TDB			
S26	129	S25 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S27	0	(((filter$3 with rule) with treat) same (encrypt$3)) and S26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S28	7	(((filter$3 with rule) with treat) same (encrypt$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:30
S29	7	(((filter$3 with rule) with treat) same (encrypt$3)) and (DNS or domain)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:30
S30	7	(((filter$3 with rule) with treat) same (encrypt$3)) and (address or session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:55
S31	7	(rule with based) and S30	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:01
S32	5448	h04l63/0263.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S33	6652	h04l63/0281.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S34	12973	h04l63/1416.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S35	2805	S23 and (S24 or S32 or S33 or S34)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S36	2466	S35 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S37	2466	S36 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S38	0	(((filter$3 with rule) with treat) same (encrypt$3)) and S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S39	0	((receiv$3 with packet)same rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:32
S40	0	((receiv$3 with message)same	US-PGPUB; USPAT;	ADJ	ON	2017/03/08

		rule) and "20050138353".pn.	USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			14:32
S41	0	((receiv$3 same message) same rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:32
S42	1	((receiv$3 same message) and rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:33

EAST Search History (Interference)

< This search history is empty>

4/ 5/ 2017 3:44:40 PM
C:\ Users\ jlee16\ Documents\ EAST\ Workspaces\ 14757638-030117.wsp

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" ' ' ' '

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	1	J. Xu et al., "Design and Evaluation of a High-Performance ATM Firewall Switch and Its Applications", IEEE Journal on Selected Areas in Communications, 17(6): 1190-1200, June 1999	
/J.T.L/	2	C. Benecke, "A Parallel Packet Screen for High Speed Networks", Proceedings of the 15th Annual Computer Security Applications Conference, 1999	
/J.T.L/	3	R. Funke et al., "Performance Evaluation of Firewalls in Gigabit-Networks", Proceedings of the Symposium on Performance Evaluation of Computer and Telecommunication Systems, 1999	
/J.T.L/	4	S. Suri et al., "Packet Filtering in High Speed Networks", Proceedings of the Symposium on Discrete Algorithms, 969-970, 1999	
/J.T.L/	5	U. Ellermann et al., "Firewalls for ATM Networks", Proceedings of INFOSEC'COM, 1998	
/J.T.L/	6	V. Srinivasan et al., "Fast and Scalable Layer Four Switching", Proceedings of ACM SIGCOMM, 191-202, 1998	
/J.T.L/	7	M. Degermark et al., "Small Forwarding Tables for Fast Routing Lookups", Proceedings of ACM SIGCOMM, 4-13, 1997	
/J.T.L/	8	S,M. Bellovin et al., "Network Firewalls", IEEE Communications Magazine, 50-57, 1994	
/J.T.L/	9	W.E. Leland et al., "On the Self-Similar Nature of Ethernet Traffic", IEEE Transactions on Networking, 2(1); 15, 1994	
/J.T.L/	10	G. Brightwell et al., "Counting Linear Extensions is #P-Complete", Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, 1991	
/J.T.L/	11	M. Al-Suwaiyel et al., "Algorithms for Trie Compaction", ACM Transactions on Database Systems, 9(2): 243-263, June 1984	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	12	D. Comer, "Analysis of a Heuristic for Full Trie Minimization", ACM Transactions on Database Systems, 6(3): 513-537, Sept. 1981	
/J.T.L/	13	R.L. Graham et al., "Optimization and Approximation in Deterministic Sequencing and Scheduling: A Survey", Annals of Discrete Mathematics, 5: 287-326, 1979	
/J.T.L/	14	E.L. Lawler, "Sequencing Jobs to Minimize Total Weighted Completion oTime Subject to Precedence Constraints", Annals of Discrete Mathematics, 2: 75-90, 1978	
/J.T.L/	15	J.K. Lenstra et al., "Complexity of Scheduling Under Precedence Constraints", Operations Research, 26(1): 22-35,1978	
/J.T.L/	16	R. Rivest, "On Self-Organizing Sequential Search Heuristics", Communications of the ACM, 19(2): 1976	
/J.T.L/	17	W.E. Smith, "Various Optimizers for Single-Stage Productions", Naval Research Logistics Quarterly, 3: 59-66, 1956	
/J.T.L/	18	Bellion, "HIgh Performance Packet Classification", http://www.hipac.org (Publication Date Unknown)	
/J.T.L/	19	2011 Oct 18 - (EP) Communication Pursuant to Article 94(3) - App 06 758 213.0	
/J.T.L/	20	2011 Jun 09 - (US) Notice of Allowance - App 11/390,976	
/J.T.L/	21	2012 Jun 26 - (EP) Extended Search Report - App 05857614.1	
/J.T.L/	22	2012 Jun 09 - (AU) Notice of Acceptance - App 2006230171	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	23	2011 Nov 11 - (AU) Second Office Action - App 2006230171	
/J.T.L/	24	2013 Jan 17 - (CA) Office Action - App 2,600,236	
/J.T.L/	25	2013 Jan 16 - (CA) Office Action - App 2,594,020	
/J.T.L/	26	2012 Nov 20 - (EP) Communication under rule 71(3) - App 06 758 213.0	
/J.T.L/	27	2013 Apr 18 - (EP) Decision to Grant a European Patent - App 06758212.0	
/J.T.L/	28	2011 Aug 25 - (US) Non Final Rejection - App 12/871,806	
/J.T.L/	29	2012 Feb 06 - (US) Final Rejection - App 12/871,806	
/J.T.L/	30	2012 Aug 07 - (US) Non Final Rejection - App 12/871,806	
/J.T.L/	31	2012 Nov 26 - (US) Final Rejection - App 12/871,806	
/J.T.L/	32	2013 Apr 04 - (US) Notice of Allowance - App 12/871,806	
/J.T.L/	33	2015 Jan 14 - (EP) Extended Search Report - App 10819667.6	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

/J.T.L/	34	2014 May 26 - (CA) Office Action - App 2010297968	
/J.T.L/	35	2015 May 25 - (AU) Notice of Acceptance - App 2010297968	
/J.T.L/	36	2015 May 14 - (US) Non Final Rejection - App 13/940,240	
/J.T.L/	37	2015 Nov 27 - (US) Final Rejection - App 13/940,240	
/J.T.L/	38	2015 Jul 10 - (WO) Communication Relating to the Results of the Partial International Search for International App - PCT/US2015/024691	
/J.T.L/	39	2015 Jul 23 - (WO) International Preliminary Report on Patentability - App PCT/US2013/072566	
/J.T.L/	40	2016 Jan 28 - (WO) International Search Report and Written Opinion - App PCT/US2015/062691	
/J.T.L/	41	International Search Report and Written Opinion for International App. No. PCT/US2015/024691, dated September 16, 2015.	
/J.T.L/	42	International Preliminary Report on Patentability for International App. No. PCT/US2013/057502, dated April 28, 2015	
/J.T.L/	43	International Preliminary Report on Patentability for International App. No. PCT/US2014/023286, dated September 15, 2015.	
/J.T.L/	44	International Preliminary Report on Patentability for International App. No. PCT/US2014/027723, dated September 15, 2015.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" ' ' ' '

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

	45	Statement RE: Related Application, dated July 24, 2015	
/J.T.L/	46	2015 Dec 22 - (US) Final Office Action - App 14/714,207	
/J.T.L/	47	2016 Feb 26 - (US) Non Final Office Action - App 14/253,992	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/JASON T LEE/	Date Considered	03/08/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Bradley C. Wright/	Date (YYYY-MM-DD)	2016-03-30
Name/Print	Bradley C. Wright	Registration Number	38061

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /. m ./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" ' ' ' '

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/757,638	12/23/2015	David K. Ahn	007742.00059

CONFIRMATION NO. 9492

22907
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

PUBLICATION NOTICE

OC000000092444554

Title: Rule-based network-threat detection for encrypted communications

Publication No.US-2017-0187733-A1
Publication Date:06/29/2017

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently https://portal.uspto.gov/pair/PublicPair. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8117655	B2	2012-02-14	Spielman	
	2	6147976	A	2000-11-14	Shand et al.	
	3	7610621	B2	2009-10-27	Turley et al.	
	4	9154446	B2	2015-10-06	Gemelli et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20120106354	A1	2012-05-03	Pleshek et al.	
	2	20130047020	A1	2013-02-21	Hershko et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

	3	20090240698	A1	2009-09-24	Shukla et al.	
	4	20040098511	A1	2004-05-20	Lin et al.	
	5	20100232445	A1	2010-09-16	Bellovin	
	6	20130305311	A1	2013-11-14	Puttaswamy Naga et al.	
	7	20020186683	A1	2002-12-12	Buck et al.	
	8	20090222877	A1	2009-09-03	Diehl et al.	
	9	20100107240	A1	2010-04-29	Thaler et al.	
	10	20040093513	A1	2004-05-13	Cantrell et al.	
	11	20120023576	A1	2012-01-26	Sorensen et al.	
	12	20080163333	A1	2008-07-03	Kasralikar	
	13	20020164962	A1	2002-11-07	Mankins et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

	14	20050024189	A1	2005-02-03	Weber	
	15	20110141900	A1	2011-06-16	Jayawardena et al.	
	16	20150350229	A1	2015-12-03	Mitchell	
	17	20050108557	A1	2005-05-19	Kayo et al.	
	18	20150373043	A1	2015-12-24	Wang et al.	
	19	20140317397	A1	2014-10-23	Martini	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2007109541	WO	A2	2007-09-27	Brubaker, Curtis		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

	1	2015 Nov 02 - (AU) Office Action - App 2013372879	
	2	2016 Apr 26 - (US) Office Action - App 14/745,207	
	3	2016 May 06 - (US) Office Action - App 14/714,207	
	4	2016 May 13 - (US) Office Action - App 13/940,240	
	5	2016 Jun 14 - (US) Office Action - App 14/625,486	
	6	2016 Feb 25 - (AU) Office Action - App 2014249055	
	7	2016 Feb 24 - (AU) Office Action - App 2014228257	
	8	2016 Jun 09 - (WO) International Search Report - PCT/US2016/026339	
	9	2016 Jun 16 - (CA) Office Action - App 2,888,935	
	10	2016 Jul 11 - (EP) Office Action - App 14720824.3	
	11	2016 Jul 22 - (US) Office Action - App 14/921,718	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

	12	2016 Jul 20 - (AU) Office Action - App 2013335255	
	13	2016 Oct 05 - (US) Notice of Allowance - App 14/698,560	
	14	2016 Sept 13 - (CA) Office Action - App 2,902,206	
	15	2016 Sept 14 - (CA) Office Action - App 2,897,737	
	16	2016 Sept 26 - (CA) Office Action - App 2,902,158	
	17	2016 Oct 26 - (US) Office Action - App 13/940,240	
	18	2016 Nov 21 - (US) Office Action - App 14/745,207	
	19	2016 Dec 05 - (US) Notice of Allowance - App 14/714,207	
	20	Singh, Rajeev et al. "Detecting and Reducing the Denial of Service attacks in WLANs", December 2011, World Congress on Information and Communication TEchnologies, pp. 968-973	
	21	2017 Feb 10 - (US) Notice of Allowance - App 14/625,486	
	22	2017 Feb 15 - (US) Notice of Allowance - App 14/921,718	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

	23	2017 Mar 06 - (WO) International Search Report and Written Opinion - App PCT/US2016/068008	
	24	2017 Jun 07 - (US) Office Action - App 14/745,207	
	25	2015 Sept 4 (US) Notice of Allowance - App. 14/702,755 (007742.00036)	
	26	2017 Jun 07 - (WO) International Search Report and Written Opinion - App PCT/US2016/067111	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Joshua D. Schneider/	Date (YYYY-MM-DD)	2017-07-11
Name/Print	Joshua D. Schneider	Registration Number	67,194

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14757638
Filing Date:	23-Dec-2015
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Filer:	Joshua Daniel Schneider/Holly Parker
Attorney Docket Number:	007742.00059

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	29744427
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Joshua Daniel Schneider/Holly Parker
Filer Authorized By:	Joshua Daniel Schneider
Attorney Docket Number:	007742.00059
Receipt Date:	11-JUL-2017
Filing Date:	23-DEC-2015
Time Stamp:	12:04:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$90
RAM confirmation Number	071117INTEFSW00011330190733
Deposit Account	190733
Authorized User	Joshua Schneider
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.17 (Patent application and reexamination processing fees) 37 CFR 1.19 (Document supply fees)	

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO2007109541A2_18096458.pdf	8952906 32d020e6fc053874951d75f280bdb76a36fda8dd	no	179
Warnings:					
Information:					
2	Non Patent Literature	AU_2013_372879_1st_report_17844165.PDF	180230 0db14b50d6b54fb780bc134451640ce58c5b8f84	no	3
Warnings:					
Information:					
3	Non Patent Literature	Final_Rejection__892__1449_17836139.pdf	2221034 630c07a4f486c227bd2b154764c1d52922647ed1	no	59
Warnings:					
Information:					
4	Non Patent Literature	Non-Final_Rejection__892__1449_17854388.pdf	3543506 a1ebec4955cf4c5d0cddd8921df2403ac8cbd49b	no	88
Warnings:					
Information:					
5	Non Patent Literature	Non-Final_Rejection__1449_17863955.pdf	1980426 cc2fae7e71b3f218bf284f104b06ea34ced4be21	no	59
Warnings:					
Information:					
6	Non Patent Literature	Non-Final_Rejection__892__1449_17907654.pdf	3501971 596402d50d623fd856dc9e75f0b2e46796297687	no	86
Warnings:					
Information:					

7	Non Patent Literature	AU2014249055OA_17930089.PDF	131541 2c1fd926dd8411ad1cff21014df6bf3f90176215	no	3
Warnings:					
Information:					
8	Non Patent Literature	AU2014228257OA_17930107.PDF	114304 7ec5e241c75e7cf6e0e9496d6097111f08feb5bd	no	2
Warnings:					
Information:					
9	Non Patent Literature	17920268_1_17936575.pdf	154479 327c57ef9aaf24c59b40ae7d298d36d2ea40f261	no	3
Warnings:					
Information:					
10	Non Patent Literature	17949695_1_17954003.pdf	91536 4f342d662e17ef4b0f97d50d89ea43a15f098bd2	no	4
Warnings:					
Information:					
11	Non Patent Literature	Examination_report_1107_17971763.PDF	233390 ea2ab8ea9b22be899b5e4a32d079f436a8187228	no	7
Warnings:					
Information:					
12	Non Patent Literature	Non-Final_Rejection__892__1449_17967478.pdf	1156475 3e4da35c3cb92b86749ebdf8db80e0da3f494217	no	36
Warnings:					
Information:					
13	Non Patent Literature	AUFirstEXam_17988909.pdf	265946 b205b9fb42ea35b902bd6fa3d3f1032d26b65832	no	3
Warnings:					
Information:					

14	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__INTVSUMEX__892__1449_18076047.pdf	1537046 d8a8ad44e3593cdfa76b2c0fdf963036e70bdeb1	no	38
Warnings:					
Information:					
15	Non Patent Literature	OTT01-7836061-v1-PAT_83577W-1_Corr_from_PTO_-_Office_Action_18087198.PDF	282227 53790041ea1a9ccf9b6b0c734e50b101b9b12690	no	4
Warnings:					
Information:					
16	Non Patent Literature	OTT01_-7838337-v1-PAT_83380W-1_Corr_to_PTO_-_Office_Action_18096434.PDF	393438 83111a6b651a98ad89407303a2fc324f521be058	no	6
Warnings:					
Information:					
17	Non Patent Literature	OTT01_-7861591-v1-PAT_83575W-1_Corr_from_PTO_-_Office_Action_18101654.PDF	285929 c87d71516445919f7dfca6a0e1dd62aa55e1463a	no	5
Warnings:					
Information:					
18	Non Patent Literature	18105700_1_18116178.pdf	1041266 9b9dace0d9e37e051b27e2662c18d1d91f311243	no	30
Warnings:					
Information:					
19	Non Patent Literature	Non-Final_Rejection__892__1449_18140604.pdf	1584757 a988730b4239ed429a4344dc8b1ddd5c65372a63	no	42
Warnings:					
Information:					
20	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__1449_18158549.pdf	695760 461671807412c0444aa64839e61ec9579560a367	no	14
Warnings:					
Information:					

21	Non Patent Literature	14698560_18178105.pdf	607977 4554608d6aeb135ec747c12682f1efe32009 1e51	no	6
Warnings:					
Information:					
22	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__1449_18260 634.pdf	618186 c096dbb16fe1eb240566458b09f75d6cb1c bc3b1	no	11
Warnings:					
Information:					
23	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__1449_18267 002.pdf	599424 0b2c0b642ad7a9989fab20f9bf3f01260918 d1b5	no	13
Warnings:					
Information:					
24	Non Patent Literature	Corr_from_WIPO_-_-_Notification_of_Transmittal_of_The_International_Search_Report__18522354.pdf	658968 635a0e3688a652b4c29d20455c11d91ba6d 754cb	no	13
Warnings:					
Information:					
25	Non Patent Literature	Final_Rejection__1449_185560 85.pdf	1631691 2a200860c3692152ee9c1b3f44f72aa3202e 085a	no	40
Warnings:					
Information:					
26	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__892_174810 77.pdf	437251 0d3e5ac2c20f9139ad586d4cb74a808fdbf1 daef	no	9
Warnings:					
Information:					
27	Non Patent Literature	Corr_from_WIPO__-_N__of_Transmittal_of_the_International_Search_Report_186 15129.pdf	828763 978f48233eb8c59f605a36a1854546057d64 7889	no	13
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					

28	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_18615489.pdf	1036449 7ade66e54cca57dc3119ff5ea31917bc34e07b2e	no	8
Warnings:					
Information:					
29	Fee Worksheet (SB06)	fee-info.pdf	30808 fb9ed1d3157b6bb155e309d38c9e2c4186193ba3	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	34797684		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Espacenet

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 September 2007 (27.09.2007)

PCT

(10) International Publication Number
WO 2007/109541 A2

(51) International Patent Classification:
G06Q 10/00 (2006.01)

(21) International Application Number:
PCT/US2007/064175

(22) International Filing Date: 16 March 2007 (16.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/783,577	16 March 2006 (16.03.2006)	US
60/794,006	21 April 2006 (21.04.2006)	US

(71) Applicant and
(72) Inventor: **BRUBAKER, Curtis, M.** [US/US]; 46 Monarch Bay Drive, Monarch Beach, CA 92629 (US).

(74) Agent: **O'BANION, John, P.**; O'banion & Ritchey LLP, 400 Capitol Mall, Suite 1550, Sacramento, CA 95814 (US).

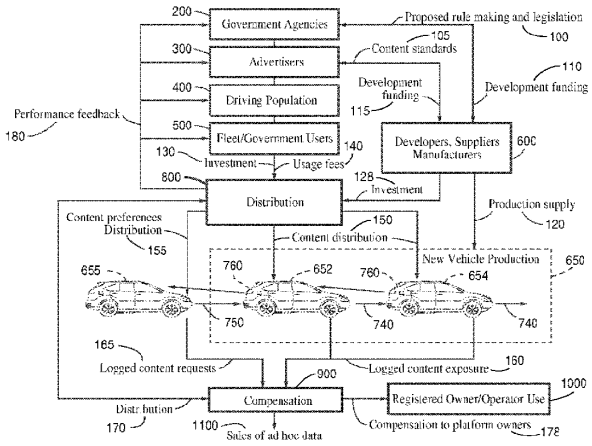
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR OBTAINING REVENUE THROUGH THE DISPLAY OF HYPER-RELEVANT ADVERTISING ON MOVING OBJECTS



(57) Abstract: A system for obtaining revenue through the display of advertising on fixed or moving objects is disclosed. Such objects receive, store, poll and extract data to present content based on the time of day, locations, and relative movements in a specific environment, where data and information stored in moving or mobile objects within that environment can be transmitted between those objects or to stationary objects, where it is then used to enable and control such displays for which the owners of those objects are then compensated. The system enables the display of hyper-relevant ad content with synchronized remote audio, personal messaging and public service alerts on surrounding objects and provides for the real-time logging and later downloading of data to confirm communications and content deliveries between objects, track and measure consumer engagement, verify consumer's direct responses to ad viewings with accountability systems.

WO 2007/109541 A2

SYSTEM AND METHOD FOR OBTAINING REVENUE THROUGH THE DISPLAY OF HYPER-RELEVANT ADVERTISING ON MOVING OBJECTS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority from U.S. provisional application serial number 60/783,577, filed on March 16, 2006, incorporated herein by reference in its entirety, and from U.S. provisional application serial number 60/794,006, filed on April 21, 2006, incorporated herein by reference in its entirety.

[0002] This application is related to U.S. nonprovisional application serial number 11/552,932, filed October 25, 2006, incorporated herein by reference in its entirety, which claims priority from U.S. provisional application serial number 60/729,919, filed on October 25, 2005, incorporated herein by reference in its entirety.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0003] Not Applicable

INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC

[0004] Not Applicable

NOTICE OF MATERIAL SUBJECT TO COPYRIGHT PROTECTION

[0005] A portion of the material in this patent document is subject to copyright protection under the copyright laws of the United States and of other countries. The owner of the copyright rights has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the United States Patent and Trademark Office publicly available file or records, but otherwise reserves all copyright rights whatsoever. The copyright owner does not hereby waive any of its rights to have this patent document maintained in secrecy, including without limitation its rights pursuant

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0006] This invention pertains generally to effectively providing advertising content with respect to a prospective consumer's desires and, more particularly, to an integrated system and method for directing hyper-relevant content to consumers through the use of wireless technologies for the exchange of information, including the compensation of users for providing or viewing content.

2. Description of Related Art

[0007] In the ad business, there are a handful of yet to be realized holy grails. They are: (1) Deliver your ad to the correct demographic (age, gender, income level, etc.); (2) Deliver it at a time its recipient is sure to see it (not when he's out for a soda or in the bathroom); (3) Pitch your ad to consumers who are truly interested in what you are selling (instead of wasting advertising dollars on those who are not); (4) Catch consumers when they're relaxed and open to suggestion (instead of preoccupied with other things); (5) Reach audiences TV can't reach and do it with more targeted spots in a single day than they'd catch on regular TV; (6) Connect with buyers at the right time (i.e.: sell them food at meal times); (7) Get your message to consumers when they are at an opportune location (for example, promote a great restaurant at meal time a couple of blocks from the place); (8) Put ads into the distribution pipeline in just seconds using the Internet; (9) Base billings on the actual content delivered and do it all electronically and automatically; (10) Give advertisers proof their ads actually ran and track them on a minute to minute basis; (11) Provide feedback to the agency or its clients on consumer engagement; (12) When your ad shows, let viewers buy (or at least get more information) at the push of a button. Unlike any existing commercial advertising system, the present invention delivers all of these objectives, and more, by creating a totally new kind of mobile communications platform and

forum.

[0008] ADVERTISING.

[0009] Madison Avenue is working to outdated media models and needs to figure out emerging media fast or it stands to lose billions of dollars to others who will. Over the next decade, major money will be set in motion to create entirely new ad platforms and new ways to reach consumers in what today is a $250 billion industry. In the process, the ways and means of the contemporary ad business are going to be turned inside out, not so much because of the present invention, but because of the many emerging technologies that make it possible. For years, marketers have taken their best shots at consumers. Much of it is creative guesswork which follows available technology and distribution streams that were invented for other purposes. Television, for example, developed as a communications resource and quickly evolved into a form of free entertainment where marketers could insert the products and services others wished to sell into the paths of consumers while they were having a good time. It was not important if those people were really interested in the products and services; TV was simply the best way to expose products and services to consumers because TV had traffic. However, ad executives are beginning to recognize how much money is being wasted on antiquated media plans. For the first time in history, TV Spot ads were the biggest loser in ad spending for 2005, sinking 9.5% to $15.5 billion, because viewers have 'left the building.' Yet, newspapers, magazines, cable, and syndication all showed gains, with the category of outdoor advertising rising by 9.8% to $3.5 billion.

[0010] While consumers are looking for new things to do and new ways to entertain themselves, marketers are looking for audiences. However, audiences today are increasingly sophisticated about avoiding advertising messages. What is needed isn't just any audience, but an audience that truly cares about what advertisers have to say and sell, and those ad messages have to be bright, quick, and relevant to the new audience's current interests and lifestyle. Today, the gold rush is toward the Internet and to what has been

termed the "3rd screen," those tiny carry-around displays found on cell phones, iPods, and PDAs. Once again, marketers want to insert themselves (and their content) into our everyday business and fun. It is estimated that as much as 25% to 30% of the $100 billion spent each year on brand advertising will soon find its way to such mobile screens, but will users who pay for such services accept advertising? To borrow a statement from a highly-placed marketing industry executive: "If I'm a 22-year old male and I've downloaded four 3D games to my phone in the last 30 days, chances are pretty good I'd be interested in seeing a Sony PS3 commercial on my device." He may be right. Recent studies have determined that kids like watching ads as long as they represent something they're interested in. Look at the Super Bowl, where large numbers of viewers tune in primarily to watch the ads. Consumers like these want to participate, want more to talk about, and want ultimately to have a say, so they can certainly take the time to tell advertisers about the kinds of content they would like to see. Yet, today's marketers have failed to recognize that there are technologies emerging today that can open dialogs between consumers and creatives and still leave the field open for expression and execution by the professionals in it.

[0011] New canvases are needed along with the audiences to go with them, but to secure them will require more than repurposed TV spots for tiny screens on the go. What is required is a systemic rebirth of the ad game including novel applications and pragmatic distribution. But more than anything, it requires marketers to get more in touch with consumers who are more in touch with themselves, with consumers who are articulate enough to tell us at least two things: 1) who they are, and 2) what they want. Technology can enable this, but there needs to be an economic reason for consumers to opt into the game. The present invention has been conceived to provide just that.

[0012] VISUAL CONGESTION

[0013] American cities are converging on BladeRunner-like visual clutter, and few regulatory brakes have been applied to this accelerating buildup. Electronic displays on taxi tops vie with sign-wrapped busses and trailers, bus

shelters plastered with ads, lighted store signs, and a profusion of billboards, many with revolving panels and flashing lights, and now many with radio-enabled audio. The situation promises to worsen. Nanoscale components promise larger, cheaper, high-resolution video screens that are bound to find their way into signs, surfaces, and products of all kinds. We are already inundated with visual ads: our daily sensory diet includes thousands of commercial impressions, from pop-ups and animations in Web content to TV's full arsenal of 30-second spots, now with product placements embedded in what remains of the entertainment. With increasingly new technologies and eye-catching designs competing for drivers' attention, regulatory agencies, traffic engineers, and advocates are beginning to question which of these potential distractions may also pose a risk to driving. To what extent can commercial signage be blamed for accidents? What do we know about the nature of attention and distraction? Can this proliferation be rationally controlled?

[0014] Surveys show that signs and billboards indeed compromise traffic safety, especially at intersections and on curves. Flashing lights, motion, visual clutter, and novelty (e.g., the Times Square / Las Vegas Strip effect that is replicating so quickly in major cities) are implicated as part of the problem. Additionally, research on driver distractions confirms that visual complexity compromises safety by forcing drivers to scan the environment longer for street signs, turns, or critical landmarks. Researchers using eye-tracking devices to monitor drivers in traffic are finding that video signs are more distracting than static signs and can act as catalysts, increasing ad gazing of all types, even in unsafe situations. Similar studies are documenting the effects of visual distractions on both young and old drivers to determine what constitutes safe, manageable amounts of information, and the effects of animation, video, and moving panels on drivers, in efforts to set standards so that electronic signs and billboards are legible and non-distracting. To be non-distracting, however, is to contradict the entire purpose of outdoor advertising, and therein lies the problem.

[0015] It is undisputed that people are easily distracted. Theories of attention point out relationships between mental excitation/interest and the ability to perform tasks. We function best somewhere between boredom and over-stimulation. What researchers have found is that new or unexpected stimuli trigger involuntary responses and the more bored or unfocused we are, the more susceptible we are to these surprises. Studies have also identified modes of visual perception: a focal, or search, mode that is narrow and specific, and an ambient mode that is a sort of default, which is not focused on anything in particular, but having better peripheral awareness. We've learned that computer users performing search tasks in the center of the screen are slowed when objects appear on the perimeter, even when they aren't consciously aware of them. The more peripheral objects, the greater the distraction. Thus, the more we direct our attention towards that periphery, the less we focus on what's in the middle of our screens, or in the middle of our roads. Researchers have also found that new, moving and looming objects command attention; that the onset of motion triggers overriding or urgent attention, possibly tapping the survival instinct; and that changes in color can capture attention. None of this proves that outdoor ads cause accidents, but behavioral mechanisms clearly come into play when drivers encounter roadside signage. The notion that content is a major factor in drawing attention is starting to be examined. Because content and distractions are inevitable, a solution may lie in controlling them and in determining exactly how, when and where they should occur. That's a tall order, but it is also a primary objective of the present invention.

[0016] PHYSICAL CONGESTION

[0017] Just as advertising seems to clutter our landscape, so do moving objects. Traffic congestion in our major cities has reached epidemic proportions, prompting nationwide studies to get a handle on the problem. In places like Los Angeles, where, in the late fifties, one could drive anywhere to its outskirts in 20 minutes, it now takes hours, regardless of the time of day. According to the 2005 Urban Mobility Study Report, released in May by the

Texas Transportation Institute of Texas A&M University, sixty-seven percent of the peak period travel was congested in 2003, compared to only 32 percent in 1982; fifty-nine percent of the major road system was congested in 2003 compared to 34 percent in 1982. The number of hours of the day when congestion is encountered has grown from about 4.5 hours in 1982 to more than 7.1 hours today. Traffic congestion is worse in the large urban areas than in the smaller ones, but even the smaller areas are unable to keep pace with rising demand. According to the study, 10 years is not an unrealistic timeframe to go from an idea to a completed project or to an accepted program due to the significant planning and development required. But in ten years at current growth rates, the urban area average congestion values will jump to the next highest classification—i.e.: medium areas in 2013 will have the congestion problems large areas had in 2003.

[0018] What does this mean in cost to consumers? In 2003, congestion (based on wasted time and fuel) cost drivers about $63.1 billion in the 85 urban areas studied. The average cost per traveler in those 85 urban areas was $794. Costs ranged from $1,038 per traveler in "very large" urban areas down to $222 per traveler in the "small" areas—and all this with fuel costing far less than it does today. Of the 85 urban areas studied, 2.3 billion gallons of fuel were wasted, an amount that would fill 46 supertankers or 230,000 gasoline tank trucks. In urban areas with populations greater than 3 million, 1.5 billion gallons of fuel (more than two-thirds of the total!) was wasted. At $2.00 per gallon, that's $3 billion tossed out by drivers in stop and go traffic. During that same period the Outdoor Advertising Association of America (OAAA) reports advertisers spent $5.5 billion on out-of-home advertising. If outdoor advertisers had instead placed that $5.5 billion in ads using the present invention, they'd not only have put their money into a superior ad platform, they'd have been able to reimburse drivers for their wasted $3 billion and still have $2.5 billion left over to spend elsewhere.

[0019] Plenty of studies have been launched to figure out what to do about our worsening traffic, but few concrete proposals have surfaced. Certainly, no

proposals have emerged suggesting that we compensate drivers for their daily delays. Just the same, until we have a meaningful cure for congestion, the present invention can, to a degree, offset owners for their wasted time and money while they experience it.

[0020] MOVING OBJECTS

[0021] For as long as there have been moving objects, people have advertised on them. From early buckboards and stagecoaches to modern trains, subways, busses and aircraft, moving objects are the basis for corporate and self promotion, personal expression, identification and advertising. Today, it is not unusual to see cars, trucks, entire busses, even independently-towed trailers adorned with wraps or ads for products and services—many of these are backlighted to draw the attention of drivers and pedestrians while they parade down city streets nationwide. One of the world's largest advertisers, ClearChannel Outdoor, markets a variety of Taxi Tops for use in city traffic atop cabs. These come in various sizes and in two, three or four sided models which are typically backlighted to display graphics at eye level to passing sidewalk or pedestrian foot traffic. Some of these have lenticular screens to create movement, built-in LED readout pads, or larger LED panels to produce scrolling text, or more elaborate displays with flash type animation. The latter can be optionally linked to an onboard GPS system so it can be programmed to show only on specific streets or in special areas of the city. On these displays, ClearChannel's clients control the content, not in real time, but well in advance of street exposure. ClearChannel also offers a 14" x 36" flat, bolt-on trunk mounted sign which is positioned more or less at eye level to following motorists. ClearChannel's Taxi Media division refers to these as advertising "tonnage" since the car behind will view the same static, print ad for 5 to 20 minutes (the time a vehicle spends behind it in traffic in such places as New York City).

[0022] Another company, MotionLED, sells a long, slim LED panel which can be attached with suction cups to the interior of a vehicle's windows where it can scroll text messages horizontally, similar to those present in retail stores.

These units are available in four lengths, from 8 to 40 inches, and in a choice of lettering in one of three colors. All of these are piecemeal efforts toward the presentation of advertising messages in public spaces and represent little more than a "shotgun" approach to demographic targeting. Advertisers using these techniques can only hope they will get exposure in the right part of town or at the right time of day and to people who may be inclined towards their product.

[0023] DISTRIBUTION

[0024] Madison Avenue is working aggressively to convert its costly, labor-intensive and still largely paper-based process of buying and billing media. Even the Internet has yet to develop the crucial rules of business or programming schemas for buying and selling online that Madison Avenue truly needs. A recently released status report compiled by the American Association of Advertising Agencies (AAAA) shows that the Internet has achieved only one out of nine essential steps for conducting all electronic advertising, giving it the worst "discrepancy" rates (the percentage of advertising buys that don't run as originally ordered) of any major medium. That puts the Internet on par with out-of-home, radio, and network TV as the least progressive electronic business trading partners. Even the most analog of all media—magazines and newspapers—have made greater electronic business strides than the Internet and are today capable of at least taking orders electronically. The advertising community needs to engage in a massive combined effort before it can claim independence from the labor-intensive manual steps of paper processing and human input which drives up the cost of media buys and produces accounting inaccuracies. The present invention represents not merely an ad platform to deliver hyper-relevant content, but is one which is totally electronic from the ground up, integrating creativity, distribution, tracking, measurement, engagement, accountability and compensation into a single, verifiable, automated closed-loop network. As comprehensive and seamless a system has been previously unheard of in the world of contemporary advertising.

[0025] TELEVISION

[0026] Advertisers place ads everywhere from skywriting to urinals and from grocery store check-out dividers to the fruits and veggies themselves. However, it has always been the full motion video display that delivers the goods. Advancements in flat screen technology have allowed displays to creep into elevators, gas pumps and restrooms—wherever someone with a need to pause for a few seconds is present. Just as relentlessly, marketers are pursuing consumers who are on the move. With nearly 200 million U.S. subscribers to wireless services, marketers are wondering if ads beamed to wireless devices such as cell phones, Blackberries and hybrid devices will evolve into a viable media platform without upsetting their users. Some have referred to GPS cell phones as "the silver bullet" since they promise to let marketers send retail pitches to mobile users who might be in the vicinity of their stores. Chrysler Corporation is launching its own Mobile Phone TV Channel called "The Jeep Channel" which will actually run TV style commercials on cell phones.

[0027] From tiny screens to huge ones: ClearChannel's Outdoor Division and Digital Advertising Network, a Montreal provider of digital screen networks, have teamed to place hundreds of 4 x 16 foot video displays in shopping mall food courts across the country. Among other things, these will show the same kinds of 30-second TV spots you can see in your living room. And despite declines in viewership due to ad-skipping Digital Video Recorders (DVRs) and media alternatives such as the Internet, American viewers still spend between four and eight hours per day, per person, glued to their TVs—more than any other nation—but with Japan a close second. If these hours are spent watching commercial television, it's a fair guess they're watching about 15 minutes of commercials as well. Look again at the 2005 Urban Mobility Study Report. In the "very large" areas studied, there were 61 hours of delay per traveler per year, which is 219,600 seconds a year. In television ad terms that's nearly thirty 30-second commercial spots per day, and nearly sixty 15-second commercial spots each day. In Los Angeles, the numbers are

even better. Angelinos experience 93 hours of delay per traveler per year or 334,800 seconds a year. That equals 44.64 30-second TV spots per average day, or nearly 90 15-second spots per day.

[0028] MEASUREMENT

[0029] Getting a handle on who's watching what in terms of advertising is critical to proving the worth of a media platform. This need for proof has spawned a variety of devices, programs and companies—some are now household words—whose job it is to measure the existing ad viewer base. ClearChannel is evaluating Requests for Proposals (RFPs) looking for new electronic devices to measure its huge radio audiences. Arbitron, a firm specializing in ad measurement, has developed a device called a portable people meter (PPM), a passive electronic device intended to replace the old-fashioned paper diary methods of documentation. Nielsen Media Research, meanwhile, plans a "portfolio" strategy toward adopting devices to improve the accuracy of its TV ratings services, which today also measure the time-shifted viewing of DVRs, video-on-demand and other competing platforms such as the Internet and mobile media. In December 2005, Nielsen Outdoor delivered its first wave of out-of-home demographic data to reveal the most likely people to see advertising on billboards. Nielsen convinced respondents to wear GPS-equipped pager size devices called Npods, then combined their respondents' traffic patterns with a map of outdoor advertising sites to determine who passes what kinds of outdoor ads, and when. Nielsen's data does not provide demographics on a per user basis for individual outdoor sites; it only gives advertisers a sense of what consumers could have been exposed to and roughly how often. The methods for gathering and applying ad measurements are woefully lacking in an industry that, in other respects, is mature and widespread.

[0030] Fundamental to ad measurement is defining what constitutes an "impression" or a "view." Special software has been created to measure billboard views. Systems for television identify the number of household impressions, the time of day video-on-demand (VOD) programs are viewed

[0031] The present invention does not have these problems. First, the present invention is not inserting commercials into an entertainment stream, it is showing ads exclusively. Secondly, since every showing is essentially "requested" by an electronic device on one moving object or another, all such requests and completed deliveries are confirmed as they occur and are logged for later downloading. Such integral measurements reveal what content was viewed, precisely where it was viewed (based on GPS data), when and by whom it was viewed (in significant demographic detail), and for exactly how long. The system also documents whether or not any impulse information was requested or if any purchases were made as a result of the viewing. Finally, the system can the track geographic movements on the part of moving objects after content viewings to confirm local area effectiveness—for example driving to a specific hotel or restaurant immediately after seeing an ad for it. Furthermore, every content request—whether or not it resulted in a confirmed delivery—is recorded on the hard drive of every involved moving object. This means that a detailed 24-hour map—a "data snapshot," if you will—can be

reconstructed to tell marketers where consumers went, when they went, who may have been with them at the time, what they were looking for as they did and whether or not in some cases they found it. To the best knowledge of the Applicant, to date, no other organization, system, means or technology has conceived or proposed offering such an exacting and automated capacity to deliver, measure, collect, process, assess, re-create, distribute, confirm, and then measure again the absolute effectiveness of conventional or hyper-relevant advertising and other types of consumer content on such a widespread scale and, in addition, to reward the average consumer for so doing.

[0032] TARGETING

[0033] Geo-destination targeting is a process of combining IP-based targeting—a very common technique that allows advertisers to target ads based on the location of a user—with, for example, information about the city a user is searching for. For example, if a user in San Francisco is searching for an address in Austin, Texas, online marketers can target airline ads advertising cheap fares from San Francisco to Austin.

[0034] In the same way, the present invention can poll information from a moving object. For example, by using its onboard GPS Navigation system with its selected destination and route and then coupling that information with an owner's stored profile, a wide variety of highly directed ads can immediately be triggered for presentation on any of the moving objects it might encounter en route: retail stores of high interest, restaurants with favorite foods, hotels, trip stops or other points of interest that are known to meet his or his family's preprogrammed interests. Additionally, if onboard data indicates a history in searching out or purchasing certain kinds of items, such as men's leather boots, for example, and the traveler is passing through a town where there is a manufacturer specializing in fine leather boots, the present invention can "borrow" the displays of surrounding objects as the traveler nears town or passes through it, and call that fact to his attention. The providers of those borrowed displays will be compensated in kind for their use.

[0035] BEHAVIORAL TARGETING

[0036] Behaviorally-targeted advertising is a way for marketers to get better aquatinted with their buyers. The Internet allows researchers to track buyers after the fact, to measure the things they look at, browse through or order. When they go back for more they can be "retargeted" with relevant advertising, relevant because they've already expressed significant interest in it, or perhaps in something related to it. Retargeting is used to cross-sell customers who previously bought something, or to contact prospects again in an attempt to lead them to a conversion event, such as a sale, a download or a newsletter signup. This works better with some groups than with others but it's another way for potential buyers to tell potential sellers who they are and what they want through their actions. Why not take this idea to the next level—as with the present invention—where buyers and sellers actually cooperate in such an exchange and where each side benefits greatly from the effort?

[0037] BUZZ TARGETING

[0038] Nielsen BuzzMetrics, a company which specializes in the measurement of consumer-generated media and word of mouth, claims, "In a world where word of mouth is on steroids, marketers need to focus just as much on the negative buzz as on the positive," then goes on to characterize most advertisers as "ill-equipped" to respond to the quick-acting blogospheres so famous for churning out bad news at prodigious rates. The real 'read-between-the-lines' news here is that today's consumers are quite willing to speak out, and speak out loudly, about having better products and services. In other words, when it comes to understanding their customers, advertisers no longer have to be reactive, they can be proactive. They can ask. This is something marketers have not often bothered to do. Learning what buyers really want and really care about—what truly turns them on—and using that to mutual advantage is a critical part of the present invention.

[0039] INTERACTIVITY

[0040] Remember the last item on the list of advertising holy grails? Buy at the

push of a button? XM Satellite Radio is preparing to ship portable MP3 players that will do just that, at least for music. A deal with Napster lets users push a button to "bookmark" songs they hear, and then the next time they dock their player with their computer it automatically buys those songs over the Internet. This is possibly the start of a trend. The present invention, however, goes a few steps further, thanks to a totally integrated advertising and distribution infrastructure. When users in moving objects in the field see an ad that intrigues them, they can push a button to get immediate information (such as pricing and availability), or they can request other things such as having a brochure sent to their computer. If they really like what they see and hear, however, they can buy the item on the spot. No need to dock with the Internet to complete a transaction, because credit and shipping have all been set up in advance, as will be explained later. You can even request a day or two to change your mind before the product ships. Imagine you're major film studio releasing a big movie for the weekend. You've budgeted a substantial ad spend to promote the grand opening with significant print and TV spots to generate excitement. How would you like to be able to deliver a mind-blowing 30-second trailer with surround sound to 100,000 teenage boys driving at 6:00 PM on a Friday night just as they're trying to figure out what they're doing that weekend? Then follow it up with a push button opportunity to have tickets waiting at a theater just minutes from their precise locations along with an electronic discount at a nearby Burger King? The present invention allows exactly such a promotion to be executed, both instantly and seamlessly.

[0041] THE NEW CANVAS

[0042] Computer and display technologies are considerably more advanced than the world of advertising which uses them. Liquid crystal displays (LCDs), Plasma and Digital Light Processing (DLP) have hit their stride and, although they are still expensive for many consumers, they are today produced in volume and their costs are falling. LCDs were invented around 1963 and were first intended as slimmed-down replacements for bulky CRTs or as screens for wall mounted TVs. Scaling up to large surfaces, unfortunately, was a problem.

Instead, LCDs became the standard display for everything from watches to laptop computers and, as is commonly known, are rapidly replacing conventional lighting including brake lights and tail lamps on production automobiles.

[0043] A newer product, Organic Light Emitting Diodes (OLEDs), pioneered and patented by Kodak/Sanyo, now promise that original vision with higher levels of brightness and sharpness not possible with previous technologies. OLEDs are self-luminous but don't require the backlighting, diffusers or polarizers required by LCDs. OLEDs consist of two charged electrodes sandwiched on top of organic light emitting material, which eliminates the need for mercury lamps and yields a thinner, lighter display having very low power consumption. These displays are tough enough to use in portable devices and automobiles, can be viewed at angles up to 160 degrees and are able to produce clear, distinct images, even in bright light. OLEDs also produce high image resolutions, and because each pixel can be turned on or off independently, they can create multiple colors in a very fluid, smooth edged display. They are 20% to 50% cheaper than LCD processes yet utilize plastics that make them tougher and more rugged. Manufacturers claim processes that are akin to the "printing" of newspapers and anticipate panels that are bendable and potentially formable with no inherent barrier to large size glass and displays. In other words, these should be very cheap in the future.

[0044] Meanwhile, scientists at the Fraunhofer Institute for Applied Polymer Research (IAP) in Potsdam are making OLEDs transparent. While metal oxide coatings in earlier OLEDs made them opaque, researchers are investigating transparent physical properties. Such displays can be switched on and off to create graphics or video on demand, embedded in normal glazing. Because these new panels interfere little with visible light or views, their development is ideal for such applications as heads-up displays in car windshields or for the kinds of displays anticipated by the present invention. Of significance is that under the proposed business model, capital investment

will become available to refine processes and develop the necessary production equipment for the earlier supply of OLED displays on a cost-effective basis, volume-matched to an established and mature transportation industry.

[0045] GOVERNMENT AGENCIES

[0046] It may be beyond the practical scope of this document to assess all of the potential areas of interface with respect to the U.S. government and the present invention. Although the U.S. government has many ongoing programs relating to moving object telecommunications, the applicant is unaware of any specific government prior art that would conflict with this invention. One envisions the government's role as essentially responsive and supportive towards the present invention by providing or assisting in the aspects of technical assessment, rulemaking, the creation of new standards and legislation. There are areas, however, where the U.S. government is independently or with private contractors exploring programs where the intent or results could overlap and lead to similar conclusions or cooperative implementations. Here are three such examples:

[0047] 1) The U.S. Department of Transportation has launched its Intelligent Transportation System (ITS) program, designed to improve transportation safety and mobility and enhance productivity through the use of advanced communications technologies. ITS encompasses a broad range of wireless and wire line communications-based information and electronics technologies which, when integrated into the U.S. transportation infrastructure and into vehicles themselves, should relieve congestion, improve safety and enhance American productivity. One such ITS study involves the creation of a LIGHT VEHICLE FORWARD-LOOKING, REAR-END COLLISION WARNING SYSTEM for eventual integration into passenger cars worldwide. This study attempts to establish guidelines for the creation of a driver warning system which can prevent or reduce rear end collisions.

[0048] In some respects the proposed system is similar to the present invention in the sense that it proposes the use of a forward looking proximity

sensing technology to read the speed of a vehicle in its forward path, calculate the range and closing speeds and then issue an 'impact warning' or a 'following too close warning' if conditions warrant, one that will be noninvasive to the driver of the following (host) vehicle. ITS properly assesses the available data on driver inattention (some of which was previously taught) but then fails to make recommendations consistent with its own and common findings. For example, Section 3.2.1, Background for the ITS guidelines, states: "The primary rear-end collision causal factor is driver inattention to the driving task (approximately 66% to 77%). Driver inattention in this context includes both inattention and distraction. Drivers are constantly scanning the roadway environment (i.e., looking down the road, left side, right side, scanning the mirrors and attending to internal and external stimuli). Drivers can only focus well on one thing at a time because the eyes focus together. So, for example, when drivers are attending to other stimuli they may not be able to adequately perceive the roadway in front of the vehicle. It is often necessary for drivers to take their eyes off the roadway and "attend" to other stimuli when operating in-vehicle controls and possibly carrying on conversations. Often drivers use multiple glances to attend to other stimuli thus taking their eyes off the roadway. These glances distract the driver and lead to inattention to the driving task. The glances may be momentary or of extended duration. Driver distraction accounts for approximately 11% to 24% of driver inattention. Drivers can also exhibit a behavior where they are focused on the roadway ahead but don't perceive the changes that are occurring. This "looked but didn't see" phenomenon is also indicative of driver inattention. This is similar to the previously discussed problems resulting from distractive advertising.

[0049] Unfortunately, ITS, in its recommendations, goes on to assume a very common solution found in various moving objects such as aircraft, trains or other types of machinery: that of installing a prominent visual warning indicator on the instrument panel of the vehicle, possibly augmented by an audio and a haptic (force feedback) warning, or a thumping on the throttle pedal. In other

words, at a time when an inattentive driver is supposed to be re-engaging his thoughts and responding to an intense vehicular situation on the road ahead of him, his attention, based on ITS recommendations, is being diverted by yet more visual, audible and physical stimuli. As noted hereinabove, researchers have determined that new or unexpected stimuli trigger involuntary responses, and the more bored or unfocused we are, the more susceptible we are to these surprises. Also discussed above is the phenomenon of computer users performing search tasks, such that the more their attention is directed towards the periphery of their desired focus, the less they focus on the middle of their screens or the meaningful target. Imagine a warning light goes off on the on the instrument panel accompanied by an audible warning and a thumping on your right foot. Your natural impulse may be to look first at the light then possibly towards the floor until you collect your thoughts and by then, based on studies, the prospect of overreacting is high. All this when your attention should be outward on the car in front of you which represents an imminent collision. We've also learned that new, moving and looming objects command attention and that the onset of motion triggers overriding or urgent attention, possibly tapping the survival instinct, and also that changes in color can capture attention. But interpreting this as a potential solution is overlooked by ITS' engineers. We have a long and effective history of putting brake lights in prominent locations on vehicles that might stop quickly in front of us. It works. Perhaps a more natural and less distractive solution would be to utilize rear-facing video displays on the vehicles in front of us—as taught by the present invention—to provide color and graphic transitions for 'following too close' with more intense warnings or warnings with more impact (supported by the audible cues) upon more imminent potential collisions. Such a warning would audibly alert a driver to a situation which would be supported by directing his visual attention precisely where it should be to avoid an accident. This would be enabled by a similar proximity technology that ITS is proposing, then adding a returning wireless signal to the leading vehicle.

[0050] Upon full implementation, the present invention represents a more

effective solution to the ITS proposed collision avoidance and 'following too close' visual warning since it provides a means to trigger and present attention-grabbing color and light changes prominently on the aft surfaces of moving objects which are in certain modes designed to capture the attention of the operators of following moving objects. It is the intent of the present invention to facilitate numerous such novel safety solutions and these are further explained in the subsequent text.

[0051] 2) The U.S. Emergency Alert System (EAS) was designed by the Federal Communications Commission so that important emergency information could be sent quickly to targeted specific areas. EAS alerts not only broadcast media but also cable television, satellite, pagers and new forms of digital technology such as Direct Broadcast Satellite, High Definition Television, and Video Dial Tone. FCC rules have required broadcasters to monitor at least two independent sources for emergency information, ensuring that it is received and delivered to viewers and listeners in a timely manner. However, technology has moved on. Today, significant new methods are available to improve the capabilities of the present EAS. Satellites can be used to deliver EAS messages within seconds with high available levels of security without the geographical limitations of today's EAS. The Internet is a further impact-worthy technology since it offers redundant or back-up path communication with valuable follow-up capabilities. However, a private study on EAS effectiveness, completed in 2002, identifies three main concerns preventing EAS from becoming a truly effective system. One is that there is no concerted government or industry effort that combines EAS and other alerting techniques with existing and new technologies such as wired and wireless Internet, cell phones, PDAs and pagers to form a combined and seamless warning system. An FCC Report from the same period allocated increased numbers of EAS event and location codes so that local emergency managers and law enforcement officials could plan vastly improved local emergency public information warnings. Those new codes, according to the report, could lead to valuable information displays that are not currently

connected to the EAS, such as changeable highway message signs. Every state, county, part of a county, and offshore (marine) area, has a specific number and hundreds of allocated numbers are unused. These could effectively identify unique areas or zones for hazardous weather conditions, nuclear power plants, military bases, neighborhoods or even groups of individuals such as police, firefighters, FEMA or other personnel, provided that the equipment is in place to facilitate those communications.

[0052] One aspect of the current invention is that any moving object so equipped becomes, in fact, a rolling billboard, well suited to delivering location-sensitive, real time information to other moving objects within the area. Weather information such as flash flood, tornado or hurricane warnings or on the spot highway information such as traffic conditions, detours, road-out, or turn-back situations.

[0053] 3) In a similar effort, Motorola recently signed a contract with The Michigan Department of Transportation (MDOT) for what Motorola calls a "Wireless Super Highway" program. The project represents an initial deployment of a wireless network aimed at supporting the previously mentioned U.S. Government Vehicle Infrastructure Integration (VII) initiative. Motorola and the State of Michigan are exploring ways to establish a roadside network that can reduce accidents and road congestion by wirelessly connecting vehicles to the roadside and to other vehicles. MDOT is helping to fund the deployment of Motorola's system in Southfield, Michigan, as part of the State's ongoing investment in real-world testing of practical Vehicle Infrastructure Integration applications. MDOT is also supporting the research and development efforts of private sector firms as well as Original Equipment Manufacturers. Motorola's vision of wireless future roadways includes: vehicles that could detect potholes, ice-patches or other road hazards, then wirelessly transmit that information to other nearby vehicles so that they can avoid the hazard; and a panic brake alert application that can operate in foggy conditions and in which trailing vehicles could receive an in-vehicle alert recommending they brake immediately. Government and private industry

projects like these could share, utilize and benefit from the present invention because its parallel development and mass-market deployment will be driven by private investment in commercial advertising and in the development of personal media platforms that promise new incomes to consumers or the equivalent of new production vehicles that are less costly to operate.

[0054] INTEGRATION

[0055] We see an advertising industry in relative disarray, desperate to develop new platforms in the aftermath of falling numbers for old media (like TV) while chasing after the new ones (cell phones and iPods) like gadget freaks at the local Best Buy. All the while the solution has been staring them in the face: capture consumers on their drives to and from work each day. This is perhaps the "4th screen": a unique media platform totally dedicated to the display of ads. For a truly dedicated platform, however, integration must occur at a variety of levels:

[0056] 1) Advertising. Advertisers can start by cleaning up their own act by a) electronically developing a new creative alliance with the public and by connecting their creatives and managers to that pipeline, and b) incorporating distribution, measurement, consumer feedback, tracking consumer engagement, content delivery accountability and compensation into a single automated system.

[0057] 2) Manufacturing. As previously explained, the technology exists today to fully implement the present invention. Making it cost effective requires the acceleration and integration of manufacturing processes appropriate to the higher volume production of OLED displays to ensure even lower costs and permit mass-market installations on moving objects across the board, industry wide. Even here, proper integration must be thoughtful and paramount. In terms of traditional components, the present invention has the capacity either to replace or to incorporate into a single revenue-producing part for automated manufacture the following items from standard automotive production: tail lights, turn signals, brake lights, back up lights, license plate light and side marker lamps including their molded/metalized plastic housings, reflectors,

lenses, bulbs (or LEDs), gaskets and connector seals (2 per side), center mount stop lights, vehicle brand and model logos or graphics with attach hardware; panel finishes with decorative trims including primers, surface preparation, finish painting, molding or plating; license plate recess structures and lamp mount assemblies, attach points and frames; and, finally, the independent stamping, painting and distribution of license plates and plate frames together with annual DMV registration sticker production, distribution and consumer attachment, together with all overhead, shipping, assembly and direct labor related thereto. How nice to be able replace all that with a single part that not only launches an industry, but puts money back into a new car owner's pockets in an age of skyrocketing fuel costs.

[0058] 3) Government. As previously discussed, there are numerous programs where development of the present invention can enhance or enable better solutions to current government programs. Of greater importance is government participation on proposed standards, rulemaking, legislation and compliance. It is in the best interests of all concerned that the use of the present invention as a rich, mobile communications resource is exploited beyond mere marketing. It should be developed, from the outset, as a highway safety system in its own right by coordinating the interests of such government agencies as the National Highway Traffic Safety Administration (NHTSA), the Federal Highway Administration (FHWA), the National Telecommunications and Information Administration (NTIA), the Research and Innovative Technology Administration (RITA), the National Oceanic and Atmospheric Administration (NOAA) and National Weather Service (NWS), and the Bureau of Transportation Statistics (BTS), as well as other international agencies and commissions. This ensures commerce and system compatibility across the board and across borders, in terms of highway signage, hazard and weather warnings, vehicle identification and signage, vehicle lighting and safety systems and public service announcement and alert networks such as the EAS, to name but a few. For the same reasons, the U.S. Armed Forces may need to be peripherally involved. The coordination of state and local agencies

to incorporate standards for police, firefighters and similar first responders as part of a versatile and failsafe mobile communications system is just as important as the involvement of the Federal Government. A tall order, but considerably simpler than reaching the same levels of consensus and production readiness as were necessary in areas such as vehicle standards for crashworthiness, fuel economy and emissions.

[0059] 4) Financial. The integration of financial interests is critical to getting a project of this magnitude launched. Commercial advertising is clearly the financial driver so it is reasonable to expect significant investment, directly or indirectly from the world of large corporate advertisers and their agencies along with companies having core stakes in communications, transportation or media. As is later explained, governments are likely to contribute to the development of segments they feel is in the best interest of the public or in areas that are in line with their agency's charter, programs or objectives. A third leg in investment may come from the individual motor companies, who will appreciate that the sale of moving objects which can also generate incomes for their owners (and is therefore tantamount a product having a lower cost of operations) is likely to gain favor with the consumer and that competition could quickly drive acceptance of products incorporating the present invention industry wide. A final leg of support will come from one or more of the major communications or outdoor advertising companies that will emerge as gatekeeper for this new platform. The real money will be in content Distribution and Compensation.

[0060] 5) Compensation. The present invention introduces a novel and powerful means to reward the entire driving population, from the beginning student driver to daily commuters; from carpools to commercial fleet operators; and from the lowest income drivers to the wealthiest, delivering to all an ability to earn income as they sit in traffic, or alternatively, to lower their costs of transportation by allowing the use of their personal assets in a profitable public forum. In terms of market size for the present invention, the applicant envisions an orderly phase-in of video-equipped moving objects, with

ultimate market penetration limited only by the total numbers of moving objects produced worldwide.

[0061] COMPENSATION

[0062] There are certainly instances where the driving population has been enlisted to promote or advertise products and services using their personal vehicles for profit. These have been limited in scope and technology, are costly, relatively inconvenient and generally inconsistent with average consumer lifestyles. The method involves paying drivers to wrap their personal cars in ads touting products such as ice cream, juice bars or Internet services. The driver's job is simple: drive to and from work, pick up the kids, run errands—and be willing to operate as a traveling billboard. Some companies offer drivers the free use of a new ad-wrapped car, while other drivers are paid $300 to $400 a month to allow the wrapping on their own vehicles. Critics call it another example of creeping—and creepy—commercialism. As mentioned previously, taxi owners in some major cities are being allowed to place ads on the outside of their cabs. Leasing ad space in this way provides taxi owners and drivers with additional revenue which helps them offset the costs of adding wheelchair-accessible vehicles and similar mandated requirements. Cab owners and the drivers who lease them split revenues from the advertising, which has been estimated at around $400 per car per month.

[0063] As will be seen in a later description of the present invention, registered owners of appropriately equipped moving objects may be similarly compensated, but through a novel combination of private and public entities which control content and monitor compensation, operate automated accountability systems and integrate multiple media resources, financial partnerships and transportation support industries. Ironically, the huge revenues and personal incomes promised by the present invention are made possible by the very thing that causes millions of drivers each day to waste their precious time and money: traffic congestion.

[0064] CONCLUSION

[0065] Madison Avenue, up to now, has been reactive instead of proactive. It hires other entities to follow up after the fact to determine whether or not their content was actually delivered, and if it was, whether or not it went to the right parties. It has no effective procedures in place for judging ad "performance" (other than post analysis assumptions by creatives and the evaluation of sales) to determine what, if anything, the public thinks about the content they believe was delivered. Madison Avenue is about creative guesswork. It's about "following" media technologies rather than leading them. It would be extraordinarily advantageous for marketers to have a channel through which consumers could actively or even passively inform advertisers about the things they truly want to see and hear, for advertisers to fill those channels with content about products and services consumers really want and need, and to provide this content at a time and place of the consumer's choosing. For the first time in advertising history, the present invention enables a self-monitoring mobile network in which consumers can request specific content; view it, hear it, accept, reject or praise it; provide immediate and direct feedback on that content to the creatives and managers involved; and allow those creatives to modify and resubmit that content for distribution. Marketers are able to receive real time confirmation on that distribution along with priceless data on its engagement, effectiveness and acceptance, and the presenters of that content are financially rewarded on a per ad, per screen basis for the use of their platforms just as though they were partners in the same industry, which they are.

[0066] The applicant is unaware of the existence of any commercially-viable system capable of generating revenue for the general driving population through the display of targeted or hyper-relevant video advertising on moving objects which is governed and controlled by stored database profiles in other moving objects. Nor is the applicant aware of any single, closed-loop ad platform which allows consumers to request specific kinds of content, to distribute that content, to confirm delivery of that content, to measure its effectiveness, to account for and compensate such deliveries, and to create

new content based upon direct consumer feedback and confirmed in-field performance. The present invention offers a unique opportunity to turn around the status quo in the world of advertising. It promises new channels of communication with consumers, new sources of public and private capital for investment plus significant ROI with shared revenue to the driving population. It further promises the alignment of multiple essential industries for the manufacture of unique video displays, the improvement of moving object safety and cost effectiveness, the environmental clean up of transportation corridors and the sharing of just compensation with the owners and operators of a new kind of mobile communications and advertising platform.

SUMMARY OF THE INVENTION

[0067] The present invention describes a system, apparatus and method for obtaining revenue through the display of either conventional, targeted or hyper-relevant advertising on moving objects which receive, store, poll and extract data to present ads and other types of information based on the time of day, their location and their movements relative to other objects in a specific environment, and where data and information stored in moving or mobile objects within that environment can be transmitted between said objects, or to stationary objects where it is then received, polled, extracted and used to enable and control such displays for which the owners of those objects are then compensated. A proposed embodiment describes the development, production, deployment and operation of an integrated audio/video and data communications system capable of presenting hyper-relevant commercial advertising with synchronized audio, real time road, weather and emergency alerts, personal, fleet or government communications, mobile signage as well as vehicle branding, illumination and safety systems on and between moving objects. The business model portion describes a means for business development, technological adoption, funding, rulemaking, certification, media creation, content distribution, consumer utilization and user/owner operations and compensation. The apparatus section defines the placement of lightweight video displays on or integral to the body panels, exterior finishes

and/or glazing of both moving and stationary objects with an electronic means for the wireless transmission of stored, encoded user profiles containing the ad viewing preferences for the occupants of one moving object, to the receiving system in another moving or fixed object. The system enables the display of hyper-relevant ad content with synchronized remote audio, personal messaging and public service alerts on surrounding objects and provides for the real-time logging and later downloading of data to confirm communications and content deliveries between objects, track and measure consumer engagement, verify consumer's direct responses to ad viewings with accountability systems for moving object owner/operator Just Compensation. The invention further enables the widespread, non-invasive, profile-driven, ad hoc collection of privacy-compliant data for research purposes relating to consumer movements, travel patterns, buying habits, interests, needs and preferences.

[0068] The present invention also defines a high-volume production solution in which data and information contained in objects moving within the environment can be transmitted, received, polled, extracted and used to control or modify the audio and video output on viewed moving objects based on the viewer's specific interests, preferences, habits and needs, the needs or conditions of the environment or the requirements of those who are responsible to monitor safe and secure movements within it. It further describes a means for the low cost conversion of production vehicles so they can display video and transmit synchronized audio to other vehicles. Considerations regarding the apparatus involve the placement of video displays on or integral to the body panels of existing production vehicles, exterior finishes and/or glazing with an electronic means for receiving, storing, queuing and displaying ad content, and for the wireless transmission of stored audio or audio codes to a viewing vehicle's internal sound system. The present invention also includes a method for compensating the owners of moving objects for the use of their assets as mobile advertising and communications platforms and further defines a means to generate revenue

from the ad hoc collection of hyper-relevant data through the deployment and use of those platforms.

[0069] By allowing an object to learn a little about your personal history, background and experiences, together with a little information about your short or long term goals, needs or desires and by then granting that object—whether the object is small enough to carry in a pocket or purse or large enough to ride in—permission to passively convey that information to other nearby objects at certain times and places in your life, you permit those other objects to interact with you or with your own object and your own life in a way in which the net experience can enhance, enrich or inform. Focusing for the moment on a single embodiment of the invention—and on a moving object which is large enough for people to ride in—one can envision a scenario in which an individual (or a group of individuals) riding in such a moving object which, as just suggested, possesses some information about the people it is carrying—for example, a little about "who they are" and "what they want"—and in which that object can transmit that information to other nearby objects (whether those objects are mobile or fixed). Once those nearby objects receive and process that transmission, they can respond by presenting very special information of significant value to the individuals riding in the first object. Imagine, in the above scenario, an individual seated in such a land-based moving object who is viewing the road ahead. Let's assume he is also controlling or guiding his moving object so his eyes are where they are supposed to be: on the road and on any moving objects in his path. Assume the object in which he is riding now transmits unique information concerning his personal interests, needs, habits, or experiences, then passively, but without disclosing any confidential information, additionally transmits general data about who he is (age, sex, marital status, educational level, occupation, number of children, area of residence, etc.) combined with a little information about the moving object in which he is riding and its recent movements, to another object or objects nearby. If the information is received by a similarly equipped moving object, that object can now process that information and

draw from an internal library of stored data, data that is of unique interest or of significant value to the individual who is in another object which is following and watching. For example, if data stored in the library of a moving object ahead is converted into a digital signal containing audio information and is transmitted wirelessly to a moving object that is following, then the individual who is inside the following object can be immersed in audible sounds that are of genuine interest and value to the individual(s) inside. If that library data is processed into video information and is then delivered to a video display positioned prominently on rear portions of the moving object ahead, then the individual seated at the controls of the following object can also see images displayed on the object ahead of him which can be further synchronized to the audio information, all of which is derived from the information transmitted from his own moving object, and which is therefore of great personal interest or value. Thus, a set of carefully prepared preferences in the form of personal information transmitted from one moving object to another, or to fixed objects nearby, can—when combined with data relating to the environment and the movement of the objects within it—trigger or enable many forms of audio visual imagery that can address the previously mentioned twelve objectives in commercial advertising. What if such transmitted and displayed audio and visual information is not merely based on a person's preferences and moving objects, but on the conditions of the surrounding environment itself? Once again, in an independently controlled, land-based moving object—one which might be negotiating a highway or following electronic guideways or tracks—if there were a serious slowing or blockage of other moving objects or a hazardous condition ahead, that information could be received by one or more such moving objects and could then be simultaneously and prominently displayed on those other moving objects or on nearby stationary objects, thereby alerting all occupants and observers to any local and potentially serious conditions. Such displays might simultaneously alert the operators of moving objects in foggy conditions to the slowing of multiple vehicles some distance ahead, to the presence of detours, one-way traffic, icy surfaces, flash

flooding or tornados, or to conditions such as landslides, a bridge out or extended construction. One way to do this is by displaying a graphic and pictorial message on the display surfaces of the moving object immediately ahead. In one such example, information triggering such an audio or visual presentation might come from a wireless signal targeting a specific geographical point or route, or from a broader signal that might blanket an entire town or part of a city. Triggering information could also come from previously downloaded instructions or from a preprogrammed internal resource library able to interact with the Internet or with the navigational system of an individual moving object. Thus, at a predetermined time and place during its travels, moving objects could display critical information, alerts or warnings either to or upon other moving or fixed objects in the environment which could then be viewed by the occupants of those moving objects or by individuals in the immediate area (such as pedestrians or foot traffic) or by other means (such as traffic monitoring cameras) capable of viewing such moving objects from remote locations. Although this latter kind of audio visual presentation might at first seem similar to on-board GPS navigation systems, which place prerecorded audio/visual content on displays inside a moving object, the visual content of the present invention is displayed on the outer surfaces of moving objects or on nearby fixed objects—generally at eye level or within clear line of sight of the moving object's operator as in the case of a land-based vehicle—and is therefore generally intended for viewing through the windows of another moving object or from outside of a moving object. Thus, the location of the display of the present invention can be considerably more effective and a great deal safer than displays located along a roadside or on the interior of a moving object, because operators do not need to take their eyes off the other objects moving in their paths to focus on the interior of their conveyance or to focus and track signage, illumination or warnings that are stationary at roadside. This is the reason we put brake lights on the moving vehicles in front of us, and not on a warning light on our vehicle's instrument panel. Moreover, such video presentations are timely and reflective of

immediate conditions since they can be electronically updated, deployed, triggered and displayed instantly and in real time wherever there are appropriately equipped moving objects. Further, when such images or sounds are generated using interactive onboard database libraries they can be modified in real time to incorporate the needs and characteristics of both the moving objects and their operators. Importantly, all such content is monitored for safe and timely presentation because all delivery is ultimately controlled by the speeds and relative motions between moving objects themselves, the specific locations of those objects in the environment and the condition of the environment itself.

[0070] If moving objects are able to exchange data sufficient to enable conventional, targeted or hyper-relevant audio/video commercial advertising and time-sensitive, location-specific communications, then they can also display highly personalized messages and personal advertising, enable personal sponsorships, assist in law enforcement or emergency operations, produce a unique means for the branding of moving objects and offer many exciting opportunities for the lighting, operating and safety systems of moving objects and for their basic registration and identification. For example, a land-based moving object might display the name or logo of its owner's favorite sports team or political candidate, as a kind of "electronic bumper sticker". Another owner might display a promotion or an ad for his own small business and do it at precise times of the day or night and in meaningful venues, such as his home neighborhood or business or university campuses. By adding a means for law enforcement to communicate with moving objects and a method for the owners of mobile objects to communicate with their own property, lost, stolen or speeding moving objects would be able to announce their presence and alert others in the vicinity. Importantly, such displays will enable the manufacturers of moving objects to incorporate and periodically change the name, branding, functional designs or styling of their moving objects simply by modifying the electronic data controlling the content of its default display. Another significant improvement will come with the

introduction of an all-electronic system for the registration and licensing of moving objects. The display's ability to present powerful, well illuminated external graphics and nomenclature on moving objects and to further encrypt and link such data electronically to the moving object itself will result in a system where all moving objects, upon acquisition by an owner, will immediately be programmed to display identifying numbers (i.e., license plates) properly and prominently in accordance with set standards and such content would be updated each year if annual registrations are required. All such electronic procedures would be encrypted and documented to prevent tampering or hacking without otherwise triggering companion regulatory monitoring systems. One can see that such a system, applied again in the area of land-based road vehicles, could eventually eliminate the need for the manufacture, distribution, installation, maintenance, changing and/or replacement of vehicle license plates altogether. If such a system were properly and securely designed it could also prevent the theft and false use of such vehicle identification. Just as significantly, annual DMV registrations could be conducted solely online and paid registrations would be sent electronically via the Internet directly to vehicles themselves, eliminating the cumbersome process of printing, distributing and installing new registration stickers each year. However, by far the greatest benefit to the use of this invention is that it allows the operators of moving objects to keep their eyes, their focus and their attention on the other moving objects in play around them, and not on the ever-increasing array of brightly-animated billboards, roadside signage and other distractions competing for their visual attention. In fact, the present invention offers the distinct possibility of cleaning up the landscape by enabling significant reductions—and quite possibly the eventual elimination altogether of conventional signage and advertising in high traffic environments.

[0071] Using today's off-the-shelf technology, one could easily assemble an operating demonstrator of the described invention. However, it might be more expensive than necessary and would certainly lack the integration, legislation

and marketability vital to inaugurating such an ambitious and widespread program. To succeed, such an effort is likely to require an international consensus in, but not limited to, such areas as proposed rulemaking, legislation, testing, compliance, design, production and performance, in the realm of product development; the coordination of multiple national interests in terms of highway, airway or waterway traffic management, safety and infrastructures; general telecommunications, telematics and technology adoption as well as the integration of national, state and local environmental and weather services, to name but a few. Of equal importance are standards and practices for content, content display, delivery, distribution, engagement tracking, accountability and finance in the areas of advertising, and also coordinated developments in data processing, displays, telematics, body panels and glazing for the mass market production of moving objects on the international manufacturing side. None of this will happen without money and clear incentives to generate appropriate capital and cash flows to make this invention a commercial reality. It is therefore another prime objective of this invention to demonstrate not merely a capable and operable systems technology, but additionally a general business model designed to stimulate capital investment, the application of development funds, appropriate investment in R&D and the capital equipment necessary to produce cost-effective end products, the proper monitoring and effective use of those products or services and finally to foster a means and enable a system to financially reward all who participate, from the advertisers and agencies who will pay to use the invention's ad platform to the manufacturers of moving objects that will introduce what will be the equivalent of more cost-efficient moving objects as the result of incorporating this invention to the governments who will assure better and safer public services through the adoption of this invention to the new entity(ies) that will profit through the distribution of content through this invention to the many transportation support industries which, through partnerships, will enable fuel, insurance and other incentives to stimulate acceptance of this invention and, perhaps most importantly, to the

numerous fleet, business and general mobile population users who will ultimately offer up their private and personal moving objects to be used as public communications and advertising platforms for profit.

[0072] Commercial advertisers will continue to deal with selected ad agencies and will develop creative content in the same ways as they do today, but they will do it under the new industry standards and practices defined under the present invention. Content producers will continue to work with their ad agencies, creating end products appropriate to the selected media, then media buyers will purchase ad slots and schedule content, but it will be done over the Internet. Submitted content will be first reviewed for conformance to standards and practices and technical requirements, and then encoded for time, venue, and relative priority over other scheduled ads or content types. Once content is encoded, the best method for distribution is determined (cable, satellite, wireless), fees are attached, and the scheduled content is uploaded to the network. Distribution methods are discussed in the drawings, but in practice, final method for delivery may depend on the infrastructure available in the various markets.

[0073] Law enforcement and military and government-related public service content is periodically uploaded in a similar fashion, starting with quality and conformance standards for graphic content, followed by similar time, venue, and priority encoding over other types of content. Typically, government or public service content will have a display priority over ads. The triggering of public service alerts is critical and is sometimes accomplished through external systems. In the case of the roadwork alert which saved mom from a delay in her trip, generic audio and visual content was pre-loaded into her hard drive (perhaps at the factory) while actual triggering for the event was accomplished by an on-board GPS input having time and location constraints (a moving object entering a defined area at a certain time of day) or through a localized broadcast radio signal.

[0074] Fleet and business users such as taxicabs, delivery vans, or car rental agencies, or even large commercial carriers and government-owned and

operated fleets such as U.S. Postal Service vehicles or GSA carpools will submit specialized content under their fleet contracts. After similar approvals and scheduling, fleet and government content is uploaded via the Internet and is distributed to fleet parking or maintenance garages and storage areas in the same way as family, consumer, and commercial advertiser content is distributed in business, university, or mall parking garages.

[0075] It is anticipated under the present invention that law enforcement, fire departments, and perhaps even military users would be granted unique access, enabling these users to override any ongoing, in-field content displays in the interests of public safety. For example, if police in a land-based or airborne moving object were able to "take possession" of the video display on the exterior of a land-based moving object which is presumed to be lost or stolen, is involved in a car chase, or is posing some immediate hazard or threat to others or to the environment, such possession could release prerecorded data from the hard drive in that moving object—and in other nearby moving objects—so that visual warnings and other types of displays could appear prominently and simultaneously on a multitude of moving or stationary objects within the area.

[0076] The applicant envisions that, except in rare cases, all users would pay for the right, privilege, and opportunity to distribute content using the present invention and that a portion of these payments, after expenses, will be paid to the individual owners or operators of the various moving or stationary objects that comprise the ad platform and were involved in the delivery of that particular content. The present invention introduces an integral system of electronic accountability to assure this.

[0077] General consumers will pay for the distribution of their own ads and personal messages, even when such displays are on their own moving objects, although such personal use will likely be priced at a discount. Of course, such personal use reduces the opportunity for these users to earn greater revenue by displaying content for big brand advertisers over their own.

[0078] Professional advertisers will pay a premium to use the system,

especially during prime hours and venues. This parallels established norms in the industry which are based upon reaching specific markets at certain times of the day and in specific locations delivering a certain number of impressions to a preferred demographic. With the present invention, fees charged will be based on the going rates for the media type, content, and application, but with payments based only on deliveries that are electronically confirmed.

[0079] Government and public service users may have content distributed under special contracts or circumstances and such contracts might possibly use public funds.

[0080] Financially, the present invention is a little like offering stock in a public company. The company's shareholders own the moving objects—its communications platform—which is used from time to time to distribute the company's products. A shareholder's financial investment comes through his purchase, maintenance, and operation of his own transportation. His return on investment (ROI) comes in the form of a payment for services rendered or as a dividend based on the company's performance. The more a shareholder invests in the company—buying and using more moving objects or by using them more often—the greater his ROI. The larger the number of shareholders, the bigger the company's distribution network and the greater its potential for revenue.

[0081] However, earlier investment will be required from a number of resources. Seed money from a coalition of key entities who are those most likely to benefit from the new platform is likely to occur first. The advertising industry has the driving incentive and is the long term beneficiary; thus, early investment may be from the more entrepreneurial content producers, media buyers, and ad agencies, along with their large corporate clients, and finally the traditional competing major media platforms (television, Internet and outdoor). Next, the Federal and local governments are investment candidates, principally in supporting R&D, legislation, and in the operational areas of highway traffic safety, and public communications. Finally, the manufacturers of moving objects will invest in their own competitive design and development

efforts together with investment from government and transportation support industries such as petroleum, insurance, banking, computing, electronics, and telecommunications, along with State Department of Transportation Agencies and others.

[0082] The kinds of moving objects that will launch the system in a land-based embodiment are likely to fall into roughly four initial categories: 1) New Vehicle Production; 2) Pre Existing Vehicles (or aftermarket installations); 3) Vehicle Conversions (the replacement of existing body panels such as rear deck lids or doors on SUVs, minivans, or station wagons and truck tailgates) with their original body panels converted to accept the appropriate display technologies; and 4) Modular "add-on" packages suitable for use on trucks, trailers, RV's, motor homes, and on very old or unusual types of vehicles.

[0083] 1) New Vehicle Production in a preferred embodiment, a land-based moving object such as an automobile will contain a small electronics package that will interface with other on-board equipment such as GPS navigation, audio entertainment, and perhaps newer telematics systems, if available. This package will include a transmitter, which sends a wireless encoded signal with information on the vehicle type and VIN (or comparable identifying information) along with encoded user profiles or user codes which define the preferences and personal interests for each occupant selected, to moving object receivers or fixed object receivers within range. Signals may be broadcast in omnidirectional patterns, depending on the application, but in cases involving motor vehicle applications in traffic, such signals are most likely to be transmitted in a generally forward-looking pattern having a horizontal and vertical spread of from 15 to 30 degrees or that typically illuminated horizontally by a motor vehicle's headlamps. This spread may ultimately be governed by rulemaking, and could further be automatically adjusted by local road, personal preferences, or traffic conditions. The electronics package will include, on each vehicle, an antenna to receive such signals, a motion sensor to measure the speed of the receiving vehicle, a rear-looking proximity sensor to measure the closing speeds of any following

vehicle(s), and a decoder to process the signals transmitted from such vehicles. The package will contain antennas for receiving and transmitting information wirelessly from network access points (NAPs), an upload/ download transceiver, a central processor, and a hard drive for storing all information received that is downloaded from a network or is logged in the field as a result of intercommunication between various moving objects. When signals are received from similarly equipped nearby vehicles, they are typically in the form of user codes which define the nature of that vehicle's occupants along with their content preferences (as in the case of hyper-relevant advertising) together with information on the vehicle itself relating to a specific VIN and including specifications on the physical characteristics of that particular moving object. In most cases, these requests are used to poll the onboard hard drive in a viewed (or displaying) vehicle and to then queue the necessary content for a video display based on predetermined delivery protocols. Specific instructions governing the delivery of content are encoded with that content. Content can be stored on board a viewed vehicle, a viewing vehicle, or on both. Video content stored on a viewed (display) vehicle is normally queued and displayed from that vehicle's self contained hard drive storage medium. However, video content that is queued from storage in a viewing vehicle must be wirelessly transmitted to the viewed (display) vehicle for presentation on that vehicle's external display means (unless it is intended for an in-vehicle display). By contrast, audio content queued from storage in a viewed (display) vehicle must be transmitted wirelessly to the viewing vehicle for reproduction and playback over its internal sound system. Thus, in practice, and to avoid unnecessary short range transmissions of audio and video content, the system will first choose to store all content in all moving objects so that only user/content codes are transmitted between vehicles. In this way the video content itself is never transmitted to another vehicle, but is queued and displayed solely within the viewed (display) vehicle's system. At the same time, any audio content related to that display of video is queued, synchronized and released for audio reproduction over the internal sound

system of the viewing vehicle. All such presentations are controlled by the motion and proximities of the moving vehicles involved, their relative speeds, their locations and relative positions, the time of day, and a variety of other factors bearing on subsequent signals received from the viewing vehicles, from other vehicles, and from the environment, and those generated by the presenting vehicle itself.

[0084] 2) Pre Existing Vehicles are those that have been manufactured prior to availability of the present invention, or simply those without the invention; however, owners or users should be able to purchase, lease, or otherwise add versions of the New Vehicle Production package to such moving objects. Aftermarket packages do not need to add the video display portion of the technology unless they wish to earn money from the display of content. If they wish to view hyper-relevant content and/or control what they see and hear from moving objects using the full technology, they can buy and install a stripped-down version of the full production system. Such an aftermarket version would have the ability to receive, process, store, encode, and transmit data including content requests, VIN data, and user/occupant profiles or user codes. It would also have the ability to log content requests, information relating to the content presented by other vehicles, and its owner's responses to viewed content. All of this information remains stored on the hard drive of any Pre Existing Vehicle for later downloading to the network.

[0085] 3) Vehicle Conversions will involve installations of a New Vehicle Production package, but on a panel by panel basis in terms of the video display. Such installations are perfect for fleet or limited production applications like taxis or commercial vans, particularly those which operate in high-density traffic areas. The most cost effective way to implement such conversions is to isolate the display portion of the technology to body components which are easily removable or replaceable, and often set into their own easily serviceable shock mitigation mountings such as the rear hatches of SUVs or minivans, truck tailgates, and doors or trunk lids of passenger cars. The electronics package, proximity sensors, antennas,

receivers, and transmitters can be easily integrated into existing body structures. Indeed, such conversions for city transit and taxi fleets are anticipated as a form of beta-test and preproduction ramp-up and as market test deployments of the present invention.

[0086] 4) Modular "add-on" packages which offer full system capability (proximity and motion sensing, data transmission, processing and storage as well as displays) that can be "bolted-on" to large, unusual or older types of vehicles to allow their owners revenue generating potential are easily managed. Such applications would be for trucks and busses, or even large or medium sized fixed roadside signage or billboards under the right circumstances. Imagine a full-sized SEARS or WALMART truck-trailer rig carrying large panel displays with the company logo, which is also able to read the specific preferences and shopping interests of passing or surrounding motorists and then instantly queue and display products of genuine interest to them.

[0087] It is therefore an object of the present invention to provide a system and method for obtaining revenue through the display of advertising content and other types of audio/video information on the exterior surfaces of mobile objects which can receive, store, contain, poll, extract and use information for this purpose which has been transmitted from other fixed or mobile objects within its vicinity.

[0088] It is another object of the present invention to allow data and information which is stored in one mobile object to be transmitted to another mobile or fixed object in the environment where that data is then received, polled, extracted and used to control the display of ad content or other types of information on the surfaces of such other objects.

[0089] It is a further object of the present invention to display and permit the viewing of such displays at precise times of the day and in exacting geo-locations, further governed by the relative speeds, angles, proximities or movements of other moving or stationary objects within the environment.

[0090] It is another object of the present invention to control the visual displays

on moving objects which are in motion so that such displays are not distractive to the process of operating moving objects within the immediate vicinity.

[0091] It is yet another general object of the present invention to provide a means for the owners of such mobile or fixed objects to be compensated for the use of their property as it relates to the above referenced system.

[0092] It is yet another general object of the present invention to permit the widespread use of personal vehicles for revenue producing activity.

[0093] It is yet another general object of the present invention to compensate owners and operators of moving objects for the confirmed use of their assets.

[0094] It is yet another general object of the present invention to convert drivers' wasted time and money in traffic into incomes, thereby increasing the tax base.

[0095] It is yet another general object of the present invention to make new vehicle ownership and/or operation virtually cost free.

[0096] It is yet another general object of the present invention to stimulate the earlier consumer adoption of alternate energy vehicles by incorporating into them the revenue-generating advantages of the present invention.

[0097] It is a further general object of the present invention to allow government agencies, or those responsible for the safe and proper use of such moving objects, to override the display of advertising or lower priority utilization of the invention to facilitate communications which may be of greater importance in terms of public safety and well being.

[0098] It is another object of the present invention to allow advertisers to submit ad content together with delivery information for approval and subsequent distribution to moving objects.

[0099] It is a further object of the present invention to allow the general driving population to select the kinds of advertising content it would like to view and display, and to further enter into contracts defining their rights and responsibilities to use that content, and to receive compensation for such use.

[00100] It is another general object of the present invention to facilitate an online community through which users of the present invention can register

their moving objects, establish memberships and submit user profiles containing their personal preferences and user criteria.

[00101] It is yet another object of the present invention to allow fleet and government users of moving objects to use the present invention to determine the kinds of advertising content or other types of information they would like to view and display, and to enter into contracts defining their fees and compensation for such use.

[00102] It is a another object of the present invention to facilitate a system in which users can identify "who they are" and "what they want" and then be rewarded for providing that information by being able to control what they see and hear with respect to ad content that is presented to them.

[00103] It is another object of the present invention to permit the distribution of advertising or sponsorship content, private or personal content and public service or emergency content directly and simultaneously to multiple moving objects where it can be stored, retrieved and displayed upon demand.

[00104] It is a further object of the present invention to allow content to be encoded for unique deliveries (such as for time and place, under specific conditions and circumstances or to specific demographics) and to enable contracts with clients, customers and entities who wish to pay for such encoding.

[00105] It is a further object of the present invention to allow users to request that specific kinds of content be displayed on their own or on other moving objects on a predetermined or spontaneous basis, and to optionally pay for that service.

[00106] It is still another object of the present invention to permit users to delete, or prevent the display of, certain kinds of content on moving objects, on a predetermined or spontaneous, real-time basis, and to optionally pay for that service.

[00107] It is another object of the present invention to enable the display of advertising and sponsored content on the exterior surfaces of moving objects when such objects are parked or are non-moving and that such content be

related to the immediate surroundings and/or be controlled by the presence of both pedestrians and handheld electronic devices.

[00108] It is a further object of the present invention to provide a means to store information and data relating to any delivered content requests, any "delete" requests or any "prevent" requests on board a moving object together with a means for subsequently uploading that information for the purpose of tracking, measurement, accounting and compensation.

[00109] It is yet another object of the present invention to enable the wireless, automated downloading of encoded user codes or profiles to moving objects.

[00110] It is a further object of the present invention to enable the wireless, automated uploading of encoded public service content (such as public alerts and weather warnings) together with venue-specific or time-specific triggering criteria to the on-board storage devices of moving objects.

[00111] It is another object of the present invention to enable the wireless, automated downloading of encoded commercial ad content, together with encoded delivery information, to the on-board storage devices of moving objects.

[00112] It is another object of the present invention to enable the wireless, manual uploading of encoded personal content by private citizens, together with encoded delivery information, directly to the on-board storage devices of moving objects from home or personal networks.

[00113] It is another object of the present invention to allow users to spontaneously request additional information, to purchase merchandise or otherwise respond to electronic offers and advertisements as they view such content from or while operating moving objects.

[00114] It is a further object of the present invention to provide a means for logging and storing information on board a moving object relating to the delivery of audio or video public service content, including content requests, and to provide for the later uploading of such information for tracking, engagement measurement, accounting, and compensation purposes.

[00115] It is a further object of the present invention to provide a means for

logging, documenting and storing information on board a moving object relating to the delivery of audio or video advertising or sponsorship content, or content requests, and to provide for the later uploading of that information to a network for tracking, engagement measurement, accounting, and compensation purposes.

[00116] It is a further general object of the present invention to provide a means for logging, documenting and storing information on board a moving object relating to the delivery of audio or video personal use content, and for the later uploading of that information to a network for the purpose of tracking, engagement measurement, accounting, and compensation.

[00117] It is a further object of the present invention to enable the display of video content on the exterior surfaces of one's own moving object, such content generated previously and stored, or created spontaneously in real time (such as an instant personal text message), and optionally, to enable and cause the audio portion of that content to be synchronized to said video and wirelessly transmitted to another moving object for its reception and listening.

[00118] It is another object of the present invention to enable a means for the owners of current production motor vehicles to easily and cost-effectively exchange certain of their motor vehicle's body panels for revenue-producing video display body panels which then permit them to be compensated for the use of their property as it relates to the above referenced system.

[00119] It is another object of the present invention to enable the cost-effective fleet conversions of personal and commercial motor vehicles through the exchange of vehicle body panels and the addition of electronics to allow individuals or small business fleet owners to profit from the use of their vehicles as multi-media communications platforms.

[00120] It is a further object of the present invention to enable the simultaneous uploading and downloading of information and content from a network to large numbers of parked or moving objects for the purpose of updating on-board libraries, or for the purposes of tracking, engagement measurement, accounting and compensation.

[00121] It is a another object of the present invention to enable the uploading of information stored in moving objects relating to content, time, place, nature and trigger for any logged delivery, and to then process and to feedback that information to authorized government users, advertising agencies, advertisers or registered fleet, business or personal users for the purposes of tracking, engagement measurement, accounting, compensation or billing.

[00122] It is a further general object of the present invention to display conventional, targeted or hyper-relevant advertising, public service content and other types of information transmitted to moving objects on the internal video displays of such moving objects.

[00123] It is a further general object of the present invention to display conventional, targeted or hyper-relevant advertising content, public service content and other types of information on the internal video displays of moving objects with the presentation of said displays governed and controlled by the speed, location, contents, time of day, proximity and nature of the moving object and of other nearby moving or stationary objects within an environment.

[00124] It is another general object of the present invention to permit the selling, scheduling and display of hyper-relevant advertising content, together with public service content, personal content and other types of information, on video displays which are located on the interior of moving objects.

[00125] It is another object of the present invention to permit the distribution, display and documentation of conventional, targeted or hyper-relevant advertising, public service content, personal content and other types of information, on video displays located on the interior of moving objects, and to financially compensate the owners or operators for such display.

[00126] It is another object of the present invention to upload user codes which have been transmitted on an ad hoc basis between moving objects in the field for the purpose of tracking consumer movements by VIN, demographics, time, place, interests and other factors, for the purpose of research, marketing and planning.

[00127] It is another object of the present invention to enable the sale of user

codes and information relating to the movements of consumers in the field by VIN, demographics, time, place, interests and other factors for the purpose of research, marketing and planning.

[00128] It is another object of the present invention to convert the ad industry's enthusiasm and its need for unique advertising platforms into capital investment in said invention, thereby stimulating companion investment from private industry and government.

[00129] It is a further object of the present invention to use its ability to generate incomes for the general driving population to stimulate further investment from industry and government.

[00130] It is another object of the present invention, through its ability to generate incomes for the driving population, to leverage the competitive interests of manufacturers causing them to incorporate the invention into their high volume production of moving vehicles, said higher volumes reducing the costs for manufacture and making the product more accessible to the driving population.

[00131] It is a further object of the present invention to enable a system wherein a moving object can detect and learn the traffic patterns and signal sequences at highway intersections, convey that information to other moving objects, synchronize that information with said objects and then calculate the time remaining at such locations within which content can be safely displayed.

[00132] It is a further object of the present invention to enable a system for the geo-tracking of moving objects in a manner that will not violate civil liberties, since tracking data cannot be lawfully generated in the absence of a subpoena.

[00133] It is a further general object of the present invention to permit the use of its video display(s) for entertainment purposes or for static presentations on moving objects when enabled by appropriate audio and video devices.

[00134] It is a further object of the present invention to provide a novel system for reducing the spacing between moving objects when such objects are in stopped, or near-stopped modes, thereby conserving significant amounts of

wasted city traffic lanes especially at traffic signals, intersections, on ramps and turning lanes.

[00135] It is a further general object of the present invention to allow law enforcement to remotely override or take command of a moving object's active display to confirm moving object identification, highlight lost or stolen moving objects or to use a moving object as a mobile hazard, lighting or communications platform.

[00136] It is a another object of the present invention to electronically display moving object identification, licensing and registration at all appropriate times and to further allow the driving population, including law enforcement, to electronically capture and record such identification upon demand.

[00137] It is a further object of the present invention to incorporate all of the normally required lighting, safety, branding, licensing and registration systems, to the greatest extent possible, into the digital video display(s) of future moving objects.

[00138] An aspect of the invention is a system, comprising: a first object; a transmitter in the first object; a second object; a receiver in the second object; and a profile comprising data regarding a user associated with the first object; wherein the profile or a subset of the profile is transmitted from the first object to the second object; wherein content is presented to the first object; and wherein at least a portion of the content is based on the profile or subset of the profile transmitted from the first object to the second object.

[00139] In one mode, the profile is stored in the first object. Another embodiment of this aspect further comprises compensation to a user associated with the second object for presenting content. In another mode, the first object is capable of motion. In other modes, the first object is a vehicle, a device in a vehicle, or a handheld device. In other modes, the second object is a vehicle or is fixed or movable signage.

[00140] In another mode, the first object is a vehicle; and the profile further comprises data regarding other users or potential users associated with the first object. In another mode, the first object and the second object exchange

information relating to relative positions, speeds, and motion of the first and second objects; information relating to the character, configuration, and properties of the first and second objects; information relating to surrounding objects; and information relating to surrounding locations; or any combination thereof. In another mode, presentation of the content is influenced by information relating to scheduling patterns of nearby traffic signals. In still another mode, the content further includes content not based on said profile.

[00141] Another embodiment of this aspect further comprises a priority system relating to presentation of the content based on a nature of the content. In one mode of this embodiment, a nature of the content is classified as emergency content; content relating to a surrounding environmental condition; registration and identification content relating to the second object; public safety content; or a combination thereof.

[00142] In another mode, relative motion data from the first and second objects determines whether content is presented and whether presented content is presented as animated video, static video, or a combination of both. In another mode, the content includes audio content, video content, or a combination of both; wherein the audio content is presented by the first object; and wherein the video content is presented by either the first object or the second object.

[00143] In another mode, the first and second objects are vehicles; the content comprises positioning information relating to the first and second objects; and the content indicates to an operator of the first object an optimum stopping position. In another mode, speed and positioning information is exchanged between all objects within transmission range; and the content presented to the first object indicates to an operator of the first object relative braking conditions of any objects in front of the first object.

[00144] In another mode, the second object has a user associated with the second object; and at least a portion of the content presented to the first object is created by the user associated with the second object. In another mode, a third party purchases a right to present content on the second object; and the second object presents content based on preferences of the third party. In a

further mode, the right is based on a fixed or relative geographical area; a time of day; a period of available display time; or any combination thereof.

[00145] In another mode, the profile is transferable to other objects at an option of any user associated with the first object. In another mode, the content is viewable by persons other than those associated with the first object. In another mode, the content is presented in a manner to render the content not viewable by individuals other than those associated with the first object.

[00146] Another embodiment of this aspect further comprises a display integrated with the second object; wherein at least a portion of the content presented to the first object occurs on the display. In another mode, presentation of the content occurs on an exterior portion of the second object.

[00147] Another embodiment of this aspect further comprises a first storage medium associated with the first object; and a second storage medium associated with the second object; wherein data related to presentation of the content is stored in the first and second storage media. Another mode of this embodiment further comprises a central server wirelessly connected to the first and second objects; wherein the data related to presentation of the content is uploaded to the central server. In a further mode of this embodiment, a compilation of uploaded data in the central server is offered for sale. In one mode of this embodiment, the data related to presentation of the content includes time of display; subject matter of said content; duration of display of the content; a subset of the profile; or any combination thereof.

[00148] In one mode, presentation of the content occurs in an interior portion of the first object. Another embodiment of this aspect further comprises compensation to the user associated with the first object for receiving content, viewing content, or any combination thereof.

[00149] In another mode, information related to identities of all adjacent and nearby objects is exchanged between and stored in the first object and any adjacent or nearby objects. In another mode, the first and second objects exchange information related to audio playing in the first object; and the content presented to the first object comprises video content synchronized to

the audio. In another mode, the content presented to the first object is limited by a user associated with the second object.

[00150] Another aspect of the invention is a computer implemented method, comprising: compiling a unique profile of a first user based on analysis of data provided by the first user; associating the profile with a first object; transmitting the profile or a subset of the profile to a second object; and presenting content to the first user; wherein the first object is associated with the first user; wherein the content originates from the second object; and wherein at least a portion of the content is based on the profile or subset of the profile transmitted to the second object.

[00151] An embodiment of this aspect further comprises compensating a user associated with the second object for presenting content to the first user.

[00152] Another embodiment of this aspect further comprises prioritizing display of the content based on purpose of the content; wherein purpose of the content is advertising; informational; traffic related; safety related; news related; region specific; political; mere frivolity; or any combination thereof. One mode of this embodiment further comprises pre-empting presentation of the content based on surrounding environment of the first and second objects; presence of emergency circumstances; public interest; or any combination thereof.

[00153] Other embodiments of this aspect further comprise prioritizing display of content based on preferences of the first user; transferring the profile to other objects at an option of the first user; displaying registration and identification information for the second object on the second object; or displaying content created by a user associated with the second object on the second object.

[00154] Another embodiment of this aspect further comprises displaying indicators of optimal traffic and view positioning on the second object to the first user; wherein the first objects and the second objects are vehicles.

[00155] Other embodiments of this aspect further comprise pre-empting display of the content in the presence of external wireless signals for emergency or traffic direction purposes; presenting audio content to the first user using the

first object; presenting video content to the first user using the first object, the second object, or a combination of the first and second objects; or exchanging information relating to relative positions, speeds, and motion of the first and second objects; information relating to the character, configuration, and properties of the first and second objects; information relating to surrounding objects; and information relating to surrounding locations; or any combination thereof, between the first object and the second object.

[00156] Another embodiment of this aspect further comprises determining relative motions of the first and second objects; and presenting no content or content as animated video, static video, or a combination of animated and static video, based on the relative motions of the first and second objects.

[00157] In other modes, the content is presented on a display integrated with the second object, or the content is presented on an exterior portion of the second object.

[00158] Other embodiments of this aspect further comprise storing data related to presenting the content in the first and second objects; uploading data related to the presenting the content to a central server wirelessly connected to the first and second objects; or offering a compilation of uploaded data from the central server for sale. In another embodiment, the data related to presenting the content includes time of display; subject matter of the content; duration of display of the content; a subset of the profile; or any combination thereof.

[00159] A still further aspect of the invention is a method, comprising: populating a source object with content; and presenting the content to a recipient object in response to a unique profile or portion thereof associated with the recipient object that is provided by the recipient object to the source object.

[00160] Yet another aspect of the invention is a system, comprising: a content storage device; and means for presenting content stored on the content storage device to a recipient object in response to a unique profile or portion thereof associated with the recipient object that is provided by the recipient

object to the source object.

[00161] Further aspects of the invention will be brought out in the following portions of the specification, wherein the detailed description is for the purpose of fully disclosing preferred embodiments of the invention without placing limitations thereon.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

[00162] The invention will be more fully understood by reference to the following drawings which are for illustrative purposes only:

[00163] FIG. 1 illustrates a general embodiment and overview of the present invention.

[00164] FIG. 2 is a diagram showing the relationship of governments and manufacturers to the present invention.

[00165] FIG. 3 is a diagram showing the relationship of advertisers and manufacturers to the present invention.

[00166] FIG. 4 is a diagram showing the relationship of the driving population and fleet or government users to the present invention.

[00167] FIG. 5 is a block diagram depicting an owner registration process for the present invention.

[00168] FIG. 6 illustrates a first embodiment of a land-based moving object using the invention.

[00169] FIGS. 7-10 illustrate an aftermarket body panel conversion for a sport utility vehicle (SUV).

[00170] FIGS. 11-13 illustrate an aftermarket body panel conversion for a passenger sedan or Taxi.

[00171] FIGS. 14-16 illustrate an aftermarket body panel conversion for a station wagon.

[00172] FIG. 17 is a block diagram depicting the electronic vehicle packages for the present invention.

[00173] FIGS. 18A-18B are a block diagram depicting the Distribution model of the present invention.

[00174] FIG. 19 is a block diagram depicting the Compensation model of the present invention.

[00175] FIGS. 20-23 are illustrations showing a land-based vehicle and three basic types of displays.

[00176] FIGS. 24-27 are illustrations showing four different types of content display.

[00177] FIG. 28 is a diagram showing geo-specific content distribution.

[00178] FIG. 29 is a diagram showing content purchase and encoding by content type.

[00179] FIG. 30 is a diagram showing content viewing based on FIG. 28.

[00180] FIG. 31 is a block diagram showing content protocols and queuing in a viewed vehicle.

[00181] FIG. 32 is an illustration showing geo-specific content distribution in a rural area.

[00182] FIGS. 33-34 are illustrations showing the display interactions between moving objects in a city and in a freeway environment.

[00183] FIG. 35 is a diagram of the Intersection Clock for measuring the time available for display.

DETAILED DESCRIPTION OF THE INVENTION

[00184] Referring more specifically to the drawings, for illustrative purposes, the present invention is embodied in the system and method generally shown in FIG. 1 through FIG. 35. It will be appreciated that the system and apparatus may vary as to configuration and as to details of the parts, and that the method may vary as to the specific steps and sequence, without departing from the basic concepts as disclosed herein.

[00185] FIG. 1 illustrates a general embodiment and overview of the present invention by showing some of the essential elements which must interact to launch such a unique advertising and communications platform: first, the user base (comprised here of Government Agencies 200, Advertisers 300, the Driving Population 400, and Fleet/Government Users 500); the Developers, Suppliers, and Manufacturers of moving objects 600, (in this embodiment,

production automobiles); the Distribution entity (or entities) 800, the Compensation entity 900 (shown separate here for clarity; in practice, this entity would likely be combined with the Distribution entity), and the body of Registered Owners and Operators, represented at 1000. Although a given embodiment might include a large number of such groups with wide variations of interactions between them, the groups listed herein are some of the most basic and essential to a widespread deployment of the present invention. Such relationships will range from development funding and investment to the manufacture, implementation, operation, and maintenance of the system. A fundamental element to early planning is the proposed rulemaking shown at 100, followed by the legislation of design, performance, and compliance standards for the operating aspects of the emerging system. Such effort represents a give-and-take objective and creative exchange between government and industry following which policies will emerge that all the parties can live with. Precedents and parallels exist for such efforts between government and transportation, and are well known with respect to establishing even more stringent standards for automotive performance, such as, for example, The Department of Transportation's Federal Motor Vehicle Safety Standards (FMVSS) concerning vehicle operating standards and crashworthiness; the EPA's Clean Air Act Amendments (CAAA) or National Low Emission Vehicle (NLEV) Standards for vehicle emissions or NHTSA's Corporate Average Fuel Economy (CAFE) Standards for fuel economy. Such standards will be negotiated essentially between the transportation industry suppliers and automakers 600 and appropriate Government Agencies 200, with input by any other interested parties. Content standards 105 defining how conventional, targeted and hyper-relevant advertising is ultimately presented to consumers will most likely be established concurrently with the operating and distribution portions of the system. This interaction will be between the advertising community 300, the manufacturing body 600, the distribution entity 800, and its compensation unit 900, with input from concerned government entities, fleet and government operators 600 and from the driving population.

[00186] It is envisioned that very early funding for R&D and technology development may come from the investment arms 110, 115 of the advertising and media community on the commercial side, and from the government for exploration on the highway/traffic safety and public service side. This early development funding would be combined with funding provided by the major automakers and their suppliers 600, resulting in prototype operating systems, and leading eventually to full production supply 120, with such production to be integrated with regularly scheduled vehicle production. There are also specific, highly targeted operating niche markets ideal for introducing this platform on a controlled basis, such as fleet and taxi operations, which will be explained later. It should be noted that there are also as many different potential scenarios and models for program funding since interest, participation, and investment is expected from many private sector entities, foundations, institutions, or government agencies. Another likely investment scenario is reflected at 128, in the form of potential investment in the Distribution entity by the transportation manufacturers themselves, because their end products are essential components to this new advertising and communications platform.

[00187] Private investment 130 from the user body can assume many forms, such as state and local government funding in support of innovative law enforcement applications (some of which have been previously described); direct equity investment from advertisers 300 or from big media owners; private investment from the general driving population 400 or from fleet and business users 500 (other than their investment in private vehicle ownership), such investments coming perhaps in the form of equity in the Distribution entity 800, perhaps through an IPO. Once Distribution is operational, however, the user body will commence paying Usage Fees 140 to place content on the new platform.

[00188] The output side of the Distribution unit 800 is the delivery of content (as discussed in the preceding section) distributed directly to the vehicles registered in the network through channels 150, 155, and are explained later.

Content 150 represents conventional, targeted and/or hyper-relevant audio and video ad content, public service content, personal content and encoded personal profiles from fleet or government users and the general driving population. Content 155 represents the delivery of personal preferences to Pre Existing Vehicles 655 which use aftermarket systems sold through retailers or installed as upgrades at automobile dealerships. Pre Existing Vehicles 655 are able to wirelessly transmit VIN, model data, content requests and ad control signals 750 to New Production Vehicles 652, 654, and then receive audio and view video content derived from that data on moving object video displays 760. Fully equipped New Production Vehicles 652, 654 will send similar VIN, content and control requests 740, receive audio content internally and view video content on displays 760 which are integral to those vehicles, exterior surfaces or glazing. As previously explained, all such content and control requests are logged on both new and aftermarket platforms for later wireless downloading as shown by 160, 165 via network access points (NAPs) to be discussed in a later section.

[00189] The Compensation unit 900, collects all data downloaded from registered moving objects and compares content requests with content deliveries (discussed in greater depth later), and confirms actual content deliveries by matching these data. Confirmed distribution information is subsequently returned to the Distribution unit 800 (which may be the same as Compensation unit 900) as shown at 170. A critical step in content delivery measurement, accounting and compensation occurs at this stage. The applicant believes that it is important for any such system to be able to identify and prevent what has become known in the Internet advertising industry as "click-fraud." This is a process in which users, entities or software create fraudulent requests for content deliveries (viewings) in an effort to demonstrate greater interest in a specific ad or site than really exists. In the case of the present invention, this could be attempted by individuals to get paid for presenting ads that were not actually viewed. At this stage, an exchange of data 170 between the Compensation unit 900 (which has

downloaded logged vehicle data) and the Distribution unit 800 takes place which involves the matching of specific VINs on moving objects together with the time, place and the physical movements of those objects to determine the likelihood of fraud. This process is explained in greater detail in a following section. Once in-field content deliveries have been authenticated, the Compensation unit 900 can approve payments to the registered vehicles that have had their display of content confirmed via the mechanism at 170. This applies to all registered production vehicles 652, 654, and in some instances to the vehicles which only view content such as vehicles having aftermarket installations 655. The Distribution unit 800 can then feed back in-field performance measurements to the general user body as indicated at 180. The Compensation unit 900 has, among numerous tasks discussed in a later section, two key functions: the payment of financial compensation to Registered Platform Owner/Operators 1000, as shown at 178; and the sale of ad hoc collected data to marketers and researchers, as indicated at 1100.

[00190] FIG. 2 shows potential relationships between Government Agencies 200 and Developers, Suppliers and Manufacturers 600 relative to the funding, regulation and use of the present invention. Although there are many such possible combinations, named are a few of those agencies that may have a bearing on some of the Regulatory issues 220 and public service usage issues 240. The National Highway Traffic Safety Administration (NHTSA) 202, for example, would have a clear role in establishing vehicle standards, including testing and compliance procedures, just as it has had in other Department of Transportation (DOT) programs, some of which have been previously mentioned. The Federal Highway Administration (FHWA) 204 has a vision to create the best transportation system in the world. In partnership with the overall highway and transportation community, its charter is to assure the safest and most efficient highway and intermodal transportation systems possible, in which crashes, delays and congestion are significantly reduced, where roads protect ecosystems, where pedestrians and bicyclists are accommodated and where transportation services are restored immediately

after disasters and emergencies. The present invention is capable of making significant contributions to all of these specific objectives. A prime goal of the National Telecommunications and Information Administration (NTIA) 206, is to bring dramatic growth and change to the nation's economic, social and political life through a fundamental mission of promoting market-based policies that can lower prices to consumers and encourage innovation, while harnessing the resources of the Federal government to support spectrum-based technologies that enhance efficiency and productivity. Clearly, the broad application of the wireless spectrum to produce commercial and public communications opportunities that also benefit consumers financially, are within NTIA's charter. The Research and Innovative Technology Administration (RITA) 208 is dedicated to the advancement of DOT priorities for innovation and research in transportation technologies and concepts. Innovations that will improve our mobility, promote economic growth, and ultimately deliver a better integrated transportation system. The agency's charter is to foster the exchange of ideas and information in a high-priority incubator committed to research and to getting innovative ideas from the laboratory into the field. RITA can effectively assess the present invention's ability to clean up distractive highway signage stimuli, adopt more effective direct vehicle collision warning systems, incorporate state-of-the-art techniques in the enforcement of drunk driving laws and the delivery of emergency medical services and generally, through the present invention, dramatically improve the design and management of highway safety programs. The National Weather Service (NOAA) 210 has a current program in place called "Flooding Ahead Turn Around Don't Drown", an attempt to reduce the high numbers of lives lost each year by drivers whose vehicles are swept away while trying to cross heavily flooded areas. This program has previously involved posting a plastic sign on a small metal stand where the road disappears beneath the water. The program has enjoyed limited effectiveness but is a logistics nightmare in terms of deployment on an urgent basis. Tornados, landslides, hurricanes, flash floods, wildfires: all have similar

impact and problematic solutions when it comes to protecting the public. The present invention, however, is, in fact, a rolling billboard having instant communications whose content (including animated, mobile, warning signage complete with flashing lights) can be deployed instantly where ever it is. Thus, NOAA's involvement in early rulemaking could prove a tremendous benefit to public safety. The Bureau of Transportation Statistics (BTS) 212 is responsible for assessing the relationships between transportation and the economy on an ongoing basis, including our transportation system's share of Gross Domestic Product, employment and transportation expenditures. Its work bears heavily on such previously discussed areas as urban congestion and the direct costs to consumers in wasted fuel and time. This area alone justifies the early involvement and sustained tracking of BTS to document the tangible long term benefits of the present invention. Finally, there are numerous other agencies 214 whose capabilities can come to bear on the present invention's implementation, and their coordinated efforts must be multinational in scope.

[00191] Usage 240 indicates just few of the potential applications worthy of funding by Federal Governments. Such funding 110 is to be directed in part towards supporting the research and development efforts of automotive Developers, Suppliers and Manufacturers 600. The principal areas for development are Telematics 610, the means for implementing communications between moving objects; Data Processing 620, methods for decoding, storing, polling, extracting, queuing, encoding and uploading data and content for distribution via the present invention; Displays 630, the evolution of cost-effective displays from current or new technologies for incorporation into high volume production vehicles of all kinds; and Panels & Glazing 640, the use of automotive glazing as platforms for content display.

[00192] Proposed Rulemaking and Legislation relationships 100. Upgrades in telecommunications and content handling, operating systems, displays, including hardware and software for the present invention after its initial introduction are indicated at 125. Investment is shown at 128, suggesting the

possibility of automakers and their suppliers taking equity positions in the Distribution entity (or entities). At 142, Usage Fees are paid to the Distribution entity 800 for government or public service content downloads indicated at 152, which are then stored on vehicle hard drives. Such fees would likely be paid, part in advance, based upon negotiated service contracts between various government agencies and the Distribution entity. The balances would be paid later, once in-field content deliveries have been confirmed from logged downloads. At 161, logged public service content requests (and optionally, confirmed deliveries) are downloaded from aftermarket platform installations. At 162, logged public service content requests and logged public service exposures are similarly downloaded to Compensation 900 for processing and confirmation. At 182, confirmed public use content exposure is returned to Distribution where it can then be translated into effective measurement information regarding engagement and the precise time, place, circumstances for content delivery and whether or not specific and appropriate actions were taken by the recipients on a timely basis in response to such content deliveries (In other words, did they act on a specific audio/visual display presented to them in the field?). Finally, at 186, documented performance is fed back to the appropriate Government Agencies 200. This feedback will vary with the needs of the specific agencies involved and would perhaps be accomplished under contract between Distribution and that specific agency of government. An example of such measurement and feedback would be the confirmation to NOAA that a specific number of vehicles were turned back from a flash flood zone and were directed over an alternate route well in advance of an actual crisis, along with geo-specific mapping showing the positions and numbers of vehicles simultaneously exposed to the audio/visual alert (via the present invention), the precise timing and movements of those vehicles after that alert (based on logged GPS data) and the movements of those invention-equipped vehicles that did not heed the alert, so that alert effectiveness can be determined.

[00193] FIG. 3 is a diagram showing the relationships of advertisers and

manufacturers to the present invention. Although the advertising community 300 is multifaceted, it has been defined collectively as three elements: the media buyers 305 (entities responsible for purchasing and scheduling ads in various media), the advertising agencies and their clients 310, and the content producers 315 (entities typically hired by the ad agencies to create, produce and execute products for media placements). The applicant envisions these groups, individually and collectively, influencing and guiding proposed standards 106 for creative content and system functionality, key elements of which are listed in Content Standards 320. Note that the development of these standards will be augmented at 100 by the interface with U.S. and Foreign Government Agencies 200. These groups will combine their essentially creative and marketing powers and their political and legislative experience to shape rulemaking for such issues as: Graphics & Animation Standards (determining, for example, the distractive qualities of animations with regard to driver attention and establishing criteria for such displays); Content Standards & Formats (limitations on certain kinds of ad content relative to specific demographics, or the manner in which certain presentations can be made and to whom); Telematics Standards (the technologies that will be applied in allowing moving objects to talk to each other); Proximity & Venue Regulations (determining times and locations in which certain kinds of ads might not be permitted, or might be limited in scope or content); methods and schemes for Demographic Encoding (classifying the various types of products and ads so they can be matched to consumer request profiles and properly tracked for measurement, accountability and compensation); Impulse Response Standards (uniform methods allowing consumers to request information on products or to order and purchase products safely while using their moving objects and to securely link such orders with credit and shipping information; Field Override Standards (the criteria and procedures allowing law enforcement to take command of an ongoing display in the interests of public safety or need); assuring conformance with current and anticipated NHTSA Standards; Compliance & Regulation (developing testing and compliance

procedures to assure standards in manufacturing and use; and Compensation Standards (the development of accounting, billing and general compensation procedures and contracts including defining industry fair practices, ownerships, taxation, disbursements and similar consumer related business issues). At 134, Joint Production Specifications are implemented with the manufacturing teams 600 and are incorporated into the network's operating systems by the Distribution unit 800.

[00194] Paths 130 and 143 represent two of the key financial channels for the advertising community. Although there are numerous scenarios for investment to occur, the most likely is through equity, loan or advancement by the advertising or media industry as a whole, because these represent both a significant user and beneficiary. As noted hereinabove, there is a serious need for improved ad accountability, demographic effectiveness and tracking of engagement, and there is no question that advertisers and large media buyers are desperate to find new ways of reaching consumers and in recapturing defections from commercial television to the Internet. With so much at stake in the industry, the logical core investors for the present invention are, the major Media Buyers 305, the Advertising Agencies and their Clients 310, the content Producers 315, and, of course, the operators of traditional media and advertising platforms such as commercial television. One reason this makes so much sense is that this Advertising community 300, which comprises these three entities, will also become the network's largest user and payer of User Fees 143.

[00195] Again, 120 represents the supply path for New Vehicle Production 650, and 153 represents the uploading of Advertising Content, along with encoded profiles, upgrades and distribution instructions via the Internet, to individual vehicles 652, 654, 655.

[00196] Path 167 indicates Logged Content Requests from Pre Existing Vehicles, while path 164 shows the upload path for Logged Advertising Requests and Logged Advertising Exposure from New Vehicle Production. As it was with Confirmed Public Service Use, path 173 indicates Confirmed Ad

Distributions sent back to the Distribution unit for ad performance assessment, engagement tracking, measurement, accountability, fraud exposure and compensation. Once data is processed by the Distribution unit 800, it can provide performance feedback 183 to Media Buyers, Ad Agencies or Advertisers in a variety of formats, including data on the direct daily deliveries to specified demographics with the exact times, places and durations for such impressions, along with consumer views and opinions, related information requests, resulting purchases and other criteria, all at multiple levels of depth in accuracy and measurement previously unavailable in the advertising industry.

[00197] It is also worth noting that with the creation of such a widespread, flexible and mobile video platform, it is only a matter of time before the major news and entertainment media companies realize that the present invention offers an exceptional means to reach consumers with rich content presentations while they are on the go, yet are in a safe and relaxed mode to receive such information. For cable leaders such as Fox News, the present invention offers a unique mobile forum for delivering breaking news and local event alerts and thus represents a huge potential revenue stream for all general media and telecommunications.

[00198] FIG. 4 is a diagram showing the relationship of the Driving Population 400 and Fleet / Government Users 500 to the Distribution unit 800. Both of these user groups will be discussed in terms of Online User Communities, one referenced at 410 for the General Driving Population, the other at 510 for Fleet Business and Government Users. Examples of these and how they work have been described in previous text. Over time, such communities may take on a variety of forms; however, the applicant envisions most of these being operated by the individual automakers, aftermarket producers or retail dealership bodies responsible for the design and manufacture of the moving objects themselves. For purposes of this discussion, these communities are defined in four sections, each representing an online activity. For the Driving Population these would be: (1) Registration 420, which can begin at the

dealership with the recording of a vehicle's VIN, a process which can be completed at home with final licensing online; (2) Membership 430, where each member of a family can join the community by creating his own User Name and Password; (3) Preferences 440, where each new member can follow easy online prompts in multiple choice, pull down menu, check box or text write-in format to define his personal interests, wants, needs, desires, capabilities and experiences, these in terms of a pair of profiles defining "who he is," and "what he wants" as these preferences relate to his personal lifestyle and to the kinds of advertising he would like to view or present; and (4) Personal Use 450, where a member—typically upon approval of the Registered Owner who is the designated System Administrator—can elect to create and upload a variety of personal messages, sponsorships or advertising they would like to display to others for personal or business purposes and for which they will be billed at a discounted rate if presented on their own vehicle.

[00199] These online sections are similar to those used for the Commercial or Fleet Business User body or for Government Users, except they are tailored for business and commercial applications and are structured to accommodate a multiplicity of moving objects or vehicles: (1) Registration 520, where a business or fleet owner can register a number of vehicles to be driven by drivers under contract to that business; (2) Operator Profiles 530 where a business manager is responsible for identifying his drivers and informing them of the network's system and rules; (3) Preferences 540, where a business or government fleet manager can establish the communications, viewing and presentation preferences for his own drivers and his fleet; and (4) Fleet/Government Official Use 550, where registered business owners or fleet managers can enter into contracts with the Distribution entity 800 to display their own company's advertising, branding or promotions. The applicant anticipates that a number of individually operated advertising and promotion businesses may spin off from such commercial platforms wherein small business owners might purchase dual-purpose vehicles with the intent of

operating a fleet of mobile ad platforms around the clock in key markets, to train and manage drivers for such an enterprise, and to then charge advertisers for the presentation of content by specialized venue or times which might be otherwise unavailable. This would not be unlike privately-operated auction businesses which have spun off from the popular Ebay model. An embodiment for such a fleet application is discussed in a later section concerning moving object fleet adoption and production. The combined upload path for Owner/Operator Profiles is shown at 114.

[00200] As previously explained, Vehicle Registrations for the present invention are linked to Vehicle Identification Numbers (VINs) and are cross-checked with DMV records for information which, from a legal or business perspective, might preclude a membership approval. Such precautionary measures are well known in the industry and follow commonly established prudent business and legal practices. Owner/Operator Profiles 530 and Preferences 440, 540 may be subjected to similar scrutiny; however, it is the objective of such profiles to define the nature of the content which is to be viewed by such owners and operators, and to a lesser degree, to determine what they will be displaying to other members and to the public at large. In terms of what is actually displayed to the public under the present invention, all content is thoroughly monitored and approved under strict standards and practices which have been established through the joint efforts between government and business, as described in the foregoing sections. Approved and Encoded Owner/Operator Profiles for both Personal and Fleet/Government Users are uploaded at 116 to specific vehicles by VIN, or by an equivalent vehicle identifying process which links registered owners to their vehicles. As occurred previously with Advertising and Public Service content, personal content for the general Driving Population and Fleet or Government Public Service and Business content is uploaded to New Vehicle Production at 154. Additionally, Personal Preferences for controlling the viewing characteristics from Pre Existing Vehicles are uploaded to these vehicles at 118.

[00201] An important byproduct of the present invention (in addition to its ability

to request and confirm the delivery of profile-enabled hyper-relevant content), is its ability to simultaneously, and even passively, track and measure all such requests and deliveries, including any actions taken by consumers as the result of such deliveries while in the field, then to gather and compile such data in terms of consumer movements by time, venue and VIN, all relative to their demographic and psychographic profiles. This kind of information can be easily generated through the interaction of moving objects using the present invention, and through moving object interactions with other kinds of compatible, profile-driven mobile devices in the field. As each moving object or mobile device communicates with others in an effort to match transmitted user code "requests" with stored content, as in the case of the present invention (or to match User Codes as disclosed in the applicant's nonprovisional patent application serial number 11/552,932, filed October 25, 2006, entitled: "METHOD AND APPARATUS FOR OBTAINING REVENUE FROM THE DISTRIBUTION OF HYPER-RELEVANT ADVERTISING THROUGH PERMISSIVE MIND READING, PROXIMITY ENCOUNTERS AND DATABASE AGGREGATION", incorporated herein by reference in its entirety), these moving objects emit encoded signals which describe the essential nature, makeup and interests of a seeking party. Regardless of matched content requests, delivered content, or attempted or consummated in-field communications, all such moving objects or mobile devices may, if so programmed, receive and store in-field transmissions from all other such moving objects and devices. Each of these transmissions is time-stamped and identified by device and location. The codes for any such attempted or consummated communications can then be collected and uploaded to the Compensation unit 900 and the Distribution unit 800 when these moving objects are linked to a network.

[00202] This level of verifiable information on consumer demographics, psychographics and interests, when coupled with their movements and travels, can be of extraordinary value to market researchers and planners. These include: architects and developers, retail store and mall planners, high

schools and universities, concert and event producers, resort and theme park planners, transportation planners, law enforcement, government lawmakers and of course advertisers and marketers. The sale of this data is indicated at 1100 in FIG. 1. The downloading of special instructions for the collection of ad hoc research and planning data based on independently contracted or measured studies is shown at 1120 in FIG. 4. The uploading of such ad hoc collected in-field data is shown at 1140.

[00203] Logged Personal Use Authorizations (request signals permitting or preventing personal content to be presented to a viewing vehicle) are uploaded from all vehicles at 167 to the Compensation unit 900. Logged Personal Use Exposure (data confirming the presentation of personal content to a viewing vehicle) is uploaded at 168 to the Compensation unit 900 via Network Access Points (NAPs) in the same manner as logged Advertising or Public Service Exposure is uploaded from moving objects. Such logged exposure is sent to Distribution 800, where it is matched with Personal and Fleet/Government Use Profiles as shown at 175. Once content deliveries are matched and authenticated (by confirming that the codes on delivered content match the codes on the receiving moving object and also cross-check with the originally uploaded content), then the Compensation unit authorizes the fees charged for such Personal Use Exposure to be either billed to the Registered Owner 1000 or subtracted from any Compensation that is to be paid to that Registered Owner as indicated at 178.

[00204] FIG. 5 is a block diagram depicting a typical owner registration process for the present invention. The basic procedure for completing online registrations are commonly known today, so it is the purpose of this diagram to describe the steps and decisions a consumer might make in engaging with the business of viewing and displaying hyper-relevant ads and personal communications. Two parallel engagement paths are shown, reflecting a preferred embodiment including a land-based vehicle. Both paths describe a consumer's entry into the distribution network beginning at 402 for Pre Existing (or aftermarket) Vehicles and at 404 for New Production Vehicles.

[00205] Beginning at 402, the consumer of a Pre Existing Vehicle bears the responsibility for buying, installing and setting up the hardware and software through which he participates in the distribution network 800. This can be accomplished through a purchase of the electronics package from an automotive dealer (followed with installation by that dealer) or it might result from the purchase of the package from an automotive accessories or aftermarket retailer and could be installed by the owner himself. Regardless, the process of registration and membership which follows is essentially the same for both user paths.

[00206] At 422, using a computer, a modem and an online browser to interact with the aftermarket manufacturer's web site, the prospective user submits his Vehicle Identification Number (VIN) and other required information, such as (pending final registration and contractual requirements) his Driver's License number and other necessary information such as the brand, year, make and model of his vehicle, unless such data is provided for in the VIN, and Credit Information. The physical characteristics of each vehicle—height, width, driver's eyepoint (or eye envelope), number of occupants when at full capacity, etc.—are pre-encoded, either as part of the registered VIN, or under each owner's vehicle profile by make and model. In practice, these specifications are transmitted between moving objects so that optimum, yet minimum, spacing between moving objects is always established when stopping in traffic with precise line-of-sight viewing angles based on the different vehicle types. For example, a driver's forward sightline through a windshield at a height typical of a low sedan or sports car to the rear area of a tall SUV will result in a more upward angled sightline and a specific bumper to bumper vehicle spacing requirement; conversely, a line-of-sight through the windshield of a taller SUV to a video display on the aft surfaces of a low sports sedan would result in a more extreme downward viewing angle and yet different kind of vehicle to vehicle optimum spacing; and finally where an SUV to another SUV of similar height would produce a more horizontal sightline and yet another specification for vehicle spacing. In other words, because interacting vehicles

talk to each other and exchange VIN numbers, the lead or stopped vehicle is able to tell a vehicle approaching from the rear precisely the best place to stop for the optimum viewing of its rear mounted display. In every case, the proximity measurements and the vehicle-to-vehicle spacing (further discussed in FIG. 17) is governed by vehicle codes so that optimum sightlines are established for content delivery and so that the tightest practical spacing between all so equipped vehicle types is assured, which conserves traffic lane consumption under practical traffic conditions. Vehicle-to-vehicle lane space conservation enabled by a visual range/stopping indicator is a valuable byproduct of the present invention.

[00207] Continuing the online registration process at 434, each new user has the opportunity to register, or allow other drivers or passengers in the family (or in the business if a fleet application) to register, along with the ages and genders of any children or other family members who might be passengers in the vehicle under that VIN. At this point, each family member can establish his own user name and password if they wish. If that person is underage, or if it is preferred by the Registered Owner (who normally becomes the System Administrator for the VIN), then he or she will control access to the system and to any profiles that are later completed for such family members.

[00208] At 438, these user names (or nickname handles) are programmed into the vehicle's User Selector 780 (explained in more detail in FIG. 7). This control allows consumers to switch the viewing preferences on-the-fly from one person to another, or combinations thereof. However, final control can always remain with the vehicle's System Administrator. In other words, dad controls who gets to see what while riding in dad's car.

[00209] At 443, family members are allowed, in the privacy of their own home, to select their individual ad viewing preferences. Here, each member of the family (or the authorized users in a business) can execute multiple choice, click-on, or write-in-the-box text responses which allow them to define "who they are" and "what they want" in terms of their personal interests, wants, needs and experiences, and in the kinds of advertising they would like to view.

This profiling technique is explained in detail and is the subject of the applicant's nonprovisional patent application serial number 11/552,932, filed October 25, 2006, entitled: "METHOD AND APPARATUS FOR OBTAINING REVENUE FROM THE DISTRIBUTION OF HYPER-RELEVANT ADVERTISING THROUGH PERMISSIVE MIND READING, PROXIMITY ENCOUNTERS AND DATABASE AGGREGATION", incorporated herein by reference in its entirety.

[00210] Using an individual's home or office computer, a networked laptop, a PDA or even a cell phone, user personal profiles can be updated and submitted periodically from nearly any location having network access. Also, because ad preferences can be highly personal in nature—and because they directly influence the kinds of products and services, or the kinds of entertainment and lifestyles a user is interested in or curious about—it is possible for users, at 443, to select and control the timing and circumstances for all outgoing content requests. For example, if an individual is interested in certain kinds of personal products or subject matter which he prefers remaining confidential, when he completes this portion of his Personal Ad Viewing Preferences, he can limit such content requests, for example, to only the times he is alone in his vehicle. It is also possible to control the external display viewing angle so that others in vehicles adjacent to a viewed vehicle are unable or less able to see any content that is displayed.

[00211] In a similar manner, a user can prevent certain kinds or all kinds of advertising to be presented to him by other objects at the time he is operating or is inside his own moving object. If a user finds certain content to be of little or no personal interest, or if he finds it offensive or objectionable, he can prevent its exposure to himself and to others who may be with him or are in the immediate vicinity. The present invention accomplishes this simply by deleting or preventing content requests based on a specific user's stored profile. When a user prevents the display of such content to himself, he also precludes the displaying party from earning any compensation from such display. Thus the present invention is in many ways a very democratic

process.

[00212] For parents of young children, the system is a tremendous advantage. Under a preferred embodiment defining a land-based moving object, when kids are traveling in their parents' vehicle, parents can prevent certain ads or content which they feel are inappropriate from being displayed on moving or fixed objects around them. When the kids are no longer in the vehicle, those ads can be switched back on or allowed.

[00213] At 445, the Registered Owner of a Pre Existing Vehicle can also determine his own and his family's Viewing Protocols. Preferences can be switched on or off depending upon the occupants of the vehicle, or whether the party responsible for the vehicle wishes to allow or to prevent ads from being viewed by any other specific party. Research reveals that kids today truly enjoy watching commercials as long as they deal with subjects they are interested in. So if kids are misbehaving, parents might just threaten to shut off their ad viewing preferences for the rest of the way home.

[00214] A wide variety of ad viewing features are expected to be implemented by the individual manufacturers of moving objects under the guidelines framed by the Distribution network 800 and government regulations relating thereto. For example, such features might allow users to give weight to each family member's preferences in terms of time sharing during use (e.g., 20% to dad's preferences, 30% to mom's preferences, with the kids splitting the remaining 50% evenly, assuming they've been good). These preferences are interpreted into signals broadcast to other moving or stationary objects in the vicinity, thereby controlling the variety and nature of the ads polled and selected for presentation by such other objects. Based on each vehicle manufacturer's specifications and on network content guidelines, the application of user preferences can be further controlled, either automatically or manually, based on the time of day and event location. For example, if mom is running around all day doing errands, then picks up the kids and delivers them home or to a friend's house between 3:00 PM and 4:00 PM, she can set the preferences to favor herself up until 3:00 PM, then engage the kids preferences for an hour,

then instruct the vehicle to switch them back automatically to hers after they've been dropped off, or she can do this manually. Just as in the design and execution of vehicle air conditioning and entertainment control systems, it will be up to each manufacturer to design and integrate its own version of these controls for marketing, human factors and user friendliness under its own quality control and operating standards, providing of course they also comply with any federally or more universally mandated system standards.

[00215] At 455, after completing membership, viewing, and protocol preferences, the newly Registered Owner of a Pre Existing Vehicle is presented with the network's Distribution and Compensation contract terms and conditions which he must read and sign electronically. Finally, at 465, he submits his profile package and executed contracts online to the Distribution entity 800 for approval.

[00216] In the second engagement path, beginning at 404 (and also under a preferred embodiment using a land-based vehicle), an owner has purchased or leased a New Production Vehicle with the ad display technology built in. As we saw in the family scenario, the dealership has pre-registered the vehicle using the new owner's Driver's License number which has been linked to the new product's VIN. At 420, this new owner completes his registration process using the automaker's Home Enrollment community web site.

[00217] It is beyond the scope of this document to describe the various potential methods of consumer profiling or content encoding, because these are straightforward processes well known to those skilled in the fields of demographic and psychographic analysis and in the arts of interpreting the subjective elements that comprise human interest and commercial engagement. Regardless, the process begins in FIG. 5 at 420 for New Production Vehicles (continuing through steps 432, 436, 442, 444, 446), and at 422 for aftermarket vehicles (continuing through 434, 438, 443 and 445), as consumers are asked in separate profiles to generally define "who they are" and "what they want" in terms of relative life experiences, expectations, beliefs, interests and objectives regarding various types of products or

services. This may extend to specific brands, product makes, companies or even political affiliations. Such profiles are executed in guided, online question and answer sessions which combine multiple choice questions and unstructured text responses designed to encourage individuals to better know and reveal themselves and their unique personalities. These profiles can be later analyzed for hidden relational values and meanings utilizing proprietary deep-search software designed to identify personal characteristics that individuals are often unable or unwilling to define for themselves. The methods for creating and gathering such personal information through profiling are well known to professionals in the fields of psychology and marketing. Also known are the methods of quantifying, weighting, characterizing, prioritizing, integrating and ultimately linking such results to the selling of products and services, along with methods of encoding and encrypting such data once it is created. What is novel is the present invention's method of directly asking consumers—and asking in significant detail—about the commercial content they are most interested in seeing and hearing about, and then enabling them, through a technological structure and system, to request, poll, queue and present such content on a time and venue specific basis at a time they are most open and receptive to such information.

[00218] The following steps, Registration of Additional Family Members (432); Assignment of Family/User Names to Preference Selector (436); Family Member Selection of Personal Ad Viewing Preferences (442), and Registered Owner Determines Viewing Protocols (444), are essentially the same as discussed for the Pre Existing Vehicle registration path.

[00219] At 446, however, the new vehicle owner is given a chance to determine his vehicle's Display Preferences, something preexisting vehicles are unable to do unless they are equipped with an external or internal video display. Generally, most content scheduling will be performed at the media buy level. In other words, there is a media exposure hierarchy which determines the value of a given ad's impressions based on the platform's ability to reach specific audiences at specific times with specific and hyper-relevant

messages—and for the first time with the present invention—in very precise locations. Such media buys will be significantly more valuable to certain advertisers and will therefore command high price tags to the advertiser. If a Registered Owner is able to deliver large numbers of impressions in high-value markets, then he would also logically share in the receipts generated by that particular platform, in this case his own vehicle's VIN. For this reason the applicant envisions small business spin-offs involving individuals or small companies that could register large numbers of moving objects primarily to circulate ads within the high value target markets such as the downtown areas densely populated cities. Should this generate unnecessary traffic flow within these areas, procedures could be put in place to prevent such random increases.

[00220] Because content deliveries are essentially automated and represent sophisticated media buys (sensitive to content type, viewer demographics, locations, delivery times, etc.), and because most consumers will always want to optimize the revenue generated by their delivery platforms, it is best for consumers to set their display preferences to automatic. Automatic display references are designed to generate the greatest revenue by targeting and giving priority to the highest value markets first. In this regard, at 446, both the consumer and the Distribution entity are without conflict of interest. In determining one's own display preferences it is also possible to be relatively selective. For example, profiles will allow Registered Owners to preclude (or "blacklist") any companies whose products or services it prefers not to advertise, promote or display. In so doing, that owner also forgoes revenue from those precluded display ad opportunities. Examples might include individuals who wish to boycott certain products or companies. Another might be political candidates for one party or another, especially near election time. Therein lies another responsibility for Distribution, and an inherent feature of the present invention: political promotions in and around polling places can be electronically monitored and prevented. The reverse is also true. If an individual favors a particular company or product, he can request a priority for

the display of content relating that company's products or services. At his option, he can also buy a corporate sponsorship for that entity. However, each such selection is likely to have revenue consequences for the Registered Owner.

[00221] At 448, media platform owners are able to implement another step in determining the use of their assets: selecting their Personal Use Preferences for their own moving objects. Because personal ad placement decisions also bear on the VIN's overall ability to generate income, only the System Administrator for that VIN (usually the Registered Owner) is permitted to authorize them. This is done easily and privately by the consumer following prompts on his user/community web site. Such personal use is typically charged at a discount since a family or individual will be using his own asset, but clearly such use will reduce revenues from that individual's display of content for others.

[00222] At 452, family members (or small businesses) are allowed to create and submit their own personal ad content for display on their own or on other moving objects. Such content can range from simple neighborhood business ads to very spontaneous advertisements applied to vehicles on the spur of the moment, such as displaying a High School's home team logo at game time. At 454, owners are given the chance create personal messages. These can be posted instantly and spontaneously, or on a scheduled basis, on an owner's own vehicle, or on other vehicles based on a standard rate. Such messages can also be accompanied by audio content sent wirelessly to a viewing vehicle's on-board audio system, or released within a viewing vehicle from its internal hard drive, based on a received code. There are many such examples of personal ads, sponsorships or messaging: a political candidate might email you an animated electronic bumper sticker from their campaign office which, if you approve, you can then send directly to the back of your car at the click of a mouse. Another such spontaneous message might be a "For Sale" sign on the back of a vehicle, linked to "impulse request" electronics as a means for obtaining information on-the-fly (a feature described in more detail

at 782 in FIG 7). Another example might be a "Just Married" sign appearing on, perhaps, all of the vehicles in a wedding party, or a "Need Help" alert if problems are encountered on an open highway. Any number of spontaneously posted personal messages is possible providing they meet the Distribution entity's Standards and Practices for Personal Content review and are approved at 842 in FIG 8. As explained later, this unit can electronically screen and then lock out certain graphic content that may be commonly viewed as offensive in terms of public exposure, or beyond the bounds of reasonable free speech. Such content is submitted by the Registered Owner online and once screened, can be scheduled for automated release, or can be stored on the VIN's hard drive for spontaneous or manual release by the owner in the field. The display of Personal content will be accompanied by a standard fee for the level of exposure anticipated (based on the time, place and market for that impression) less any discounts, and the transaction would show up on the VIN owner's monthly statement. Personal Use charges would normally be discounted and debited against the Registered Owner's monthly income check. The broadcast of Personal Ad Content to other moving objects, however, would constitute a media buy. Such purchases are scheduled online at the going rates (again, based on the time, place and market for such impressions) and might possibly include discounts to large users or long-term memberships within the network.

[00223] The steps of Registered Owner Agreement with Operating Contract Terms (456); Agreement with Compensation Contract Terms (458); and Registered Owner Submits Profile for Approval and Distribution (460) are similar steps to those previously described for Pre Existing Vehicles.

[00224] Step 470 indicates an ongoing process whereby Registered Owners are able to, or in fact, encouraged to periodically update their profiles and memberships for the viewing of hyper-relevant content, and to submit any new personal content for approvals to the Distribution entity 800.

[00225] It is not the intent of this disclosure to teach the ways in which personal profiles should be structured, but to leave that to the marketers and planning

experts skilled in the art of interpretive research for consumer interests and responses. That said, it is an object of the present invention to facilitate a means to learn the degree to which individuals are interested in, curious about, or leaning towards, purchases in such areas as transportation, foods, clothing, real estate, banking, finance, investment, consumer goods, toys, medicine, entertainment, social networking, communications, education, advanced technologies, sports, politics, current events and the like, along with relative specifics on the timing for such interests or prospective purchases, together with identifying the kinds of information that link such interests to specific kinds of lifestyle and content delivery. It is also an object of the present invention to allow for special events, for example when a mother is searching for birthday ideas for a teen son, or a husband for a wife's anniversary. With the ability to include such hyper-relevant interests and needs into the system and to later remind users of upcoming events, automatically and on a timely basis, the present invention is able to take hyper-targeted or hyper-relevant marketing and promotion to entirely new levels of performance.

[00226] FIG. 6 illustrates a first embodiment of a land-based moving object 650 where the integration of the hyper-relevant advertising display system can be clearly seen. The vehicle design and package shown follows an anticipated design evolution timeline and exhibits rear body surfaces that could naturally accommodate the display technology. A formed, printed OLED (or alternative) display 760 is present, with surfaces contoured to meet the desired rear deck lid and body panels of the subject vehicle. The display 760 is seamless and, in this example, runs the full width of the rear (5th) door; however, numerous configurations are feasible. The display 760 would be placed above the rear bumper impact zone, but may ultimately be considered a replaceable automotive crash part.

[00227] It is quite clear from this illustration that the proper design and integration of automotive digital rear ends can thoroughly enhance the aesthetic qualities of production automobiles while they optimize the

functionality of the components they replace such as tail lights, turn signals, center mount stop light, back up lights, license plate lights, recesses, plates, frames and registration. At the same time, the single panel, lightweight display offers complete freedom for the automaker's model and branding, and in fact, introduces, for the first time ever, an ability to animate the way a vehicle brands, identifies and/or expresses itself. Of greatest importance, however, is the area of display 760, which can extend the full width of the rear hatch, and enables full motion video for the presentation of advertising content. A primary advantage of using formable and flexible organic light-emitting diode (OLED) displays for automotive applications of the type proposed by the present invention is that such display panels can be formed consistently with the design objectives of the original vehicle. By example, the incorporation of a conventional flat panel display in the size and type of panel shown in the figures would consume a prohibitive amount of the inner body panel cavity which is necessary for other vehicle functions. Also, because flat panel displays are not flexible, they cannot be integrated flush with a contemporary automobile's surface contours. This means that with the exception of tiny flat panel sizes which are too small for displays which can be read at appropriate distances, flat panels will produce undesirable surface reflections and significantly unrefined design appearances. OLED displays, FOLED (flexible organic light-emitting diode) displays or PHOLED (phosphorescent organic light-emitting diode) displays plus FOLED substrates which can be laminated into various types of automotive glazing, when combined represent an unending array of affordable video display opportunities for production body panel surfaces. Shown here at area 765 is a single corporate logo (in this case Apple Computer) in what might be called a "sponsorship" mode. This mode is commonly used while traveling at freeway or highway speeds, is designed for easy reading from greater distances and would permit only minor color changes or enhancements so that it would not attract the attention of nearby drivers. The display panel's background in this example could carry the same color as the vehicle's exterior finish allowing complete emphasis to

be placed on the logo (the current ad content) as it is presented in this example. The moment this vehicle begins to slow, the logo would softly dissolve and brake light "zones" would appear simultaneously on the right and left sides of panel 760, along with the federally mandated center mount stop light just above the Apple logo seen here. At the same time, it is likely that license plate identification would appear in large, easy to read, well-illuminated graphics, perhaps in the center or to one side, depending on the automaker's default design. It is possible that brake light/turn signal/marker light portions of the digital rear end could change color and transition from pale amber through bright amber to amber-red, to rich bright red for the hardest braking. Such transitions in color and brightness, spread over more time and a greater panel area (while retaining the familiar left side / right side tail light visual separations which can help drivers gauge distance) provide increased levels of information relating to stopping urgency, compared to current brake warnings which transition between full on or full off, and which can lead to over-stimuli and panic stops as they so often do today. Of importance in the present invention is that during any speed or maneuvering changes the ad content slate is gently wiped clean so as to be totally non-distractive. At this moment, in fact during any vehicle maneuvering, vehicle lighting, licensing and FMVSS safety and performance systems take clear precedence over any other visual or graphic imagery on that portion of the vehicle. In other words, the present invention needn't introduce any new changes in the ways moving objects are viewed today. Drivers who are engaged with the present invention need not take their eyes off the objects moving in their paths as they must do today when viewing roadside advertisements and signage. In practice, the graphic surface character of a moving object may simply dissolve and change before a driver's eyes, but only at predetermined times (generally when fully stopped), and then always by transitioning to greater levels of safety and visual standardization at critical times. The present invention, therefore, promises not only richer, more relevant and meaningful commercial communications, but also greater operational highway and traffic safety through the optimization

of uniform vehicle lighting and safety systems. The creation of common visual and lighting standards for motor vehicle braking, turning or hazard alerts, particularly in the form of solutions that can intercommunicate between multiple vehicles to more smoothly convey slowing or arising hazardous conditions to following drivers will have a greater positive impact on highway safety than do today's variety of unrelated designs and visual subsystems. The present invention allows such standardization and functional optimization for road safety and operations, while at the same time opening up greater opportunities for vehicle design creativity, product styling, branding, and free market expression. The possibilities are unlimited.

[00228] One of several possible locations for the electronics package which enables the present invention is indicated at 660. In practice, the entire unit would, in terms of today's technology, be roughly the size of a paperback book and could be located almost anywhere.

[00229] A roof location is indicated at 712 for the download antenna to receive both content and delivery instructions from antennas in parking garages, residences or on the open highway. An upload antenna is indicated at 715 for transmitting on-board data and information relating to in-field content requests and deliveries to network access points for measurement, accountability, confirmation and compensation. These antennas can be combined into a single unit or can be placed individually in numerous locations on moving objects. A possible location for the receiver which detects encoded content requests broadcast from other vehicles, as well as a potential location for a rear-looking proximity sensor (which is further described in FIG 7), is indicated at 744. The vehicle spacing technology of the present invention, described hereinabove, enables display 760 to produce a color "spot" or visual target in the area 765, which then changes color (from green, through amber, to red) to encourage drivers to close up and position themselves at the optimum distance for viewing content and for the closest practical spacing between vehicles in an effort to conserve lane area, based on their precise vehicle types.

[00230] A front-mounted location is shown for the code transmitter 742 which sends VIN numbers, encoded user profiles and content requests, or combinations thereof, generally forward to a variety of vehicles or stationary objects for the purpose of selecting and queuing content from their internal or integral system data bases. Transmitter 742 could also be used to transmit video data from the requesting (viewing) vehicle for display reproduction on such other vehicles or on surrounding fixed or mobile objects which are equipped to interact with the present invention.

[00231] A general position is indicated for the optical sensor 1820, which reads traffic signal light color transitions and cross traffic flows as part of the Intersection Clock 1800. The Intersection Clock 1800 is an independent system which determines the time available for the display of video content at times vehicles are paused in traffic, and generally at times vehicles are stopped for traffic intersections. Optical sensor 1820 would be placed at or above eye level to the vehicle's operator and, in the case of the land-based moving object 650, could be integrated into the back side of the interior center rear view mirror case, as is often the case with headlamp sensors in contemporary passenger cars.

[00232] FIGS. 7-10 illustrate a low-cost flat panel embodiment of the present invention in a SUV 651. This application represents a non-optimized version of the present invention, suitable only for the limited production conversion of existing vehicles rather than fully-integrated OEM production. The basic elements comprising an aftermarket body panel conversion are shown as: a flat panel video display 761; a sheet metal or composite structural shell or pan 763, which provides both structure and protection for the electronic components; and a glass or plastic protective shroud 766, which both seals and keeps the video display 761 clean and secure. These elements are separately assembled, then mounted in various types of body panels from current production, after which they will be weather tested and final checked for electronic performance. The electronics package is shown at 690 and is described in more detail in a later section. Additional components may be

required and depend upon the types of vehicle and installation required. FIGS. 7-10 show four views of a typical installation an SUV type vehicle. All of the examples indicated in FIGS. 7 through 16 represent conversions of existing production automotive body panels as opposed to installations on an original equipment assembly line. The intent is to address this lower cost, lower volume market as an interim step in bringing the invention to market at an earlier date and at more affordable development costs.

[00233] Two types of installations for SUVs are shown in FIGS. 7-10, a vertical mount in the sheet metal portion of the lower rear hatch (FIGS. 7-8, 10), and a horizontal mount which is viewed through the SUV's rear window (FIGS. 9-10). Both are designed to provide excellent viewing sightlines with respect to the occupants of a following (viewing) vehicle without consuming significant amounts of interior space or vehicle utility in the host SUV. A vertical installation is indicated at 767, and is preferred if there are no inherent obstacles such as an externally mounted spare tire (as shown in FIGS. 9-10). The horizontal video panel mount, shown at 768, can fold out of the way in the event large cargo must be carried. When in position, however, the display shown with mount 768 directs its video image upward into a partially silvered mirror, actually a flat glazed panel 769, where it is reflected rearward for viewing through the SUVs rear window. Since panel 769 is partially silvered on its lower (front) surface, it reflects a clean image and the driver's rear vision is unobstructed. The picture image output at the flat screen is, of course, reversed electronically for this application. For cargo access or maintenance, the mirror panel 769 swings away against the overhead as shown in position 771.

[00234] Today's off-the-shelf displays can perform the display functions nearly as well as the more advanced displays discussed herein and perform on a near-cost effective basis within the proposed business models. It is a simple matter to modify the aft hatch of a common SUV to incorporate a conventional flat screen television or monitor into its non-glazed sheet metal portion. It is also quite reasonable to position a flat screen monitor horizontally (on its back

facing up), then place a partially silvered mirror at roughly a 45 degree angle above this display so that the image can be viewed through the rear window of the SUV without compromising the driver's rear view through this same rear window as also shown above and in FIGS. 12-13 and 15-16. Such a mounting retains the display within the vehicle, protected from weather and vandalism, and does not require modification of the external sheet metal surfaces. The mirror and sightline bending solution represents a novel installation of a large scale flat-panel display in a contemporary vehicle.

[00235] FIGS. 11-13 illustrate a general embodiment of the present invention in a passenger sedan or taxi 653. The most common installation for sedans or taxis will most likely be the vertical trunk mount 767. However, until vehicle licensing, plate lighting and registration issues are addressed, the rear license plates will need to be relocated to provide a full width display as shown at 773 in FIG. 11. Again, this unit comprises a structural pan and a video panel assembly 775 along with a protective weatherseal glazing 766. These installations would be made, fully tested and color-matched to vehicles to special purchase order. Installations would then be performed in only minutes by removing the original trunk (which would later be converted to a video display) and by installing the electronics package 690, along with wiring, into the vehicle's power and control systems. It is anticipated that the display system (which is normally on when the vehicle is operating) could be separately controlled by the driver and that such control would be exercised via a handheld remote which interacts directly with electronics package 690. This package, as will be later seen, contains the upload/download antennas, the central processor, and the hard drive for content and delivery instruction storage, along with supporting systems, sensors and drivers to control the video display. In FIGS. 12-13, a horizontal interior mounting 768 (like the SUV) is shown beneath the rear window on what is termed the package shelf. Again, a partially silvered or one-way mirror 769 allows the reversed video image to be properly viewed from the vehicle's exterior without obstruction to the driver's sightlines through the sedan's rear window.

[00236] FIGS. 14-16 illustrate a general embodiment of the present invention in a station wagon 656. Again, the vertical mount full assembly 775 is shown before installation in the lower sheet metal of the station wagon's rear hatch, with its protective glazing cover at 766. As a secure alternative without the necessity of modifying any exterior body panels whatsoever, a flat panel display can be easily mounted on the interior of the station wagon with minimal infringement on the vehicle's cargo capacity below the window line with a horizontal mount 768, in the same configuration as in the SUV. The partially silvered mirror is shown again at 769 (in both side and end views), and will swing away in the event more interior space is required. Again, interior installations are not the optimum solutions as with fully integrated new vehicle production, but they are viable for the operation of a robust conversion market which will allow the users of new or used production vehicles to realize significant revenue streams from their own motor vehicles and the present invention early on. As before, the electronics package 690 to drive either of the display installations is also shown.

[00237] In terms of market size for the aftermarket conversion segment of the present invention, the applicant envisions an orderly phase-in based on the upfitting of video-equipped interchangeable body panels for the most popular makes and models of current production vehicles. Later, these panels (such as rear hatches and doors, trunk lids and pickup truck tailgates) will likely be offered as options through new car dealerships and sold in the same way as any other high-end automotive accessory. Eventually, when it becomes apparent that the present invention can generate significant revenue for all vehicle owners—indeed, incomes which can virtually pay for the purchase of the vehicle—the present invention will find its way into full original equipment manufacturing for motor vehicles and will be mass-marketed accordingly.

[00238] The present invention would be covered under traditional automotive and property insurance just as any other automotive component. As a removable panel, the present invention is easily replaced in the event of impact damage, theft, or other types of loss. Theft, at least for the purposes of

generating revenue for the display of content, is not likely to yield success for the thief due to the integral safeguards of the network, discussed elsewhere. In terms of cost, such a product might today add, conservatively, $2,000 to the base price of a vehicle when fully installed. Normally, in the world of automobiles, this would be totally unacceptable but this happens to be a revenue-producing component. Using the simple income streams previously established and proven for the display of non-video vehicle advertising—and even without the commanding visual performance or the extraordinary flexibility of demographic and proximity hyper-relevant targeting—the present invention could completely pay for itself in less than 10 months and then produce positive cash flow for its owner. Meanwhile, the costs for converting to a vehicle containing a system according to the present invention would be virtually unnoticed in the financed monthly purchase or lease payments.

[00239] The applicant is unaware of the existence of any commercially-viable, low cost panel conversion alternative capable of generating revenue for the mass-market and general driving population through the display of hyper-relevant video advertising on moving objects, let alone the transmission of audio sounds to viewing vehicles, the subsequent control of such content by said viewing vehicles and the electronic distribution, measurement, engagement tracking and the later downloading of mass-market, ad hoc collected information together with owner/operator compensation.

[00240] FIG. 17 is a block diagram depicting electronic vehicle packages for the present invention. With respect to land-based vehicles, New Vehicle Production is represented at 650, and Pre Existing Vehicles are represented at 655. Inside each New Production Vehicle is an electronics package 660, which has been incorporated into the vehicle's complement of electronics. Also standard is an external video display 760, shown in the embodiment as a rear-facing configuration, intended for viewing by a following vehicle, although side panel or frontal viewing is anticipated. Video imagery 764 is viewable by the occupants of a following (viewing) moving object.

[00241] The Pre Existing Vehicle 655 also has an on-board electronics package

680; however, it does not have an integrated video display. It is possible, as previously discussed, for such owners to purchase modular or add-on video displays so that they can benefit from the advertising display revenue opportunities. Such displays, however, are not likely to have the high degree of integration of a full Production Vehicle.

[00242] Looking first at the New Vehicle Production package, note the forward-looking signal 740 transmitted from each vehicle depicted. Signal 740 is directed generally forward from code transmitter 742, and typically contains content requests (as previously discussed) comprising encoded specifications about the specific VIN including its brand, make, model, and year, and therefore its physical dimensions, perhaps its color, method of purchase (buy vs. lease), whether or not it is a rental car, its home state of registration, perhaps even data relating to its mileage or condition. Many options are possible and this data can be interpreted into a wealth of valuable cues for marketers. Signal 740 also sends encoded "content requests" based on user codes and profiles for drivers and passengers who have completed them and who have engaged their user names at user selector 780 which enables such "requests" to be included in the VIN's mobile broadcast. A Pre Existing Vehicle 655 is capable of broadcasting a similar signal, shown at 750. However, as an option, transmitter 742 can be configured to transmit digital packets comprising 6, 10, 15, 20, or 30 second commercial video spots over short distances for immediate queuing and display on a viewed vehicle. Under most circumstances, transmitter 742 only needs to transmit DMV and user code content requests for the purpose of selecting and queuing content from the on board library of a viewed (display) vehicle. However, in unusual or special cases where specific content may not available in a viewed vehicle's database, content can drawn from the viewing vehicle and be transmitted wirelessly for display if both vehicles are so equipped.

[00243] Numerous means exist to transmit and receive such wireless signals (RF, optical, acoustical), any of which may vary in wavelength, strength, range, spread, duration, modulation, or encoding, and while such variations

may be dictated by venue, by the type of moving objects, by the numbers or speeds of moving objects, by weather conditions, by cost, by manufacturer, by federal or local regulations, or by the override or integration requirements with other systems and factors, it is anticipated that such signals will not interfere with other transmissions and comprise a roughly a horizontal spread pattern and range generally consistent with that of standard vehicle headlamp spreads used in night driving. In other words, the strongest signal will be transmitted straight ahead, in the direction a moving object is traveling, while the strength of that signal will fall off gradually to either side. In this way, VIN and user codes can be simultaneously received from following vehicles in differing strengths from side to side, but receiver 744 will always favor the strongest signal, which is typically from the moving object which is immediately rearward in the same path or traffic lane. It is further anticipated that to accommodate curved road conditions, RF transmission is spread laterally by either electronic or mechanical means (for example, by linking a highly directional antenna to the vehicle's steering as is done increasingly with turning headlamps, except electronically rather than mechanically) so that content requests are not merely directed forward, but also in the direction of the anticipated path, curve, or lane change.

[00244] Looking first at New Vehicle Installations 600, we see incoming content requests represented by signals 740 (750 for Pre Existing Vehicles), received at receiver 744, where they are passed on to decoder 746. Once decoded, this information is sent to central processor 722, where it is polled and matched with previously established marketing criteria which in turn permits the selection and queuing of hyper-relevant ads, public service, or personal content from hard drive 716. If signal 744 contains digital information for the reproduction of video, it will be decoded as such at 746, processed at 722, and sent to the display drivers 762, for presentation based on previously established delivery protocols.

[00245] Before content is released from on-board hard drive 716, two important things must occur. First, the amount of time available for a display of content

must be determined; however, this is optional. Second, that content must be reviewed at 722 for any overriding priorities, such as Public Service Alerts, Proximity Priorities, Personal Priorities, or Law Enforcement Priorities, any of which may preempt normal commercial messages. The task of determining the available time for content deliveries is done via the Intersection Clock 1800. Since traffic stop lights represent ideal times for content deliveries, it is important to know the timing of the traffic lights at a particular location, that is, i.e. when the light will change from red to green, and at what point in the traffic light sequence a vehicle equipped with the present invention has arrived. The Intersection Clock 1800 is an electronics component that uses a vehicle's on board GPS system (or its own internal GPS type of system) to identify a specific location or intersection on a city street or roadway where infrastructures (such as traffic signals or freeway onramp monitors) are used to regulate traffic. Once it has identified a given location using the GPS, the Intersection Clock 1800 checks its own database to see if there is any stored information that will provide the signal timing sequence for this particular intersection. Next, it searches for incoming radio signals from other vehicles equipped with the present invention already in that intersection in an effort to obtain or confirm the traffic signal sequence and to synchronize its clock with any other vehicles already there. If none exist, the Intersection Clock 1800 will then open a location file and create a traffic signal signature for that venue and will store that data in its on board database. It will do this using optical sensor 1820 which reads sequential amber, red, and green light changes and records the timing between these changes for all traffic flow directions. Once these timings are known, processor 722 can select and queue content corresponding to the remaining times available. The Intersection Clock 1800 is explained in FIG. 35, and content priorities are explained in FIG. 31.

[00246] While being constantly monitored for any incoming priority overrides at central processor 722, queued content is checked against the on-board speed/motion sensor 774 and the on-board proximity sensor 770, which establishes a vehicle range signal 772, necessary to calculate the proximity

and the relative positions and closing speeds between a viewed and a viewing vehicle. When previously established delivery criteria are met (content, time, place, speed, position, priorities, and previous deliveries), the selected content is released to display drivers 762 and to audio transmitter 725. The display drivers send video content to display 760, which enables the video imagery indicated at 764. If audio has been requested from the viewing VIN, it is synchronized to the video imagery and transmitted wirelessly from transmitter 725 directly to the requesting VIN's FM radio via vehicle interface 730. Alternatively, codes representing the requested audio content are sent wirelessly to the viewing vehicle via antenna 712 and transceiver 714 to hard drive 716, where they are used to queue the audio content corresponding to the video, and where it is then converted at processor 722 and delivered to vehicle interface 730 for reproduction over the requesting VIN's on-board sound system.

[00247] Two antennas are indicated with respect to the instant invention, one at 712, another at 715. Incoming antenna 712 receives transmission signals for the downloading of content and data via transceiver 714 for Encoded Owner/Operator Profiles 116; General Content Distribution 150; Public Service Content (road/weather hazard alerts, upgrades, etc.) 152; hyper-relevant ad Content 153; Driving Population Personal and Fleet/Government Public Service Content 154; and special programming instructions for ad hoc communications between vehicles 156. Antenna 715 enables the uploading of data and information gathered in the field which has been saved and stored on hard drive 716. Such information includes, but is not limited to: all Logged Content Exposure 160; Logged Public Service Exposure 162; Logged Advertising Requests from specific VINs 163; and Logged Advertising Exposure 164. Antenna 715 also enables the uploading of ad hoc research collected and stored on moving objects' hard drives (or on board memories) while in the field. Antennas 712, 715 can be combined into a single unit, depending on system design and the methods of distribution, and can be placed in a variety of locations on moving objects.

[00248] All content, along with distribution instructions (to whom and under what circumstances it is to be delivered), is uploaded from the Distribution unit 800, to hard drive 716 via transceiver 714. Such content has been previously and precisely encoded to conform to established advertising, public service, or personal content encoding guidelines and delivery instructions. Likewise, VIN information and the personal profiles associated with it are similarly encoded and uploaded at transceiver 714 to hard drive 716.

[00249] When content delivery is requested within a specific area (e.g., by a sponsor of a convention or exhibitor at a convention at the downtown convention center), these coordinates are wirelessly loaded via the Internet, along with the content, into the hard drive of all VINs operating within that physical area, for example, citywide. When central processor 722 receives information from a VIN's on board GPS system indicating that a vehicle is entering a designated area for content display, it automatically processes such requests and queues that content for display. Normally, advertising content is overridden by any emergency or a vital public service alert, should these occur in a common venue at the same time.

[00250] The on board vehicle power supply is indicated at 726. This would have a battery back up system to assure that license and registration displays are always operational and that the vehicle systems remain useable in the event of public service communications emergencies.

[00251] A vehicle interface is indicated at 730. This is a systems integration component which assures the proper interaction of the present invention with other components from standard mass production. Typical examples would be an interface which assures that incoming audio linked to a video to be displayed on a viewed vehicle is properly routed to the audio system of a viewing vehicle, that content displayed on a specific VIN's external display can also be monitored on that vehicle's internal display(s), or that a GPS navigational system, if separate, for example, is properly linked to the present invention's central processor 722 and to the Intersection Clock 1800.

[00252] At 780, the User Selector permits a Registered Owner and, if desired,

any member of a family or business, to activate his personal preferences with regard to that VIN's outgoing content requests. Again, the individual user names, passwords, preferences, and their individual priorities are maintained online and are authorized for use only on a specific VIN and then only by its System Administrator (usually the Registered Owner). The human interface will likely be a small touch screen which presents the user names that are currently active for the VIN (in other words, a text or icon listing of the individuals whose profiles are currently active and influencing the display of advertising and communications on other moving or stationary objects in the vicinity). Such a display might optionally indicate the relative percentages to which each user influences outgoing content requests and possibly which user's content requests are currently being displayed.

[00253] Linked to User Selector 780 is the Impulse Request unit 782. This component stores authorized user names along with securely encoded contact and credit information to facilitate on-the-fly communications and purchases by the vehicle's registered occupants while in the field. If a teen sees a commercial for a new skateboard, for example, he only needs to touch the screen next to his name to have information on that product sent to his email address, said address having been previously stored. He can just as easily have it sent from his mom's car to his pals. If mom spots an ad for a new book, or even a new blouse, she can buy those items at the touch of a button because her credit information—and even her clothing size—would have been previously encoded and stored. When she gets home, confirmation of her purchase will be on her computer.

[00254] At 794 is the Instant Messenger. How many times have you wanted to send back a message to someone who is following too closely? Or create a special sign for school, a ball game, a sale, event, or a play? How about instant, easy to remove bumper stickers? The Instant Messenger allows operators to pre-store text messages and special designs which can be called up and presented at the push of a button or verbal command. It also allows instant signs to be typed in using an optional keyboard or through the vehicle

interface 730, to receive input from cell phones or PDAs; however, software in central processor 722 continues to monitor all entries and precludes any offensive or objectionable words or content based on established system standards and practices.

[00255] The VIN/Plate Report 795 allows users to temporarily reveal another vehicle's license plate or identification and to cause it to remain displayed until a requesting VIN moves out of range or disengages its request. This report function can additionally record that license plate and VIN number for later access by the Registered Owner meaning that no one any longer has to search for a pen and paper to write down another driver's license number. If there is an accident involving multiple vehicles equipped with the present invention (such as a hit and run or a parking lot impact while you are away), such impacts are read by the proximity sensor 770, which then polls and collects information on all of the VINs in the immediate vicinity along with a time stamp, a GPS location and the speed of the host vehicle at the time. That data is then recorded into the hard drive for later downloading and potential use by law enforcement or insurance.

[00256] A Law Enforcement chip 748 can be programmed to enable a variety of features. First, this chip allows external law enforcement units (such as a pursuing Highway Patrol car or a helicopter overhead) to override the active external displays of a vehicle equipped with the present invention. Such overrides might cause a vehicle to reveal itself as stolen, for example, assuming such a report has been filed by its Registered Owner. In another example, surfaces on the subject vehicle might be caused to pulse or illuminate animated warnings in the event of such a pursuit, or perhaps to act as a primary source of illumination in the event of an open road accident or a disaster. The Law Enforcement chip can also sense tampering or hacking within the system and to optionally place a prominent advisory on the vehicle's external display, or to even lock certain systems including, but not limited to, suspending compensation to users who are in violation of the law. Technologies unrelated to the present invention are being explored to monitor

and confirm erratic driving behaviors which could indicate drivers who may be under the influence of alcohol or drugs. By linking such alternative technologies via the vehicle interface 730, and by further confirming such behaviors via proximity sensor 770 and speed/motion sensor 774, the Law Enforcement chip could permit an override of operational displays to replace them with an "erratic vehicle warning" designed to warn other vehicles or alert law enforcement in the area.

[00257] Thus far, we've learned that people don't really object to viewing ads about subject matter they are interested in. We've learned that kids embrace advertising when it deals with things that are part of their lifestyles and are curious about. We've seen that it is possible for consumers to create profiles that tell advertisers "who they are" and "what they want" so that marketers are able to select, design, and deliver hyper-relevant content to those individuals on a time- and location-specific basis. We've learned that content can be distributed to moving objects where it can be stored for future use or presented in real time on external video displays and through the audio systems of other moving objects. And we've learned that consumers can be compensated for using the exteriors of their own moving objects as commercial video platforms. So, with all this, it's certainly possible to apply the same technologies to present hyper-targeted content on internal video displays 765 inside moving objects as well.

[00258] Imagine a high-end executive taxi or a commercial SUV that is able to present hyper-relevant video displays both inside and outside the same vehicle and can accommodate content requests simultaneously by separate parties, one party outside in the traffic environment, the other inside riding as a passenger. Outside the Executive SUV, surrounding vehicles would interact as previously explained, requesting content electronically which is presented on the external surfaces of the vehicle. Such displays would most likely be placed on the rear facing Executive SUV surfaces so they can be easily viewed by vehicles following. They could also be placed on the sides of the Executive SUV so they can be easily seen by pedestrians on sidewalks or by

the occupants of other vehicles moving in parallel traffic lanes. But the inside of the vehicle would be configured differently. The interior would be more of a surround sound mobile theater tailored to combine a live travel experience through the presentation of highly-targeted information or advertising. Basic targeting would be done on a time and venue-specific basis; in other words, when passing retail stores, scenic attractions, and similar points of interest, any of these might be further described in informative detail or in graphic terms to enhance one's travel experience. Imagine displays embedded in glass that could superimpose graphics and information on the insides of windows so that such images would relate to, and in fact almost be superimposed over, passing real-world environments, events, and surroundings. Alternatively, envision a center-mounted touch screen console that carries a real-time camera-produced view of the passing cityscape, where all an occupant has to do is touch the screen with a finger to obtain real time information on those surroundings: the interiors of restaurants with menus, the inventory of special boutiques, or, perhaps, previews for new Broadway shows. Now envision a tiny wireless device that a person might carry in a pocket or purse which, like the hard drive in a moving object, is able hold all of your personal user codes and profiles and can transmit those codes via antenna 712, transceiver 714, and processor 722 to content hard drive 716 in your Executive SUV, so that hyper-relevant content that relates specifically to you and your interests can be queued and presented on the vehicle's interior displays.

[00259] Such a personal mobile device has been disclosed in the applicant's nonprovisional patent application serial number 11/552,932, filed October 25, 2006, entitled: "METHOD AND APPARATUS FOR OBTAINING REVENUE FROM THE DISTRIBUTION OF HYPER-RELEVANT ADVERTISING THROUGH PERMISSIVE MIND READING, PROXIMITY ENCOUNTERS AND DATABASE AGGREGATION", incorporated herein by reference in its entirety, and is referred to herein as MMx. MMx is able to receive, store, poll, extract, and transmit data and information in a similar manner to the moving

object electronics packages depicted in FIG. 17 at 660 and 680. When an MMx device is programmed with information about a person's interests and objectives, it can then communicate this information to other MMx devices, or to any vehicle or stationary object that is equipped with the present invention. In other words, by carrying an MMx mobile device, pedestrians can interact with moving objects in the much the same way as moving objects interact with each other. By electronically telling nearby moving objects who they are and what they want, pedestrians can have the same kinds of hyper-relevant ads and other types of information presented to them on the exterior of nearby vehicles. If a person with such a mobile device rides inside a Pre Existing Vehicle that isn't equipped with the present invention, that mobile device can engage with other moving objects in its path that are equipped with the invention and can then request and control the display of hyper-relevant content on that vehicle's exterior displays. At the same time, an individual carrying a properly programmed MMx device can ride inside the kind of Executive SUV described above, and at that user's option, convert that vehicle's normally targeted content into hyper-relevant content deliveries. Thus, a simple cross-town trip in a luxury SUV equipped with the present invention now becomes a rich guided tour like none other, because it is pointing out features and details of personal interest and curiosity. Such experiences would resolve themselves through the sound systems of the Executive SUV and a complement of advanced interior video displays 765. Such limited production fleet and special purpose vehicles are anticipated as a normal part of test marketing and full production ramp up for the present invention.

[00260] EARLY PRODUCTION

[00261] Early deployments are likely to be prototypes of Production Vehicles and specially designed fleet applications such as taxis, passenger-carrying commercial vans, SUVs, and crossover vehicles. It is also anticipated that early introductions of the present invention will be in the aftermarket conversion segment in which current, new production vehicles are upfitted with

easily exchanged body panels (such as rear hatch/doors on SUVs and tailgates on trucks) which replace the original components with those having built-in video displays. An electronics package containing a full hard drive and all telematics systems would be placed in a convenient spot elsewhere in the vehicle. This aftermarket package would, in one embodiment, include a radio transmitter with a directional antenna to send short range FM signals to a following (viewing) vehicle which would then be able to enjoy sounds through its own internal sound system, synchronized to the visual presentation on the aft display of the aftermarket conversion vehicle.

[00262] Using today's off-the-shelf technology, one can easily assemble an operating version of the described invention in the form of an aftermarket conversion. The simplest implementation is that of modifying any of the large numbers of aft-facing body panel and glass elements which comprise contemporary passenger sedans, pickup trucks, or SUVs. Most of these have hinged rear hatches which, by virtue of those attachments, are easily removed from the main body structure. This means that a low cost-of-entry business opportunity exists for conversions. In practice, this would involve a new vehicle owner who, after placing an order, would drive to an assembly station where his original hatch, tailgate, or trunk would be removed and be replaced by a modified or remanufactured product containing the display technology of the present invention. The flat-screen video display and wiring harness would be typically incorporated into the sheet metal portion of the aft door assemblies. These components could also be installed on the interiors of certain vehicles or on the horizontal surfaces of interior package shelves or deck lids. These are shown more specifically in FIGS. 6-16. Metallic structures would be modified to accept the new video display, displacing, if necessary, latch handles or rear window wipers. A tinted, formed, and tempered glazing panel would be fitted over the video display for both weather and vandalism protection and to provide a well-integrated appearance. The entire assembly would then be weather-sealed and tested. A wiring harness would be attached via a connector to an electronics package installed, in most

cases, beneath the rear seats or cargo shelf of the vehicle. This package would contain, among other things, a hard drive for the storage of advertising and display content, a central processor to control content distribution, a speed and vehicle motion sensor to govern content displays, an aft-looking proximity sensor to determine the presence of a following vehicle and to track its range and closing speeds, a wireless receiver to receive content with distribution instructions, a wireless transmitter to later upload in-field content delivery histories to the network and, optionally, an optical drive for the manual loading of content and control software. There would also be a hardware interface linking the electronics package to an on-board GPS navigational system for the distribution of location-sensitive content. The package would include an audio transmitter to send a corresponding audio channel to a viewing vehicle, either to its standard FM radio or via a special radio for receiving short range, encoded directional audio content signals. All of this would be controlled by the central processor and powered by the vehicle's on board power supply. When completed, the finished product need not appear substantially different from its original design except that it would contain a unique revenue-generating video display inside its newly attached rear hatch, tailgate, trunk, or door.

[00263] As an added feature, the electronics package might include an instant messenger provision that would allow a vehicle owner to place personal messages on the display at certain times. It is anticipated that such messaging would be submitted online and would therefore be screened for standards and practices and for any unwelcome content.

[00264] The greatest benefit in such an early deployment of the present invention is that it can quickly generate revenue for the owners of aftermarket conversions. Such revenue will quickly pay for the conversion itself, then go on to make the purchase and operation of the vehicle practically cost free, a significant accomplishment at a time drivers and owners are strained by increasing fuel costs and mounting traffic. Indeed, the presence of worsening bumper-to-bumper traffic sets the stage for the present invention in that

registered owners can now be compensated for their wasted time and fuel expenditures in traffic each year simply by becoming part of a commercial television advertising platform, one capable of totally offsetting their costs for fuel, leases, or purchases.

[00265] Vehicle owners will be paid based upon the number of impressions they deliver relative to the value of the demographic and the market served. As full scale production emerges, increasing numbers of vehicles equipped with the present invention will be able to interact. However, until there are large numbers of interacting vehicles, the advertising displayed on them will remain relatively generic, more often targeted to specific locations, demographic groups, or times of day, rather than to the specific interests of participating individuals. With increasing new vehicle installations 660, and more Pre Existing (aftermarket) installations 680, fully targeted and hyper-relevant advertising will emerge. Until that happens, the Applicant anticipates that the use of MMx-type devices will help enable the transition to full hyper-relevant public advertising and personal messaging. And, as previously mentioned, it is possible that business models will emerge to allow the Registered Owners of Pre Existing Vehicles 655 to be compensated for requesting and viewing hyper-relevant advertising. It is also conceivable, therefore, that the users of MMx-type devices could be compensated by advertisers for viewing targeted and hyper-relevant content.

[00266] Continuing with FIG. 17, Aftermarket Installations 680 are similar to New Vehicle Production installations 660, but do not include a video display, display drivers, audio transmitters, GPS, or as large a processor, hard drive, or memory. Personal (user code and profile) content is received for storage in a similar manner to full production units via antenna 712, and includes the downloading of General Personal Preferences for non-display vehicles 118; the downloading of Content Preferences 155; the downloading of Public Service Content (road/weather hazard alerts, etc.) 152; Ad Content downloads 153; and any special software or instructions 156 relating to the ad hoc collection of data (normally vehicle-to-vehicle) for widespread monitoring and

measurements. All downloaded content is stored on hard drive 719 and is processed at 718, where it is converted into encoded electrical signals for forward-looking transmission via code transmitter 752. Signal 750 is received by other vehicles equipped with the present invention via their receivers 744.

[00267] Vehicle Power Supply 726; Vehicle Interface 730; User Selector 790; Impulse Request unit 782; Instant Messenger 794; and VIN/Plate Report 795 serve the same functions in Aftermarket units as in New Production Units. If equipped with an interior on board display 765, such aftermarket installations could optionally present hyper-relevant advertising to their occupants, subject to safety standards for interior video displays.

[00268] After field use, processor 718 uploads to the network all in-field content requests that have been stored on hard drives 719 via upload/download transceiver 714 and antenna 715. In so doing, the following types of information are sent to the Compensation unit 900: Logged In-Field Content Requests from non-display vehicles 165; Logged Advertising Requests by VIN, by venue and time 163; Logged Personal Use Authorizations (including any view blocking or personal ads) 167; and Logged Personal Use Exposures or impressions 168 by VIN, venue, and times.

[00269] FIGS. 18A-18B show a block diagram depicting a Distribution model 800 for the present invention. This business unit (shown here separated from the compensation unit for clarity) is defined in terms of the elements essential for receiving, processing, and delivering a variety of content types to various moving or fixed objects in the field. Secondarily, FIGS. 18A-18B suggest potential funding relationships with the key parties to such a venture. At 110, potential incoming funding is indicated from various interested Government Agencies to Developers, Suppliers and Manufacturers of moving objects. At 115, the same is shown from the Advertising community, which could include large media companies or the advertisers themselves. By and large, however, it may be the makers and sellers of moving objects themselves that would support investment in such a Distribution entity, and that is shown as potential investment 128 and ongoing system upgrades 125 as part of production.

[00270] Across the top of FIG. 18A are represented the primary external user groups, comprising Government Agencies 200, Advertisers 300, the general Driving Population 400, and Fleet and Government Users 500. Each of these participating groups, which could be comprised of many sub-groups contributing to content production, submits such content in the same way they would if they were placing content with platforms such as network television. Participating Government Agencies thus submit public service content, such as state and local signage, hazard advisories, federal emergency content or local highway communications as well as vehicle licensing and registration matters at 250. Commercial advertising content submittals of all types are shown at 350. The input of Operator Profiles and Personal Content for the Driving Population is shown at 114, while the submission of Profiles and Content for Commercial Fleet and Government Users is shown at 116. Note that Government use has been depicted at both 250 and 116. Although Government use will resolve itself in many ways and applications, the depictions here assume that the uses anticipated at 250 relate more to regulatory issues and oversight in such areas public transportation and safety or highway development, whereas government use at 116 is presumed to be more vehicular in nature, such as law enforcement, border patrol, GSA, US Postal, and similar applications.

[00271] The first step in processing incoming content for Distribution is monitoring it for conformance to established content guidelines, standards and practices. This stage addresses both the message and the messenger in the sense that the content must meet approved content guidelines and the technical specifications required by the delivery platform, similar to the kinds of content and technical requirements that have to be met in configuring media for network television or outdoor billboards. These steps are shown at 802 for Government Agencies and at 804 for commercial Advertisers. Processing for the Driving Population is shown at 806 and for Fleet/Government Users at 808. Each of these steps involves the computer screening and approval of user profiles, the approval of user contracts and the monitoring of

subsequently submitted personal and business content. Methods and procedures for such monitoring and approvals are well known in the industry and ample precedents exist in parallel forms of media buys and content delivery. However, it is anticipated that increasingly sophisticated forms of image recognition and content rating methodologies will evolve, as will an increased use of the Internet for all delivery and accounting functions, which reduces the need for and costs of human intervention.

[00272] In contrast to major Government and Advertiser users, the Driving Population and Fleet/Business users will engage in the creation of exacting user profiles in order to define their terms of service, the delivery of their content and their use of the platform. Online profiles are completed by all consumers and businesses reflecting the essential "who I am" and "what I want" (WIA/WIW) qualities defined in the previously disclosed MMx patent application. They next enter into service agreements which define the responsibilities and limitations of each party, establish fees and costs and the range of potential earnings for each user type and variation. These steps are indicated at 806 for the Driving Population and at 808 for Fleet users. These are then brought together at 840 where Owner/Operator Profiles (which define user interests, wants, needs, and experiences together with their demographic and psychographic data, provided in non-identifiable formats which include no personal information) are approved and encoded to allow marketers to correlate specific types of hyper-relevant advertising content with specific combinations of user codes.

[00273] The next step, at 842, is the Review and Approval of Owner/Operator developed content. After content is approved, it is passed through the system for delivery encoding (described below). Once contract accounts are established, they are routinely processed at 854, Automatic Content Monitoring, where they are automatically monitored for consumer-requested changes, compliance, and consistency, all by computers programmed to also isolate and provide alerts for content nonconformance or contract violations. This business unit 800 will ultimately be linked to the Compensation Unit 900

and to any Customer Service components for the enterprise.

[00274] The first stage encoding of content following approvals is to determine the time of delivery; this step is shown at 820 for Public Service and commercial Ad content and at 844 for the Driving Population and Fleet/Government use. Time encoding determines a specific time of day that content is to be released to any requesting or non-requesting moving or fixed objects. In nearly all cases, emergency or hazardous road condition alerts, detours, blockages, flooding, and the like will be granted a time release which corresponds to the time of the event or emergency. Emergencies, as we will soon learn, are generally always given a higher delivery priority over other types of content. For example, if there is a traffic accident at a certain intersection and a detour is necessary, the time requirement would extend from the time the accident is first reported to the traffic response section of the network until the accident has been cleared from the area. If congestion is caused instead by road work that occurs, from 7:30 AM to 3:15 PM on a daily basis, then that is the time encoding that specific alert will carry. Both of those examples have a delivery priority over commercial advertising in that immediate area and the graphic nature of the content itself would be pre-generated and stored on all moving object hard drives likely to be in areas that would need it.

[00275] The next step in encoding is for location, or venue, as shown at 822 and 846. Venue encoding is, of course, critical for any type of proximity advertising or location-based communications. These can be in the form of relatively tight coordinates, such as an intersection or a specific address, because it will most likely be GPS based, at least initially. It might also be specified as a broader area, for example, as several city blocks surrounding a specific location such as a stadium, mall, airport, or theme park.

[00276] The third method of encoding is priority encoding which is shown at 824 and 848. Again, emergencies are given top priorities over all other types of content delivery including paid priorities. An important type of priority is based of the payment of priority fees, essentially for a preferred delivery priority over

other content in high value locations, or times of day, if not both.

[00277] The final encoding step is that of determining delivery fees based on the market value of specific times, places, and priorities that have been requested and scheduled. This step is shown at 828 and is not unlike establishing values that are attached to prime time television versus programming that airs during the middle of the day or middle of the night and varies due to the demographics and viewership at those times. There is no hard value for delivering a marketing message. It is worth something different to everyone. Therefore, any dollar figure is possible and that value is frequently established in a bid market.

[00278] The methods of delivering commercial advertising or public service content to the platform are more consistent and regulated than content such as consumer-generated personal content or small business content. A key step in determining the costs to consumer and fleet users, therefore, is in determining the actual methods of delivery to the active requested platforms, as is shown at 850. Such distributions would involve the Internet together with cable, satellite, or wireless and may vary widely with locations and available infrastructures. Once determined, however, content from all four basic user groups is uploaded at regular intervals at 830 and 852 to the various distribution infrastructures, represented at 832.

[00279] One vital function for the present invention, once it reaches a reasonable level of deployment, is the noninvasive, mass collection of content requests and deliveries by and from all moving objects in the field at all times of the day and night for any and all purposes. What this information represents, essentially, is any request for content by a moving object (with each moving object able to describe the precise nature, interests, experience and histories of its occupants based on WIA/WIW profiling) by location, by time of day, and by priority. This information is tracked through any other moving or fixed object which can store such a request for later uploading to the network and ultimately to the venture entity. However, all such information is collected in a non-identifiable, privacy-compliant format and, therefore,

cannot by itself reveal any confidential or personal information on users of the platform. The actual tracking of physical movements could only be reconstructed by using computers to link all of the requests from a single moving object to all of the other objects or fixed locations it has communicated with, and thereby to create a venue based "contact map" comprised of time and place, optionally with any requests or response to such requests. This is information that is massively collected and valuable to many kinds of marketers and planners. However, such tracking would only be reconstructed on a specifically identifiable party and revealed by the venture entity under a lawful subpoena. The instructions for the general collection of mass data and its insertion for downloading by the platform are shown at 890.

[00280] At 880, all documented in-field requests, all logged content distributions (or attempted distributions) together with any in-field responses to content deliveries (such as driving to a specific retailer immediately after being alerted to a "discount sale" at that location) for a requesting (viewing) moving object, are cross-checked by computer with the corresponding delivering (viewed) moving object. Such data could further correlate the demographics and interests of drivers and participating passengers traveling on various roadways at various times of the day including the types of vehicles, travel ranges, points of origin and destination, route variations or detours, even in some cases documenting the reasons for such changes; in short, a rich new body of data relating to the daily movements of drivers throughout our rural and urban transportation systems and community infrastructures worldwide. This data is then confirmed with the Distribution entity 800 to be certain such data has in fact been distributed into the network and was active during those claimed viewing periods. These are important steps incorporated to prevent the generation of false delivery claims for compensation, the equivalent of "click fraud" found increasingly in the online advertising business. This two-way data transfer is indicated at 170, as is the forwarding of confirmed delivery information to the Compensation Unit 900.

[00281] The aggregate distribution of content is shown at 150 in FIG. 18B.

Once content has been uploaded at 830 and 852 and its means of distribution has been selected via 832, content is distributed via the Internet (cable, DSL), satellite, or wireless networks, or combinations thereof, using electronic distribution infrastructures as indicated at 150 for receipt and distribution at a multiplicity of potential locations and environments. Included are: direct distribution to single family residences 860 and/or network access points (NAPs) in neighborhoods via the Internet, satellite or wireless networks such as WiMax; the same for residences but to condominiums, apartments, mall complexes or parking garages 862; direct distribution using the same infrastructures to office buildings, malls, retail stores and commercial, government or public service signage installations 864; direct broadcast to busses, trains, fleet commercial and/or public transit routes, airports, train terminals, docks and major roadways 870; direct broadcast to passenger vehicles on the highway via satellite, Internet NAPs or wireless such as WiMax, etc. 868; direct distribution to fleet vehicle parking or maintenance garages including emergency or temporary sites 866; direct to rural or remote locations such as outlaying towns or villages, rural highways, harbors, mountain, desert, beach or offshore locations 872; or other types of emerging and popular locations 874 where mobile proximity communications or commercial communications is desired or necessary.

[00282] The diagram in FIG. 18B further includes an antenna 151, which provides a wireless transmission point (a 2-way NAP or satellite downlink) for transmitting content, user codes and delivery instructions to other mobile or stationary antennas. A receiving antenna 172 is also present, typically found on moving objects or on stationary objects equipped with the present invention. Such antennas 172 not only receive content requests with user codes and delivery instructions, but also return encoded confirmations regarding the delivery of content by time and place along with accurate tracking information which bears on consumer engagement plus encoded data from a multiplicity of moving objects participating in the widespread collection of data on an ad hoc basis.

[00283] FIG. 19 is a block diagram depicting the Compensation model of the present invention. As previously mentioned, the compensation functions have been separated here for clarity but would likely remain an integral part of the Distribution unit 800 or of the primary venture entity. Although this unit can include numerous variables, FIG. 19 suggests a basic and essential flow of information and revenue with which to enable compensation to be paid to platform users.

[00284] This flow begins with composite data downloads from all platform vehicles. Such inflow is referenced at 905 and represents, in this example, data downloads from the hard drives of New Production Vehicles 660 and from the hard drives of Pre-Existing Vehicles 680. Such downloads would also include composite data from the ad hoc collection of user codes communicated between authorized or programmed moving or fixed objects, indicated at 1140. As previously mentioned, the widespread collection of such data has been heretofore unavailable. Its uploading from moving objects to the Distribution unit is shown in FIG 9 at 1160, and its sale to marketers and researchers is indicated at 1100.

[00285] While the inflow of raw in-field data may vary with vehicle types and delivery missions, incoming information will fall generally into two categories: Logged Content Requests from all vehicles (including Personal Use Authorizations from non-display vehicles) depicted here at 165, and all Logged Content Exposure (including completed or partially completed content deliveries) depicted here at 160. Within each of these categories, three content types are shown: For Logged Content Requests 165, there are Logged Public Service Requests from Specific VIN Numbers 161; Logged Advertising Requests from specific VIN numbers by venue and time 163; Logged Personal Use Authorizations from specific VIN numbers (including any view blocking or personal ads) 167; and for Logged Content Exposure 160, there are Logged Public Service Exposure 162; Logged Advertising Exposure 164; and Logged Personal Use Exposure or impressions by specific VIN, venue and times 168.

[00286] This information is next computer cross-checked laterally between categories. In other words, between the specific VINs involved, all documented Advertising Requests 163 are compared with all documented Advertising Exposures 164, thereby confirming both an in-field request and an exposure (an actual delivery) between these specific VINs, also verifiable by time and place. This comparative process is completed by computer and only when they are conclusively matched for each content type, are they encoded as being confirmed. Thus, at 910, all Public Service Deliveries are confirmed for a specific VIN; at 920, all Advertising Deliveries are confirmed for a specific VIN; and at 930, all Personal Use Deliveries are confirmed for a specific VIN.

[00287] The next step in this fully automated process is to determine that this content was actually released for distribution by the Distribution entity 800 at the times and with the proper encoding for it to have been requested and delivered in the field by the VINs in question based on their confirmed interactions. This means that the confirmed content collected at 910, 920 and 930 is routed to a Fraud Detection & Compliance Screening unit 940, where it is compared to the originally distributed data and content codes. This two-way cross-checking of all data is indicated in FIG 9 at 170. At the same time, Confirmed Ad exposures vs. distributions are indicated at 173; confirmed Personal and Fleet/Government exposures vs. distributions are indicated at 174,175; and confirmed Public Use exposures vs. distributions are indicated at 182. Why is this cross-checking important?

[00288] CLICK FRAUD

[00289] As previously mentioned, "click fraud" is a term given to a method of generating clicks (or apparent requests) for ads on the Internet in an effort falsely tally online "hits" and thereby show interest in those items—or responses to key word selections in search formats—in order to receive greater payments for those ads by reflecting increased apparent value, where, in fact, those ads have not actually been viewed at all. The present invention could be vulnerable to such fraud unless precautionary methods are implemented. Imagine, for example, a couple of teens using their own

vehicles, each of which is equipped with the present invention. What would prevent them from parking those vehicles in a driveway for an extended period in which one vehicle was allowed to constantly request content and another vehicle constantly display the content in order to show confirmed viewings or "impressions" and to then be paid for these viewings? There are a number of ways to prevent such fraud—and still others will emerge once such technologies are deployed—but as in most businesses and systems, combating fraud and assuring security must be a sustained activity. Meanwhile, there are a few basic monitoring and preventative procedures offered by the invention itself.

[00290] First, it is anticipated that such fraud or misuse of the invention would, or could, be treated like many infractions of the laws when operating moving objects. Such infractions could be linked to a person's driver's license in such a way that if you were convicted of such fraud, your right to generate income using the system of the present invention could be revoked, just as your driver's license could be suspended. In terms of generating proof of infractions, certain inherent systems exist in the invention which could be used to defeat such misuse. For example historic patterns for the actual requesting and delivery of content will be established over time and will be recognizable by monitoring computers set up to do precisely that. The requesting and delivery of content is itself a source of checks and balances. Each request is linked to a specific VIN, thus a pattern of requests from each unique vehicle is established over time as the vehicles operates (time, place, routes, consistencies, etc.). The same is true for the vehicles receiving such requests. Over time a "normal" pattern of requests and responsive deliveries are stored on each vehicle's hard drive in the same way as cell phone calls to certain parties are documented and stored for later use in accounting and billing. Furthermore, each such request and responsive delivery is linked not only to the respective VINs involved, but to the registered owner of those VINs, and to authorized use profiles connected to that registered owner which are on file in that user's account. Thus any sustained misuse can be traced to

a specific user as well as to any specific irregular pattern of misuse. Next the precise time and place of each request and each delivery is documented via GPS, along with exacting data as to the speed, the relative speed, proximity, attitude and direction of travel for the all of the vehicles involved. Also, of course, the consecutive number of similar requests and deliveries are carefully counted along with the duration of each delivery (since completed deliveries are important to the quality of service and to ultimate billings and compensation). There are also common methods of determining when drivers and passengers are actually inside a vehicle and which seats they are occupying as is used in seat belt and automotive safety systems. There are further methods which enable actual vehicle tracking over time. Thus, in the case of the teens, repetitive requests and deliveries between the same vehicles, which are apparently parked (regardless of their occupants), would place the event out of the normal "pattern envelope" and content deliveries could be subject to investigation and possible suspension. When such vehicles are moving there will be attentive drivers at the wheel and impressions made at progressive locations would likely be valid. Motion, speed, and proximity sensors within the system can further identify conditions during content deliveries. When time-linked to GPS information, specific time and place correlations can be made, and GPS tampering could be easily traced and documented. Indeed, tampering with linked GPS inputs with respect to a compensation system would probably be a Federal violation based on anticipated rulemaking for the present invention. It is conceivable that a pair of vehicles could follow each other at slow speeds and then stop, causing a number of content delivery events to occur over a prolonged period, but in fact such instances could also constitute legitimate content impressions or deliveries since their occupants must be attentive and viewing uniquely queued hyper-relevant content tailored to those drivers. GPS can also identify recognizable traffic patterns and relate them to specific environments, such as differentiating bumper-to-bumper traffic on a freeway or a surface street from a pair of vehicles parked in a residential neighborhood, or alone on a rural

highway. Additionally, if required, the Distribution system can compare and confirm surrounding traffic patterns by electronically reading the movement patterns of adjacent traffic equipped with the present invention. Again, in terms of differentiating traffic patterns that would be generated over periods of use, any repetitive incidence of two or more vehicle VINs which consistently request and display content to each other would become suspect. It can also be assumed that any great lengths to falsify content requests and deliveries between vehicles is going to be far more trouble that it is worth, will compromise the rights of the registered owner and (short of tampering or hacking the electronics which are monitored and protected under alternative criteria) is likely to result in the actual exposure of content to the persons involved anyway. A further barrier against fraudulent claims of content delivery is by comparing all claimed matched requests and deliveries to the original content uploaded to the network for distribution. Such content always contains release codes which describe the nature, time, and place that the content is to be uploaded to vehicle hard drives and is therefore available in the network for deliveries. These codes and/or their content may be changed as many as several times per day, thus, if artificial content or content codes are fraudulently generated they could be identified, along with the vehicles transmitting them.

[00291] Upon final confirmation, distribution fees are calculated for each content category, by specific VIN. These are shown in FIG. 19 as Public Service fees 915; Advertising fees 925; and Personal Use fees 935. The relative values for various fees are discussed in a later section; however, Public Service fees 915 and Advertising fees 925 represent income for the platform owner/user, while Personal Use fees 935 usually represent a cost to the owner/user, because he is displaying his own content on his own VIN or is paying to have his own content displayed on other VINs in the platform network. In other words, the Personal Use fees 935 will, in most cases, be deducted from any revenue accumulated by that VIN for the display of Advertising or Public Service content to others.

[00292] Once fees are calculated, a designated billing unit can invoice and collect Usage Fees from all platform participants. This would include contract fees and bid rates charged to major brand advertisers or government users. Such fees can be routed from a collecting unit, in this case the Distribution unit 800, to the Compensation unit 900, for disbursement to participants. Government Agencies are billed at this stage for the delivery of any Public Service content by platform users and this is shown at 990.

[00293] With fees properly calculated and invoiced, each content segment can submit final totals and compensation can be sent to the Driving Population, Fleet/Government users, and all other participants who have allowed their personal property to be used in this novel advertising and communications platform. This step is shown at 950 for Public Service utilization, at 960 for Advertising use, and at 970 for Personal use or for any other User-generated content exposures. Again, payments for the display of user-generated content typically involves debiting one's own account for one's own use of his moving object against revenues that VIN may have earned. These direct payments to Registered Owners and Operators 1000, are indicated in FIG 19 at path 178.

[00294] At 980 is a feature of the Compensation system which can allow co-payments, financial partnerships, or promotional sponsorships with entities such as automakers, banks, petroleum companies, insurance companies, and others. Any of these might offer promotions with incentives for the use of this unique advertising platform and these could eventually take many forms. For example, a petroleum company might offer free gas plus a premium for buying their brand instead of simply receiving ad dollars from the entity. This kind of co-compensation might apply to automotive insurance, credit cards, or to even to the automakers themselves. A manufacturer might, for example, integrate the present invention first into its offerings of what are sure to be more costly alternate-energy vehicles, and then rely on their revenue-generating potential to offset their higher acquisition costs for consumers. Thus, the present invention, appropriately integrated into fuel-efficient vehicle planning and production would actually stimulate the earlier adoption of such advanced or

more costly products.

[00295] FIGS. 20-23 are illustrations showing a land-based vehicle with three examples of displays based on modes of operation and their relationships to the environment and to other moving or fixed objects. Although there will be numerous methods for integrating displays FIG. 20 depicts a typical 4-door passenger car 1010 of the anticipated period having a digital rear end and a contemporary, low-profile one-box design. Its relatively elevated rear hatch puts the digital display well above its rear bumper impact zone, in excellent line of sight for the occupants of most following (viewing) moving objects. In this example, the overall surfaces and default color of the vehicle's contoured OLED video display blends well with its inherent design lines.

[00296] FIGS. 21-23 depict three different kinds of displays. Although there are numerous possible kinds of displays, steady-state vehicle 1020 in FIG. 21 presents an image that might be seen when a vehicle is at speed, cruising in a steady state during daylight hours, in which there are few, if any, speed or maneuvering changes, as might occur on an open road or freeway. Such a display would be static and quite similar to the graphics seen on vehicles in traffic today. These images might be allowed to introduce minor animations, such as the hair waving in image 1022, or they might dissolve softly into other images, but only when the vehicles on which they are displayed are in stopped or near-stopped conditions. Standards and practices will be established for all such animations and image transitions. Even minor animations or changes will likely be precluded at speed since they could be distractive to the operators of vehicles nearby. Thus, displayed graphics using the present invention, as shown in FIG. 21, are not dissimilar at all to what is on the road today.

[00297] Transitional-state vehicle 1040 in FIG. 22 illustrates a condition characteristic of any vehicle that is making changes in speed or direction. All such changes—slowing, rapid braking, accelerating, turning, creeping slowly forward or backward—would cause nonessential imagery to quickly dissolve to be replaced by all federally mandated lighting and safety systems (assuming

these become digital and not part of a traditional independent lighting system). Such digital lighting would include a pair of tail lights at optimum spacing with turn signals and brake lights 1042, a center-mount stop light 1046, plus backup lights and reflectors. If the license plate and registration systems are also generated via digital video, as shown at 1048, these too would instantly reappear during any vehicle speed or attitude changes unless federal or local requirements ultimately dictate their presence at all times. If commercial imagery of any kind is presented at such times, these would be minimal, non-animated and non-distractive, all very similar to the kinds of branding seen on automobiles today.

[00298] Stopped vehicle 1060 in FIG. 23 depicts a display on a vehicle that is fully stopped. When the speed sensor in a display (or viewed) vehicle indicates a non-moving condition, and its proximity sensor indicates a requesting vehicle or device within range (or even in the absence of such electronics requests), then that display vehicle is able to queue and present full motion, conventional, or hyper-relevant video imagery 1062. If the display vehicle should drift slowly forward, the full motion video imagery could, under most scenarios, dissolve and be replaced by the lighting, licensing and safety systems shown in FIG. 21. Rulemaking and resulting Federal Motor Vehicle Safety Standards (FMVSS) would be adopted after thorough consumer and safety testing to determine the speed and motion boundaries for full motion video animation, transitions and deliveries, and the appropriate start and cutoff timings based on the relative speeds and the movements of the other vehicles involved.

[00299] It is worth noting that at night or during periods of darkness or under potentially hazardous conditions, all lighting systems will be displayed. There are some genuine advantages to land vehicles having digital rear ends. One of these is graphics standardization for critical operations. The size and lateral separation of taillights combine to provide valuable cues to any vehicles following as to the range or distance to vehicles ahead. When taillights are of different sizes and have different lateral spacing, the effectiveness of these

cues is diminished. The present invention allows for the widespread standardization of these important visual elements. It additionally allows for intercommunications between all vehicles having digital video body panels or glazing to display early warnings and even graduated warnings during slowing or stopping. In the event a vehicle leading a long lane of vehicles at speed begins to slow, then all vehicles could simultaneously receive a slowing alert via radio and that signal would introduce a uniform amber taillight alert that would shift gradually towards red as all vehicles slow at roughly the same rate. This feature alone could prevent the very common increasingly exaggerated stops as brake lights flash on without warning in a lane of traffic at speed.

[00300] FIGS. 24-27 are illustrations of four types of displayed content. 1100 depicts an Emergency type display. Most of these will be in the Public Service category and would be stored and deployed by Federal, State or local governments. This would not preclude personal or consumer emergency buys however. Emergency graphics can be stored in all hard drives or can be uploaded to vehicles based on their locations and travel environments. Emergency content is typically embedded with instructions for distribution at precise times and under exacting conditions, usually triggered by local area wireless signals, GPS coordinates at precise time periods, or through vehicle to vehicle wireless transmissions. Note that emergency displays will cause all vehicle license and registration information to immediately reappear, assuming they are digitally represented. Emergency content transmissions will have higher priorities than all other types of content and would be triggered by a proximity to, or entry upon, a hazardous area often defined by GPS coordinates.

[00301] At 1120, a typical Proximity advertisement is shown. A consumer in a following vehicle might request such proximity content be displayed on nearby objects, or these might appear passively based on a proximity media buy. In an example to be later described, Proximity buys could be based on a time of day (e.g., meal time) and, most certainly, on a location (e.g., the city blocks

surrounding a restaurant. Graphics might include animated signage, such as the right turn arrow depicted in Proximity illustration 1120. In the case of a drive-thru restaurant, graphics on a viewed vehicle immediately ahead in the drive-thru line could display a pictorial and even an animated menu in rich video imagery, along with current prices.

[00302] The present invention uses existing onboard GPS Navigational systems to deliver ads at precise locations determined by the advertiser or by the media buying agencies. By coupling specific content stored on board a vehicle's internal hard drive to specific geographical locations (e.g., a city block, an entire section of a city, or a length of rural highway), advertisers can target specific demographic groups by area and can call attention to specific products or services while drivers or consumers are close to them. This is called proximity advertising. The ability to advertise restaurants, promote special sales or points of interest, to capture spontaneous interest, or to inform those who may be unfamiliar with an area is powerful and much sought after in the world of marketing. In practice, the desired GPS coordinates are coupled with the ad content at the time of upload. When a vehicle's GPS system later indicates travel within those specific boundaries, then those ads are either queued or are given priority over other content.

[00303] At 1140 is an example of Sponsorship content. For example, a convention promoter or exhibitor could purchase time or content for the city streets and freeways surrounding a convention center. As vehicles equipped with the present invention approach sponsored venues, such as theme parks, sports stadiums, national parks, or airports, content representing those sponsors could appear on all of the objects moving in and around that immediate area.

[00304] Another common form of sponsorship is likely to be where marketers, entities, or individuals purchase time and space on the surfaces of moving objects as a free courtesy or a service enhancement for viewing parties. Imagine two vehicles equipped with the present invention stopped one behind the other at a traffic signal in which the vehicle behind is able to view the

external display surfaces on the vehicle ahead. Assume the viewing vehicle is at that moment tuned to a radio station, using an onboard entertainment system, or listening to a portable handheld device such as a future iPod, satellite portable, MMx, or phone. When such equipment in or around a viewing vehicle is equipped with a means to wirelessly broadcast an encoded signal describing the content it is currently using, then a vehicle ahead is able to enhance that use by introducing visual content synchronized to a consumer's current audio environment. In other words, if the occupants of a viewing vehicle are listening to a satellite radio station that is playing specific music, that music code (or the content itself) could be transmitted forward to the viewed vehicle, and the display of that vehicle could then present video material which is both related to and is synchronized with the audio content being received or consumed in the viewing vehicle. The logo or the tag lines of the sponsor offering such free entertainment or marketing enhancement would of course be displayed somewhere on the video display within the line of sight of the viewing vehicle. Naturally, these commercial sponsorships could be turned off or locked-out by any properly equipped viewing vehicle or any compatible portable device within range.

[00305] At 1160 is an example of a Personal media content placement. Such media can be generated by consumers or professionals and can be uploaded by users themselves. If personal ads are placed on other vehicles, they will pay the going media rate for the anticipated location, time of day for the number of impressions. If such content is placed on an owner's own vehicle, then that cost would be deducted from revenues earned from the display of content for others.

[00306] It is worth noting that a major application of the present invention will be that of displaying commercial advertising in large indoor and outdoor parking lots and structures by using the rear surfaces of parked cars. In this way, consumers can even earn revenue while they are shopping, by presenting commercial advertising to passing motorists who are looking for parking places or to pedestrians on foot who are walking past rows of parked cars on

their way to the retail spaces. This proximity application alone will be of significant value to the parking spaces surrounding retail stores. Imagine the large number of vehicles parked in spaces near a major mall anchor such as a Nordstrom's or a major brand restaurant or theater chain that could display specials or show film trailers to families passing on their way from the lot into the mall. Proximity sensors on board each vehicle could activate such ads as pedestrians approached and passed behind them. These displays can also easily be targeted by proximity, venue, or time of day, and when consumers further carry handheld MMx units which broadcast a consumer's "who I am" or "what I want" encoded preferences, then parked moving objects are able to display hyper-relevant content to those pedestrians.

[00307] EXAMPLE 1

[00308] FIG. 28 is a diagram showing geo-specific content distribution. It depicts several city blocks with in a representative downtown area. Main Street is shown at 1280 and 1st street at 1200. The Convention Center is located at 1220. A McDonald's Drive-thru is shown at 1240, and a Hilton Hotel is shown at 1260. 3rd Street is a one-way street, as indicated by the arrow at 1284, and temporary road work is shown at 1250. In terms of content media buys, Apple Computer has purchased the several square block area surrounding the Convention Center, but only during visitation hours for the electronics show. This area is indicated at 1222. McDonald's restaurant, 1240, has a renewable lease for the city block area immediately surrounding its restaurant and the boundaries for this media area is indicated at 1242. However, McDonald's has also purchased media rights to the subsurface parking garage for the convention center on a 24/7 basis, such additional space being represented at 1244. Hilton Hotels, meanwhile, has leased the areas surrounding its hotel but has also negotiated exclusive rights to traffic flowing along Main Street a half block from the Hotel. Each of these areas has boundaries defined by GPS coordinates and each has an individual priority for content deliveries based on the time of day. The fees for such areas and their relative priorities are established by the anticipated level of exposure—

typically based on the number of targeted impressions they can deliver at any given time—in the same way as outdoor billboard advertising is valued. Specific content purchases are described in FIG. 29. In FIG. 30, we will take a drive North on Main Street to experience the kinds of content that will be seen by four different types of users during their travels.

[00309] FIG. 29 is a diagram showing content purchase and encoding by content type. Across the top are the Column headings of Sponsorship, Proximity, Personal, and Emergency, representing the four content categories discussed in FIGS. 24-27. On the left side, from top to bottom, are the headings of Content, Time Encoding, Venue Encoding, Exposure priority, and Fee range. Together, these represent the kinds of media buys described in FIG 28.

[00310] Reading from top to bottom in the Sponsorship column, at 1305, we see Apple's purchase of the Consumer Electronics Show at the Downtown Convention Center. At 1325, we see that Apple has purchased the prime time hours when the Convention Center is open, from 7:30 AM to 6:00 PM during the run of the electronics show. At 1345, we also note that Apple has purchased the several square block area surrounding the Convention Center which includes all of the approach routes to entry and parking. The Exposure Priority assigned for Apple's sponsorship (the preference with which Apple's promotion is given over other types of content) is shown at 1365 as Level 2, with Level 1 being highest. Finally, the Fee Range, at 1385, is "High", based on the show and on the high value business traffic at this venue.

[00311] The Proximity content column at 1310 reflects McDonald's and Hilton Hotel's Local Venue advertising buys. Both companies, at 1330, have selected media purchases on a round-the-clock or 24/7 basis. 1350 indicates McDonald's buy of the streets immediately surrounding its restaurant but, as shown in FIG. 28, also includes the entire Convention Center underground parking garage in an effort to attract hungry convention goers. 1370 indicates a Level 3 priority (from a total of four), meaning that Apple's sponsorship at Level 2 would take priority if there were a conflict in time and place. Finally,

based on McDonald's and Hilton's annual deals for Proximity advertising, they have negotiated costs in a Medium fee range, shown at 1390.

[00312] Under Personal Content at 1315, we find a Registered Owner who wants to Promote his own business at minimal cost. An example of such content would be the Dog Walking business shown at 1160 in FIG. 27. In order to keep costs down, yet hit his target market, this person has chosen Non-Prime Advertising hours at 1335, so that during these periods he can continue to generate revenue by displaying brand advertising for big companies, but he has also selected an option which lets him manually override his own schedule to present his own or other personal ads whenever he chooses. Also, because his business operates in a localized area and involves such a personalized service, at 1355 this owner had selected his immediate neighborhood based on GPS inputs. In other words, when he ventures further from home he can earn money through the display of major brand advertising, but as soon as he re-enters his home neighborhood, his Personal or Business ads will queue up and promote his local enterprise. At 1375, we see this has resulted in the lowest Exposure Priority for his own content, allowing him to first optimize income producing content. His fees for Personal content will therefore be among the lowest available, and will simply be deducted from his monthly ad revenue, as indicated at 1395.

[00313] In the last column, Emergency, we see at 1320 that the City Department of Transportation has requested a Public Service placement, and has designated it for automatic activation. This means the network will cause the requested content to automatically appear on the displays of all moving or fixed objects equipped with the present invention operating within the specified venue in accordance with local laws and time/place specifications. At 1340 and 1360, we see that both Time Encoding and Venue Encoding will be governed by Local Road, Highway and Safety Standards During Project Durations. This simply means that "alert" or "emergency" content will be posted at the times and places where they are required. Since many of these media postings are Emergency alerts that may bear on transportation or

highway safety, they are granted the highest priority, Level 1, shown at 1380. Fees for such media are typically borne by public funds or taxpayer dollars. However, if Government agencies are using privately-owned assets to deliver its messages, the proceeds for any such Public Service media buys will be shared with the registered owners of those assets, as indicated at 1398.

[00314] FIG. 30 is a diagram showing Content Viewing referencing information from FIGS. 24-29. In FIGS. 24-27, we learned four basic types of content. In FIG. 28, we saw how certain content could be displayed selectively based on its proximity to people, places and things, and in FIG. 29, we learned about content priorities, encoding, and fees. FIG. 30 now brings all of these together to demonstrate what four different vehicle drivers (each expressing individual interests and needs) would see on the various fixed or moving objects around them that are able to communicate with the present invention as they move north on Main Street, as shown in FIG. 28, at 12:00 noon.

[00315] Across the top of FIG. 30, four different driver types are represented: at 1402 is a Soccer Mom driving an SUV with a load of kids; at 1404 is a Business Traveler who is unfamiliar with the city and is driving a rental car; at 1406 is a local Daily Commuter (who is quite familiar with the city) driving in his personal car; and at 1408, we have a disinterested driver who is using a car equipped with an aftermarket system (as described in FIG. 17 at 680) to disable advertising on the various moving objects within his point of view.

[00316] The second row indicates the preference settings each of these drivers has assigned to his particular vehicle that are currently switched on. The soccer mom at 1412 has a Family Profile engaged in her SUV with her kid's preferences also active. At 1414, the business traveler has asked his car rental company to transfer his preferences from his personal car to the rental car and has further requested the rental agency to add its local visitor support program, which will guide him through the city based on his personal interests. The business commuter, at 1416, has his normal personal profile active. The disinterested driver has all of his ad viewing preferences shut off, as indicated at 1418. So, when driving north on Main Street at noon, each of these drivers,

along with any occupants on board, is likely to see the following kinds of content in front of or around them on surrounding displays equipped with the present invention:

[00317] From 1st Street to 2nd Street, mom in her SUV will see family oriented ads derived from her own interests, mixed with the interests of her children (since their profiles have been so adjusted), as shown at 1422. At 1424, the business visitor in town will see ads and content based his own WIA/WIW profile interests, except that any proximity-based interests will reflect his current location. In other words, if one of his preferences has been set for fine Jamaican dining in his home town of Chicago, he will now be alerted to the presence of nearby Jamaican restaurants in this current location (e.g., Los Angeles), especially here at lunch time. Because our visitor has asked the rental company to add its Local Visitor Support package at 1424, he will be also shown a variety of local interests in his new travel area. If he is more interested in certain kinds of fishing or boating, than he is interested in, for example, museums, a much larger emphasis will be placed on these points of interest. At 1426, our local business commuter will be presented with content corresponding to his personal profiles that are switched on. Finally, at 1428, the disinterested driver will see nothing displayed on the objects in front of his vehicle as he moves between 1st and 2nd Streets.

[00318] Between 2nd and 3rd Street, our northbound drivers will enter the first and largest zone for a proximity media buy, the one purchased by Apple Computer at the Convention Center. Here, our mom with her kids at 1432, our business traveler at 1434, and our local commuter at 1436, will all see Apple's sponsorship imagery on the various objects around them; however, because our rental car visitor has requested local visitor support, he will also see, at 1434, a One Way Traffic Alert which will result in an absolute display priority during the last 20% of travel as our visiting driver approaches the intersection. At 1438, our disinterested driver continues to see nothing displayed on the vehicles or fixed signage around him.

[00319] Between 3rd Street and 4th Street, mom and kids at 1442, the rental

car driver at 1444, the local commuter at 1446, and even the disinterested driver at 1448, will all see a "NO RIGHT TURN" alert as they approach the intersection calling attention to a temporary roadwork and closure condition during the present hour. All vehicles will receive an alert since these have the highest priority and involve issues of traffic safety. As vehicles near the intersection, this alert overrides even Apple's high cost promotion and the disinterested driver's preferences at 1448 to not view commercial content. Apple's exposure during this hour will drop to approximately 70% of the driving time between these parallel streets. Such road hazard information would be regulated by the local area city and traffic signage infrastructure.

[00320] From 4th Street to 5th Street, mom at 1452, our rental car visitor at 1454, and our daily commuter at 1456 will see, presented on the objects before and/or around them, both the Apple promotion and Hilton Hotel's proximity ads. Apple's logos will be seen approximately 70% of the time between 4th and 5th along Main Street, and Hilton's ad will be seen about 30% of the time, due to Apple's premium fee paid for the temporary Convention Center sponsorship. Between 4th and 5th, our disinterested driver at 1458 returns to being presented with no commercial content, in accordance with his pre-established preferences.

[00321] Between 5th Street and 6th Street, mother and kids at 1462, the rental car user at 1464, and our daily commuter at 1466 will all be presented with essentially the same levels of paid content: Apple at 70% (due to the premium fee), Hilton Hotel's ads at 20% of the linear block, and McDonald's at 10% of the linear block, due to the surrounding surface street proximity area purchases which they have leased from the network. Between these streets, however, our disinterested driver at 1468, in the absence of any further road or traffic safety alerts, sees nothing displayed for his benefit.

[00322] In the final stretch between 6th Street and 7th Streets, our disinterested driver continues to have no commercial content displayed, as shown at 1488. However, our soccer mom with her kids at 1482, our rental car driver at 1484, and our daily commuter at 1486 will all continue to view ads based on their

previously scheduled proximity media buys and their content delivery instructions. The result is the following approximate split in content display: Apple Computer at 70% (for its premium fee), with the balance split equally between McDonald's and the Hilton (15% each), depending on linear area traveled over time. It is important to note that after 6:00 PM, when the Computer Show closes at the Convention Center, the traffic between 2nd Street and 7th Streets will no longer be shared with Apple (since the company has purchased time only during show hours). This time will now be divided between McDonald's and Hilton Hotels based on areas 1242 (for McDonald's) and 1262 (for Hilton), as shown in FIG. 28. In the remaining areas along Main Street which are not defined by the proximity content purchases shown in FIG. 28, presentations will be based upon the active personal "Who I Am"/ "What I Want" personal profiles or on preferences stored on board each vehicle, which have also been activated by their owners (or system administrators).

[00323] FIG. 31 is a block diagram showing a possible content delivery protocol between moving objects. Such a sequence typically begins at 740/750 with a local wireless signal from another moving object or from a portable, mobile hand-held device containing data and a means to transmit a combination of VIN numbers, profiles, user codes, or content requests. Such signals are received at receiver 744 and are decoded at 746. This information is then processed aboard a receiving (or viewed) vehicle, or a moving or a fixed object, as indicated at 1505. Once received, an initial question is asked at 1510: Are ads rejected? If the answer is YES, no ads are queued, as indicated at 1515, and subsequently, at 1520, the declined ad viewing instruction is logged on the hard drives of both the requesting (transmitting) and the displaying (receiving) moving objects. Eventually, this declined data delivery is uploaded to the network along with information on VIN, time, place, and demographics via transceiver 714.

[00324] If, at 1510, the answer is NO, then the preferences associated with that VIN are decoded at 1525. At 1530, a second question is asked: Is the requested content available? If the answer is affirmative, another

question/decision follows at 1540: Is there time for the requested content? Input for this decision comes from the Intersection Clock 1800, which is explained in more detail in FIG. 35. The Intersection Clock 1800 is an independent database that is linked to a moving object's GPS (geo-location or navigational) system 755, which, over time, records and learns event delay performance at precise locations, primarily at traffic lights, bridge or railroad crossings, freeway on ramps, and throughout urban or rural environments that experience heavy stop-and-go traffic. This database is linked to a short range wireless transceiver system capable of synchronizing its current database with signals from other moving objects (those equipped with the present invention) which may have arrived at the intersection earlier, and then lock onto the ongoing traffic signal sequencing at that location. Based on this information, the Intersection Clock 1800 can determine how much time remains for the display of content before stopped traffic starts to move again.

[00325] If, at 1540, adequate time remains to display the requested content, then at 1550, the system determines if there are any priority overrides to deal with. Such overrides can come from multiple sources. Block diagram elements 846, 848, and 824 represent Proximity Priorities, Personal Priorities and Public Service Priorities, respectively. These priority assignments are typically embedded with their content as release instructions and are triggered by time, place, or hierarchy as discussed in FIGS. 29 and 30. Another kind of priority override is shown at 1595. Law Enforcement and Security Priorities can be triggered from outside the system as opposed to using a preprogrammed internal protocol. The law enforcement chip at 748 is an example of a trigger which provides for the override of moving object displays by members of law enforcement in the interests of public safety. Imagine, for example, that a missing child is reported in a specific area of the city. It would be possible in only minutes to distribute a photograph of that missing child and to reproduce that image on the display panels of all equipped vehicles within several square miles of where that child was last seen. In another example, it would be possible to place "WARNING STOP WAIT" graphics on vehicle

displays in the event that Emergency Vehicles are approaching the intersection.

[00326] If priority overrides are embedded in the content, these are revealed at 1550, and content is displayed accordingly. If there are no priorities, then at 1555 content is released from the on board storage hard drive. Priority monitoring is an ongoing and constant real time process as indicated at 1560. If delivery conditions change, content queuing or display can be instantly suspended or even substituted with other content. One of the most critical steps in monitoring content deliveries is to confirm vehicle relative speeds and proximities in real time. This step is shown at 1565. When all pre-established delivery criteria has been met between a requesting and a presenting vehicle, prioritized content is sent to the presenting vehicle's display drivers, as shown at 1570, then on to its video display 760. If, during display, delivery changes are detected at 1565, it may be necessary to suspend or modify the delivery of content. For example, a presenting vehicle creeps slightly ahead in traffic, altering the viewing angle and range, and, more importantly, introducing a need for the operator of a viewing vehicle to focus on maneuvering his vehicle forward in a stop and go traffic lane. It becomes immediately critical to suspend any content delivery that could compromise the maneuvering process and to reveal all vehicle visual lighting and safety systems. An essential purpose of the present invention is to maintain, at a minimum, the safe operating conditions which exist today between moving objects and their operators. For this reason, it is anticipated that video impressions would occur only when vehicles are static, parked, or moving only within minimal acceptable limits. Thus, at 1580, any changes beyond established norms will modify content delivery.

[00327] Once content has been sent to the display drivers, the extent of the delivery will be confirmed at 1575. If the queued content has been totally delivered, then the time, place, and percentage of that delivery will be encoded and logged onto the hard drives of both the requesting and the presenting vehicles, as indicated at 1590. This is an important confirmation step as it

reveals to marketers and to the distribution network that the intended content was indeed delivered as requested and that platform owners and operators can now be properly compensated by the Compensation unit 900. Although it is not reflected in FIG. 31, content delivery, as previously discussed, includes the transmission of either audio codes or content, so that the audio portions of video content can be reproduced over the sound systems of viewing or requesting vehicles and devices. Deliveries can therefore be confirmed on several levels, the four most common being: (1) Content was NOT viewed (content requests were shut off or content was rejected); (2) Content was viewed only (requested content was displayed but sound was shut off); (3) Content was both viewed and heard (both systems functioned fully during delivery); and (4) Content caused viewer to specifically respond after such viewing (meaning that a receiving party might have driven to a specific location, requested more information on a product, or made a purchase within a specified period).

[00328] If the delivery of content is modified for any reason at 1580, then it is determined at 1582 whether minimal delivery requirements have been met to constitute an actual delivery. This is generally interpreted by the amount of content exposed to the viewer. If minimal exposure was met at 1582, then this will be logged as a percentage delivery at 1590. If minimal exposure was not met, then shorter content of a similar type can be queued (as indicated at 1545), or the delivery can simply be preempted as shown at 1586 and re-queued in its entirely at 1588.

[00329] If, at 1530, it is determined that requested content is unavailable (meaning, possibly that a hard drive may not have been recently updated from the network), then, at 1535, alternate, similar, or generic content is queued. If it is determined at 1540 that there is insufficient time to display 100% of the requested content (e.g., a 30 second spot), then, at 1545, a shorter commercial spot of the same or similar content can be substituted. Once such revised content is queued at 1535 or 1545, it is released from the hard drive, as indicated at 1555.

[00330] FIG. 32 is a diagram illustrating geo-specific content distribution in a rural area. The map shows an Interstate Highway 1610 passing north/south through a rural countryside. A rural road is shown at 1620, a river at 1630 and a bridge-out condition at 1640. Several hundred feet from the highway is a Gas Station/Market at 1650. A rectangular boundary is indicated around the Gas Station/Market area. This area defines a proximity advertising area 1660 within which specific commercial or public service messages can be delivered. Another boundary is indicated at 1670. This rectangular area defines the bridge-out warning alert area and is referred to as a Public Service Alert Area. Finally, four electronic billboard installations are represented at 1680, 1682, 1684 and 1686.

[00331] When stop and go congestion exists on the interstate, then moving objects equipped with the present invention can use other objects immediately in their paths to display commercial or public service content. It is generally anticipated that non-animated graphics (e.g., signage announcing an upcoming gas station or market stop ahead) could be placed on nearby moving objects at speed since they would be no more distractive than other types of graphics which exist today on moving objects and would, in fact, be easier to read since they are moving with the viewer at traffic speeds, as opposed to passing quickly by at roadside. However, in the absence of traffic equipped with the present invention, electronic content would have to be placed on other kinds of display surfaces, such as the billboards indicated at 1680. The difference between standard electronic billboards and those equipped with the present invention is that those equipped according to the present invention able to receive and interpret aggregated requests for commercial, personal, or public service content and then display such content to the occupants of passing vehicles.

[00332] For example, southbound traffic on Interstate 1610 will transmit advance wireless signals (each representing VINs, profiles, and user codes with content requests) to the billboards depicted at 1680. When a vehicle approaches such a billboard, the billboard has already polled its internal

storage (see FIG. 31), and will queue and display content requested by that VIN as it approaches. In this way, even single or lone vehicles using the present invention can function independently within the environment by causing highly appropriate or hyper-relevant content to appear on many types of surrounding surfaces. Imagine fuel is nearing empty on that southbound vehicle. Such a "low fuel" condition can be interpreted through the vehicle interface 730 and, once coordinated with GPS data regarding the location of the service station, can encode and broadcast a radio signal 740 via transmitter 742 to enable nearby billboards to display information on the proximity of available fueling stops. While it is true that such information could be presented on displays inside a vehicle, other types of content are better suited for showing externally on electronic billboards. For example, billboard 1680 could reveal the presence of Gas Station/Market 1650, which might otherwise be obscured from direct view of Interstate traffic. Billboard 1682 could further indicate directions to the Gas Station/Market and might feature other products and services based on the preferences and interests of the occupants of any approaching VINs. Westbound traffic on Rural Road 1620 would be exposed to electronic billboard 1694 before leaving the populated area defined by Proximity Advertising Area 1660. Normally, billboard 1694 would carry content relating to features along the road or would respond to content requests. However, in this example showing a proximity Public Service Alert area, 1670, such requested content for billboard 1684 would be overridden by the "bridge-out" alert until the condition is eliminated. Electronic billboards would have content uploaded to them using the Internet and a delivery means such as cable, wireless, or satellite. Again, embedded with the content for delivery can be specific instructions for the dissemination of that content. In the case of the "bridge-out" alert, these instructions would likely be in the form of GPS coordinates defining the perimeter of the alert area. Such a boundary is indicated at 1670. Once these boundary coordinates are identified and approved by a governing agency, they can be sent out via Internet/cable/wireless/satellite to all such electronic display devices within an

affected area. This means that all moving objects, whether or not equipped with the present invention can encounter such visual displays. Secondly, these coordinates can be sent to all moving objects equipped with the present invention as indicated at 868, 870, 872 or 974 in FIG. 18B, causing such an alert to override other types of content on any equipped vehicles that enter the area 1670 boundary. The advantage, of course, is that local governments are able to instantly deploy critical public service alerts like bridge out or flooding/turn back warnings without having to visit the site to physically set up such temporary signage as is commonly done today. Both fixed electronic signage and moving objects can be quickly changed over from commercial revenue to emergency public service purposes by carrying their audio/visual messages directly to the vehicles, venues and consumers concerned on an exacting and timely basis.

[00333] EXAMPLE 2

[00334] FIG. 33 illustrates the interactions between moving and stationary objects at a typical city intersection and will help clarify two elements relating to the queuing and display of content on moving objects: (1) allocating timing for display through the use of the Intersection Clock 1800, and (2) specific methods of vehicle-to-vehicle viewing.

[00335] A traffic intersection is shown at 1700, bounded by pedestrian crosswalks, a configuration increasingly common in city and rural environments. 1705 indicates an eight lane north/south highway. 1710 represents an east/west highway with active cross traffic. Overhanging traffic light structures 1715 are shown in two places for the north/south corridor. Each of these carries a left turn signal 1720 aligned opposite and above the left turn lane, plus a green/amber/red signal light above through traffic lanes, plus an identical light on each corner, shown as 1725.

[00336] Note first the northbound vehicles marked A through L. In this first example, vehicle A has arrived and stopped at the intersection first. Vehicle A is equipped with a production version of the present invention; however, it has not previously been through this particular intersection. As a result, as Vehicle

A approached this intersection, several things occurred: (a) the driver of Vehicle A, seeing light 1725 change from green to amber, braked and eased to a stop at crosswalk 1730; (b) a forward-looking optical sensor on Vehicle A, monitoring its approach to the signal light, sensed the signal light's color shift from green to amber; (c) sensing the color change (in the same way as its driver), Vehicle A engaged its onboard Intersection Clock 1800 to begin a recording function to document the signal's red (stop) duration before its return to green (go). By recording this elapsed time and by cross-referencing the vehicle's GPS location and its last heading (northbound), vehicle A is able to initially compile, in terms of gross timing, a beginning database for the signal sequences at this particular location.

[00337] Every signal intersection has basic and relatively consistent event timing protocols. Some locations, however, have unique event schedules, but even these can be learned by the Intersection Clock 1800 as defined by the present invention. For example, intersection traffic lights will normally halt traffic flowing in opposing directions to permit the flow of cross traffic. This process normally begins by allowing cross traffic to complete opposing left turns first. After left turns are timed out (about 12-16 seconds), those lanes are then stopped and through traffic is allowed to proceed. After a predetermined period (anywhere from 60 to 90 seconds), this process is halted and the sequence will repeat itself with traffic flowing in the perpendicular direction. Clearly, there are many variations, including one-way streets, multiple streets converging, railroad crossings, etc.; however, when coupled with GPS identification and an ability to spot the start of an event (such as a color transition from green to amber), any vehicle equipped with the Intersection Clock of the present invention can automatically construct a database by time of day for any intersection it uses. Table 1 illustrates a typical traffic signal event timing cycle.

[00338] In addition to constructing an event timing database from scratch, moving objects equipped with the present invention are also able to receive intersection event timing data from other moving objects in and around that

intersection. In other words, if another vehicle that has previously passed through this intersection arrives moments later, this second arriving vehicle will have the traffic event sequence for this intersection stored in the database of its own onboard Intersection Clock. For example, assume that vehicle H (or even vehicle M, which is currently crossing the intersection) contains such information. Each of these vehicles will automatically broadcast the event sequence for this intersection when it enters or crosses it, by wirelessly transmitting it from its Intersection Clock 1800 through transmitter 714 and antenna 715. In this way, all vehicles equipped with the present invention can immediately update their onboard database for this intersection. At the same time, Vehicle A can contribute an accurate synchronizing signal for these later arrivals because it began recording event timing for the northbound lanes beginning with the signal's light change from amber to red. Through this instant, ad hoc exchange of information at any populated intersection, all properly equipped vehicles can distribute current event timings and synchronize their internal clocks without relying on external infrastructures.

[00339] One last step for each Intersection Clock is to calculate for its respective vehicle the amount of time remaining for content presentations before the light turns green in its lane and the traffic begins to flow. From Table 1, one can see that if a vehicle (e.g., southbound Vehicle P) should arrive at the intersection later and synchronize with other vehicles at event Stage 4, then it will have approximately 92 seconds within which to queue and present video content before these vehicles begin to move again. Ninety-two seconds is adequate for two full 30-second commercial spots, two 15-second spots and a two-second dissolve to a corporate logo sponsorship before mandatory vehicle safety systems must again kick in.

[00340] Vehicle-to-vehicle communications will be governed through testing, rule making, and the administration of content delivery procedures that define where, when, and under what conditions various types of content can be displayed without compromising highway and traffic operational safety. It is essential that content not detract from a vehicle operator's need to focus on

the movements of all objects around them rather than on any graphic content those objects might be displaying, beyond federally mandated lighting and safety systems. The present invention can assure that content will only be viewed or presented when vehicles are fully stopped. It can also assure that content cannot be viewed by vehicles that are passing in adjacent lanes, because this could produce a significant distraction. The kinds of displays anticipated by the present invention can be combined with thin film overlays that can optically or electronically increase or reduce the angles at which imagery can be seen. Optical filters, for example, can be embedded into the outer protective layers for these displays. One basic filter of this kind is 3M Corporation's micro-louvre technology which optically restricts the viewing angles in flat panel displays. Still another technique, created by Sharp Corporation and Sharp Laboratories of Europe, Ltd., permits an LCD to simultaneously display different information and image content in right and left views on a single display by directionally controlling the viewing angle of the LCD. This makes it possible to provide information and content tailored to specific users depending on the precise angle at which they view the display. Such an application could, for example, direct requested hyper-relevant video content directly rearward to a following vehicle, while the view from vehicles passing at more oblique angles could cause the same imagery to dissolve into the default body color for a given vehicle, or into content appropriate for generic or non-requested viewing.

[00341] A primary reason for selective or controlled viewing is that content requests are generally private and based on non-identifiable information requests. If an individual in a following (viewing) vehicle has allowed preferences which request content that is quite personal in nature, it would not be desirable for that content to be viewable by the occupants of vehicles in adjacent traffic lanes. Note, for example, Vehicle A, which is presenting requested hyper-relevant content to vehicle B behind it. Note the angular spread indicated at 1735. This lateral spread controlled by the previously mentioned technologies prevents the occupants of surrounding vehicles D, G,

or H from seeing what is being displayed on the rear-facing surfaces of Vehicle A. Vehicle D's exposure is blocked by vehicle B, as shown by dimension 1740. If Vehicle B were not in close proximity to Vehicle A, this condition would be detected by Vehicle A's proximity sensor 770, and the system would prevent the queuing of highly personal hyper-relevant content. Vertical viewing angles can be controlled in the same way as horizontal viewing angles to prevent, for example, the viewing of personal content from adjacent trucks or busses having seating positions that are inherently higher relative to the ground. Additionally, all such imagery would not incorporate animations or otherwise distractive content until the surrounding viewing vehicles have come to a complete stop.

[00342] Note that at 1745, Vehicle D has requested content from Vehicle C. Vehicle C can select and queue that content; however, it cannot present it until Vehicle D has come to a full stop at a predetermined range behind Vehicle C, such spacing predicated on the respective VINs of the two vehicles. Such optimum spacing is reflected by Vehicles G and H, at dimension 1750. Here, vehicle G is a high SUV and vehicle H is a low two-door sports coupe. The VIN numbers exchanged between these vehicles during the requesting protocol has identified the respective heights of each vehicle along with the eye envelope for an average percentile driver in the following (viewing) vehicle. This information yields an optimum viewing range between these two objects. Furthermore, as vehicle H closes the gap with vehicle G, a small green dot will appear on the rear-facing display of Vehicle G. As the driver of Vehicle H continues forward, this spot will grow increasingly amber and finally red which indicates the optimum stopping point for best viewing through vehicle H's windshield. At this point, the dot will disappear and content viewing will commence. This fore/aft vehicle spacing feature of the present invention will additionally conserve thousands of square feet of space in traffic lanes simply by allowing vehicles to maintain more efficient vehicle-to-vehicle tandem spacing.

[00343] By contrast, vehicles K and L have reached optimum spacing, as

shown at distance 1755; however, vehicle K cannot present content because both vehicles are drifting slowly forward in the same lane. Once both vehicles reach a full stop, they can commence content display. On the other hand, Vehicle K has made an automatic content request of Vehicle J at a relatively distant range shown at 1760. Because vehicle J is at a full stop, it might be allowed to queue and present certain kinds of static content (such as a non-animated corporate logo) until Vehicle K is fully stopped at optimum spacing behind vehicle J.

[00344] FIG. 34 shows a section of freeway with lanes in one direction, having a center divider 1765 and a carpool lane 1770. Moving at consistent freeway speeds, Vehicle B may make content requests forward to Vehicle A, as shown at 1775, however, such requests will be fulfilled only on a limited basis due to relative vehicle speed and range protocols. During day and night hours at speed, commercial imagery is likely to be limited to small centrally-located display areas on digital rear-ends and animation would not be permitted unless vehicles are fully stopped. This is because animated or moving images can distract nearby drivers. At the same time, protocols would not want to dissolve or delete commercial imagery before engaging a vehicle's lighting and safety systems as this could introduce dramatic changes in object appearance while they are underway. Additionally, during night driving hours, all lighting and safety systems would remain active on all moving objects, regardless of speed, proximity, or location since uniform taillights, running lights, and turn signals are vital elements in allowing drivers to judge the distances and conditions of vehicles ahead.

[00345] An exception might occur between stopped or extremely slow stop and go traffic as depicted in the far right lane 1780. Such a condition could be caused by a backed-up off ramp. If, over time, such blockages on heavily traveled freeways become repetitive, these conditions would gradually be recorded on the Intersection Clocks of moving objects equipped with the present invention. Estimates of such delays can then be monitored for consistency and certain kinds of content or public service alerts can be

displayed. In such cases, vehicles can use their on board transmitters to measure the relative movements in long rows of vehicles and opportunities can be identified for the queuing and display of short duration content while these vehicles are near-stationary. In lane 1780 from top to bottom, Vehicle I is presenting nonspecific (generic) commercial content to Vehicle J (which does not possess the present invention), Vehicle L is presenting hyper-relevant content to vehicle M (which has requested it), and vehicle M is presenting generic content to vehicle N. Of significant value in such situations is the ability of any vehicle fitted with the present invention to synchronize public service or traffic safety displays with other properly equipped vehicles. As previously mentioned, freeway speed changes, when communicated uniformly by radio between multiple vehicles simultaneously, followed by a uniform response (such as causing all of the vehicle's rear lighting systems to glow amber (for caution) and then transition at the same rate to red-amber and then red at uniform brightness levels (as opposed to individual brake lights flashing instantly on without warning), will result in considerably safer driver control and in the virtual elimination of progressively exaggerated slowing which leads to rear-end collisions. The U.S. Government currently has programs in place to develop such highway technologies which could easily adopt or interface with the present invention. One such program is the Forward-Looking Rear-End Collision Warning System (FCW) designed to explore and ultimately deploy driver warning methodologies. The digital vehicle rear-end and lighting safety systems anticipated by the present invention conforms to all of the targeted Warning Display Characteristics and to the Following-Too-Closely Warning Methodologies dictated by the study since it approaches the FCW warning display in a distinctly novel way. Of equal importance is the present invention's consumer adoption plan—one driven by commerce rather than legislation—because it enables participating consumers to generate revenue and, as a result, represents a unique opportunity for new technology adoption. Suppose we wanted to stimulate the broad adoption of energy-efficient vehicles. By incorporating the present

invention into such vehicles first, we allow consumers to generate significant personal revenues, which effectively offset their inherently higher manufacturing, acquisition, and infrastructure costs.

[00346] FIG. 35 is a block diagram of the Intersection Clock 1800, a device that enables the recording of traffic signal timing sequences and measures the time available for the display of content at locations where traffic flow is controlled by infrastructure. The Intersection Clock is linked to a vehicle's onboard GPS navigation system 755 (normally through vehicle interface 730), which introduces vehicle heading and location data to the Intersection Clock as indicated at 1805 on an ongoing basis in real-time. The Intersection Clock is also linked to an optical sensor 1820, which, in a traditional land-based traffic environment, is forward-looking and, in a preferred embodiment, reads the colors of traffic signal lights as the vehicle approaches them. This sensor seeks and monitors the presence of a green light, which is characteristic of traffic "go" conditions, then activates to an "alert" status when the green light transitions to amber, responding in the same way as a driver would to the light color change. Color transitions are received and documented at 1815, where they are assigned a GPS location using traditionally available electronic means. The moment this amber light transitions to red, a time-stamped signal is sent to clock component 1810 and a Location File is opened for that venue based on the vehicle's last direction of travel and its current position. At that moment, the Intersection Clock 1800 checks for previously stored information for this location. If, at 1825, it is determined that no sequence code or synchronizing signal is stored, event time recording is triggered at 1830, commencing with the light's transition from amber to red. At the same time, a default time-remaining signal 1835—an average based on stored data for traffic signals in the area—is forwarded to Intersection Clock 1880, which allows certain content to be queued. Meanwhile, at 1840, the red/stop cycle timing (which began with the amber to red transition) is logged for the vehicle's direction and location for storage in its clock's database 1850. In the absence of further incoming data, this information will be logged in this vehicle's

database for future use at these GPS coordinates. If there is indeed data in database 1850 which relates to this location, then that signal sequence code data is retrieved at 1845, then passed from the data base as shown in path at 1855 to 1860, where the sequence code is then synchronized to the red/stop cycle just logged for this heading and location.

[00347] However, it is also possible for synchronized signal sequence codes or non-synchronized signal codes to be received, as indicated at 1865, from other vehicles equipped with the present invention. This is accomplished via antennas 712, 715 and transceiver 714. These codes, as well as synchronizing signals, can be broadcast between vehicles that are either passing one another or arriving on the scene at different times. If a vehicle arrives that possesses signal sequence codes regarding the location, it is able to broadcast, on an ad hoc basis (from one vehicle to another), the traffic light timing sequence it has logged for this location. In this way, a vehicle that does not originally have the timing sequence can receive it as shown at 1865, and can then synchronize this sequence at 1860 using the red/stop cycle event recording it is either processing or has logged at 1840. When a new or updated code sequence has been received from another vehicle, or has been recorded for a specific location using new data, it is sent to database 1850, as indicated at 1870, for storage and use when that vehicle returns to the same location. Conversely, when a vehicle that possesses the sequence code in its database for a particular location arrives after a vehicle which has begun recording the amber-red event start cycle, that vehicle can then synchronize its sequence code with the earlier arriving vehicle.

[00348] The final step for the Intersection Clock 1800 is to calculate the time remaining for the display of content. This is accomplished by identifying the current point in the timing cycle (based on the amber to red transition for a given direction by any vehicle, and as shown in more detail in the description for FIG. 33), and then determining, at 1880, the time remaining before the red (stop) light transitions to green (go) for a given direction of travel. Once that is determined, content packages fitting the remaining time can be queued and

released from the content hard drive 716, as shown at 1555. Bear in mind that the Intersection Clock 1800 merely defines the time within which moving objects equipped with the present invention can display imagery before it must be terminated in favor of other operating systems. This process does not in any way control the physical operation of motor vehicles or moving objects.

[00349] EXAMPLE 3

[00350] Finally, a much more basic example of a preferred embodiment of the present invention is the incorporation of such a system into the family car. Bringing home an automobile with the present invention built in could be reminiscent of bringing home the first family television, video recorder, or computer of years past.

[00351] Dad decided it would be a family surprise—a new Lexus 'Crossover' car—rugged enough for family vacations, yet refined enough for the office and for mom to do lunch with her friends. It came in two models, one basic, the other with Lexus' new on-board ad display system, something the company called an "ad/hybrid." Other than this, the models were identical. With financing, the slight increase in cost for the ad/hybrid was barely noticeable in the monthly payment, but the window sticker made it clear the car would produce handsome annual revenue for its owner, significantly offsetting the costs of its built-in ad display technology. On the sticker, this revenue had been translated in terms of the car's annual savings in operating costs in the same way as its average fuel performance had been estimated. Dad signed the papers, the dealer pre-registered the ad/hybrid's VIN and dad headed for home.

[00352] The kids were all over the car as soon as it drove up the drive. Right away, his 8-year old daughter wanted to place picture ads for her after-school dog walking business. His 14-year old son was ready to hook up his DVD player so that he and his friends could watch wide screen tailgate movies on the lawn. In fact, both kids seemed to know more about the technology than dad, and mom just looked on disapprovingly from the door, irked at the thought of such blatant commercialism. Indeed, a car that shows

commercials!

[00353] That night, dad logged onto the well-crafted Lexus site which had the look and feel of a welcoming online community. It allowed him to create user names for each family member and to finish the registration process he'd begun at the dealership. Quietly and thoughtfully, dad completed his user profile by following the easy prompts, describing himself, his interests, and those of his family. He noticed that he was never asked any truly personal information in the profile—just age, gender, occupation, educational level, and the like—all in easy to answer multiple choice questions, which also encouraged him to describe the things he liked and was genuinely interested in. He guessed correctly that everything was somehow linked to the new car's VIN.

[00354] When he was done he clicked "send." Later that evening, when he stepped to the garage for another look at his new car, he was surprised to see that its new license plate was softly glowing on the car's otherwise dark rear digital display. What an improvement, he thought, to no longer have to bolt on metal plates and add new stickers each year.

[00355] The next morning, when pausing behind another car at a boulevard stop on his way to work, the display on the car ahead burst into light and color, greeted dad with his own user name and welcomed him to the Lexus ad network. Minutes later, behind another vehicle on the freeway on ramp, he viewed a 30-second spot for his favorite ball club, a promotion for ABC's Monday Night Football, and was offered 50% off for his birthday at the Sports Chalet a few blocks from his home. He had completely forgotten that next week was his birthday!

[00356] Dad parked the new Lexus in his regular spot in the company's parking garage, unaware that antennas overhead were already uploading the morning's recorded ad deliveries and downloading to his hard drive the latest content released to the Internet just seconds before in New York.

[00357] On the drive home, in stop and go freeway traffic, dad noticed that all of the cars in front of him, regardless of make or model, displayed a brightly

colored Nike logo that pulsed and glowed as the cars slowed and sped up. Of course! They were passing the convention center and this week was the big Sporting Goods Manufacturing Association (SGMA) Show, where Nike was a major sponsor. Smart of them to buy the local ad space, he thought to himself. A few blocks past the convention center, the Nike sponsorships dissolved to be to be replaced by logos for American Express, Best Buy, Home Depot, and NASCAR. Dad noted that when cars were moving at reasonable speeds, they were unable to display anything other than simple, non animated logos, easily read from distances; in fact, not much different from trucks and commercial vehicles seen on the streets in past decades. Dad squeezed the ad pad on his steering wheel and the small display in his instrument cluster revealed the image that was currently playing on the back of his Lexus to whomever was behind him: Victoria's Secret! He recalled that his profile allowed him to check off any sponsor whose product or service he preferred not to carry. As the freeway traffic slowed, he noticed that logos would softly fade to be replaced by standard brake or turn signal lighting, which now even changed color gradually with reduced speeds, shifting from deep amber for gradual speed reductions to brilliant red for full braking. Later, as traffic crept slowly forward, each car's license plate was prominently displayed absent any advertising. Every time his new Lexus drew close to a car ahead which was at a full stop, a green spot appeared on that car's rear-facing display and gradually changed to amber, then red, at which point he stopped and the spot vanished. This, he knew, placed him at a minimum spacing between vehicles in traffic, and at the optimum range and sightline for best viewing based on the model and VIN codes transmitted between the two vehicles. According to the reports he had read, this proximity compacting byproduct alone had conserved hundreds of square miles of wasted traffic lane space on city streets, freeing up turn lanes at many crowded intersections. Once he was fully stopped in traffic, the display on the car in front of him faded to black and music filled his own car's interior, fed through his Lexus' surround sound system. The display on the car ahead then burst

forth into a wide-screen movie trailer complete with stereo sound, which then faded out, to be replaced with brake lights, as traffic crept forward again. Stopped once again, the brake lights faded and the movie preview picked up where it had left off and finished by offering him family discount tickets at the theater in his own neighborhood. And it was his kind of movie. Dad knew the preference codes came from his own on-board profile in the Lexus, but he was unsure as to whether the video and audio content came from his car or the car ahead. He knew it could come from either.

[00358] When dad arrived home he found that his daughter had finished a little graphic ad for her dog walking service. How could he refuse to let her upload it to the family car? After all, it would only show in the immediate neighborhood, and then, only at special times of the day. In fact, the procedure was so simple, that once she completed her profile, she was able to upload her little commercial for network approval all by herself; however, the network declined to let her present her phone number since she was under the age of 18. Her brother, meanwhile, had completed his profile using his own computer and had downloaded it—again for network approval—under his own name and password using the family's wireless home network.

[00359] As dad drove to work the next morning, he was barraged by ads for snowboards, video games, a radical new soda, and previews for kid's TV shows until he realized the car was tuned to his son's new preferences and not to his own preference settings. That evening, he made sure that each family member had their own password and he proclaimed himself the ad/hybrid's official system administrator.

[00360] On Saturday, mom borrowed the Lexus to accompany two of her friends for a luncheon and a book review at the Mondrian Hotel downtown. Dad showed her how to switch off the system so it wouldn't become an 'embarrassment' to her while she chatted with her friends. Sure enough, not once was the girls' conversation interrupted by unseemly commercials on the backs of the cars ahead, although at one corner, a large SUV lit up in front of her warning of roadwork and a closed road on her usual route to the Mondrian.

Thanks to the ad/hybrid's to warn her of a traffic blockage in real time, she and her friends arrived on time, while other attendees got caught up in the delay and missed the beginning of the show. Driving home alone, and now curious, mom switched on the ad/hybrid's system. Two blocks from the Hotel, a black Escalade lit up in front of her, displaying an elegant photo of the Mondrian and thanked her for her recent visit, followed with an offer of a getaway package for two at any of the Mondrian hotels nationwide. Mom pushed the "I" button dad had told her about, and requested that information be emailed to her computer. Before mom got home, she had watched a knockout commercial for a new Clairol product, a teaser for a new high-end shoe store, and was persuaded to drive three blocks off her route to a Borders Bookstore Grand Opening. That evening, she relented and completed her own online ad/hybrid profile so she too could receive hyper-relevant ads.

[00361] A month passed and mom's Visa Statement arrived. To her surprise, it showed a $48.70 credit under a Citibank promotion, just because she had watched a few ads! That evening, she mentioned her little windfall to her husband. Dad went to his home office and returned proudly with a check from Lexus in the amount of $849.60, just because he had displayed a few ads.

[00362] Those skilled in the art will appreciate that the exemplary embodiments described herein can be implemented in various ways. For example, visual displays can be of any conventional type, such as thin film transistor (TFT) displays, organic light-emitting diode (OLED) displays, or any other type of visual display suitable for the particular context of installation and use. Network systems and devices can be server-based or peer-to-peer, centralized or decentralized, secured or unsecured, or the like. Communications and network interfaces between systems and devices can include wired (e.g., Ethernet, wire cable, optical fiber, and the like) and wireless (e.g., radio frequency, infrared, light modulation, and the like) interfaces. Systems, devices and components can be implemented using hardware, firmware, software, or any combination thereof, including programmed or programmable data processors, fixed or removable memory

or other storage media, input/output (I/O) devices and adapters, and the like. Furthermore, means for displaying the content can be fixed or removable, can be attached to or integrated into moveable or stationary objects (including but not limited to cars, trains, trucks, aircraft, watercraft, mobile telephones, wireless handheld data devices, and other devices having, or capable of, being connected to a visual display), according to context of use.

[00363] Although the description above contains many details, these should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. Therefore, it will be appreciated that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more." All structural, chemical, and functional equivalents to the elements of the above-described preferred embodiment that are known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. 112, sixth paragraph, unless the element is expressly recited using the phrase "means for."

Table 1

Typical Traffic Signal Event Timing Cycle

	North/South Traffic			East/West Traffic	
	Left Turn	Thru Traffic	Seconds	Left Turn	Thru Traffic
(1)	red/wait	amber-red/stop	3 sec	red/wait	red/wait
(2)	red/wait	red/wait	12 sec	← green/go	red/wait
(3)	red/wait	red/wait	68 sec	← red/wait	green/go
(4)	red/wait	red/wait	3 sec	red/wait	amber-red/stop
(5)	← green/go	red/wait	14 sec	red/wait	red/wait
(6)	red/wait	green/go	78 sec	red/wait	red/wait

CLAIMS

What is claimed is:

1. A system, comprising:
a first object;
a transmitter in said first object;
a second object;
a receiver in said second object; and
a profile comprising data regarding a user associated with said first object;
wherein said profile or a subset of said profile is transmitted from said first object to said second object;
wherein content is presented to said first object; and
wherein at least a portion of said content is based on said profile or subset of said profile transmitted from said first object to said second object.

2. A system as recited in claim 1:
wherein said profile is stored in said first object;

3. A system as recited in claim 1, further comprising:
compensation to a user associated with said second object for presenting content.

4. A system as recited in claim 1:
wherein said first object is an object capable of motion.

5. A system as recited in claim 4:
wherein said first object is a vehicle or a device in a vehicle.

6. A system as recited in claim 4:
wherein said first object is an handheld device.

7. A system as recited in claim 1:
wherein said second object is a vehicle.

8. A system as recited in claim 1, wherein said second object is fixed or movable signage.

9. A system as recited in claim 1:
wherein said first object is a vehicle; and
wherein said profile further comprises data regarding other users or potential users associated with said first object.

10. A system as recited in claim 1:
wherein said first object and said second object exchange information relating to relative positions, speeds, and motion of said first and second object; information relating the character, configuration, and properties of said first and second objects; information relating to surrounding objects; and information relating to surrounding locations; or any combination thereof.

11. A system as recited in claim 1:
wherein presentation of said content is influenced by information relating to scheduling patterns of nearby traffic signals.

12. A system as recited in claim 1:
wherein said content further includes content not based on said profile.

13. A system as recited in claim 1, further including:
a priority system relating to presentation of said content based on a nature of said content.

14. A system as recited in claim 13:
wherein a nature of said content is classified as emergency content; content

relating to a surrounding environmental condition; registration and identification content relating to said second object; public safety content; or a combination thereof.

15. A system as recited in claim 1:

wherein relative motion data from said first and second objects determines whether content is presented and whether presented content is presented as animated video, static video, or a combination of both.

16. A system as recited in claim 1:

wherein said content includes audio content, video content, or a combination of both; and

wherein said audio content is presented by said first object; and

wherein said video content is presented by either said first object or second object.

17. A system as recited in claim 1:

wherein said first and second objects are vehicles;

wherein said content comprises positioning information relating to said first and second objects; and

wherein said content indicates to an operator of said first object an optimum stopping position.

18. A system as recited in claim 17:

wherein speed and positioning information is exchanged between all objects within transmission range; and

wherein said content presented to said first object indicates to an operator of said first object relative braking conditions of any objects in front of said first object.

19. A system as recited in claim 1:

wherein said second object has a user associated with said second object;

and

wherein at least a portion of said content presented to said first object is created by said user associated with said second object.

20. A system as recited in claim 1:

wherein a third party purchases a right to present content on said second object; and

wherein said second object presents content based on preferences of said third party.

21. A system as recited in claim 20:

wherein said right is based on a fixed or relative geographical area; a time of day; a period of available display time; or any combination thereof.

22. A system as recited in claim 1:

wherein said profile is transferable to other objects at an option of any user associated with said first object.

23. A system as recited in claim 1:

wherein said content is viewable by persons other than those associated with said first object.

24. A system as recited in claim 1:

wherein said content is presented in a manner to render said content not viewable by individuals other than those associated with said first object.

25. A system as recited in claim 1, further comprising:

a display integrated with said second object;

wherein at least a portion of said content presented to said first object occurs on said display.

26. A system as recited in claim 1:

wherein presentation of said content occurs on an exterior portion of said second object.

27. A system as recited in claim 1, further comprising:

a first storage medium associated with said first object;

a second storage medium associated with said second object;

wherein data related to presentation of said content is stored in said first and second storage media.

28. A system as recited in claim 27, further comprising:

a central server wirelessly connected to said first and second objects;

wherein said data related to presentation of said content is uploaded to said central server.

29. A system as recited in claim 28:

wherein a compilation of uploaded data is offered for sale.

30. A system as recited in claim 29:

wherein said data related to presentation of said content includes time of display; subject matter of said content; duration of display of said content; a subset of said profile; or any combination thereof.

31. A system as recited in claim 1:

wherein presentation of said content occurs in an interior portion of said first object.

32. A system as recited in claim 1, further comprising:

compensation to said user associated with said first object for receiving content, viewing content, or any combination thereof.

33. A system as recited in claim 1:

wherein information is exchanged between said first object and any adjacent or nearby objects related to identities of all objects.

34. A system as recited in claim 1:

wherein said objects exchange information related to audio playing in said first object; and

wherein said content is video content synchronized to said audio.

35. A system as recited in claim 1:

wherein content presented to said first object is limited by a user associated with said second object.

36. A computer implemented method, comprising:

compiling a unique profile of a first user based on analysis of data provided by said first user;

associating said profile with a first object;

transmitting said profile or a subset of said profile to a second object; and

presenting content to said first user;

wherein said first object is associated with said first user;

wherein said content originates from said second object; and

wherein at least a portion of said content is based on said profile or subset of said profile transmitted to said second object.

37. A method as recited in claim 36, further comprising:

compensating a user associated with said second object for presenting content to said first user.

38. A method as recited in claim 36, further comprising:

prioritizing display of said content based on purpose of said content;

wherein purpose of said content is advertising; informational; traffic related;

safety related; news related; region specific; political; mere frivolity; or any combination thereof.

39. A method as recited in claim 38, further comprising:

pre-empting presentation of said content based on surrounding environment of said first and second objects; presence of emergency circumstances; public interest; or any combination thereof.

40. A method as recited in claim 36, further comprising:

prioritizing display of content based on preferences of said first user.

41. A method as recited in claim 36, further comprising:

transferring said profile to other objects at an option of said first user.

42. A method as recited in claim 36, further including:

displaying registration and identification information for said second object on said second object.

43. A method as recited in claim 36, further including:

displaying content created by a user associated with said second object on said second object.

44. A method as recited in claim 36, further including:

displaying indicators of optimal traffic and view positioning on said second object to said first user;

wherein said first objects and said second objects are vehicles.

45. A method as recited in claim 36, further including:

pre-empting display of said content in the presence of external wireless signals for emergency or traffic direction purposes.

46. A method as recited in claim 36, further including:

presenting audio content to said first user using said first object.

47. A method as recited in claim 36, further including:

presenting video content to said first user using said first object, said second object, or a combination of said first and second objects.

48. A method as recited in claim 36:

exchanging information relating to relative positions, speeds, and motion of said first and second object; information relating the character, configuration, and properties of said first and second objects; information relating to surrounding objects; and information relating to surrounding locations; or any combination thereof, between said first object and said second object.

49. A method as recited in claim 36, further comprising:

determining relative motions of said first and second objects;

presenting no content or content as animated video, static video, or a combination of animated and static video, based on said relative motions of said first and second objects.

50. A system as recited in claim 36:

wherein said content is presented on a display integrated with said second object.

51. A system as recited in claim 36:

wherein said content is presented on an exterior portion of said second object.

52. A system as recited in claim 36, further comprising:

storing data related to presentation of said content in said first and second objects.

53. A system as recited in claim 52, further comprising:

uploading said data related to said presentation of said content to a central server wirelessly connected to said first and second objects.

54. A system as recited in claim 53, further comprising:

offering a compilation of uploaded data from said central server for sale.

55. A system as recited in claim 54:

wherein said data related to presentation of said content includes time of display; subject matter of said content; duration of display of said content; a subset of said profile; or any combination thereof.

56. A method, comprising:

populating a source object with content; and

presenting said content to a recipient object in response to a unique profile or portion thereof associated with said recipient object that is provided by said recipient object to said source object.

57. A system, comprising:

a content storage device; and

means for presenting content stored on said content storage device to a recipient object in response to a unique profile or portion thereof associated with said recipient object that is provided by said recipient object to said source object.

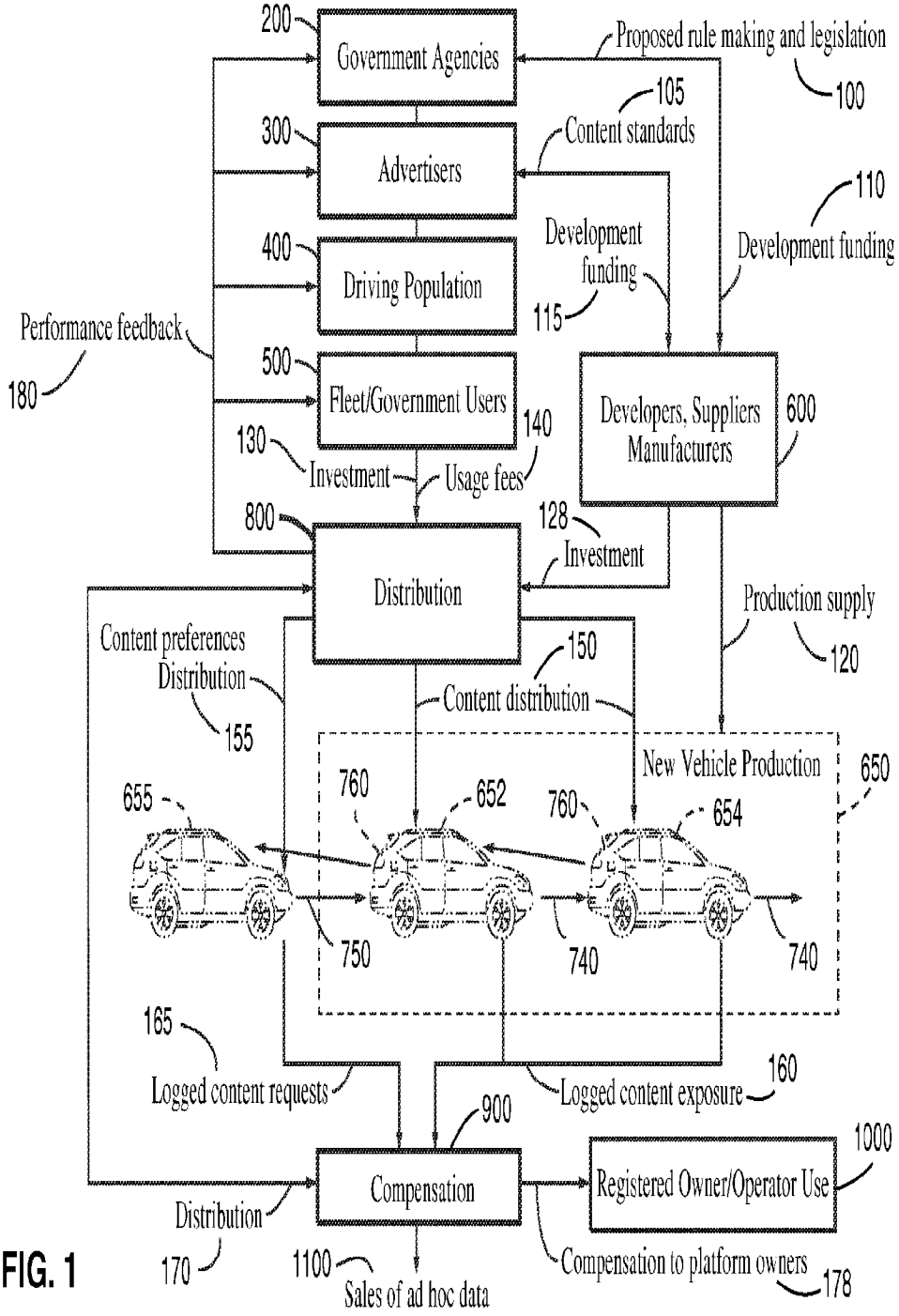

200
Government Agencies
Proposed rule making and legislation
100
105
Content standards
300
Advertisers
110
Development funding
400
Driving Population
Development funding
115
Performance feedback
180
500
Fleet/Government Users
Developers, Suppliers Manufacturers
600
140
130
Investment
Usage fees
800
128
Investment
Distribution
Production supply
120
Content preferences
Distribution
155
150
Content distribution
New Vehicle Production
650
655
760
652
760
654
750
740
740
165
Logged content requests
Logged content exposure
160
900
1000
Compensation
Registered Owner/Operator Use
Distribution
170
1100
Sales of ad hoc data
Compensation to platform owners
178

FIG. 1

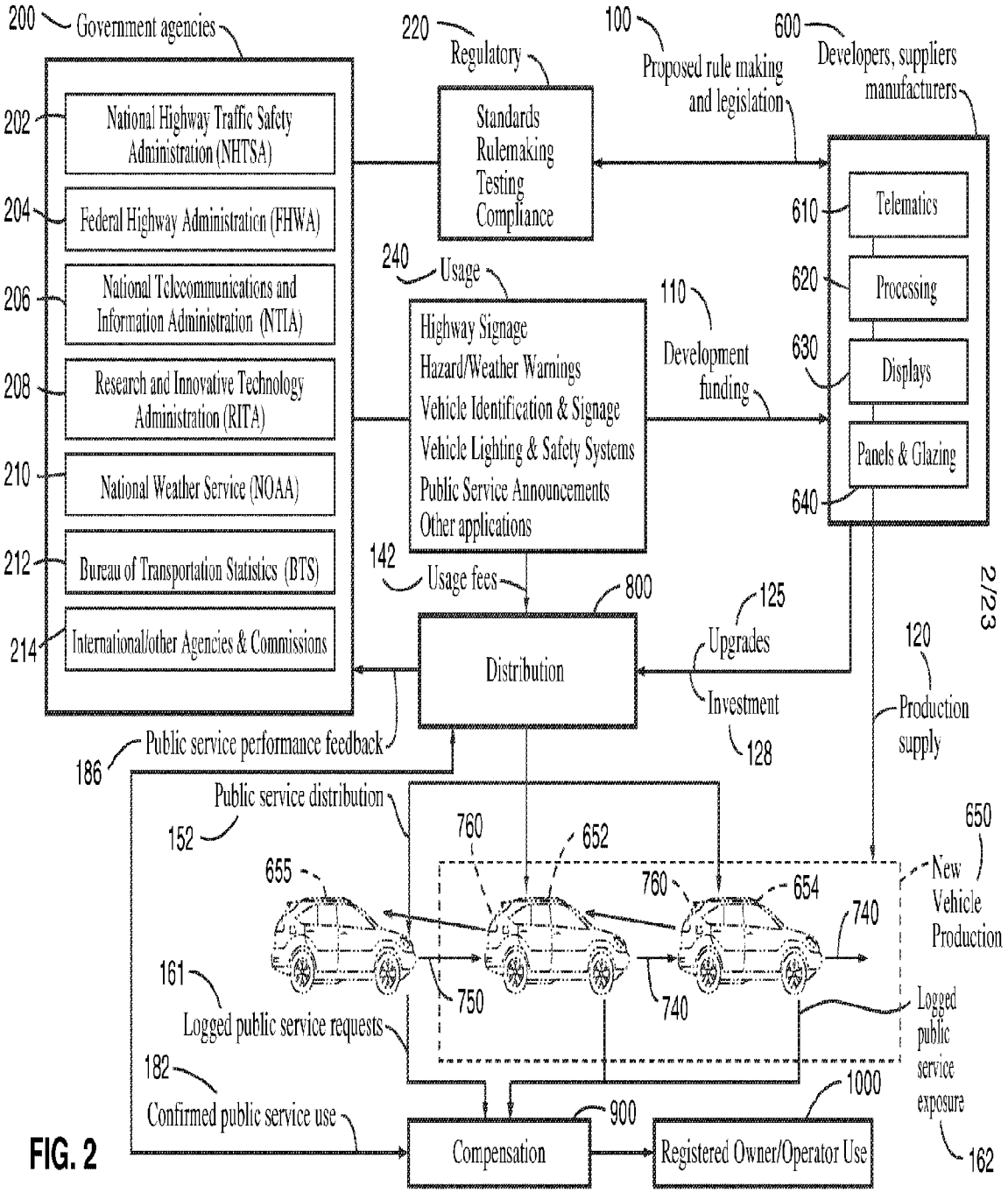

200
Government agencies
202
National Highway Traffic Safety Administration (NHTSA)
204
Federal Highway Administration (FHWA)
206
National Telecommunications and Information Administration (NTIA)
208
Research and Innovative Technology Administration (RITA)
210
National Weather Service (NOAA)
212
Bureau of Transportation Statistics (BTS)
214
International/other Agencies & Commissions
220
Regulatory
Standards
Rulemaking
Testing
Compliance
100
Proposed rule making and legislation
600
Developers, suppliers manufacturers
610
Telematics
620
Processing
630
Displays
640
Panels & Glazing
240
Usage
Highway Signage
Hazard/Weather Warnings
Vehicle Identification & Signage
Vehicle Lighting & Safety Systems
Public Service Announcements
Other applications
110
Development funding
142
Usage fees
800
Distribution
125
Upgrades
Investment
128
120
Production supply
186
Public service performance feedback
152
Public service distribution
760
652
655
760
654
740
650
New Vehicle Production
161
Logged public service requests
750
740
Logged public service exposure
182
Confirmed public service use
900
Compensation
1000
Registered Owner/Operator Use
162

FIG. 2

2/23

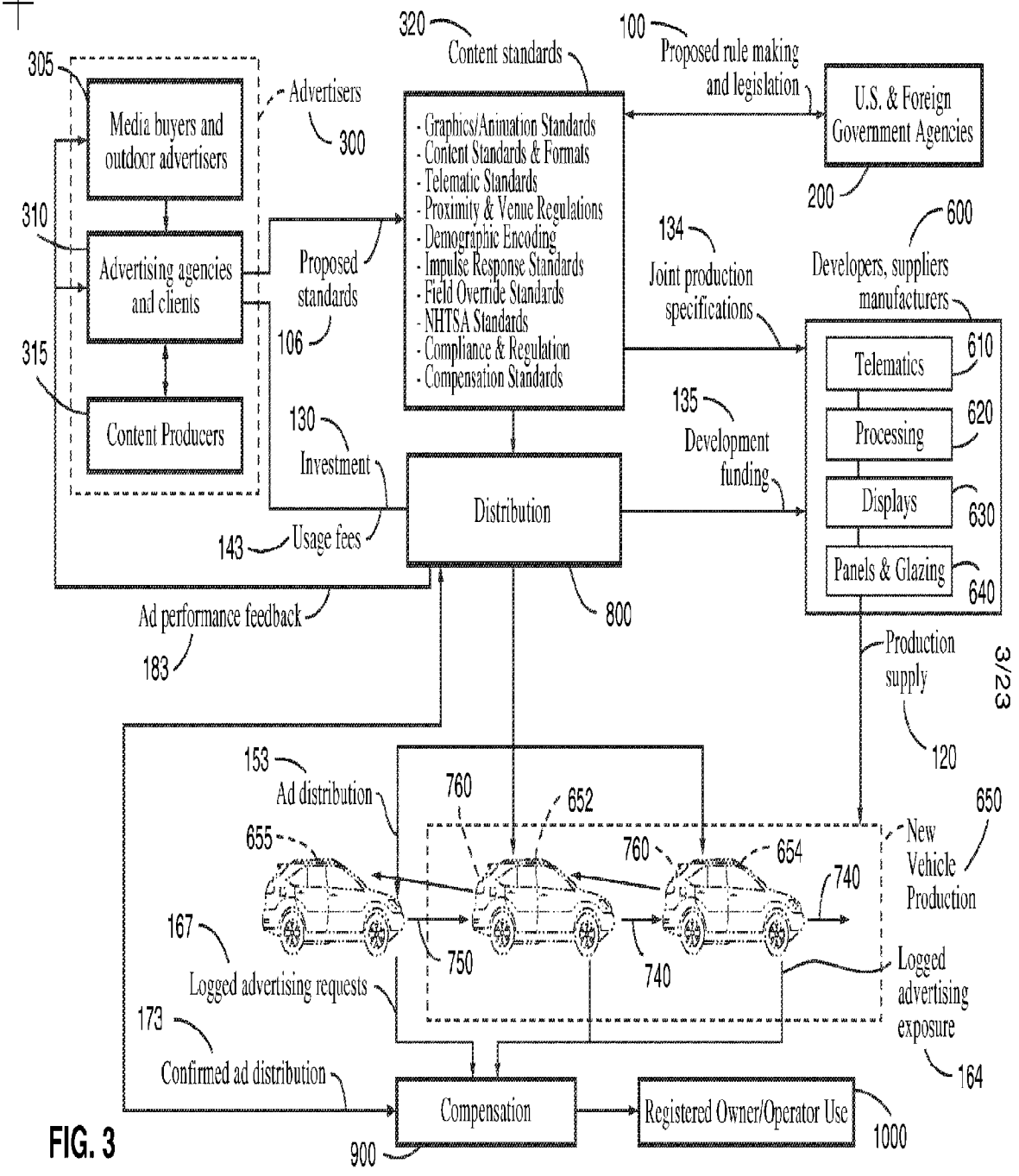

320
Content standards
100
Proposed rule making and legislation
U.S. & Foreign Government Agencies
200
305
Media buyers and outdoor advertisers
Advertisers
300
- Graphics/Animation Standards
- Content Standards & Formats
- Telematic Standards
- Proximity & Venue Regulations
- Demographic Encoding
- Impulse Response Standards
- Field Override Standards
- NHTSA Standards
- Compliance & Regulation
- Compensation Standards
310
Advertising agencies and clients
Proposed standards
106
134
Joint production specifications
600
Developers, suppliers manufacturers
315
Content Producers
130
Investment
135
Development funding
610
Telematics
620
Processing
630
Displays
640
Panels & Glazing
143
Usage fees
Distribution
800
Ad performance feedback
183
Production supply
120
3/23
153
Ad distribution
760
652
650
New Vehicle Production
655
760
654
740
167
750
740
Logged advertising requests
Logged advertising exposure
164
173
Confirmed ad distribution
Compensation
900
Registered Owner/Operator Use
1000

FIG. 3

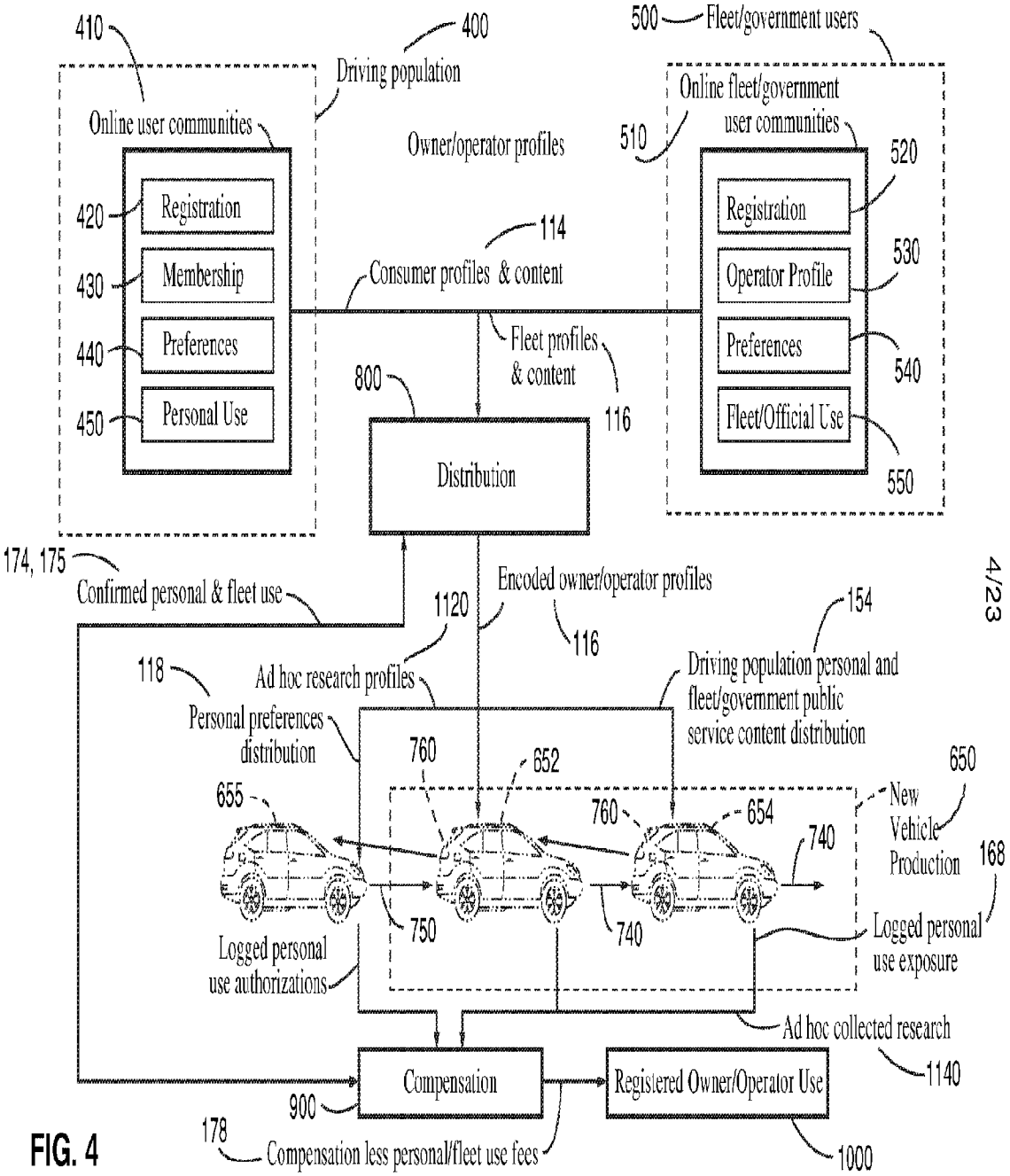

410
400
Driving population
500
Fleet/government users
Online user communities
Online fleet/government user communities
Owner/operator profiles
510
520
420
Registration
114
Registration
530
430
Membership
Consumer profiles & content
Operator Profile
440
Preferences
Fleet profiles & content
Preferences
540
800
450
Personal Use
116
Fleet/Official Use
550
Distribution
174, 175
Confirmed personal & fleet use
1120
Encoded owner/operator profiles
116
154
118
Ad hoc research profiles
Driving population personal and fleet/government public service content distribution
Personal preferences distribution
760
652
650
655
760
654
740
New Vehicle Production
168
750
740
Logged personal use exposure
Logged personal use authorizations
Ad hoc collected research
1140
Compensation
Registered Owner/Operator Use
900
178
Compensation less personal/fleet use fees
1000

FIG. 4

4/23

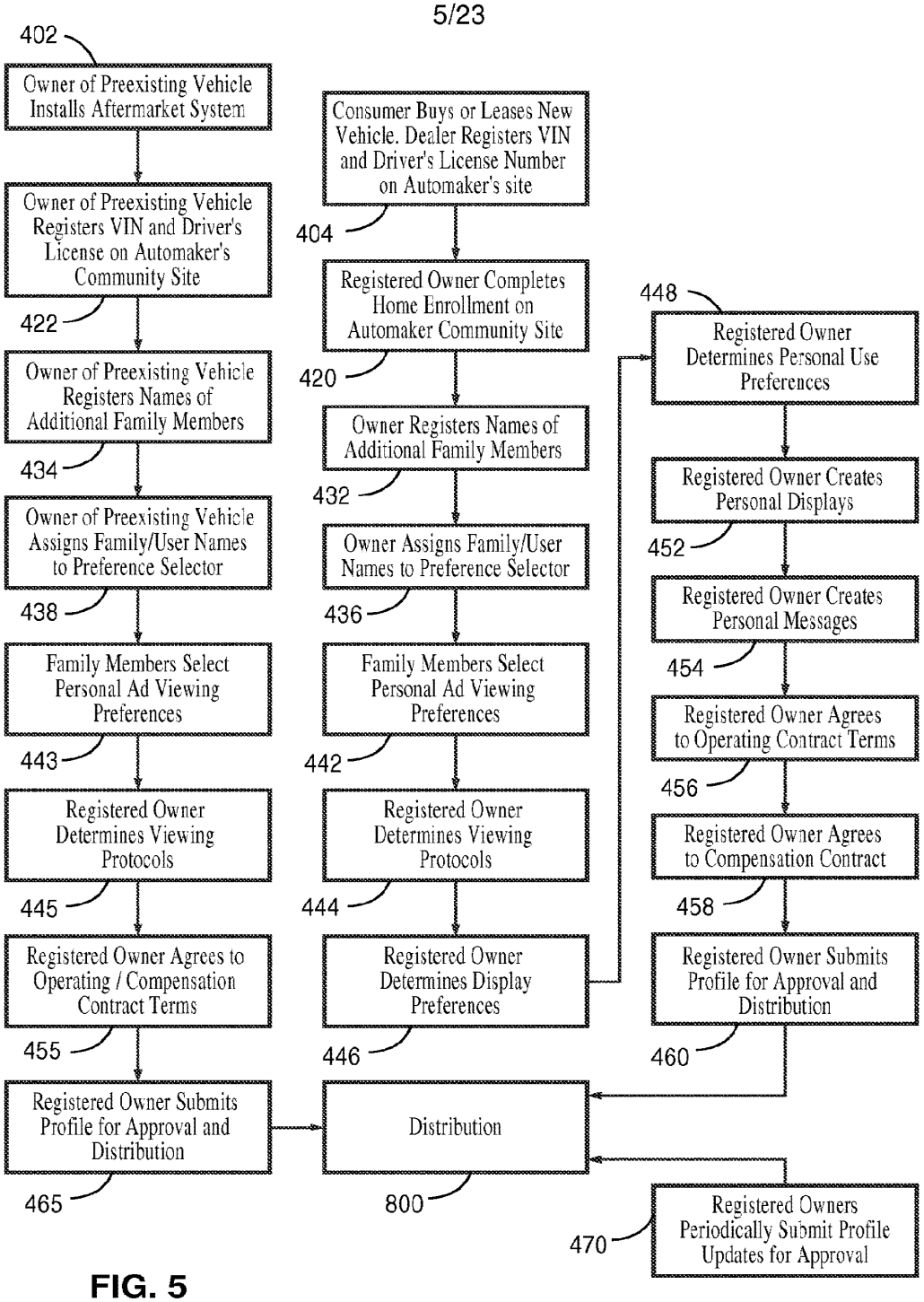

402
Owner of Preexisting Vehicle Installs Aftermarket System
Owner of Preexisting Vehicle Registers VIN and Driver's License on Automaker's Community Site
422
Owner of Preexisting Vehicle Registers Names of Additional Family Members
434
Owner of Preexisting Vehicle Assigns Family/User Names to Preference Selector
438
Family Members Select Personal Ad Viewing Preferences
443
Registered Owner Determines Viewing Protocols
445
Registered Owner Agrees to Operating / Compensation Contract Terms
455
Registered Owner Submits Profile for Approval and Distribution
465
Consumer Buys or Leases New Vehicle. Dealer Registers VIN and Driver's License Number on Automaker's site
404
Registered Owner Completes Home Enrollment on Automaker Community Site
420
Owner Registers Names of Additional Family Members
432
Owner Assigns Family/User Names to Preference Selector
436
Family Members Select Personal Ad Viewing Preferences
442
Registered Owner Determines Viewing Protocols
444
Registered Owner Determines Display Preferences
446
Distribution
800
448
Registered Owner Determines Personal Use Preferences
Registered Owner Creates Personal Displays
452
Registered Owner Creates Personal Messages
454
Registered Owner Agrees to Operating Contract Terms
456
Registered Owner Agrees to Compensation Contract
458
Registered Owner Submits Profile for Approval and Distribution
460
Registered Owners Periodically Submit Profile Updates for Approval
470

FIG. 5

FIG. 6

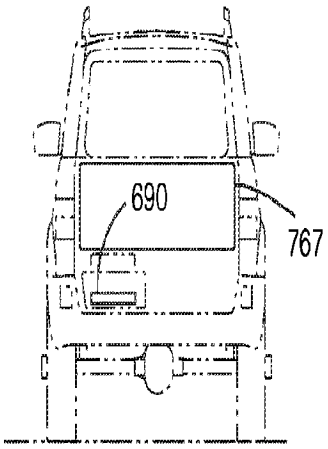


FIG. 7

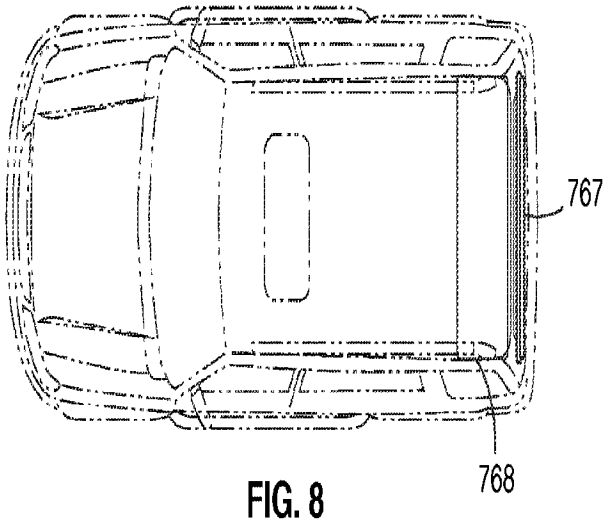


FIG. 8

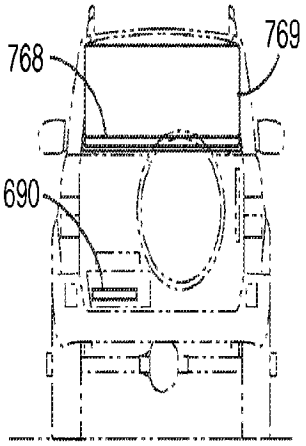


FIG. 9

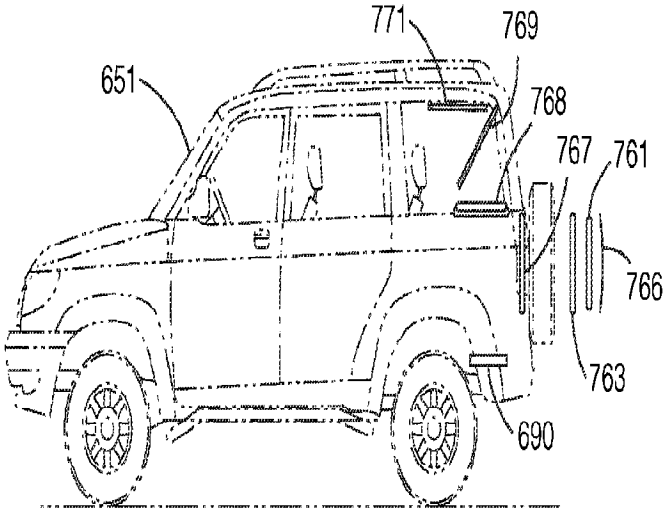


FIG. 10

FIG. 12

FIG. 11

FIG. 13

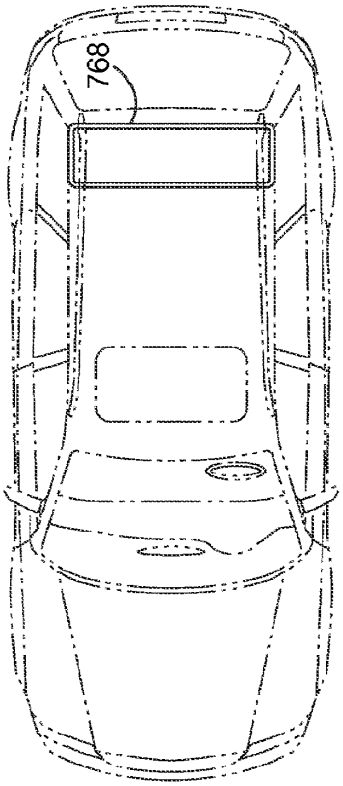


FIG. 15

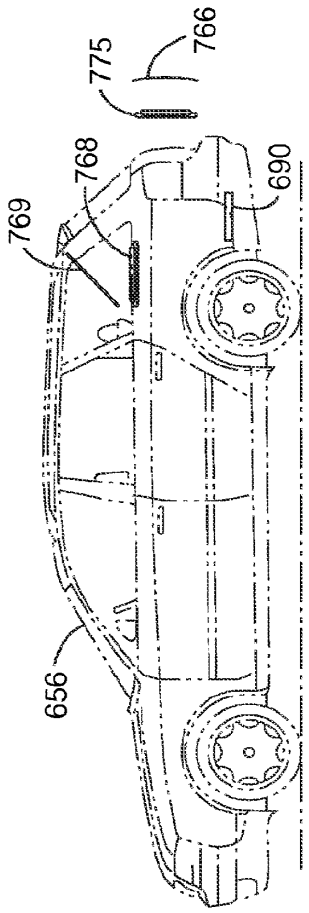


FIG. 16

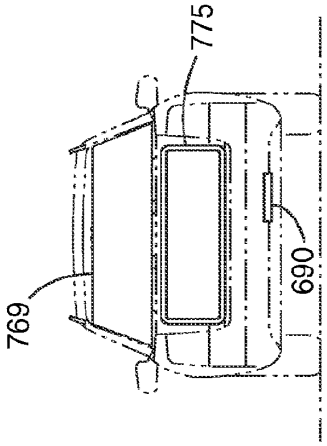


FIG. 14

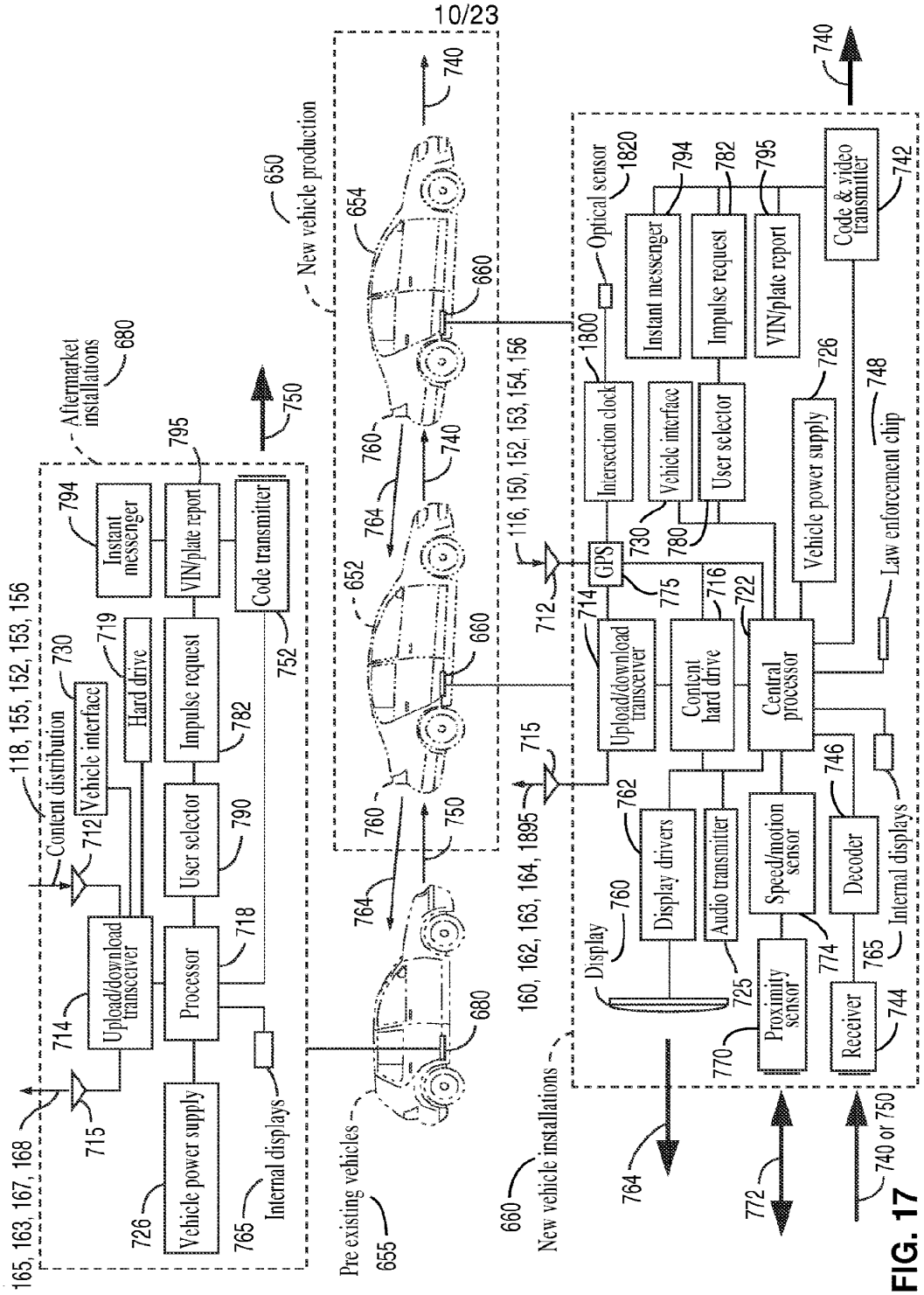

Aftermarket installations
680
Content distribution
118, 155, 152, 153, 156
Vehicle interface
730
Hard drive
719
Instant messenger
794
VIN/plate report
795
Code transmitter
752
Impulse request
782
User selector
790
Upload/download transceiver
714
Processor
718
Vehicle power supply
726
Internal displays
765
165, 163, 167, 168
715
712
750
New vehicle production
650
654
652
660
760
764
740
Pre existing vehicles
655
680
116, 150, 152, 153, 154, 156
160, 162, 163, 164, 1895
New vehicle installations
660
Optical sensor
1820
Instant messenger
794
Impulse request
782
VIN/plate report
795
Code & video transmitter
742
Intersection clock
1800
Vehicle interface
730
User selector
780
Vehicle power supply
726
Law enforcement chip
748
GPS
775
Upload/download transceiver
714
Content hard drive
716
Central processor
722
Display drivers
762
Audio transmitter
725
Speed/motion sensor
774
Decoder
746
Internal displays
765
Display
760
Proximity sensor
770
Receiver
744
764
772
740 or 750

FIG. 17

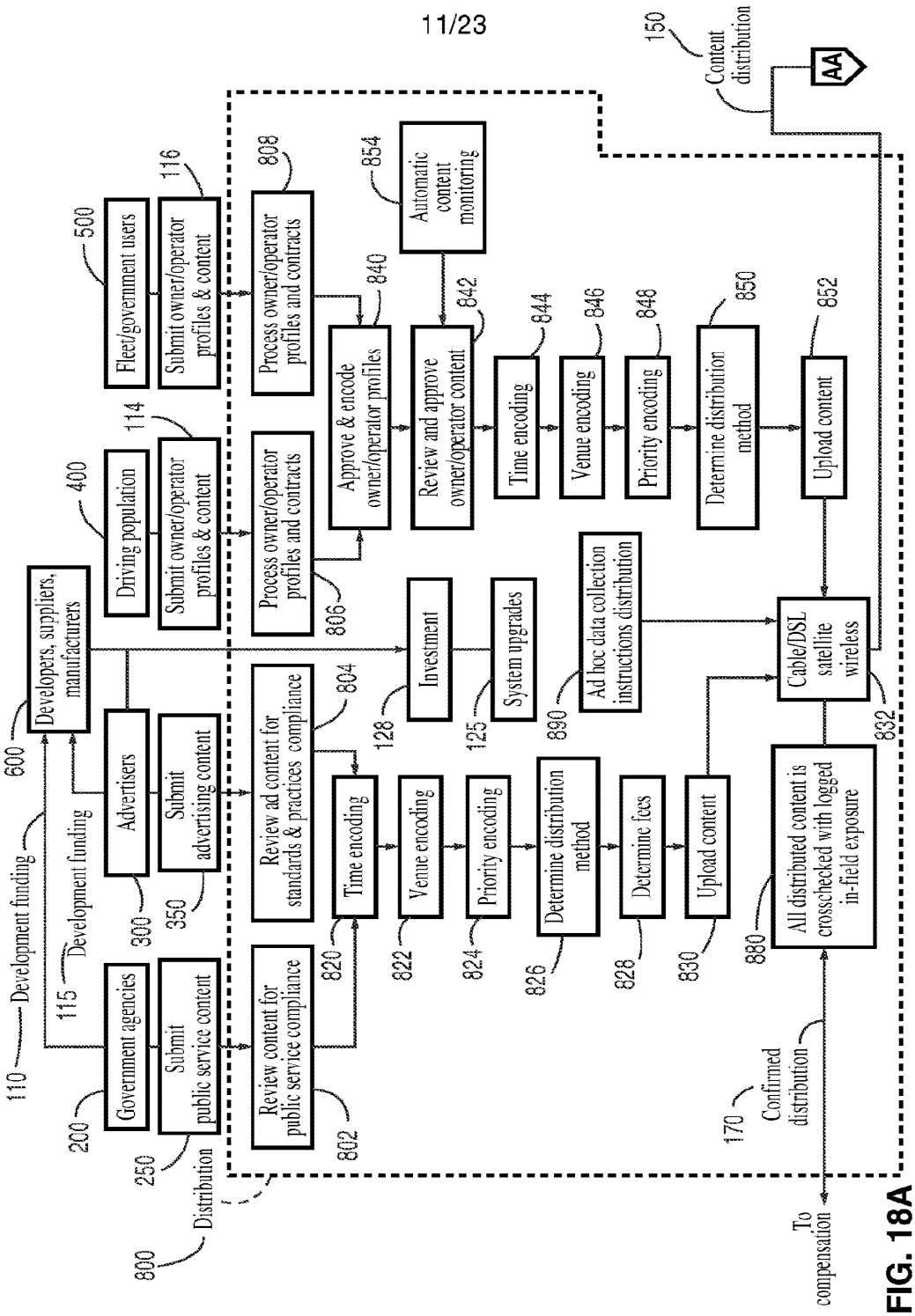

Content distribution
150
AA
Fleet/government users
500
Submit owner/operator profiles & content
116
Process owner/operator profiles and contracts
808
Automatic content monitoring
854
Approve & encode owner/operator profiles
840
Review and approve owner/operator content
842
Time encoding
844
Venue encoding
846
Priority encoding
848
Determine distribution method
850
Upload content
852
Driving population
400
Submit owner/operator profiles & content
114
Process owner/operator profiles and contracts
806
Investment
128
System upgrades
125
Ad hoc data collection instructions distribution
890
Cable/DSL satellite wireless
832
Developers, suppliers, manufacturers
600
Development funding
110
Development funding
115
Advertisers
300
Submit advertising content
350
Review ad content for standards & practices compliance
804
Time encoding
820
Venue encoding
822
Priority encoding
824
Determine distribution method
826
Determine fees
828
Upload content
830
Government agencies
200
Submit public service content
250
Review content for public service compliance
802
All distributed content is crosschecked with logged in-field exposure
880
Confirmed distribution
170
To compensation
Distribution
800

FIG. 18A

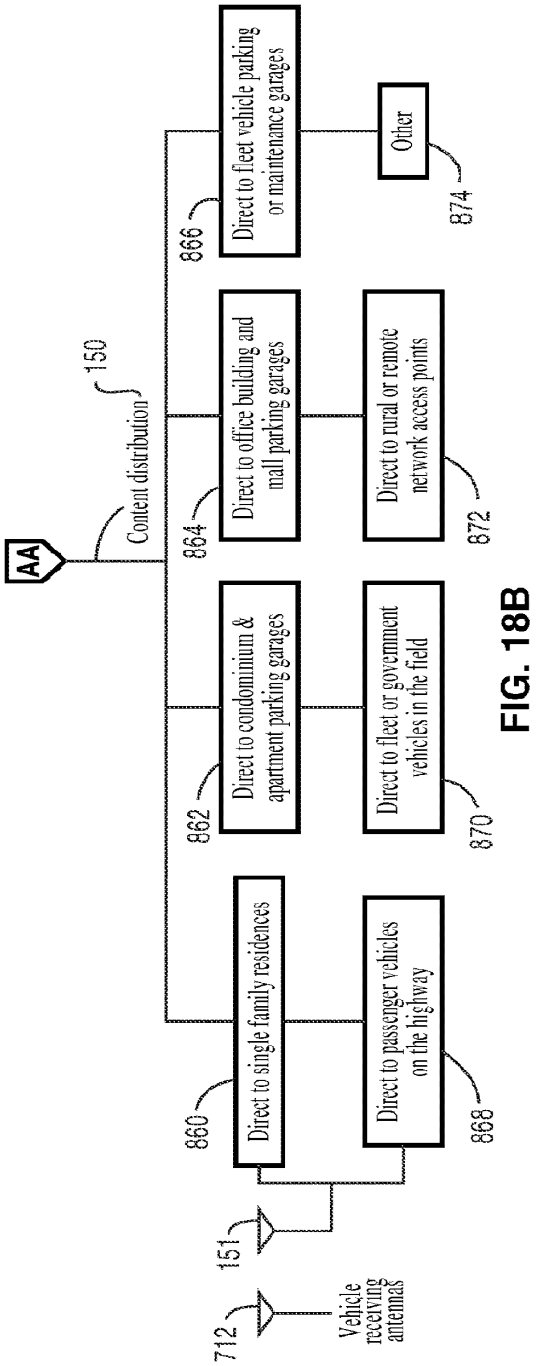

AA
150
Content distribution
860
Direct to single family residences
862
Direct to condominium & apartment parking garages
864
Direct to office building and mall parking garages
866
Direct to fleet vehicle parking or maintenance garages
868
Direct to passenger vehicles on the highway
870
Direct to fleet or government vehicles in the field
872
Direct to rural or remote network access points
874
Other
151
712
Vehicle receiving antennas

FIG. 18B

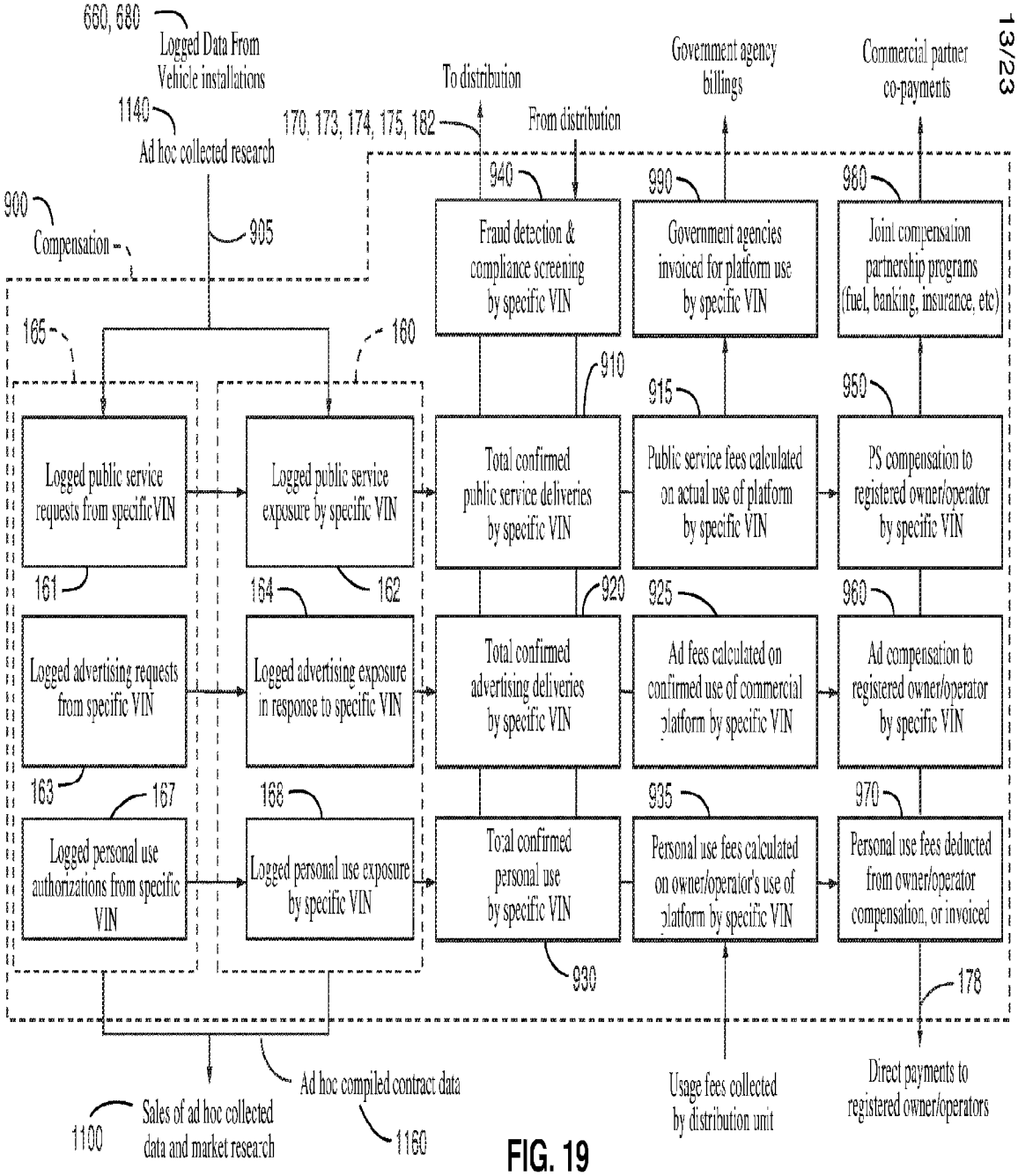

660, 680
Logged Data From Vehicle installations
1140
Ad hoc collected research
170, 173, 174, 175, 182
To distribution
From distribution
Government agency billings
Commercial partner co-payments
900
Compensation
905
940
Fraud detection & compliance screening by specific VIN
990
Government agencies invoiced for platform use by specific VIN
960
Joint compensation partnership programs (fuel, banking, insurance, etc)
165
160
910
915
950
Logged public service requests from specific VIN
Logged public service exposure by specific VIN
Total confirmed public service deliveries by specific VIN
Public service fees calculated on actual use of platform by specific VIN
PS compensation to registered owner/operator by specific VIN
161
154
162
920
925
960
Logged advertising requests from specific VIN
Logged advertising exposure in response to specific VIN
Total confirmed advertising deliveries by specific VIN
Ad fees calculated on confirmed use of commercial platform by specific VIN
Ad compensation to registered owner/operator by specific VIN
163
167
168
935
970
Logged personal use authorizations from specific VIN
Logged personal use exposure by specific VIN
Total confirmed personal use by specific VIN
Personal use fees calculated on owner/operator's use of platform by specific VIN
Personal use fees deducted from owner/operator compensation, or invoiced
930
178
Ad hoc compiled contract data
1160
1190
Sales of ad hoc collected data and market research
Usage fees collected by distribution unit
Direct payments to registered owner/operators

FIG. 19

FIG. 20

FIG. 21

FIG. 22

FIG. 23

FIG. 24

FIG. 25

FIG. 26

FIG. 27

1262
1242
1222
McDonald's
Hilton
Apple
7th Street
1240
1260
6th Street
Hilton
Hotel
1244
5th Street
Convention
Center
4th Street
1250
Roadwork
3rd Street
1220
1284
2nd Street
Main Street
1st Street
1200
NORTH
1280

FIG. 28

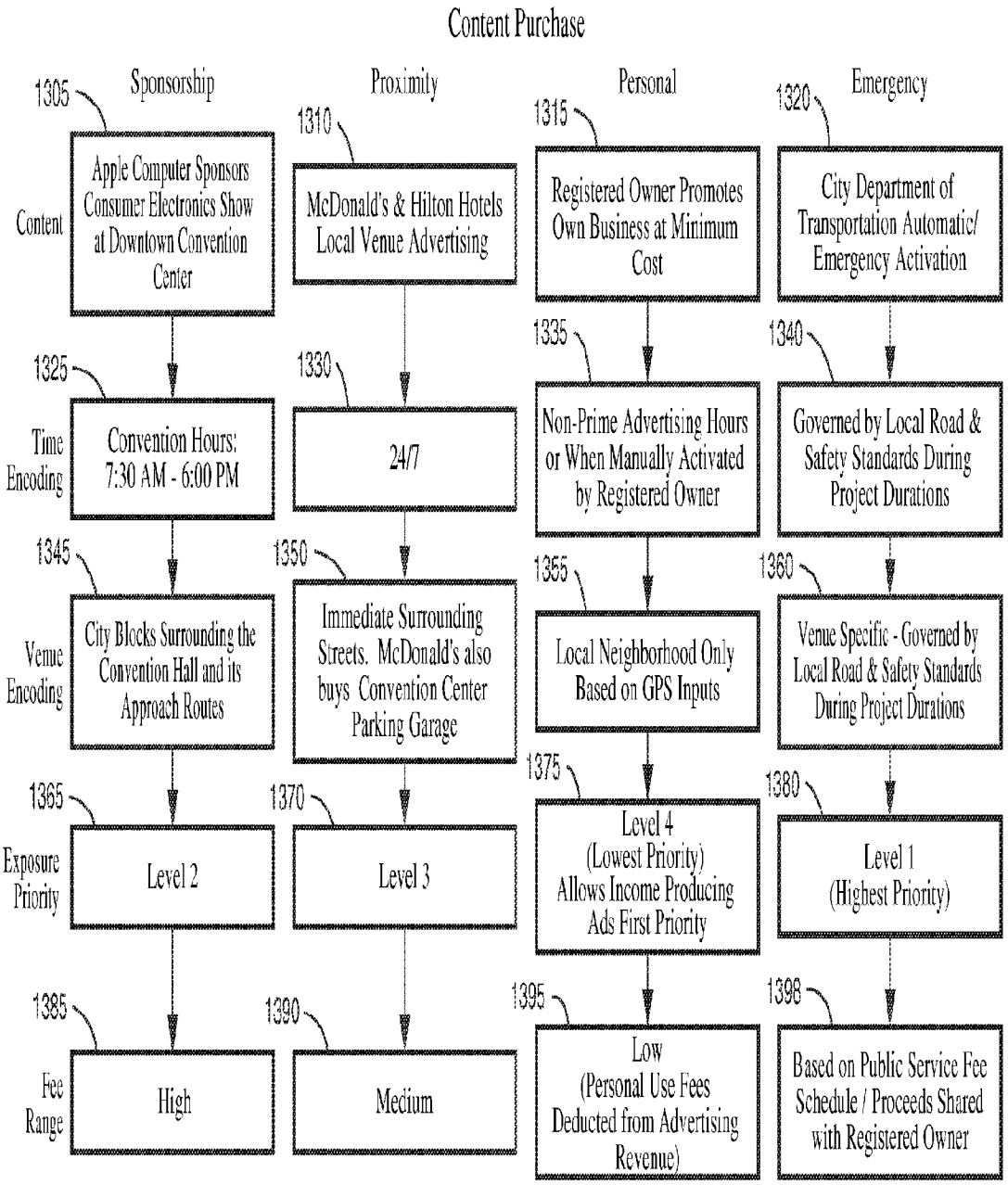

Content Purchase
Sponsorship
Proximity
Personal
Emergency
1305
1310
1315
1320
Content
Apple Computer Sponsors Consumer Electronics Show at Downtown Convention Center
McDonald's & Hilton Hotels Local Venue Advertising
Registered Owner Promotes Own Business at Minimum Cost
City Department of Transportation Automatic/ Emergency Activation
1325
1330
1335
1340
Time Encoding
Convention Hours: 7:30 AM - 6:00 PM
24/7
Non-Prime Advertising Hours or When Manually Activated by Registered Owner
Governed by Local Road & Safety Standards During Project Durations
1345
1350
1355
1360
Venue Encoding
City Blocks Surrounding the Convention Hall and its Approach Routes
Immediate Surrounding Streets. McDonald's also buys Convention Center Parking Garage
Local Neighborhood Only Based on GPS Inputs
Venue Specific - Governed by Local Road & Safety Standards During Project Durations
1365
1370
1375
1380
Exposure Priority
Level 2
Level 3
Level 4 (Lowest Priority) Allows Income Producing Ads First Priority
Level 1 (Highest Priority)
1385
1390
1395
1398
Fee Range
High
Medium
Low (Personal Use Fees Deducted from Advertising Revenue)
Based on Public Service Fee Schedule / Proceeds Shared with Registered Owner

FIG. 29

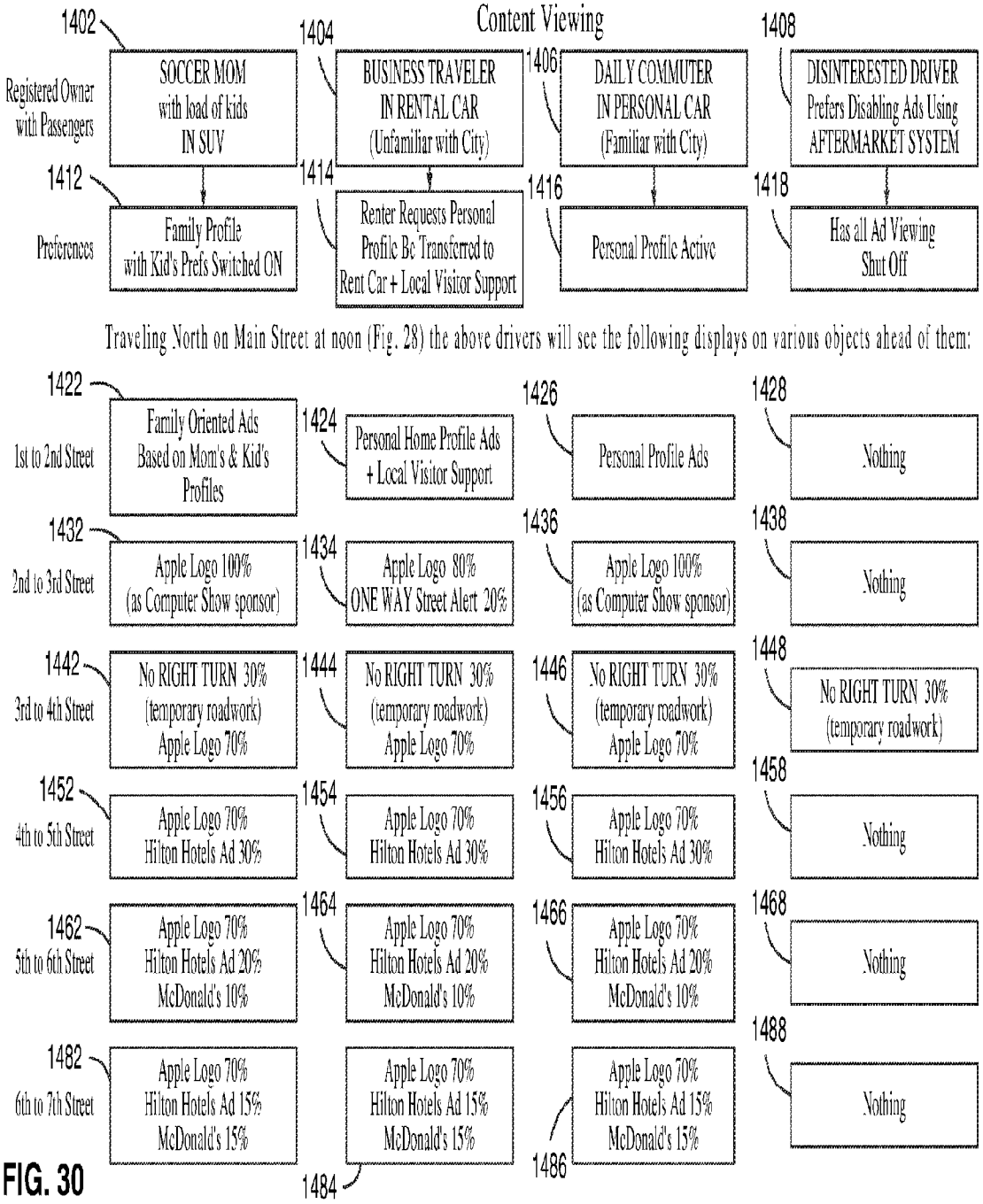

Content Viewing
1402
1404
1406
1408
Registered Owner with Passengers
SOCCER MOM with load of kids IN SUV
BUSINESS TRAVELER IN RENTAL CAR (Unfamiliar with City)
DAILY COMMUTER IN PERSONAL CAR (Familiar with City)
DISINTERESTED DRIVER Prefers Disabling Ads Using AFTERMARKET SYSTEM
1412
1414
1416
1418
Preferences
Family Profile with Kid's Prefs Switched ON
Renter Requests Personal Profile Be Transferred to Rent Car + Local Visitor Support
Personal Profile Active
Has all Ad Viewing Shut Off
Traveling North on Main Street at noon (Fig. 28) the above drivers will see the following displays on various objects ahead of them:
1422
1424
1426
1428
1st to 2nd Street
Family Oriented Ads Based on Mom's & Kid's Profiles
Personal Home Profile Ads + Local Visitor Support
Personal Profile Ads
Nothing
1432
1434
1436
1438
2nd to 3rd Street
Apple Logo 100% (as Computer Show sponsor)
Apple Logo 80% ONE WAY Street Alert 20%
Apple Logo 100% (as Computer Show sponsor)
Nothing
1442
1444
1446
1448
3rd to 4th Street
No RIGHT TURN 30% (temporary roadwork) Apple Logo 70%
No RIGHT TURN 30% (temporary roadwork) Apple Logo 70%
No RIGHT TURN 30% (temporary roadwork) Apple Logo 70%
No RIGHT TURN 30% (temporary roadwork)
1452
1454
1456
1458
4th to 5th Street
Apple Logo 70% Hilton Hotels Ad 30%
Apple Logo 70% Hilton Hotels Ad 30%
Apple Logo 70% Hilton Hotels Ad 30%
Nothing
1462
1464
1466
1468
5th to 6th Street
Apple Logo 70% Hilton Hotels Ad 20% McDonald's 10%
Apple Logo 70% Hilton Hotels Ad 20% McDonald's 10%
Apple Logo 70% Hilton Hotels Ad 20% McDonald's 10%
Nothing
1482
1484
1486
1488
6th to 7th Street
Apple Logo 70% Hilton Hotels Ad 15% McDonald's 15%
Apple Logo 70% Hilton Hotels Ad 15% McDonald's 15%
Apple Logo 70% Hilton Hotels Ad 15% McDonald's 15%
Nothing

FIG. 30

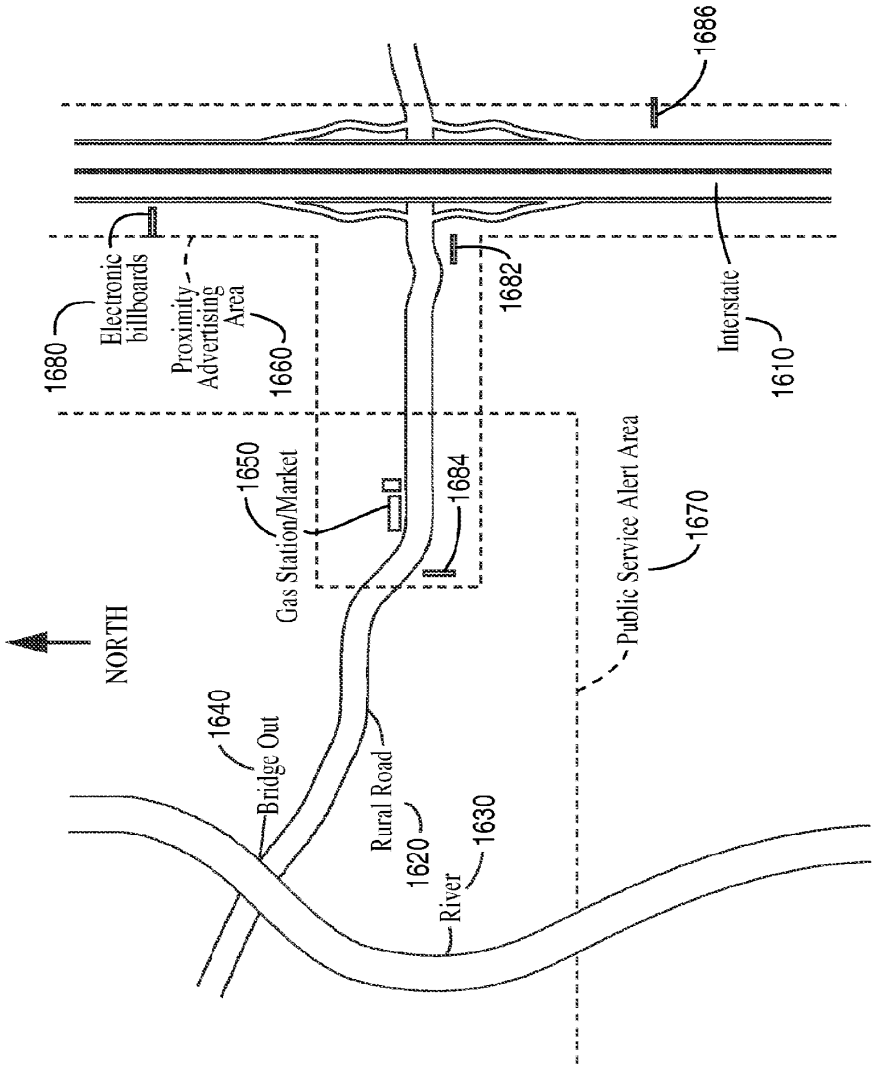

1686
Electronic billboards
1680
Proximity Advertising Area
1660
1682
Interstate
1610
1650
Gas Station/Market
1684
Public Service Alert Area
1670
NORTH
1640
Bridge Out
Rural Road
1620
River
1630

FIG. 32

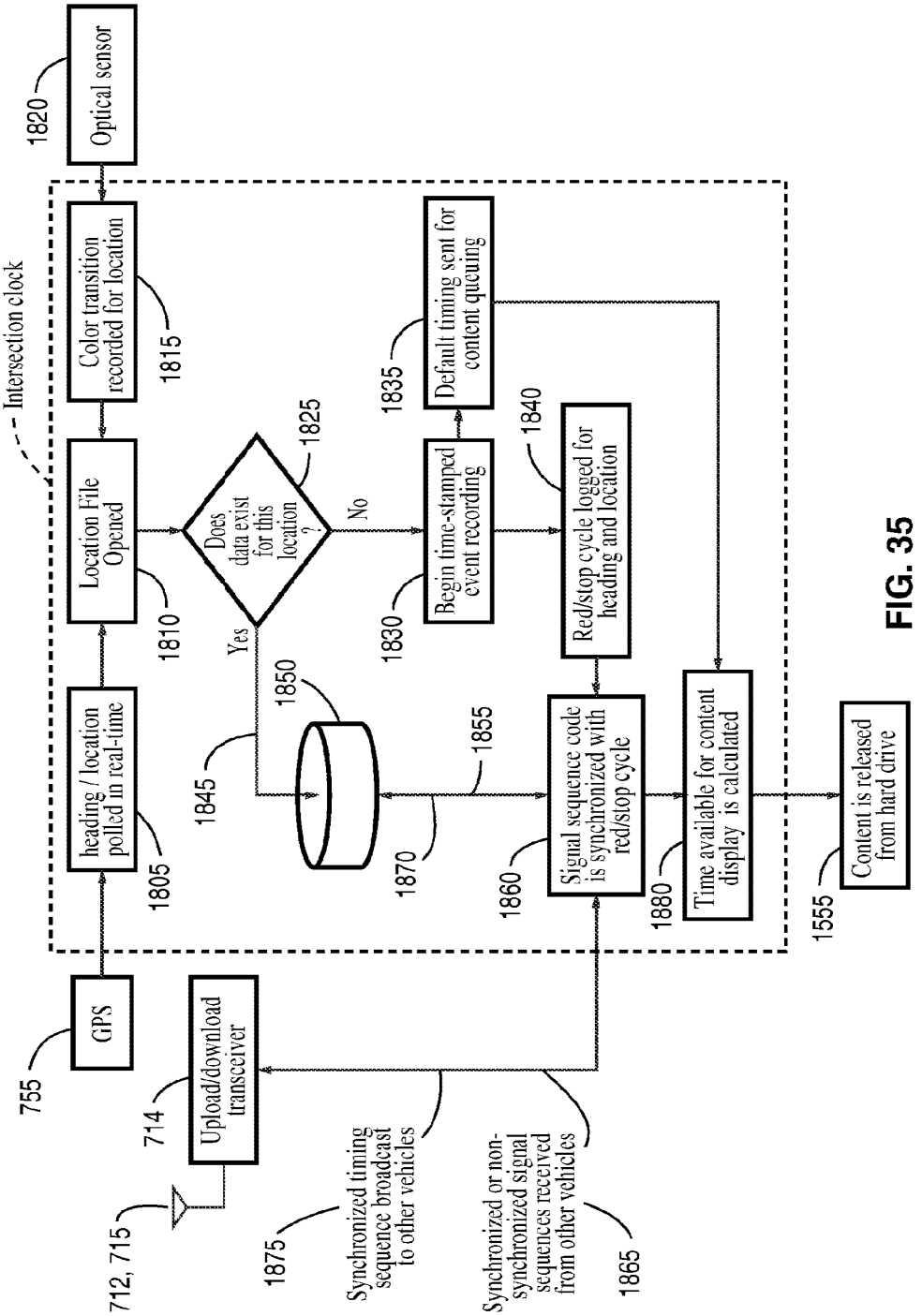

1800
Intersection clock
1820
Optical sensor
Color transition recorded for location
1815
Location File Opened
1810
heading / location polled in real-time
1805
Does data exist for this location ?
1825
Yes
No
1835
Default timing sent for content queuing
1830
Begin time-stamped event recording
1840
Red/stop cycle logged for heading and location
1850
1845
1855
1870
1860
Signal sequence code is synchronized with red/stop cycle
1880
Time available for content display is calculated
1555
Content is released from hard drive
755
GPS
714
Upload/download transceiver
712, 715
1875
Synchronized timing sequence broadcast to other vehicles
Synchronized or non-synchronized signal sequences received from other vehicles
1865

FIG. 35

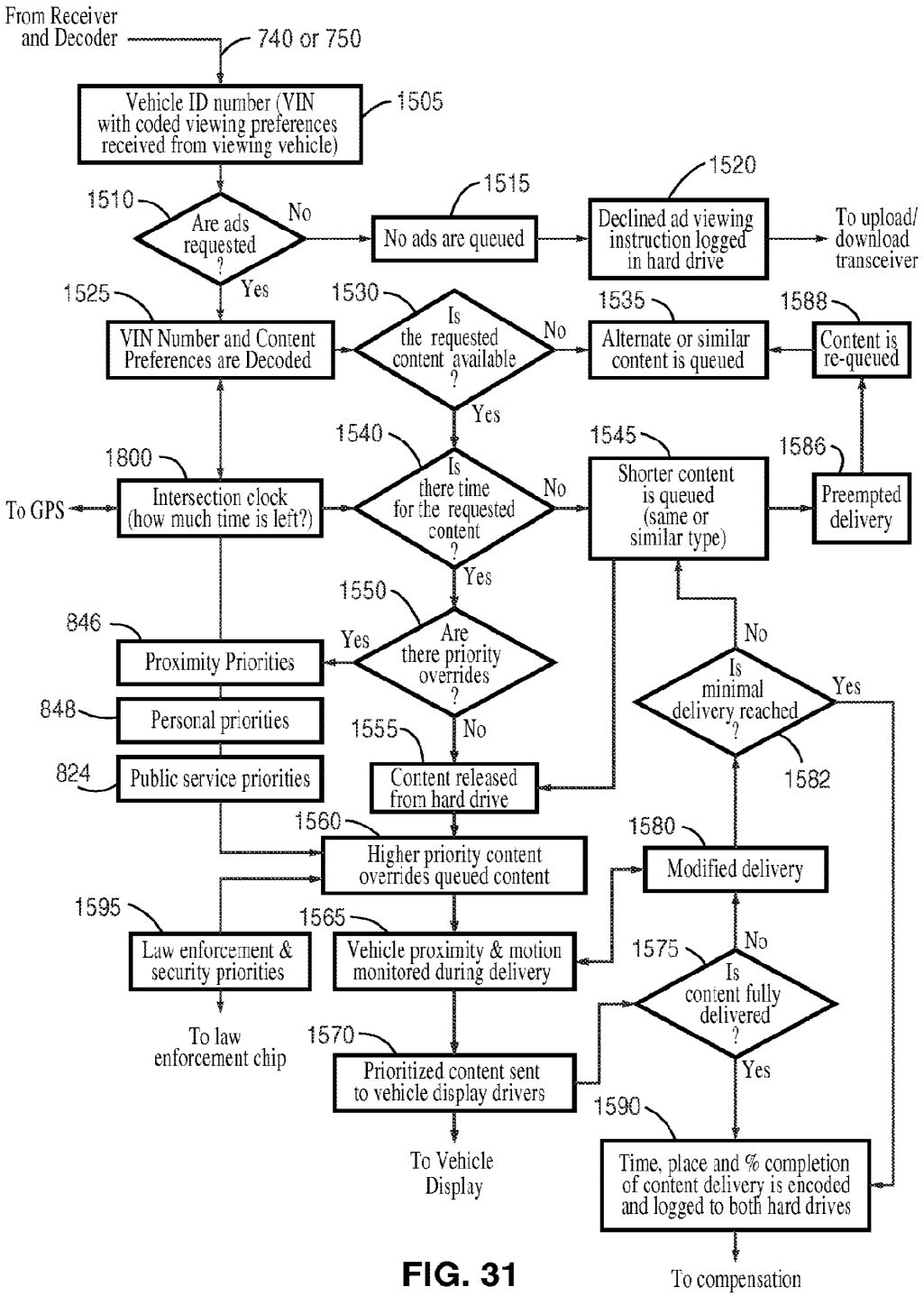

From Receiver and Decoder
740 or 750
Vehicle ID number (VIN with coded viewing preferences received from viewing vehicle)
1505
1510
Are ads requested ?
No
1515
No ads are queued
1520
Declined ad viewing instruction logged in hard drive
To upload/ download transceiver
Yes
1525
VIN Number and Content Preferences are Decoded
1530
Is the requested content available ?
No
1535
Alternate or similar content is queued
1588
Content is re-queued
Yes
1540
Is there time for the requested content ?
No
1545
Shorter content is queued (same or similar type)
1586
Preempted delivery
1800
To GPS
Intersection clock (how much time is left?)
Yes
1550
Are there priority overrides ?
Yes
846
Proximity Priorities
848
Personal priorities
824
Public service priorities
No
1555
Content released from hard drive
No
Is minimal delivery reached ?
Yes
1582
1560
Higher priority content overrides queued content
1580
Modified delivery
1595
Law enforcement & security priorities
1565
Vehicle proximity & motion monitored during delivery
No
1575
Is content fully delivered ?
To law enforcement chip
1570
Prioritized content sent to vehicle display drivers
Yes
1590
To Vehicle Display
Time, place and % completion of content delivery is encoded and logged to both hard drives
To compensation

FIG. 31

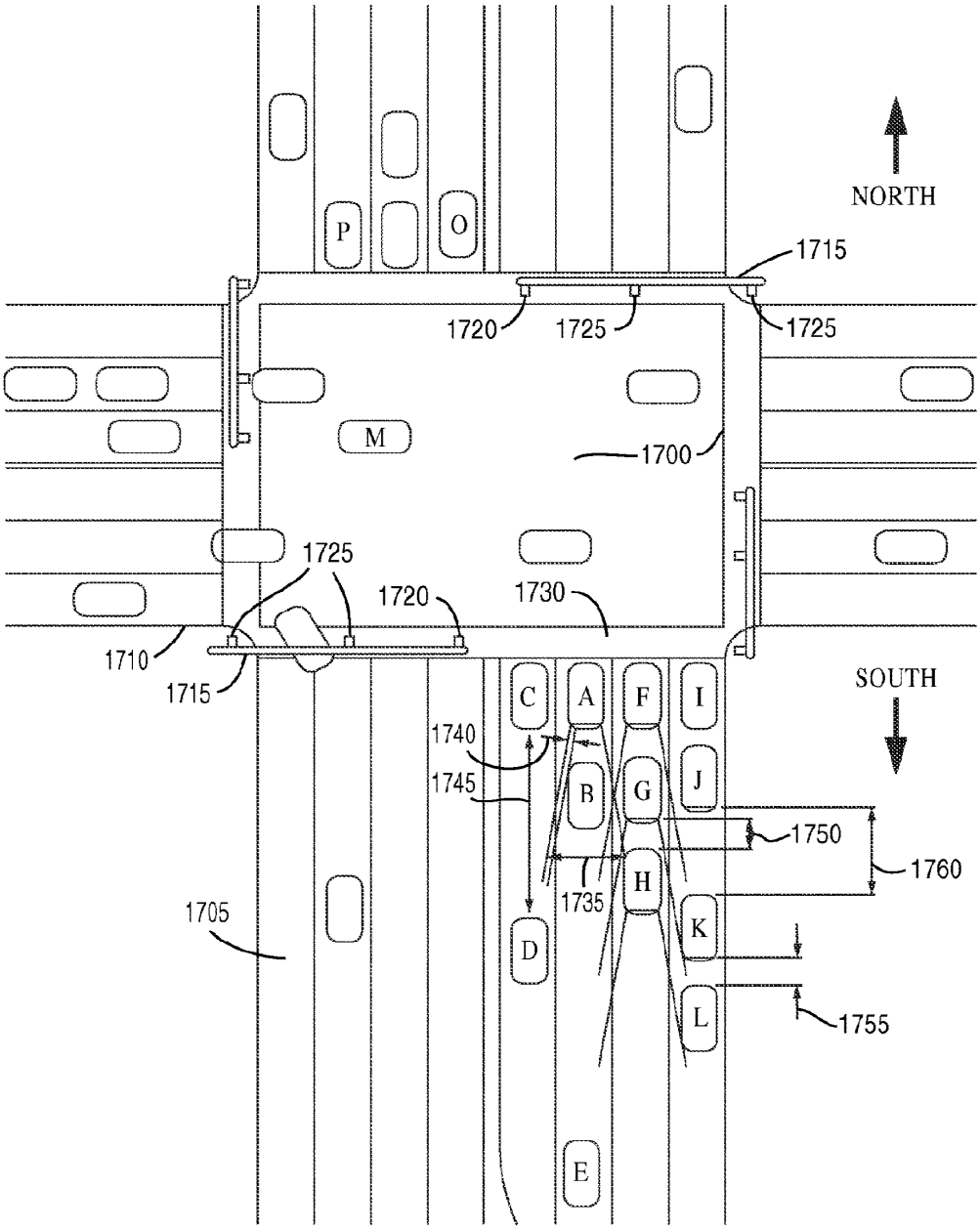

NORTH
SOUTH
P
O
M
1715
1720
1725
1725
1700
1725
1720
1730
1710
1715
C
A
F
I
1740
1745
B
G
J
1750
1760
H
1735
K
D
L
1755
1705
E

FIG. 33

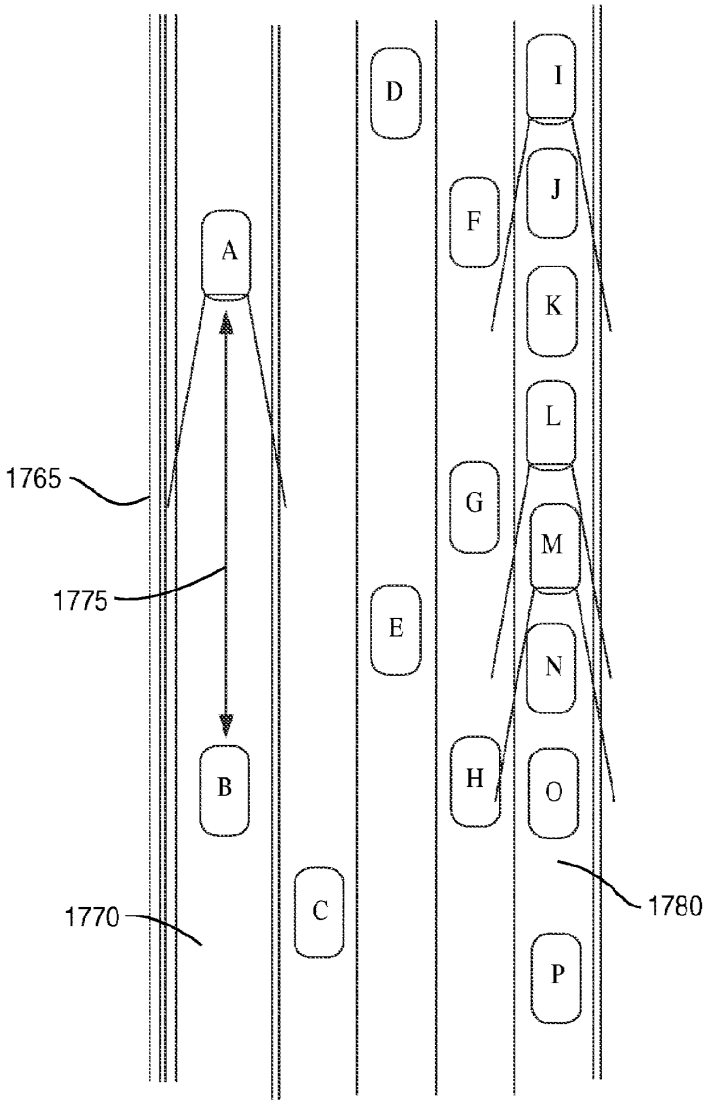


FIG. 34

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/026339

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L12/26
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, INSPEC, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/093513 A1 (CANTRELL CRAIG [US] ET AL) 13 May 2004 (2004-05-13)	1,31,32
Y	abstract paragraph [0012] - paragraph [0044]; figure 1 paragraph [0065] - paragraph [0069]	2-30, 33-43

X	US 2012/023576 A1 (SORENSEN AMANDA [US] ET AL) 26 January 2012 (2012-01-26)	1,31,32
Y	abstract paragraph [0006] - paragraph [0012]; figure 3	2-30, 33-43

X	US 2008/163333 A1 (KASRALIKAR RAHUL [US]) 3 July 2008 (2008-07-03)	1,31,32
A	abstract paragraph [0009] - paragraph [0010]; figure 2	2-30, 33-43

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 June 2016	09/06/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	San Millán Maeso, J

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/026339

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004093513 A1	13-05-2004	AR 042020 A1	08-06-2005
		AU 2003290674 A1	03-06-2004
		CN 1720459 A	11-01-2006
		EP 1558937 A2	03-08-2005
		JP 2006506853 A	23-02-2006
		JP 2010268483 A	25-11-2010
		KR 20050086441 A	30-08-2005
		KR 20100132079 A	16-12-2010
		US 2004093513 A1	13-05-2004
		US 2005028013 A1	03-02-2005
		US 2005044422 A1	24-02-2005
		WO 2004045126 A2	27-05-2004
US 2012023576 A1	26-01-2012	AU 2011279907 A1	28-02-2013
		CA 2805823 A1	26-01-2012
		SG 187068 A1	28-02-2013
		US 2012023576 A1	26-01-2012
		WO 2012012280 A2	26-01-2012
US 2008163333 A1	03-07-2008	NONE	

Information on Search Strategy - Pilot phase (see OJ 2015, A86)
The type of information contained in this sheet may change during the pilot for improving the usefulness of this new service.

Application Number
PCT/US2016/026339

TITLE: RULE-BASED NETWORK-THREAT DETECTION

APPLICANT: CENTRIPETAL NETWORKS, INC.

IPC CLASSIFICATION: H04L29/06, H04L12/26

EXAMINER: San Millán Maeso, J

CONSULTED DATABASES:

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: TXTE, EPODOC, INSPEC, WPI, XPESP, XPI3E, XPIEE, H04L63/0227, H04L43/06, H04L12/2602, H04L43/00, H04L63/0263, H04L63/1416, H04L63/1425, H04L63/1441

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:

EPO FORM P04442

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley
BANNER & WI
1100 13th Stree
Washington, D(
ETATS-UNIS D

DUE DATE

ART 19 AMEND
Due: 5-6-2017

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 007742.00083	Date of mailing *(day/month/year)* 6 March 2017 (06-03-2017) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2016/068008	International filing date *(day/month/year)* 21 December 2016 (21-12-2016)
Applicant CENTRIPETAL NETWORKS, INC.	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   How? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may **submit comments on an informal basis on the written opinion of the International Searching Authority** to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.

   Shortly after the expiration of **18 months from the priority date, the international application will be published** by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for **entry into the national phase** before those designated Offices. In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

   Within **19 months from the priority date, the applicant may request that a supplementary international search be carried out** by a different International Searching Authority that offers this service (Rule 45*bis*.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer EOZENOU, Bernard Tel: +49 (0)89 2399-6022

RECEIVED
MAR 17 2017
BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2014)

MAR 1 ? 2017

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742.00083		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2016/068008	21 December 2016 (21-12-2016)	4 January 2016 (04-01-2016)
Applicant		
CENTRIPETAL NETWORKS, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 3
      [ ] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [X] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

RECEIVED
MAR 17 2017
BANNER & WITCOFF LTD

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/068008

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2015/350229 A1 (MITCHELL DAVID JAMES [US]) 3 December 2015 (2015-12-03) abstract; figures 1, 3 paragraphs [0012], [0014], [0026], [0030] - [0034], [0038], [0039], [0066] paragraphs [0074], [0080], [0083], [0086] -----	1-7
A	US 2005/108557 A1 (KAYO DAVID G [US] ET AL) 19 May 2005 (2005-05-19) abstract; figures 3, 6, 7 paragraphs [0004], [0010] - [0016], [0019] - [0021], [0027] - [0029], [0058] - [0059] paragraphs [0062], [0063] ----- -/--	1-7

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 February 2017	06/03/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Hristova, Ana

1

Form PCT/ISA/210 (second sheet) (April 2005)

EX1002
CISCO SYSTEMS, INC. / Page 1328 of 1453

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/068008

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant paseages	Relevant to claim No.
A	US 2015/373043 A1 (WANG JISHENG [US] ET AL) 24 December 2015 (2015-12-24) abstract; figures 1, 2A, 2B, 3 paragraphs [0002], [0034] - [0042], [0044] - [0057], [0063] - [0072]	1-7

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/068008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015350229 A1	03-12-2015	NONE	
US 2005108557 A1	19-05-2005	NONE	
US 2015373043 A1	24-12-2015	US 2015373043 A1	24-12-2015
		WO 2016025081 A1	18-02-2016

Form PCT/ISA/210 (patent family annex) (April 2005)

Information on Search Strategy - Pilot phase (see OJ 2015, A86)
The type of information contained in this sheet may change during the pilot for improving the usefulness of this new service.

Application Number
PCT/US2016/068008

TITLE: EFFICIENT PACKET CAPTURE FOR CYBER THREAT ANALYSIS

APPLICANT: CENTRIPETAL NETWORKS, INC.

IPC CLASSIFICATION: H04L29/06

EXAMINER: Hristova, Ana

CONSULTED DATABASES: WPI, COMPDX, INSPEC, TDB, XP3GPP, XPCRYPT, XPESP, XPETSI, XPI3E, XPIEE, XPIETF, XPLNCS, XPNPL, EPODOC

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: H04L63/0236, H04L63/0263, H04L63/1408, H04L63/1416, H04L63/20, H04L63/101, G06F21/566

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:

EPO FORM P04A42

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

DUE DATE

RESP TO
WRITTEN OPINION
Final: 11-4-2017

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Applicant's or agent's file reference see form PCT/ISA/220	Date of mailing *(day/month/year)* see form PCT/ISA/210 (second sheet) **FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2016/068008	21.12.2016	04.01.2016

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

RECEIVED
MAR 17 2017
BANNER & WITCOFF LTD

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Hristova, Ana Telephone No. +49 89 2399-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	2-7
	No:	Claims	1
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-7
Industrial applicability (IA)	Yes:	Claims	1-7
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 Reference is made to the following documents:

D1 US 2015/350229 A1 (MITCHELL DAVID JAMES [US]) 3 December 2015 (2015-12-03)

D2 US 2005/108557 A1 (KAYO DAVID G [US] ET AL) 19 May 2005 (2005-05-19)

D3 US 2015/373043 A1 (WANG JISHENG [US] ET AL) 24 December 2015 (2015-12-24)

2 **Independent claims**

2.1 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

2.2 Document D1 discloses all the features of claim 1 (the references in parentheses applying to this document):

A method comprising:
receiving, by a computing device, one or more threat indicators from one or more threat intelligence providers, wherein the computing device is located at a boundary between a protected network associated with an enterprise and an unprotected network ([0074], lines: 1-7; [0039], lines: 1-11);
in response to receiving the threat indicators, combining the threat indicators based on a source address and port, a destination address and port, and a protocol type associated with the threat indicators ([0066], lines: 1-7; [0032], lines: 13-18);
generating one or more packet capture and packet filtering rules based on the combined threat indicators ([0038], lines: 7-10; [0074], lines: 12-14); and
filtering, by the computing device, on a packet-by-packet basis, at least one packet based on at least one of the one or more packet capture and packet filtering rules ([0083], lines: 3-12; [0039], lines: 13-16; [0080]).

Hence, the subject-matter of claim 1 does not meet the requirements of the PCT concerning novelty.

2.3 Document D1 also discloses the following features of claim 7 (the references in parentheses applying to this document):

> A method comprising:
> generating, by a computing device, a packet capture file comprising raw packet content and ~~threat context information, wherein the threat context information comprises a filtering rule and associated threat indicator that caused a packet to be captured~~ ([0033], lines: 1-5).

The difference between document D1 and the subject-matter of claim 7 resides in generating a threat context information, wherein the threat context information comprises a filtering rule and associated threat indicator that caused a packet to be captured.

The objective problem to be solved by claim 7 may therefore be regarded as how to associate a packet with its corresponding detected threats.

However, generating a threat context information, wherein the threat context information comprises a filtering rule and associated threat indicator that caused a packet to be captured is a common design measure for associating a packet with its corresponding detected threats. This measure is also known from D2 (see e.g. [0058], [0059]). Hence, the subject-matter of claim 7 does not meet the requirements of the PCT concerning inventive step.

3 **Dependent claims**

Additionally, the dependent claims do not appear to contain any additional technical features which, either alone or in combination with the features of any claim to which they refer, render the present subject-matter novel (Article 33(2) PCT) or inventive (Article 33(3) PCT) since their features (e.g. combining of the threat indicators based on a hostname or an URI etc.) are either known from the prior art (documents D1-D3; see cited passages in the International Search Report) or merely represent minor implementation details to the person skilled in the art.

Re Item VII

Certain defects in the international application

1 The independent claims are not in the two-part form vis-à-vis D1 in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate.

2 The features of the claims are not provided with reference signs placed in parentheses to increase the intelligibility of the claims (Rule 6.2(b) PCT).

3 Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in D1 is not mentioned in the description, nor is this document identified therein.

4 The expression "incorporated by reference" in paragraphs [0001], [0027], [0029], [0033], [0045] and [0048] of the description does not render the application self-contained according to Article 5 PCT.

Re Item VIII

Certain observations on the international application

1 The statement "within the scope and spirit of the appended claims" in the description in paragraph [0066] on lines: 2-3 implies that the subject-matter for which protection is sought may be different to that defined by the claims, thereby resulting in lack of clarity (Article 6 PCT) when used to interpret them.

2 It is unclear in claims 1 and 7 whether the protection sought is limited to the method per se or whether protection is sought for use in a specific device. For the sake of clarity, this claim should be directed to a method for use in a computing device (Article 6 PCT).

3 A subset of claims of the present application is not concise since the application comprises two independent claims of the same category, namely claims 1 and 7, neither defining complementary functions nor reflecting separate alternative technical solutions (Article 6 PCT). The number of independent claims should be limited to one independent claim in the method category.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

	Date of mailing *(day/month/year)* 7 June 2017 (07-06-2017)
Applicant's or agent's file reference 007742 00081	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2016/067111	International filing date *(day/month/year)* 16 December 2016 (16-12-2016)
Applicant CENTRIPETAL NETWORKS, INC	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   How? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with any applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may **submit comments on an informal basis on the written opinion of the International Searching Authority** to the International Bureau. These comments will be made available to the public after international publication. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established.

   Shortly after the expiration of **18 months from the priority date, the international application will be published** by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for **entry into the national phase** before those designated Offices. In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months. For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

   Within **19 months from the priority date, the applicant may request that a supplementary international search be carried out** by a different International Searching Authority that offers this service (Rule 45*bis*.1). The procedure for requesting supplementary international search is described in the *PCT Applicant's Guide*, International Phase, paragraphs 8.006-8.032.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	KOESTEL, Gilbert Tel: +31 (0)70 340-3544

RECEIVED
JUN 09 2017
BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2014)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION**	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
007742 00081		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2016/067111	16 December 2016 (16-12-2016)	23 December 2015 (23-12-2015)
Applicant		
CENTRIPETAL NETWORKS, INC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language,** the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings,**
   a. the figure of the **drawings** to be published with the abstract is Figure No. 13
      [ ] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [X] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

RECEIVED
JUN 09 2017
BANNER & WITCOFF LTD

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/067111

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/317397 A1 (MARTINI PAUL MICHAEL [US]) 23 October 2014 (2014-10-23) paragraph [0024] - paragraph [0027]	1-25
X	US 2014/283004 A1 (MOORE SEAN [US]) 18 September 2014 (2014-09-18) paragraph [0036] - paragraph [0044] claims 1-4	1-25

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 May 2017	07/06/2017

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Lamelas Polo, Yvan

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/067111

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014317397 A1	23-10-2014	CA 2909799 A1	23-10-2014
		EP 2989769 A1	02-03-2016
		US 8739243 B1	27-05-2014
		US 2014317397 A1	23-10-2014
		WO 2014172384 A1	23-10-2014
US 2014283004 A1	18-09-2014	AU 2014249055 A1	03-09-2015
		CA 2902158 A1	09-10-2014
		EP 2974212 A1	20-01-2016
		US 2014283004 A1	18-09-2014
		US 2015237012 A1	20-08-2015
		US 2016072709 A1	10-03-2016
		WO 2014164713 A1	09-10-2014

Form PCT/ISA/210 (patent family annex) (April 2005)

Information on Search Strategy - Pilot phase (see OJ 2015, A86)
The type of information contained in this sheet may change during the pilot for improving the usefulness of this new service.

Application Number
PCT/US2016/067111

TITLE: RULE-BASED NETWORK-THREAT DETECTION FOR ENCRYPTED COMMUNICATIONS

APPLICANT: CENTRIPETAL NETWORKS, INC

IPC CLASSIFICATION: H04L29/06

EXAMINER: Lamelas Polo, Yvan

CONSULTED DATABASES: WPI, EPODOC, NPL

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: H04L63/0227, H04L63/1416, H04L63/1441

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:
PROBLEM: network-threat detection for encrypted communications.
SOLUTION: receiving data indicating network-threat indicators and configuring packet-filtering rules to cause the packet-filtering system to identify packets comprising unencrypted data, and packets comprising encrypted data. When portion of the unencrypted data corresponding to one or more of the network-threat indicators, and the packet-filtering rules being configured to cause the packet-filtering system to determine, based on the portion of the unencrypted data, that the packets comprising encrypted data correspond to the one or more network-threat indicators.

EPO FORM P04A42

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2016/067111	16.12.2016	23.12.2015

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06

Applicant
CENTRIPETAL NETWORKS, INC

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

RECEIVED
JUN 09 2017
BANNER & WITCOFF LTD

Name and mailing address of the ISA:
European Patent Office
P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040
Fax: +31 70 340 - 3016

Date of completion of this opinion
see form PCT/ISA/210

Authorized Officer
Lamelas Polo, Yvan
Telephone No. +31 70 340-0

Form PCT/ISA/237 (Cover Sheet) (January 2015)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed.

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))

3. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing:

   a. ☐ forming part of the international application as filed:

      ☐ in the form of an Annex C/ST.25 text file.

      ☐ on paper or in the form of an image file.

   b. ☐ furnished together with the international application under PCT Rule 13*ter*.1(a) for the purposes of international search only in the form of an Annex C/ST.25 text file.

   c. ☐ furnished subsequent to the international filing date for the purposes of international search only:

      ☐ in the form of an Annex C/ST.25 text file (Rule 13*ter*.1(a)).

      ☐ on paper or in the form of an image file (Rule 13*ter*.1(b) and Administrative Instructions, Section 713).

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that forming part of the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-25
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-25
Industrial applicability (IA)	Yes:	Claims	1-25
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

1 **Re item V**

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Novelty and inventive step of the independent claims

1.1 **Independent claim 1**

1.1.1 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

1.1.2 Document D1 discloses (the references in parentheses referring to D1):

A method comprising:

receiving, by a packet-filtering system configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators (fig.1(102,103) "Network Gateway" "Rules" cf. [0018] "When data on a network is encrypted (e.g., by SSL or TSL) the data can pose challenges to network security appliances and routines in that it makes it difficult to inspect the data as it is transferred between the end users and servers on the Internet. This can lead to problems such as viruses being transferred over secure connections and entering the network instead of being blocked because the gateway security appliances could not inspect the data"); **and**

configuring, by the packet-filtering system, the plurality of packet-filtering rules to cause the packet-filtering system to:

identify packets comprising unencrypted data ([0024] "the network gateway may intercept and examine a DNS request 108 from the browser device 106 that is addressed to the DNS 110");

identify packets comprising encrypted data ([0024] "The network gateway 102 may be configured to make this determination so that encrypted communication from the browser device 106"); **and**

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, that the packets comprising encrypted data correspond to the one or more network-threat indicators ([0024] "Based on, for example, the URL or URI in the DNS request 108 and rules 103 indicating which destination should be decrypted and which should be passed directly to the Internet destination,

the network gateway 102 may determine" "The network gateway 102 may make the determining to pass encrypted communication through the MitM gateway 104 based on security policies or concerns").

1.1.3 The subject-matter of claim 1 is consequently not new (Article 33(2) PCT).

1.1.4 For the sake of completeness, it is pointed out that the objection of lack of novelty set out above could have also been substantiated, in view of the disclosure of prior art document D2 (see references applying to this document cited in the search report). In particular,

- D2, [0036]-[0044], claims 1-4.

1.2 **Independent claims 24,25**

A corresponding reasoning as above applies, mutatis mutandis, to the subject-matter of independent claims 24,25 which therefore is also considered not new (Article 33(2) PCT).

Novelty and inventive step of the dependent claims

Dependent claims 2-23 do not appear to contain any additional features which, in combination with those of the claims to which they refer, meet the requirements of PCT with respect to novelty and/or inventive step, because said claims are considered implementation related design options that are either known or directly derivable from the prior art documents D1,D2 (see D1-D2 and references applying to these documents cited in the search report) or a matter of normal design procedure for a man skilled in the art.

2 **Re item VII**

Certain defects in the international application

2.1 The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

2.2 Documents D1,D2 which appear to represent the most relevant prior art, should be acknowledged in the description.

3 **Re item VIII**

Certain observations on the international application

3.1 References in patent applications to other documents may relate either to the background art or to part of the disclosure of the invention. The patent specification should, regarding the essential features of the invention, be self-contained, i.e. capable of being understood without reference to any other document. Consequently, it appears that the expression "which is herein incorporated by reference" in [0001],[0024],[0041],[0053] should be deleted.

3.2 The vague and imprecise statement "Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims" in the description on page [108] implies that the subject-matter for which protection is sought may be different to that defined by the claims, thereby resulting in lack of clarity (Article 6 PCT) when used to interpret them.

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO/ISA)

General information

For all international applications, the competent International Searching Authority **(ISA)** will establish an international search report **(ISR)** accompanied by a written opinion of the International Searching Authority **(WO/ISA)**. The **WO/ISA** may be responded to by

- filing informal comments with the **International Bureau of WIPO (IB)** (where no demand for international preliminary examination **(demand)** is filed)
- filing amendments under Art. 19 PCT (this can be done whether or not a **demand** is filed)
- filing amendments under Art. 34 PCT and/or formal observations in response to objections raised in the **WO/ISA** (where a **demand** *is* actually filed)

This document explains these possibilities.

Filing informal comments

After receipt of the **ISR and WO/ISA**, the applicant may file informal comments on the **WO/ISA, directly with the IB** (see International Search and Preliminary Examination Guidelines 2.15). These will be communicated to the designated/elected Offices, together with the International Preliminary Report on Patentability **(IPRP)** at 30 months from the priority date.

Amending claims under Art. 19 PCT

The applicant may file **amended claims** under Art. 19 PCT, **directly with the IB** by the later of the following dates:

- 2 months from the date of mailing of the **ISR** and the **WO/ISA**
- 16 months from the priority date

However, any such amendment received by the **IB** after the expiration of the applicable time limit shall be **considered to have been received on time** by the **IB**, if it reaches it **before** the technical preparations for international publication have been completed (the 15th day prior to the date of publication, see PCT Applicant's Guide, International Phase, 9.013).

For further information, please see Rule 46 PCT as well as form PCT/ISA/220.

Please also note that, when filing amended claims under Art. 19 PCT, such amendments shall be **accompanied by a letter** identifying the amendments made and also the basis for the amendments in the application as originally filed (Rule 46.5(b) PCT). Where a **demand** is filed, failure to comply with this requirement may result in the amendments being ignored in the International Preliminary Examination Report **(IPER)**, see Rule 70.2(c-*bis*) PCT.

BNSDOCID: <XS_____200704010CK_L>

Filing a demand for international preliminary examination

In principle, the **WO/ISA** will be considered to be the written opinion of the International Preliminary Examining Authority (**IPEA**). Where the **WO/ISA** issued by the **EPO** as **ISA** gives a positive opinion on the international application and the invention to which it relates, filing a **demand** with the **EPO** as **IPEA** would normally be unnecessary, since a positive IPRP would anyway be established by the IB based on the WO/ISA (see also further below).

If the applicant wishes to file a **demand** (for example, to allow him to argue his case in international preliminary examination with regard to objections raised in a negative **WO/ISA** before the **IPEA** issues an **IPER**), this must be done before expiration of **3 months after the date of mailing of the ISR and WO/ISA** or **22 months after priority date,** whichever expires later (Rule 54*bis* PCT). Amendments under Art. 34 PCT can be filed with the IPEA, normally at the same time as filing the demand (Rule 66.1(b) PCT) or within the time limit set for reply to any written opinion issued during international preliminary examination by the **IPEA**.

If a **demand** is filed at the **EPO** as **IPEA** and no comments/amendments have been received by the time the **EPO** starts drawing up the **IPER** (Rule 66.4*bis* PCT), the **WO/ISA** will be transformed by the **IPEA** into an **IPER** (also called the **IPRP (Chapter II)** which would merely reflect the content of the **WO/ISA** (OJ 10/2011, 532). The **demand** can still be withdrawn (Art. 37 PCT).

Please also note that, when filing amendments under Art. 34 PCT, such amendments shall be accompanied by a letter which identifies the amendments made and also the basis for the amendments in the application as originally filed (Rule 66.8(a) PCT). Failure to comply with this requirement may result in the amendments being ignored in the **IPER (IPRP (Chapter II))**, see Rule 70.2(c-*bis*) PCT.

Filing a request for supplementary international search

The applicant may, with the **IB**, file a request for **supplementary international search** under Rule 45*bis*.1 PCT. The present **ISR** and **WO/ISA** may also be taken into account in the execution of that supplementary international search, provided that these are available to the Authority charged with this task before it starts the supplementary search (Rule 45*bis*.5 PCT).

This kind of request **cannot be filed specifying the ISA** who did the **international search**.

More information on this topic can be found in the **PCT Applicant's Guide**, Chapter 8 (http://www.wipo.int/pct/en/guide/ip08.html).

End of the international phase

Where no **demand** is filed, at the end of the international phase, the **IB** will transform the **WO/ISA** into the IPRP (PCT Chapter I) (Rule 44*bis* PCT), which will then be transmitted together with possible informal comments to the designated Offices. Where a demand is filed, the **WO/ISA** is not transformed into an **IPRP (Chapter I)** by the **IB**, but rather the **IPEA** will establish an **IPER**, (the IPER is the same as the IPRP (PCT Chapter II), see Rule 70.15 PCT).

\SDOCID: <XS_____200704010CK_I_>

Docket No.: 007742.00059\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

David K. Ahn et al.

Application No.: 14/757,638 | Confirmation No.: 9492

Filed: December 23, 2015 | Art Unit: 2438

For: Rule-Based Network-Threat Detection For Encrypted Communications | Examiner: J. T. Lee

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. § 1.111

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

In response to the Office Action dated April 12, 2017, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 12 of this paper.

Applicant requests any necessary extension of time for the submission of this paper. If any fees are required or if an overpayment is made, the Commissioner is authorized to debit or credit our Deposit Account No. 19-0733, accordingly.

18422011

Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators; ~~and~~

~~configuring, by the packet-filtering system, the plurality of packet-filtering rules to cause the packet-filtering system to:~~

~~identify~~ identifying packets comprising unencrypted data;

~~identify~~ identifying packets comprising encrypted data; ~~and~~

determining, by the packet-filtering system and ~~determine,~~ based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, ~~that the~~ packets comprising encrypted data that corresponds ~~correspond~~ to the one or more network-threat indicators; and

filtering, by the packet-filtering system:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.

2. (Currently Amended) The method of claim 1, wherein:

the one or more network-threat indicators comprise a domain name identified as a network threat; and

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query~~; and~~, the method further comprising:

determining ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine~~ that the at least one of the DNS

query or the reply to the DNS query comprises the domain name identified as the network threat.

3. (Currently Amended) The method of claim 2, wherein [[:]] the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query~~; and~~, the method further comprising:

determining ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine~~ that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

4. (Currently Amended) The method of claim 2, wherein [[:]] the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the at least one of the DNS query or the reply to the DNS query~~; and~~, the method further comprising:

determining ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine~~ that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

5. (Currently Amended) The method of claim 4, wherein [[:]] the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host~~; and~~, the method further comprising:

identifying ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to identify~~ one or more packets comprising the request.

6. (Currently Amended) The method of claim 1, wherein [[:]] one or more packets of the packets comprising unencrypted data comprise data configured to establish an encrypted

communication session between a first host and a second host, the method further comprising: ~~; and~~

routing ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route~~ the one or more of the packets to a proxy system.

7. (Currently Amended) The method of claim 6, wherein [[:]] the one or more network-threat indicators comprise a domain name identified as a network threat, the method further comprising: ~~; and~~

~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route~~routing the one or more of the packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the domain name identified as the network threat.

8. (Currently Amended) The method of claim 6, wherein:

the plurality of packet-filtering rules indicate:

one or more network addresses for which encrypted communications ~~should~~ are to be established via the proxy system, and

one or more network addresses for which encrypted communications ~~should~~are to not be established via the proxy system, the method further comprising: ~~; and~~

routing ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to route~~ the one or more of the packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications ~~should~~ are to be established via the proxy system.

9. (Currently Amended) The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising: ~~; and~~

~~the configuring the packet-filtering system to route the one or more of the packets to the proxy system comprises configuring the packet-filtering system to redirect~~ redirecting packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

10. (Currently Amended) The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising: ~~; and~~

~~the configuring the packet-filtering system to route the one or more of the packets to the proxy system comprises configuring the packet-filtering system to forward~~ forwarding copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

11. (Currently Amended) The method of claim 6, , the method further comprising: ~~wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to:~~

identifying, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and

identifying, via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data.

12. (Currently Amended) The method of claim 11, the method further comprising: ~~wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to~~ identifying, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data.

13. (Currently Amended) The method of claim 6, the method further comprising, ~~wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to,~~ responsive to determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

dropping the one or more packets generated by the proxy system;
logging the one or more packets generated by the proxy system;
dropping one or more other packets generated by the proxy system;
logging one or more other packets generated by the proxy system;
dropping one or more other packets of the packets comprising encrypted data; or
logging one or more other packets of the packets comprising encrypted data.

14. (Currently Amended) The method of claim 13, wherein the determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-

filtering rules, or data indicating a command specified by the plurality of packet-filtering rules.

15. (Original) The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI) meeting a threshold size specified by the plurality of packet-filtering rules.

16. (Currently Amended) The method of claim 6, the method further comprising: ~~wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to~~ identifying, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.

17. (Currently Amended) The method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the method further comprising ~~configuring the plurality of packet-filtering rules to cause the packet-filtering system to~~ at least one of dropping or logging packets other than the packets comprising encrypted data based on a determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host.

18. (Currently Amended) The method of claim 1, wherein:

the one or more network-threat indicators comprise a domain name identified as a network threat; and

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising: ~~;~~ ~~and~~

~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine~~determining that the one or more handshake messages comprise the domain name identified as the network threat.

19. (Currently Amended) The method of claim 18, , the method further comprising: ~~wherein the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to~~, responsive to determining that the one or more handshake messages comprise the domain name identified as the network threat, at least one of dropping or logging the packets comprising encrypted data.

20. (Currently Amended) The method of claim 18, wherein:

the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server; and

the ~~configuring the packet-filtering system to determine~~ determining that the one or more handshake messages comprise the domain name identified as the network threat comprises ~~configuring the packet-filtering system to determine~~ determining the at least one of the hello message generated by the client or the certificate message generated by the server comprises the domain name identified as the network threat.

21. (Currently Amended) The method of claim 18, wherein [[:]] the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the one or more handshake messages, the method further comprising ~~; and~~

determining ~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to determine~~ that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

22. (Currently Amended) The method of claim 21, wherein:

the one or more network addresses comprise a network address of the server and a network address of a web proxy, the method further comprising: ~~; and~~

~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to:~~

identifying one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

~~determine~~ determining that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. (Currently Amended) The method of claim 1, wherein:

the packets comprising unencrypted data comprise a certificate message for an encrypted communication session, the method further comprising: ~~; and~~

~~the configuring the plurality of packet-filtering rules comprises configuring the packet-filtering system to~~ at least one of dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. (Currently Amended) A packet-filtering system comprising:

at least one hardware processor; and

~~a~~ memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators;

~~configure a plurality of packet-filtering rules, in accordance with which the packet-filtering system is configured to filter packets, to cause the packet-filtering system to:~~

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, ~~that the~~ packets comprising encrypted data that corresponds ~~correspond~~ to the one or more network-threat indicators; and

filter:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.

25. (Currently Amended) One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators;

~~configure a plurality of packet-filtering rules, in accordance with which the packet-filtering system is configured to filter packets, to cause the packet-filtering system to:~~

identify packets comprising unencrypted data;

identify packets comprising encrypted data; ~~and~~

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, ~~that the~~ packets comprising encrypted data that corresponds ~~correspond~~ to the one or more network-threat indicators; and

filter, by the packet-filtering system:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.

REMARKS

The Office Action of April 12, 2017 has been carefully reviewed and these remarks are responsive thereto. Claims 1-14 and 16-25 have been amended. Claims 1-25 thus remain pending in this application, of which claim 1, 24, and 25 are independent. Reconsideration and allowance of the instant application are respectfully requested.

Rejections Under 35 U.S.C. § 101

Claims 1, 24, and 25 stand rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to an abstract idea without significantly more. The Office Action states, on page 4, that independent claims 1, 24, and 25 are directed to an abstract idea, i.e. organizing human activity. The Office Action further states, on page 5, that the steps could be "performed mentally, verbally, or without a machine nor is any transformation apparent." Applicant disagrees. This assertion is based on an abstraction of the claim language that ignores the clear recitation of a packet-filtering system in the claims. The Office Action's assertion that the claims are directed to organizing human activity is a very high-level abstraction of the claim language, and that high-level abstraction is untethered from the language of the claims. Describing the claims at such a high level of abstraction and untethered from the language of the claims all but ensures that the exceptions to § 101 swallow the rule. *Enfish, LLC v. Microsoft Corp.*, 2016 U.S. App. LEXIS 8699, at *16-17 (Fed. Cir. May 12, 2016). Applicant submits that the claims are not directed to any abstract idea.

"A principle, in the abstract, is a fundamental truth; an original cause; a motive; these cannot be patented, as no one can claim in either of them an exclusive right." *Le Roy v. Tatham*, 55 U.S. (14 How.) 156, 175 (1852). The claims are not directed to any fundamental truth and would not pre-empt any basic tools of scientific and technological work. Rather, amended independent claim 1 is directed to particular processes of a packet-filtering system, a term omitted from every characterization of the claims in the Office Action. Amended independent claims 24 and 25 recite similar technical features.

Furthermore, the Office Action fails to identify any concept found by the courts to be ineligible subject matter, and also fails to describe the similarities between such a concept that the instant claims. As such, Applicant submits that the claims do not describe an abstract concept, or a concept similar to those found by the courts to be abstract, such as a fundamental economic practice,

a method of organizing human activity, an idea itself (standing alone), or a mathematical relationship. The Office Action asserts, on page 4, that "the steps are similar to concepts and ideas that have been identified as abstract by the courts as organizing human activity (e.g. filtering content (BASCOM))." However, in BASCOM, the Federal Circuit **vacated a judgment of ineligibility** because the district court failed to properly perform the second step of the Mayo/Alice framework (Step 2B of the USPTO's SME guidance) when analyzing a claimed system for filtering content retrieved from an Internet computer network. See USPTO"s November 2, 2016 Memorandum on Recent Subject Matter Eligibility Decisions.

The inventive concept inquiry requires more than recognizing that each claim element, by itself, was known in the art. *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350. An inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces. *Id.* The Office Action states that "the claim does not include additional elements beyond the abstract ideas of receiving, configuring, identifying, and determining." Without conceding to the propriety of the rejection, amended independent claim 1 recites, among other features:

> identifying packets comprising unencrypted data;
> identifying packets comprising encrypted data;
> determining, by the packet-filtering system and based on a portion of the packets comprising the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
> filtering, by the packet-filtering system:
> packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and
> the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.

Applicant submit that these features, recited in the claim, are not abstract, conventional or known.

Independent claims 24 and 25 recites features similar to features of amended claim 1. As such, Claims 24 and 25 are not directed to an abstract idea for substantially similar reasons as those presented with regards to claim 1 above. In view of the foregoing, Applicant respectfully traverses this rejection and requests withdrawal of the same.

Rejections Under 35 U.S.C. § 112

Claims 1, 8 and 24-25 stand rejected under 35 U.S.C. § 112(b) as being indefinite.

The Office Action states, on page 7, that there is "a lack of antecedent basis error for the later recited 'encrypted data'." Applicant disagrees. The term "encrypted data" is used twice in claims 1, 24, and 25. However, the second recitation of "encrypted data" refers to "encrypted data that corresponds to the one or more network-threat indicators." As such, Applicant submits the rejection is traversed.

The Office Action states, on page 8, that the phrase "should be" in claim 8 renders the claim unclear. Without conceding to the propriety of the rejection, claim 8 has been amended in the manner suggested by the Examiner. As such, the rejection is moot.

Rejections Under 35 U.S.C. § 103

Claims 1-13 and 16-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Application Publication No. 2005/0138353 to Spies et al. (hereafter Spies) in view of U.S. Patent Application Publication No. 2012/0023576 to Sorensen et al. (hereafter Sorensen). Claims 14 and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Spies in view of Sorensen, further in view of U.S. Patent Application Publication No. 2004/0199629 to Bomer. For the reasons set forth below, Applicant respectfully traverses these rejections.

The Office Action, on page 10, fails to cite any portion of any document to address identifying "packet comprising encrypted data," as previously recited in the independent claims. That is, the Office Action fails to address each and every element of the claims as previously recited. Accordingly, the Office Action fails to state a *prima facie* case of obviousness.

Amended independent claim 1 recites, among other features:

> identifying packets comprising unencrypted data;
> identify packets comprising encrypted data;
> determining, by the packet-filtering system and based on a portion of the packets comprising the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and
> filtering, by the packet-filtering system:
> packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators.

Spies does not teach or suggest the above noted features. Spies discusses message management systems that have identity-based-encryption (IBE) capabilities. *See* Spies, ¶ 13. When the IBE-encrypted message is received, IBE decryption engine may use an IBE private key that corresponds to the IBE public key is used to decrypt the message and produce the unencrypted version of the message as an output. *See* Spies, ¶ 56.

Spies, however, does not discuss any determination regarding any encrypted data based on any unencrypted data corresponding to one or more network-threat indicators. On the other hand, antispam filtering and other content-based filtering of Spies is applied to a scanned and unencrypted version of a message. *See* Spies, ¶¶ 162-164. Spies discusses additional processing operations such as virus scanning, spam filtering, notifications, archiving, or security policy enforcement may be performed on the decrypted message and the resulting decrypted and processed version of the message may be provided to the recipient. *See*, for example, Spies, ¶¶ 130, 131, 143, 144, and 155. Accordingly, Spies fails to teach or suggest "determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising the encrypted data that corresponds to the one or more network-threat indicators," as recited in amended independent claim 1.

Furthermore, the Office Action states, on page 10, that "the claimed 'network-threat indicator' can be 'domain names (*e.g.*, fully qualified domain names (FQDNs)), URIs, network addresses, or the like.'" Applicant submits that Spies' disclosure of domain name (see, *e.g.*, Spies, ¶ 53) does not teach or suggest network-threat indicators, as recited in the claims. That is, while network-threat indicators may comprise a domain name identified as a network threat (see, *e.g.*, amended claim 2), not all domain names are identified as a network threat. While Spies discusses additional processing operations such as virus scanning, spam filtering, or security policy enforcement, Spies fails to teach or suggest network-threat indicators. As such, Spies also fails to teach or suggest encrypted data that corresponds to the one or more network-threat indicators, as recited in the independent claims.

Sorensen fails to overcome the above-noted deficiencies of Spies. Sorenson discusses calculating threat scores or ratings for a user account within an organization or domain. *See* Sorenson, ¶ 6.The score or rating may consider a type or quantity of activity violations that occur in relation to several attributes, such as for example: encryption status, attachment violations, identity of the parties, data patterns, words, and combinations thereof. *See* Sorenson, ¶ 9.

Sorensen, however, whether taken alone or in combination with Spies, does not teach or suggest "determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising the encrypted data that corresponds to the one or more network-threat indicators," as recited in amended independent claim 1. Sorenson also fails to teach or suggest encrypted data that corresponds to the one or more network-threat indicators, as recited in the independent claims.

Furthermore, Applicant respectfully submits that the Office Action fails to explain how to combine or provide an objective reason to combine Spies with Sorensen. While Sorenson discusses an indicator, the Office Action fails to address how the indicator of Sorenson would be combined with the system of Spies. Furthermore, the Office Action, on page 11, states that it would have been obvious for one of ordinary skill in the art to "modify the invention of Spies to include the teaching of Sorensen with threat indicator for closely monitor the risk for disclosure of information (*e.g.* data/message)," citing paragraph [0073] of Sorensen. However, as noted above, Spies discusses virus scanning, spam filtering, notifications, archiving, or security policy enforcement may be performed on the decrypted message. As such, there is no identified issue in the system of Spies that is addressed by the asserted combination, as Spies already has security policy enforcement. As such, the Office Action does not explain how one of ordinary skill in the art would combine Spies with Sorensen, or provide an objective reason why one would be motivated to combine Spies with Sorensen.

Bomer does not remedy defects of Spies and Sorensen discussed above. Claims 14 and 15, which ultimately depend on claim 1 are not rendered obvious over Spies, Sorensen, and Bomer for the same reasons as their base claim and further in view of additional features recited therein.

Independent claims 24 and 25 recites features similar to features of amended claim 1. Therefore, amended claims 24 and 25 are not rendered obvious over the proposed combination of

Spies, Sorensen, and Bomer for the same reasons same reasons discussed above with respect to claim 1. Claims 2-22, which ultimately depend on claim 1, are not rendered obvious over the proposed combination of Green and Russell for the same reasons discussed above with respect to claim 1.

CONCLUSION

All issues having been addressed, Applicant respectfully submits that the instant application is in condition for allowance, and respectfully solicits prompt notification of the same. However, if for any reason the Examiner believes the application is not in condition for allowance or there are any questions, the Examiner is requested to contact the undersigned at (202) 824-3153.

In view of the above amendment, Applicant believes the pending application is in condition for allowance.

Dated: October 11, 2017

Respectfully submitted,

By: /Joshua D. Schneider/
Joshua D. Schneider
Registration No.: 67,194

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Patent Application Fee Transmittal

Application Number:	14757638
Filing Date:	23-Dec-2015
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Filer:	Joshua Daniel Schneider/Jennifer Brady
Attorney Docket Number:	007742.00059

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
		Total in USD ($)		**700**

Electronic Acknowledgement Receipt

EFS ID:	30626577
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Joshua Daniel Schneider/Jennifer Brady
Filer Authorized By:	Joshua Daniel Schneider
Attorney Docket Number:	007742.00059
Receipt Date:	11-OCT-2017
Filing Date:	23-DEC-2015
Time Stamp:	15:24:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$700
RAM confirmation Number	101217INTEFSW00002009190733
Deposit Account	190733
Authorized User	Joshua Schneider
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Amendment_in_Response_to_Non-Final_Office_Action_Under_37 CFR1_18772974.pdf	77802 4a9b937a7fc8e695ab316097fc3f757cda491c54	yes	17

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	11
	Applicant Arguments/Remarks Made in an Amendment	12	17

Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30404 6b88417bb8055b549422cf42d8707e21a816ca70	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	108206		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/757,638	Filing Date 12/23/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $40 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $210 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

AMENDMENT	10/11/2017	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 25	Minus	** 25	= 0		x $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	=		x $210 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	GINA R GARY
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22907 7590 12/20/2017

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER
LEE, JASON T

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 12/20/2017

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/757,638	12/23/2015	David K. Ahn	007742.00059	9492

TITLE OF INVENTION: Rule-based network-threat detection for encrypted communications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/20/2018

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PTOL-85 (Rev. 02/11)

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22907 7590 12/20/2017
BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/757,638	12/23/2015	David K. Ahn	007742.00059	9492

TITLE OF INVENTION: Rule-based network-threat detection for encrypted communications

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	03/20/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
LEE, JASON T	2438	713-153000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/757,638	12/23/2015	David K. Ahn	007742.00059	9492

22907 7590 12/20/2017

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 12/20/2017

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 02/11)

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/757,638	Applicant(s) AHN ET AL.	
	Examiner JASON LEE	Art Unit 2438	AIA (First Inventor to File) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *October 11, 2017*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-25*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 7/11/17
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☒ Interview Summary (PTO-413), Paper No./Mail Date *12/7/12* .
5. ☒ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/JASON LEE/
Primary Examiner, Art Unit 2438

DETAILED ACTION

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

3. Applicant filed the response on October 11, 2017 for the office action dated April 12, 2017. Claims 1-14 and 16-25 are amended. No claim is added. No claim is cancelled. As the result of Examiner's amendment in the instant office action, Claims 1, 2, 6, 7, 13, 18, 22, 23, 24 and 25 are amended. Therefore, Claims 1-25 are pending.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 7/11/17 have been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given in a telephone interview with Mr. Joshua D. Schneider (Reg. # 67,194) on 12/7/17.

1. (Currently Amended) A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the one or more network-threat indicators comprise a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators; ~~and~~

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds ~~corresponding~~ to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

2. (Currently Amended) The method of claim 1, wherein:

~~the one or more network-threat indicators comprise a domain name identified as a network threat; and~~

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query, the method further comprising:

determining that the at least one of the DNS query or the reply to the DNS query comprises the domain name identified as the network threat.

6. (Currently Amended) The method of claim 1, wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host, the method further comprising:

routing the one or more of the packets comprising data configured to establish the encrypted communication session between the first host and the second host to [[a]] the proxy system.

7. (Currently Amended) The method of claim 6, ~~wherein the one or more network-threat indicators comprise a domain name identified as a network threat,~~ the method further comprising:

routing the one or more of the packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the domain name identified as the network threat.

13. (Currently Amended) The method of claim 6, the method further comprising:

generating, by the proxy system, one or more packets based on the filtered packets routed to the proxy system by the packet-filtering system; [[,]]

responsive to determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

dropping the one or more packets generated by the proxy system;

logging the one or more packets generated by the proxy system;

dropping one or more other packets generated by the proxy system;

logging one or more other packets generated by the proxy system;

dropping one or more other packets of the packets comprising encrypted data; or

logging one or more other packets of the packets comprising encrypted data.

18. (Currently Amended) The method of claim 1, wherein:

~~the one or more network-threat indicators comprise a domain name identified as a network threat; and~~

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:

determining that the one or more handshake messages comprise the domain name identified as the network threat.

22. (Currently Amended) The method of claim 21, wherein [[:]] the one or more network addresses comprise a network address of the server and a network address of a web proxy, the method further comprising:

identifying one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

determining that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. (Currently Amended) The method of claim 1, wherein [[:]] the packets comprising unencrypted data comprise a certificate message for an encrypted communication session, the method further comprising:

at least one of dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises

data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. (Currently Amended) A packet-filtering system comprising:

at least one hardware processor; and

memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the one or more network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators; ~~and~~

filter, based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-

filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

25. (Currently Amended) One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the one or more network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators,

packets comprising encrypted data that corresponds to the one or more network-threat indicators; ~~and~~

filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

Response to Arguments

6. Applicant's amendments filed 12/6/17 are sufficient to overcome the 35 U.S.C. 101 rejections for claims 1, 24 and 25 set forth in the previous office action. Applicant amended claims 1, 24 and 25 by reciting "filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-

filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules" and "routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators". Therefore, newly amended independent claim 1 requires a hardware device (filtering and routing) and thus qualifies the "significantly more" guideline and renders claim 1 (also 24 and 25) not directed to an abstract idea. Therefore, the 35 U.S.C. 101 rejections for claims 1, 24 and 25 have been withdrawn.

7. Applicant's amendment for claims 24 and 25 are sufficient to overcome the claim objections set forth in the previous office action. Applicant amended claims 24 and 25 to recite "hardware processor" for clarity. Therefore, the 35 USC claim objections for claims 24 and 25 are withdrawn.

8. Applicant's amendment/argument for claims 1, 8, 24 and 25 are sufficient to overcome the claim rejection for 35 USC 112(b) set forth in the previous office action. Applicant remarks for claims 1, 24 and 25 are persuasive. Applicant amended claim 8 to remove "should be" for clarity. Therefore, the claim rejection for 35 USC 112(b) for claims 1, 8, 24 and 25 are withdrawn.

9. Applicant's arguments filed 10/11/17 and telephone interview on 12/7/17 have been fully considered and they are persuasive.

Allowable Subject Matter

10. Newly amended independent claims 1, 24 and 25 are allowed over prior art of record. Dependent claims 2-23 depend on the above mentioned independent claim 1 are allowed by virtue of their dependency.

Examiner's statement of reasons for allowance

11. Newly amended independent claim 1 is allowed in view of the (examiner's) amendment and for reasons argued by applicant in page 14-17 of the Remarks, filed 10/11/2017.

The instant application is directed towards packet-filtering rules with threat indicators to identify packets comprising unencrypted data, and packets comprising encrypted data. Newly amended independent Claim 1 recites, *inter alia*, "filtering based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules"; and "routing filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators".

Prior art of record, Spies et al (US 20050138353 A1) in view of Sorensen et al (US 20120023576 A1) fails to teach alone, or suggests, at the time of the invention, the claimed features and limitations. Therefore, claim 1 is considered to be allowable.

Independent claims 24 and 25 recite similar limitations to those found in claim 1. Therefore, claims 24 and 25 are considered to be allowable for the same reasons as discussed with claim 1 above.

Examiner performed updated search and additional search does not yield other specific references that reasonably, either singularly or in combination with cited references, would result a proper rejection that would have anticipated or made obvious all the steps disclosed in the independent claims 1, 24 and 25 with proper motivation at or before the time it was effectively filed.

Dependent claims 2-23 depend upon the above-mentioned allowed claim 1 are therefore allowed by virtue of its dependency.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Any comments considered necessary by applicant must be submitted no later than payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US 20150207813 A1; Reybok et al; discloses "techniques for pooling and searching network security events reported by multiple sources; one of the indicator is specific domain name as a threat source.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/JASON LEE/

Primary Examiner, Art Unit 2438

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	14/757,638	AHN ET AL.	
	Examiner	Art Unit	
	JASON LEE	2438	

All participants (applicant, applicant's representative, PTO personnel):

(1) *JASON LEE*. (3)_____.

(2) *Mr. Joshua D. Schneider (reg 67,194)*. (4)_____.

Date of Interview: *07 December 2017*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☐103 ☒Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *n/a*.

Identification of prior art discussed: *n/a*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

The examiner confirmed authorization from Attorney of record Mr. Joshua D. Schneider (reg 67,194) to implement Examiner's Amendment based on Applicant's proposed examiner's amendment submitted by email on 12/06/2017..

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/JASON LEE/ Primary Examiner, Art Unit 2438	

Notice of References Cited	Application/Control No. 14/757,638	Applicant(s)/Patent Under Reexamination AHN ET AL.	
	Examiner JASON LEE	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2015/0207813 A1	07-2015	Reybok; Richard	G06F21/552	726/22
	B	US-				
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14757638
Filing Date	2015-12-23
First Named Inventor	David K. Ahn
Art Unit	2438
Examiner Name	J. T. Lee
Attorney Docket Number	007742.00059\US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.T.L/	1	8117655	B2	2012-02-14	Spielman	
/J.T.L/	2	6147976	A	2000-11-14	Shand et al.	
/J.T.L/	3	7610621	B2	2009-10-27	Turley et al.	
/J.T.L/	4	9154446	B2	2015-10-06	Gemelli et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/J.T.L/	1	20120106354	A1	2012-05-03	Pleshek et al.	
/J.T.L/	2	20130047020	A1	2013-02-21	Hershko et al.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

/J.T.L/	3	20090240698	A1	2009-09-24	Shukla et al.		
/J.T.L/	4	20040098511	A1	2004-05-20	Lin et al.		
/J.T.L/	5	20100232445	A1	2010-09-16	Bellovin		
/J.T.L/	6	20130305311	A1	2013-11-14	Puttaswamy Naga et al.		
/J.T.L/	7	20020186683	A1	2002-12-12	Buck et al.		
/J.T.L/	8	20090222877	A1	2009-09-03	Diehl et al.		
/J.T.L/	9	20100107240	A1	2010-04-29	Thaler et al.		
/J.T.L/	10	20040093513	A1	2004-05-13	Cantrell et al.		
/J.T.L/	11	20120023576	A1	2012-01-26	Sorensen et al.		
/J.T.L/	12	20080163333	A1	2008-07-03	Kasralikar		
/J.T.L/	13	20020164962	A1	2002-11-07	Mankins et al.		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

/J.T.L/	14	20050024189	A1	2005-02-03	Weber		
/J.T.L/	15	20110141900	A1	2011-06-16	Jayawardena et al.		
/J.T.L/	16	20150350229	A1	2015-12-03	Mitchell		
/J.T.L/	17	20050108557	A1	2005-05-19	Kayo et al.		
/J.T.L/	18	20150373043	A1	2015-12-24	Wang et al.		
/J.T.L/	19	20140317397	A1	2014-10-23	Martini		

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/J.T.L/	1	2007109541	WO	A2	2007-09-27	Brubaker, Curtis		

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

/J.T.L/	1	2015 Nov 02 - (AU) Office Action - App 2013372879	
/J.T.L/	2	2016 Apr 26 - (US) Office Action - App 14/745,207	
/J.T.L/	3	2016 May 06 - (US) Office Action - App 14/714,207	
/J.T.L/	4	2016 May 13 - (US) Office Action - App 13/940,240	
/J.T.L/	5	2016 Jun 14 - (US) Office Action - App 14/625,486	
/J.T.L/	6	2016 Feb 25 - (AU) Office Action - App 2014249055	
/J.T.L/	7	2016 Feb 24 - (AU) Office Action - App 2014228257	
/J.T.L/	8	2016 Jun 09 - (WO) International Search Report - PCT/US2016/026339	
/J.T.L/	9	2016 Jun 16 - (CA) Office Action - App 2,888,935	
/J.T.L/	10	2016 Jul 11 - (EP) Office Action - App 14720824.3	
/J.T.L/	11	2016 Jul 22 - (US) Office Action - App 14/921,718	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

/J.T.L/	12	2016 Jul 20 - (AU) Office Action - App 2013335255	
/J.T.L/	13	2016 Oct 05 - (US) Notice of Allowance - App 14/698,560	
/J.T.L/	14	2016 Sept 13 - (CA) Office Action - App 2,902,206	
/J.T.L/	15	2016 Sept 14 - (CA) Office Action - App 2,897,737	
/J.T.L/	16	2016 Sept 26 - (CA) Office Action - App 2,902,158	
/J.T.L/	17	2016 Oct 26 - (US) Office Action - App 13/940,240	
/J.T.L/	18	2016 Nov 21 - (US) Office Action - App 14/745,207	
/J.T.L/	19	2016 Dec 05 - (US) Notice of Allowance - App 14/714,207	
/J.T.L/	20	Singh, Rajeev et al. "Detecting and Reducing the Denial of Service attacks in WLANs", December 2011, World Congress on Information and Communication TEchnologies, pp. 968-973	
/J.T.L/	21	2017 Feb 10 - (US) Notice of Allowance - App 14/625,486	
/J.T.L/	22	2017 Feb 15 - (US) Notice of Allowance - App 14/921,718	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

/J.T.L/	23	2017 Mar 06 - (WO) International Search Report and Written Opinion - App PCT/US2016/068008	
/J.T.L/	24	2017 Jun 07 - (US) Office Action - App 14/745,207	
/J.T.L/	25	2015 Sept 4 (US) Notice of Allowance - App. 14/702,755 (007742.00036)	
/J.T.L/	26	2017 Jun 07 - (WO) International Search Report and Written Opinion - App PCT/US2016/067111	

If you wish to add additional non-patent literature document citation information please click the Add button [Add]

EXAMINER SIGNATURE

Examiner Signature	/JASON T LEE/	Date Considered	12/06/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH /J.T.L/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Application Number	14757638
	Filing Date	2015-12-23
	First Named Inventor	David K. Ahn
	Art Unit	2438
	Examiner Name	J. T. Lee
	Attorney Docket Number	007742.00059\US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Joshua D. Schneider/	Date (YYYY-MM-DD)	2017-07-11
Name/Print	Joshua D. Schneider	Registration Number	67,194

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J. T. L./

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUG" /T M T/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	6	"9413722".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:26
S2	2	"20160308894".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:50
S3	3	"9124552".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:51
S4	2	"9264370".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/01 15:52
S5	4	"Rule-based network-threat detection".ti.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:49
S6	6	"2004093513".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:58
S7	3	"20040093513".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:58
S8	0	"20129923576".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:58
S9	3	"20120023576".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:59
S10	2	"20080163333".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 15:59

S11	1	(S7 or S9 or S10)and indicator	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:00
S12	3	"20110055916".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:07
S13	7294	h04l63/1425.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:25
S14	13021	h04l61/1511.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S15	5447	h04l63/0263.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S16	6650	h04l63/0281.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S17	12955	h04l63/1416.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:26
S18	2796	S13 and (S14 or S15 or S16 or S17)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:32
S19	2795	S18 and @ad <"29151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:32
S20	2458	S18 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:33
S21	149	S13 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:34
S22	129	S21 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/06 16:34

S23	7306	h04l63/1425.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S24	13031	h04l61/1511.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S25	149	S23 and S24	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S26	129	S25 and @ad < "20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S27	0	(((filter$3 with rule) with treat) same (encrypt$3)) and S26	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:29
S28	7	(((filter$3 with rule) with treat) same (encrypt$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:30
S29	7	(((filter$3 with rule) with treat) same (encrypt$3)) and (DNS or domain)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:30
S30	7	(((filter$3 with rule) with treat) same (encrypt$3)) and (address or session)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 15:55
S31	7	(rule with based) and S30	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:01
S32	5448	h04l63/0263.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S33	6652	h04l63/0281.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S34	12973	h04l63/1416.cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30

S35	2805	S23 and (S24 or S32 or S33 or S34)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S36	2466	S35 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S37	2466	S36 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S38	0	(((filter$3 with rule) with treat) same (encrypt$3)) and S37	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/07 16:30
S39	0	((receiv$3 with packet)same rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:32
S40	0	((receiv$3 with message)same rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:32
S41	0	((receiv$3 same message)same rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:32
S42	1	((receiv$3 same message)and rule) and "20050138353".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/03/08 14:33
S43	3	((((filter$3 with rule) with proxy) same ((URI) or "uniform resource identifier")) and (log or drop)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/04/05 12:09
S44	3	S43 and @ad <"20151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/04/05 12:10
S45	46	(indicator with threat) same (DNS or domain) and (filter with ((URI) or (protocol version) or method or command))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/12/06 13:41
S46	3	(indicator with threat) same (DNS or domain) and (filter with ((URI) or (protocol version) or method or command)) and ((rout$3 with proxy) same indicator)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/12/06 13:43

S47	3	S46 and @ad < "29151223"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/12/06 13:43
S49	46	(indicator with threat) same (DNS or domain) and (filter with ((URI) or (protocol version) or method or command))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2017/12/06 15:14

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S48	1	(indicator with threat) same (DNS or domain) and (filter with ((URI) or (protocol version) or method or command)) and ((rout$3 with proxy) same indicator).clm.	US-PGPUB; USPAT	ADJ	ON	2017/12/06 13:47

12/6/2017 5:35:30 PM
C:\Users\jlee16\Documents\EAST\Workspaces\14757638-030117.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	Art Unit
	JASON LEE	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/05/2017	12/07/2017							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	✓	=							
9	9	✓	=							
10	10	✓	=							
11	11	✓	=							
12	12	✓	=							
13	13	✓	=							
14	14	✓	=							
15	15	✓	=							
16	16	✓	=							
17	17	✓	=							
18	18	✓	=							
19	19	✓	=							
20	20	✓	=							
21	21	✓	=							
22	22	✓	=							
23	23	✓	=							
24	24	✓	=							
25	25	✓	=							

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 9492

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/757,638	12/23/2015	713	2438	007742.00059

APPLICANTS
Centripetal Networks, Inc., Herndon, VA;

INVENTORS
David K. Ahn, Winston-Salem, NC;
Sean Moore, Hollis, NH;
Douglas M. DiSabello, Leesburg, VA;

**** CONTINUING DATA ***************************

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /JASON T LEE/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		NC	13	25	3

ADDRESS

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051
UNITED STATES

TITLE

Rule-based network-threat detection for encrypted communications

FILING FEE RECEIVED		
1305	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	Art Unit
	JASON LEE	2438

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner
h04l63/1425.cpc.;h04l61/1511.cpc.;h04l63/0263.cpc.;h04l63/0281.cpc.;h04l63/1416.cpc.;	4/3/17	JL

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	153	4/3/17	JL

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searched	4/2/17	JL
inventor name searched	4/3/17	JL
Rule-based network-threat detection searched on topic	4/2/17	JL
(((filter$3 with rule) with treat) same (encrypt$3)); (((filter$3 with rule) with treat) same (encrypt$3)) and (address or session);	4/2/17	JL
(indicator with threat) same (DNS or domain) and (filter with ((URI) or (protocol version) or method or command))	12/7/17	JL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
713	156	12/7/17	JL

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
	(indicator with threat) same (DNS or domain) and (filter with ((URI) or (protocol version) or method or command)) and ((rout$3 with proxy) same indicator).clm.	12/7/17	JL

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	**Art Unit**
	JASON LEE	2438

CPC						
Symbol					**Type**	**Version**
H04L		63	/	1425	F	2013-01-01
H04L		61	/	1511	I	2013-01-01
H04L		69	/	22	I	2013-01-01
H04L		63	/	20	I	2013-01-01
H04L		63	/	1416	I	2013-01-01
H04L		63	/	0263	I	2013-01-01
H04L		63	/	0281	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	25	
/JASON LEE/ Primary Examiner.Art Unit 2438	12/07/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	**Art Unit**
	JASON LEE	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
713	153	H	0	4	L	29 / 06 (2006.01.01)						
CROSS REFERENCE(S)												
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
726	22											

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	25	
/JASON LEE/ Primary Examiner.Art Unit 2438	12/07/2017	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14757638	AHN ET AL.
	Examiner	**Art Unit**
	JASON LEE	2438

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6	22	22												
7	7	23	23												
8	8	24	24												
9	9	25	25												
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 25	
/JASON LEE/ Primary Examiner.Art Unit 2438 (Primary Examiner)	12/07/2017 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

Docket No.: 007742.00059\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	
David K. Ahn et al.	Allowed: December 20, 2017
Application No.: 14/757,638	Confirmation No.: 9492
Filed: December 23, 2015	Art Unit: 2438
For: Rule-Based Network-Threat Detection For Encrypted Communications	Examiner: J. T. Lee

AMENDMENT AFTER ALLOWANCE UNDER 37 C.F.R. § 1.312 STATEMENT OF SUBSTANCE OF INTERVIEW, AND COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE UNDER 37 C.F.R. § 1.104(E)

Mail Stop - Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

Prior to issuance of the patent, applicant respectfully requests entry of this amendment under 37 C.F.R. 1.312 for the above-captioned patent application.

Applicant is in receipt of a Notice of Allowance and Fee Due, dated December 20, 2017. The Issue Fee is due March 20, 2017, and is being paid concurrently herewith. Prior to issuance of the patent, applicant respectfully requests entry of this amendment under 37 C.F.R. 1.312 for the above-captioned patent application.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the ~~one or more~~plurality of network-threat indicators ~~comprise~~ comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

2. (Previously Presented) The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query, the method further comprising:

determining that the at least one of the DNS query or the reply to the DNS query comprises the domain name identified as the network threat.

3. (Previously Presented) The method of claim 2, wherein the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

4. (Previously Presented) The method of claim 2, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

5. (Previously Presented) The method of claim 4, wherein the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host, the method further comprising:

identifying one or more packets comprising the request.

6. (Currently Amended) The method of claim 1, wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host, the method further comprising:

routing the one or more ~~of the~~ packets comprising data configured to establish the encrypted communication session between the first host and the second host to the proxy system.

7. (Currently Amended) The method of claim 6, the method further comprising:

routing the one or more ~~of the~~ packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the domain name identified as the network threat.

8. (Currently Amended) The method of claim 6, wherein:

the plurality of packet-filtering rules indicate:

one or more network addresses for which encrypted communications are to be established via the proxy system, and

one or more network addresses for which encrypted communications are to not be established via the proxy system, the method further comprising:

routing the one or more ~~of the~~ packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications are to be established via the proxy system.

9. (Previously Presented) The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

redirecting packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

10. (Previously Presented) The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

forwarding copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

11. (Previously Presented) The method of claim 6, the method further comprising:

identifying, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and

identifying, via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data.

12. (Previously Presented) The method of claim 11, the method further comprising:

identifying, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data.

13. (Currently Amended) The method of claim 6, the method further comprising:

generating, by the proxy system, one or more packets based on the filtered packets, comprising encrypted data, routed to the proxy system by the packet-filtering system;

responsive to determining that one or more packets generated by the proxy system ~~based on one or more of the packets comprising encrypted data~~ correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

dropping the one or more packets generated by the proxy system;

logging the one or more packets generated by the proxy system;

dropping one or more other packets generated by the proxy system;

logging one or more other packets generated by the proxy system;

dropping one or more other packets ~~of the packets~~ comprising encrypted data; or

logging one or more other packets ~~of the packets~~ comprising encrypted data.

14. (Previously Presented) The method of claim 13, wherein the determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules.

15. (Previously Presented) The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI) meeting a threshold size specified by the plurality of packet-filtering rules.

16. (Previously Presented) The method of claim 6, the method further comprising:

identifying, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.

17. (Previously Presented) The method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the

method further comprising at least one of dropping or logging packets other than the packets comprising encrypted data based on a determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host.

18. (Previously Presented) The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:

determining that the one or more handshake messages comprise the domain name identified as the network threat.

19. (Previously Presented) The method of claim 18, the method further comprising:

responsive to determining that the one or more handshake messages comprise the domain name identified as the network threat, at least one of dropping or logging the packets comprising encrypted data.

20. (Previously Presented) The method of claim 18, wherein:

the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server; and

the determining that the one or more handshake messages comprise the domain name identified as the network threat comprises determining the at least one of the hello message generated by the client or the certificate message generated by the server comprises the domain name identified as the network threat.

21. (Previously Presented) The method of claim 18, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the one or more handshake messages, the method further comprising determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

22. (Previously Presented) The method of claim 21, wherein the one or more network addresses comprise a network address of the server and a network address of a web proxy, the method further comprising:

identifying one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

determining that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. (Previously Presented) The method of claim 1, wherein the packets comprising unencrypted data comprise a certificate message for an encrypted communication session, the method further comprising:

at least one of dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. (Currently Amended) A packet-filtering system comprising:

at least one hardware processor; and

memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the ~~one or more~~plurality of network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, based on at least one of a uniform resource identifier (URI) specified by ~~the~~ a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

25. (Currently Amended) One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of ~~one or more~~ network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by ~~the~~ a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by

the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

REMARKS

Entry of the amendment herein prior to issuance is respectfully requested. Claims 1-25 remain pending in this application. Claims 1, 6-8, 13, 24 and 25 have been amended. No new matter is introduced by this paper, and no new issues are raised.

Statement of Substance of Interview

Applicant gratefully wishes to thank the Examiner for the courtesies extended in granting and conducting on January 22, 2018, a telephonic interview with Applicant's representative. During the interview, Applicant's representative and the Examiner discussed an amendments and Applicant understands that the instant amendment, which effects the changes discusses, would be entered. The changes are intended to ensure that the application issues in even better form, and are respectfully submitted not to entail a substantial amount of additional work on the part of the Patent and Trademark Office. MPEP 714.16. Favorable consideration is earnestly solicited.

Comments on Reasons for Allowance

Applicant thanks Examiner Lee for the allowance of this application. Applicant wishes to briefly respond to the Statement of Reasons for Allowance in the Notice of Allowance mailed December 20, 2017 ("Statement"). Applicant agrees that the claims are distinguishable, and respectfully submits that the specific excerpts quoted in the Statement are not the full claim language for all the claims, and are not necessarily the only reasons for distinguishing the claims from the various references, as there are many other features in the different independent and dependent claims. Also, to the extent there is any deviation between the quoted excerpts and the language of the claims, Applicant submits that the language of the claims will control for establishing the requirements of the various claims.

It is respectfully submitted that the pending claims are allowable over the art of record, and that the application remains in condition for allowance. Favorable consideration and early passage to issue of the application are earnestly solicited.

In the event the U.S. Patent and Trademark Office determines that an extension is required, applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 19-0733 referencing docket no. 007742.00059\US.

Dated: January 23, 2018

Respectfully submitted,

By: /Joshua D. Schneider/
Joshua D. Schneider
Registration No.: 67,194

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Patent Application Fee Transmittal

Application Number:	14757638
Filing Date:	23-Dec-2015
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Filer:	Joshua Daniel Schneider/Jennifer Brady
Attorney Docket Number:	007742.00059

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	31576489
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Joshua Daniel Schneider/Jennifer Brady
Filer Authorized By:	Joshua Daniel Schneider
Attorney Docket Number:	007742.00059
Receipt Date:	23-JAN-2018
Filing Date:	23-DEC-2015
Time Stamp:	11:24:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	DA
Payment was successfully received in RAM	$480
RAM confirmation Number	012318INTEFSW00010112190733
Deposit Account	190733
Authorized User	Joshua Schneider
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Issue_Fee_Transmittal_18945745.pdf	33744 818ffad71f2883d03fac770d45119b234ad5faae	no	1
Warnings:					
Information:					
2		Amendment_After_Allowance_Under_37CFR1_18945714.pdf	51066 de535d7b7ca29cebad135b884e6694f9bd4ea406	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Claims	2	10
	Applicant Arguments/Remarks Made in an Amendment	11	12

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30580 cc04b2f14b34c43a1e127893f4e5f2174d31684b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	115390		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B–FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22314-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note Use Block 1 for any change of address)

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, EFS-Web transmitted, or facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's Name)
(S-ignature)
(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
14/757,638	12/23/2015	David K. Ahn	007742.00059\US	9492

TITLE OF INVENTION: Rule-Based Network-Threat Detection For Encrypted Communications

APPLN: TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480.00	$0	$0	$480.00	03/20/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
J. T. Lee	2438	713-153

1. Change of correspondence address or indication of "Fee Address" (37CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered attorney or agent. If no name is listed, no name will be printed

1. Banner & Witcoff, Ltd.
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Centripetal Networks, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Portsmouth, New Hampshire

Please check the appropriate assignee categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies

4b. Payment of Fees(s): **(Please first reapply and previously paid fee shown above)**

☐ A check is enclosed

☐ Payment be credit card. Form PTO-2038 is attached

☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 19-0733 (enclose an extra copy of this form)

5. Change of Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Joshua D. Schneider/ Date January 23, 2018

Typed or printed name Joshua D. Schneider Registration No. 67,194

Docket No.: 007742.00059\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	
David K. Ahn et al.	Allowed: December 20, 2017
Application No.: 14/757,638	Confirmation No.: 9492
Filed: December 23, 2015	Art Unit: 2438
For: Rule-Based Network-Threat Detection For Encrypted Communications	Examiner: J. T. Lee

AMENDMENT AFTER ALLOWANCE UNDER 37 C.F.R. § 1.312 STATEMENT OF SUBSTANCE OF INTERVIEW, AND COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE UNDER 37 C.F.R. § 1.104(E)

Mail Stop - Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

Prior to issuance of the patent, applicant respectfully requests entry of this amendment under 37 C.F.R. 1.312 for the above-captioned patent application.

Applicant is in receipt of a Notice of Allowance and Fee Due, dated December 20, 2017. The Issue Fee is due March 20, 2017, and is being paid concurrently herewith. Prior to issuance of the patent, applicant respectfully requests entry of this amendment under 37 C.F.R. 1.312 for the above-captioned patent application.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

18939237

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

receiving, by a packet-filtering system comprising a hardware processor and a memory and configured to filter packets in accordance with a plurality of packet-filtering rules, data indicating a plurality of network-threat indicators, wherein at least one of the ~~one or more~~plurality of network-threat indicators ~~comprise~~ comprises a domain name identified as a network threat;

identifying packets comprising unencrypted data;

identifying packets comprising encrypted data;

determining, by the packet-filtering system and based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filtering, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data that corresponds to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

routing, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

2. (Previously Presented) The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising at least one of a domain name system (DNS) query or a reply to the DNS query, the method further comprising:

determining that the at least one of the DNS query or the reply to the DNS query comprises the domain name identified as the network threat.

3. (Previously Presented) The method of claim 2, wherein the portion of the unencrypted data comprises one or more network addresses included in the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

4. (Previously Presented) The method of claim 2, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the at least one of the DNS query or the reply to the DNS query, the method further comprising:

determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

5. (Previously Presented) The method of claim 4, wherein the one or more network addresses comprise a network address of a web proxy that generated the DNS query in response to a request received from a host, the method further comprising:

identifying one or more packets comprising the request.

6. (Currently Amended) The method of claim 1, wherein one or more packets, of the packets comprising unencrypted data, comprise data configured to establish an encrypted communication session between a first host and a second host, the method further comprising:

routing the one or more ~~of the~~ packets comprising data configured to establish the encrypted communication session between the first host and the second host to the proxy system.

7. (Currently Amended) The method of claim 6, the method further comprising:

routing the one or more ~~of the~~ packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the domain name identified as the network threat.

8. (Currently Amended) The method of claim 6, wherein:

the plurality of packet-filtering rules indicate:

one or more network addresses for which encrypted communications are to be established via the proxy system, and

one or more network addresses for which encrypted communications are to not be established via the proxy system, the method further comprising:

routing the one or more ~~of the~~ packets to the proxy system based on a determination that at least one of the first host or the second host corresponds to the one or more network addresses for which encrypted communications are to be established via the proxy system.

9. (Previously Presented) The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

redirecting packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

10. (Previously Presented) The method of claim 6, wherein:

the packet-filtering system comprises:

one or more interfaces interfacing the packet-filtering system with one or more communication links interfacing the first host and the second host, and

one or more interfaces interfacing the packet-filtering system with the proxy system, the method further comprising:

forwarding copies of packets received via the one or more interfaces interfacing the packet-filtering system with the one or more communication links interfacing the first host and the second host to the one or more interfaces interfacing the packet-filtering system with the proxy system.

11. (Previously Presented) The method of claim 6, the method further comprising:

identifying, via a communication link interfacing the first host and the proxy system, the packets comprising encrypted data; and

identifying, via an internal communication link of the proxy system, packets corresponding to the packets comprising encrypted data.

12. (Previously Presented) The method of claim 11, the method further comprising:

identifying, via a communication link interfacing the proxy system and the second host, packets generated by the proxy system based on the packets corresponding to the packets comprising encrypted data.

13. (Currently Amended) The method of claim 6, the method further comprising:

generating, by the proxy system, one or more packets based on the filtered packets, comprising encrypted data, routed to the proxy system by the packet-filtering system;

responsive to determining that one or more packets generated by the proxy system ~~based on one or more of the packets comprising encrypted data~~ correspond to one or more criteria specified by the plurality of packet-filtering rules, at least one of:

dropping the one or more packets generated by the proxy system;

logging the one or more packets generated by the proxy system;

dropping one or more other packets generated by the proxy system;

logging one or more other packets generated by the proxy system;

dropping one or more other packets ~~of the packets~~ comprising encrypted data; or

logging one or more other packets ~~of the packets~~ comprising encrypted data.

14. (Previously Presented) The method of claim 13, wherein the determining that one or more packets generated by the proxy system based on one or more of the packets comprising encrypted data correspond to one or more criteria specified by the plurality of packet-filtering rules comprises determining that the one or more packets generated by the proxy system comprise at least one of a uniform resource identifier (URI) specified by the plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules.

15. (Previously Presented) The method of claim 13, wherein the determining comprises determining that the one or more packets generated by the proxy system comprise a uniform resource identifier (URI) meeting a threshold size specified by the plurality of packet-filtering rules.

16. (Previously Presented) The method of claim 6, the method further comprising:

identifying, via a communication link interfacing the proxy system and an Internet content adaptation protocol (ICAP) server, one or more packets comprising at least one of an ICAP request, a response generated by the ICAP server, or a modified request generated by the ICAP server.

17. (Previously Presented) The method of claim 1, wherein the packets comprising encrypted data comprise packets received from a first host and destined for a second host, the

method further comprising at least one of dropping or logging packets other than the packets comprising encrypted data based on a determination that the packets other than the packets comprising encrypted data were at least one of received from the second host or destined for the first host.

18. (Previously Presented) The method of claim 1, wherein:

the packets comprising unencrypted data comprise one or more packets comprising one or more handshake messages configured to establish an encrypted communication session between a client and a server, the method further comprising:

determining that the one or more handshake messages comprise the domain name identified as the network threat.

19. (Previously Presented) The method of claim 18, the method further comprising:

responsive to determining that the one or more handshake messages comprise the domain name identified as the network threat, at least one of dropping or logging the packets comprising encrypted data.

20. (Previously Presented) The method of claim 18, wherein:

the one or more handshake messages comprise at least one of a hello message generated by the client or a certificate message generated by the server; and

the determining that the one or more handshake messages comprise the domain name identified as the network threat comprises determining the at least one of the hello message generated by the client or the certificate message generated by the server comprises the domain name identified as the network threat.

21. (Previously Presented) The method of claim 18, wherein the portion of the unencrypted data comprises one or more network addresses included in one or more headers of the one or more packets comprising the one or more handshake messages, the method further comprising determining that the packets comprising encrypted data comprise one or more packet headers comprising at least one of the one or more network addresses.

22. (Previously Presented) The method of claim 21, wherein the one or more network addresses comprise a network address of the server and a network address of a web proxy, the method further comprising:

identifying one or more packets comprising one or more packet headers comprising the network address of the web proxy and a network address of the client; and

determining that the packets comprising encrypted data comprise one or more packet headers comprising the network address of the server and the network address of the client.

23. (Previously Presented) The method of claim 1, wherein the packets comprising unencrypted data comprise a certificate message for an encrypted communication session, the method further comprising:

at least one of dropping or logging one or more of the packets comprising encrypted data based on a determination that the certificate message comprises data indicating at least one of a serial number indicated by the plurality of packet-filtering rules, an issuer indicated by the plurality of packet-filtering rules, a validity time-range indicated by the plurality of packet-filtering rules, a key indicated by the plurality of packet-filtering rules, or a signing authority indicated by the plurality of packet-filtering rules.

24. (Currently Amended) A packet-filtering system comprising:

at least one hardware processor; and

memory storing instructions that when executed by the at least one hardware processor cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the ~~one or more~~plurality of network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, based on at least one of a uniform resource identifier (URI) specified by ~~the~~ a plurality of packet-filtering rules, data indicating a protocol version specified by the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

25. (Currently Amended) One or more non-transitory computer-readable media comprising instructions that when executed by at least one hardware processor of a packet-filtering system cause the packet-filtering system to:

receive data indicating a plurality of network-threat indicators, wherein at least one of the plurality of ~~one or more~~ network-threat indicators comprise a domain name identified as a network threat;

identify packets comprising unencrypted data;

identify packets comprising encrypted data;

determine, based on a portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators, packets comprising encrypted data that corresponds to the one or more network-threat indicators;

filter, by the packet-filtering system and based on at least one of a uniform resource identifier (URI) specified by ~~the~~ a plurality of packet-filtering rules indicating one or more of the plurality of network-threat indicators, data indicating a protocol version specified by

the plurality of packet-filtering rules, data indicating a method specified by the plurality of packet-filtering rules, data indicating a request specified by the plurality of packet-filtering rules, or data indicating a command specified by the plurality of packet-filtering rules:

packets comprising the portion of the unencrypted data corresponding to one or more network-threat indicators of the plurality of network-threat indicators; and

the determined packets comprising the encrypted data that corresponds to the one or more network-threat indicators; and

route, by the packet-filtering system, filtered packets to a proxy system based on a determination that the filtered packets comprise data that corresponds to the one or more network-threat indicators.

REMARKS

Entry of the amendment herein prior to issuance is respectfully requested. Claims 1-25 remain pending in this application. Claims 1, 6-8, 13, 24 and 25 have been amended. No new matter is introduced by this paper, and no new issues are raised.

Statement of Substance of Interview

Applicant gratefully wishes to thank the Examiner for the courtesies extended in granting and conducting on January 22, 2018, a telephonic interview with Applicant's representative. During the interview, Applicant's representative and the Examiner discussed an amendments and Applicant understands that the instant amendment, which effects the changes discusses, would be entered. The changes are intended to ensure that the application issues in even better form, and are respectfully submitted not to entail a substantial amount of additional work on the part of the Patent and Trademark Office. MPEP 714.16. Favorable consideration is earnestly solicited.

Comments on Reasons for Allowance

Applicant thanks Examiner Lee for the allowance of this application. Applicant wishes to briefly respond to the Statement of Reasons for Allowance in the Notice of Allowance mailed December 20, 2017 ("Statement"). Applicant agrees that the claims are distinguishable, and respectfully submits that the specific excerpts quoted in the Statement are not the full claim language for all the claims, and are not necessarily the only reasons for distinguishing the claims from the various references, as there are many other features in the different independent and dependent claims. Also, to the extent there is any deviation between the quoted excerpts and the language of the claims, Applicant submits that the language of the claims will control for establishing the requirements of the various claims.

It is respectfully submitted that the pending claims are allowable over the art of record, and that the application remains in condition for allowance. Favorable consideration and early passage to issue of the application are earnestly solicited.

In the event the U.S. Patent and Trademark Office determines that an extension is required, applicant petitions for any required relief including extensions of time and authorizes the Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to Deposit Account No. 19-0733 referencing docket no. 007742.00059\US.

Dated: January 23, 2018

Respectfully submitted,

By: /Joshua D. Schneider/
Joshua D. Schneider
Registration No.: 67,194

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

Electronic Patent Application Fee Transmittal

Application Number:	14757638
Filing Date:	23-Dec-2015
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Filer:	Joshua Daniel Schneider/Jennifer Brady
Attorney Docket Number:	007742.00059

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**480**

Electronic Acknowledgement Receipt

EFS ID:	31576405
Application Number:	14757638
International Application Number:	
Confirmation Number:	9492
Title of Invention:	Rule-based network-threat detection for encrypted communications
First Named Inventor/Applicant Name:	David K. Ahn
Customer Number:	22907
Filer:	Joshua Daniel Schneider/Jennifer Brady
Filer Authorized By:	Joshua Daniel Schneider
Attorney Docket Number:	007742.00059
Receipt Date:	23-JAN-2018
Filing Date:	23-DEC-2015
Time Stamp:	11:19:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Issue_Fee_Transmittal_18945745.pdf	33744 818ffad71f2883d03fac770d45119b234ad5faae	no	1

Warnings:

Information:					
2	Post Allowance Communication - Incoming	Comments_on_Statement_of_Reasons_for_Allowance_18945716.pdf	17548 e484414e9b8040dc2c9dad57901e83439e5ba496	no	1
Warnings:					
Information:					
3		Amendment_After_Allowance_Under_37CFR1_18945714.pdf	51066 de535d7b7ca29cebad135b884e6694f9bd4ea406	yes	12

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Claims	2	10
	Applicant Arguments/Remarks Made in an Amendment	11	12

Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30580 d8cb535b726505666557a9e3f1e37ab5b68f9c94	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	132938		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B–FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22314-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note Use Block 1 for any change of address)

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, EFS-Web transmitted, or facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's Name)
(S-signature)
(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
14/757,638	12/23/2015	David K. Ahn	007742.00059\US	9492

TITLE OF INVENTION: Rule-Based Network-Threat Detection For Encrypted Communications

APPLN: TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480.00	$0	$0	$480.00	03/20/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
J. T. Lee	2438	713-153

1. Change of correspondence address or indication of "Fee Address" (37CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered attorney or agent. If no name is listed, no name will be printed

1. Banner & Witcoff, Ltd.
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Centripetal Networks, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Portsmouth, New Hampshire

Please check the appropriate assignee categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☐ Publication Fee (No small entity discount permitted)

☐ Advance Order - # of Copies

4b. Payment of Fees(s): **(Please first reapply and previously paid fee shown above)**

☐ A check is enclosed

☐ Payment be credit card. Form PTO-2038 is attached

☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 19-0733 (enclose an extra copy of this form)

5. Change of Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Joshua D. Schneider/ Date January 23, 2018

Typed or printed name Joshua D. Schneider Registration No. 67,194

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	Atty. Docket No. 007742.00059
David K. Ahn et al.	Allowed: December 20, 2017
Application No.: 14/757,638	Confirmation No.: 9492
Filed: December 23, 2015	Art Unit: 2438
For: Rule-Based Network-Threat Detection For Encrypted Communications	Examiner: J. T. Lee

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE UNDER 37 C.F.R. § 1.104(e)

Mail Stop - Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

Applicant thanks Examiner Lee for the allowance of this application. In brief response to the Statement of Reasons for Allowance from the Notice of Allowance, Applicant respectfully submits that the specific excerpts referenced in the Statement are not the exact claim language for all the claims, and are not necessarily the only reasons for distinguishing the claims from the various references and/or rendering the claimed subject matter eligible for patent protection, as there are many other features in the independent and dependent claims. Ultimately, Applicant submits that it is the language of each individual claim that controls.

Dated:

Respectfully submitted,

By: _____
Joshua D. Schneider
Registration No.: 67,194

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005
(202) 824-3000

18938127

OPAP JAN 23 2018 PATENT & TRADEMARK OFFICE

PART B–FEE(S) TRANSMITTAL

Complete and send this form, together with the applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22314-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note Use Block 1 for any change of address)

BANNER & WITCOFF, LTD.
1100 13th St. NW
STE 1200
Washington, DC 20005

01/23/2018 INTEFE1 00000012 14757638

01 FC:2501

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, EFS-Web transmitted, or facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's Name)
(S-signature)
(Date)

APPLICATION NO	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO	CONFIRMATION NO
14/757,638	12/23/2015	David K. Ahn	007742.00059\US	9492

TITLE OF INVENTION: Rule-Based Network-Threat Detection For Encrypted Communications

APPLN: TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480.00	$0	$0	$480.00	03/20/2018

EXAMINER	ART UNIT	CLASS-SUBCLASS
J. T. Lee	2438	713-153

1. Change of correspondence address or indication of "Fee Address" (37CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered attorney or agent. If no name is listed, no name will be printed

1. Banner & Witcoff, Ltd.
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: Centripetal Networks, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Portsmouth, New Hampshire

Please check the appropriate assignee categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies

4b. Payment of Fees(s): **(Please first reapply and previously paid fee shown above)**
☐ A check is enclosed
☐ Payment be credit card. Form PTO-2038 is attached
☒ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 19-0733 (enclose an extra copy of this form)

5. Change of Entity Status (from status indicated above)
☐ Applicant certifying micro entity status. See 37 CFR 1.29
NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
☐ Applicant asserting small entity status. See 37 CFR 1.27
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
☐ Applicant changing to regular undiscounted fee status.
NOTE: Checking this box will be taken to be notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature	/Joshua D. Schneider/	Date	January 23, 2018
Typed or printed name	Joshua D. Schneider	Registration No.	67,194

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/757,638	12/23/2015	David K. Ahn	007742.00059	9492

22907 7590 02/05/2018

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
02/05/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

eofficeaction@bannerwitcoff.com
GPD@bannerwitcoff.com

Response to Rule 312 Communication	Application No.	Applicant(s)
	14/757,638	AHN ET AL.
	Examiner	Art Unit
	JASON LEE	2438

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

1. ☒ The amendment filed on *23 January 2018* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

The Applicant filed 1/23/18 for amendment after allowance for requesting amending claims 1, 6-8, 13, 24 and 25 for correcting the clarity of the claims to ensure the application issues in even better form along with grammatical errors for notice of allowance mailed out on 12/20/2017 pursuant to 37 CFR § 1.312.
The Examiner reviewed the claim correction details on 01/31/18. These amendements do not change the scope of the claimed limiations and do not add any new matters. The amendments are purely for consistency with the language recited in the claims so to maintain clarity and consistency. Therefore, the Applicant request for the amendment after allowance pursuant to 37 CFR § 1.312 is entered.

/JASON LEE/
Primary Examiner, Art Unit 2438

Docket No.: 007742.00059\US
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	
David K. Ahn et al.	Allowed: December 20, 2017
Application No.: 14/757,638	Confirmation No.: 9492
Filed: December 23, 2015	Art Unit: 2438
For: Rule-Based Network-Threat Detection For Encrypted Communications	Examiner: J. T. Lee

AMENDMENT AFTER ALLOWANCE UNDER 37 C.F.R. § 1.312 STATEMENT OF SUBSTANCE OF INTERVIEW, AND COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE UNDER 37 C.F.R. § 1.104(E)

Mail Stop - Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

INTRODUCTORY COMMENTS

Prior to issuance of the patent, applicant respectfully requests entry of this amendment under 37 C.F.R. 1.312 for the above-captioned patent application.

Applicant is in receipt of a Notice of Allowance and Fee Due, dated December 20, 2017. The Issue Fee is due March 20, 2017, and is being paid concurrently herewith. Prior to issuance of the patent, applicant respectfully requests entry of this amendment under 37 C.F.R. 1.312 for the above-captioned patent application.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

18939237

OK TO ENTER: /J.T.L/

01/31/2018

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/757,638	03/13/2018	9917856	007742.00059	9492

22907 7590 02/21/2018

BANNER & WITCOFF, LTD.
1100 13th STREET, N.W.
SUITE 1200
WASHINGTON, DC 20005-4051

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

David K. Ahn, Winston-Salem, NC;
Centripetal Networks, Inc., Herndon, VA;
Sean Moore, Hollis, NH;
Douglas M. DiSabello, Leesburg, VA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.