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

IPR2023-01353 Page 01245

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,

IPR2023-01353 Page 01269

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

IPR2023-01353 Page 01294

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

IPR2023-01353 Page 01301

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;

IPR2023-01353 Page 01313

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;

IPR2023-01353 Page 01316

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.

IPR2023-01353 Page 01318

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
Development funding
400
Driving Population
115
Performance feedback
180
500
Fleet/Government Users
Developers, Suppliers Manufacturers
600
130
Investment
140
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

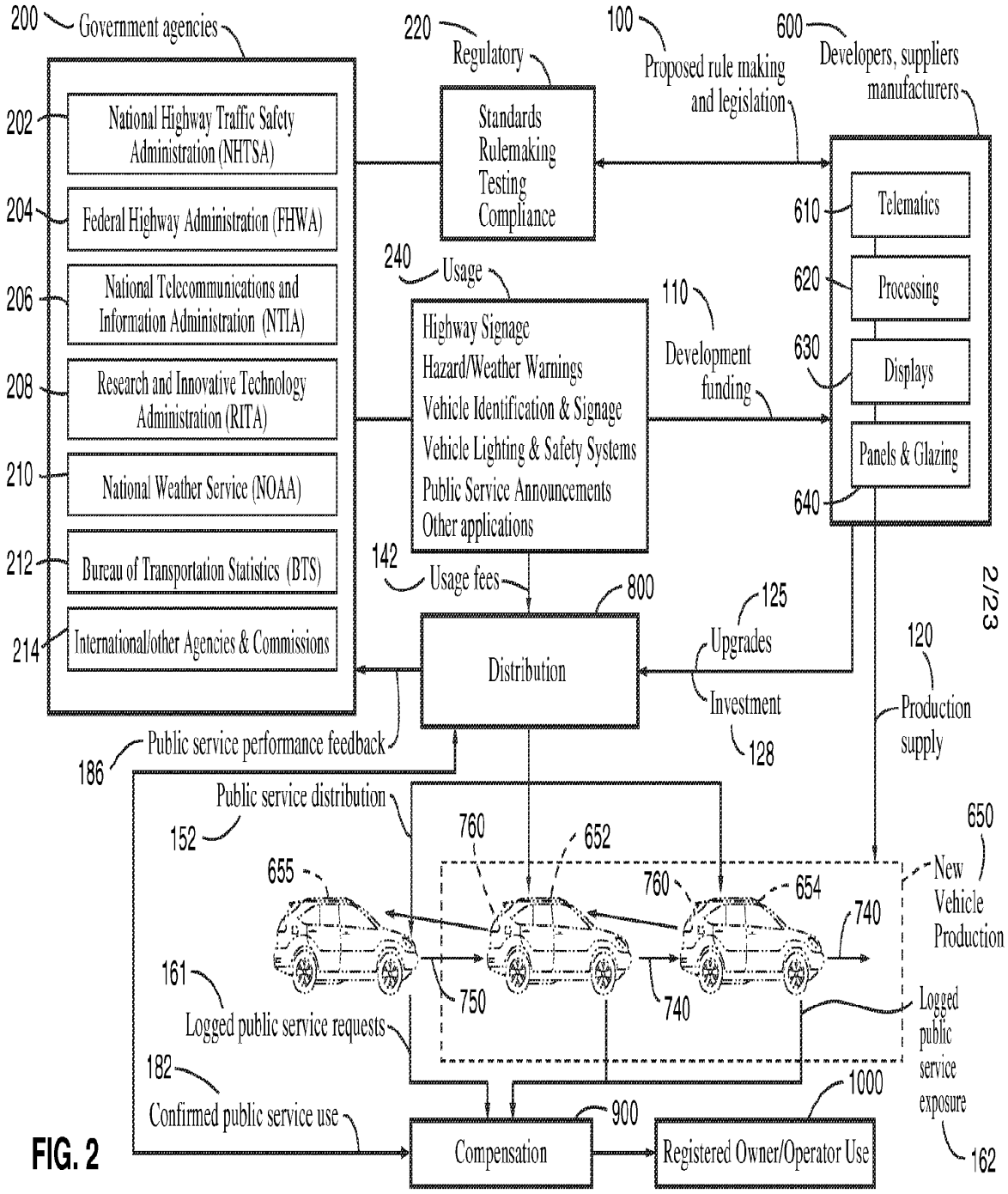

200
Government agencies
202
National Highway Traffic Safety Administration (NHTSA)
204
Federal Highway Administration (FHWA)
206
National Telecommunications and Information Administration (NTIA)
208
Research and Innovative Technology Administration (RITA)
210
National Weather Service (NOAA)
212
Bureau 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
Public service distribution
152
760
652
655
760
654
740
650
New Vehicle Production
161
Logged public service requests
750
740
Logged public service exposure
162
182
Confirmed public service use
900
Compensation
1000
Registered Owner/Operator Use
2/23

FIG. 2

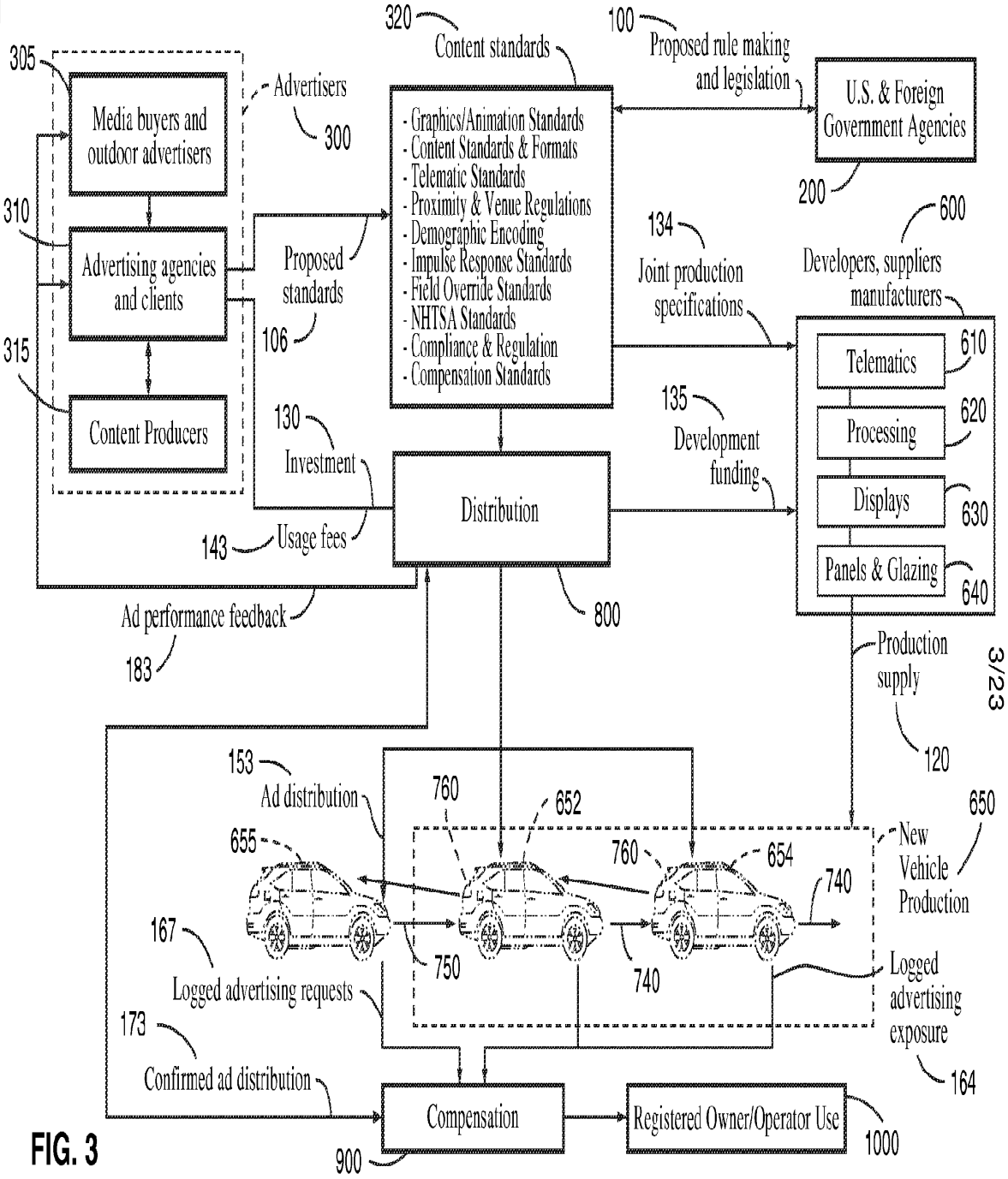

305
Media buyers and outdoor advertisers
Advertisers
300
310
Advertising agencies and clients
315
Content Producers
320
Content standards
- Graphics/Animation Standards
- Content Standards & Formats
- Telematic Standards
- Proximity & Venue Regulations
- Demographic Encoding
- Impulse Response Standards
- Field Override Standards
- NHTSA Standards
- Compliance & Regulation
- Compensation Standards
100
Proposed rule making and legislation
U.S. & Foreign Government Agencies
200
Proposed standards
106
130
Investment
143
Usage fees
Distribution
134
Joint production specifications
600
Developers, suppliers manufacturers
135
Development funding
Telematics
610
Processing
620
Displays
630
Panels & Glazing
640
Ad performance feedback
183
800
Production supply
120
3/23
153
Ad distribution
760
652
655
760
654
650
New Vehicle Production
740
167
750
740
Logged advertising requests
Logged advertising exposure
164
173
Confirmed ad distribution
Compensation
900
Registered Owner/Operator Use
1000

FIG. 3

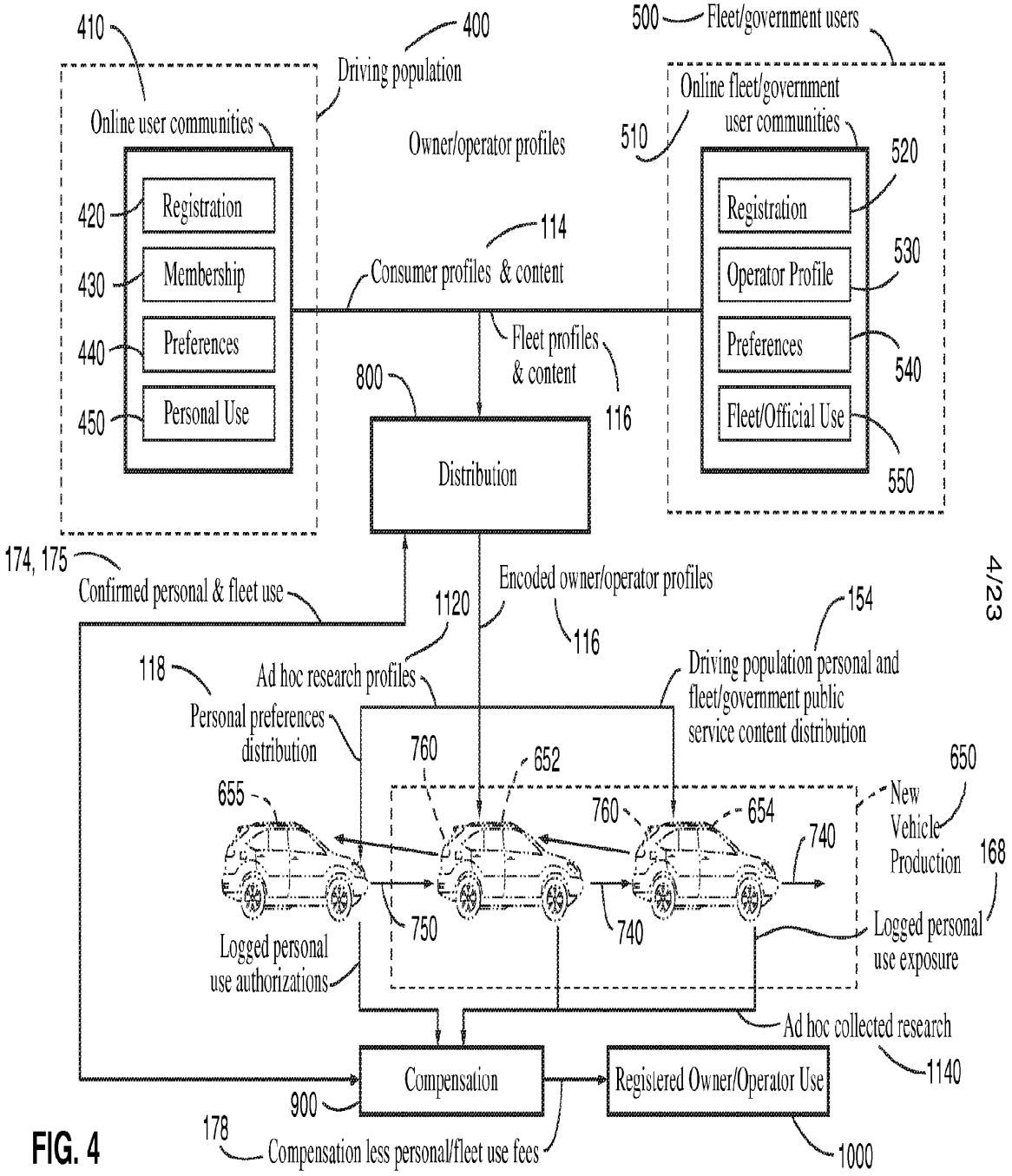

410
400
Driving population
500
Fleet/government users
Online user communities
Owner/operator profiles
Online fleet/government user communities
510
520
420
Registration
114
Consumer profiles & content
Registration
430
Membership
530
Operator Profile
440
Preferences
Fleet profiles & content
Preferences
540
800
450
Personal Use
116
Fleet/Official Use
Distribution
550
174, 175
Confirmed personal & fleet use
Encoded owner/operator profiles
1120
154
116
118
Ad hoc research profiles
Driving population personal and fleet/government public service content distribution
Personal preferences distribution
760
652
650
655
760
654
New Vehicle Production
740
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

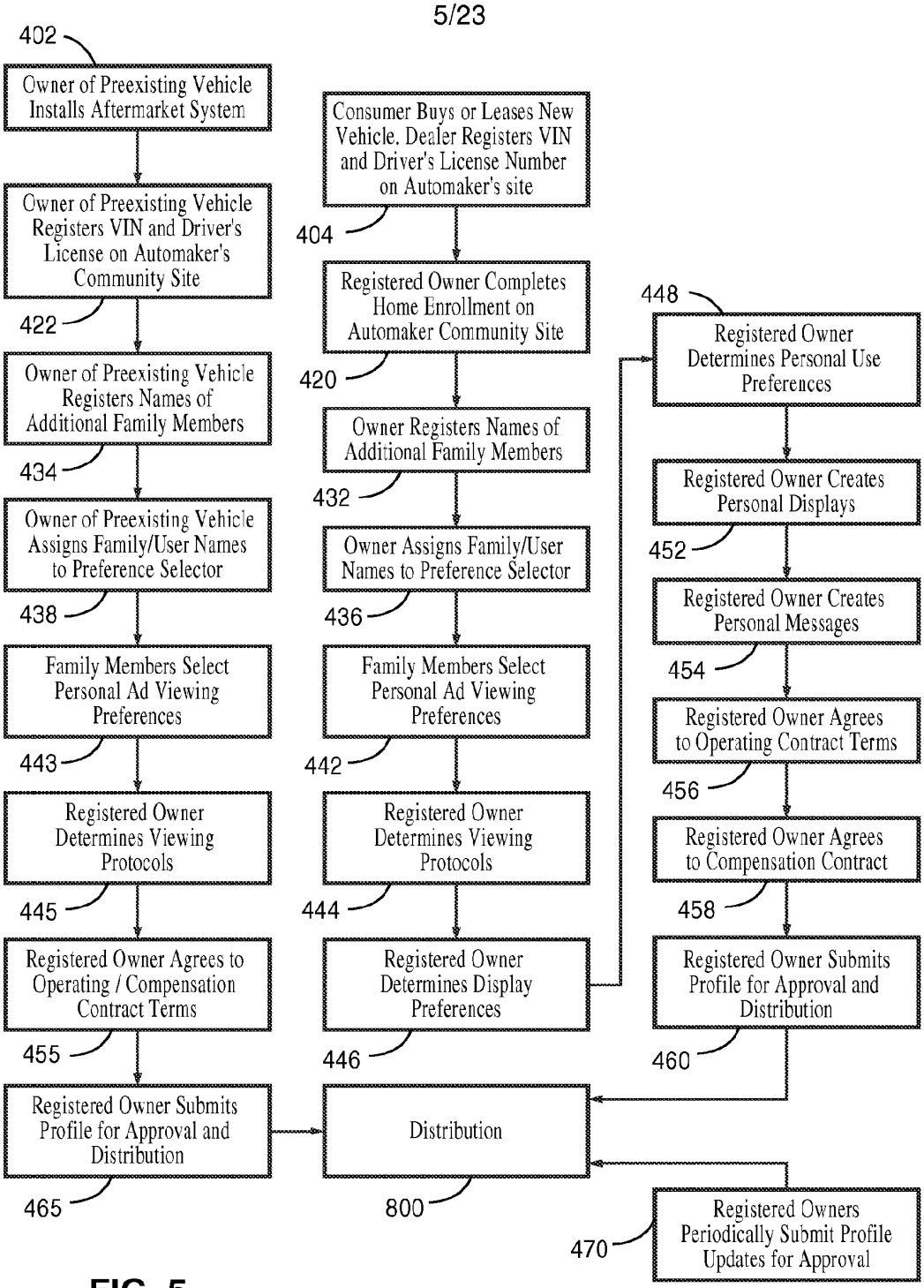

402
Owner of Preexisting Vehicle Installs Aftermarket System
Owner of Preexisting Vehicle Registers VIN and Driver's License on Automaker's Community Site
422
Owner of Preexisting Vehicle Registers Names of Additional Family Members
434
Owner of Preexisting Vehicle Assigns Family/User Names to Preference 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

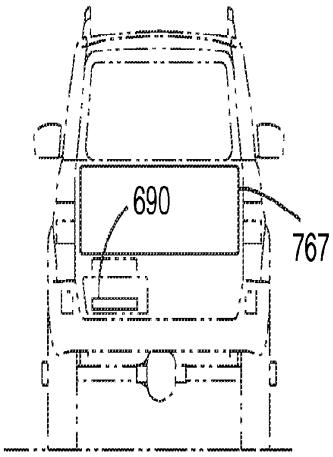


FIG. 7

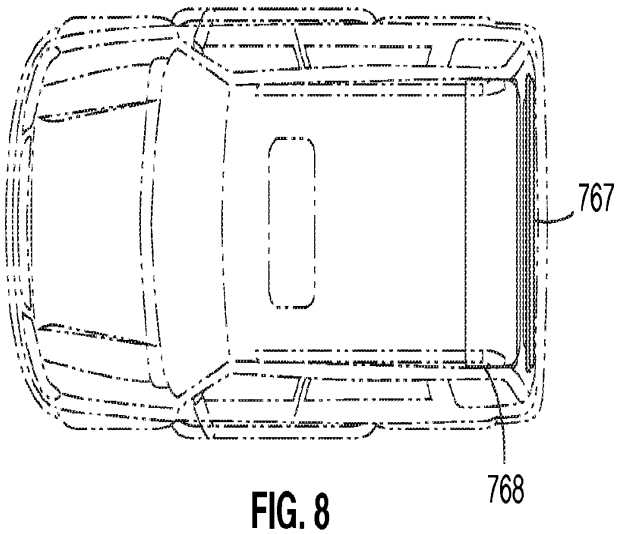


FIG. 8

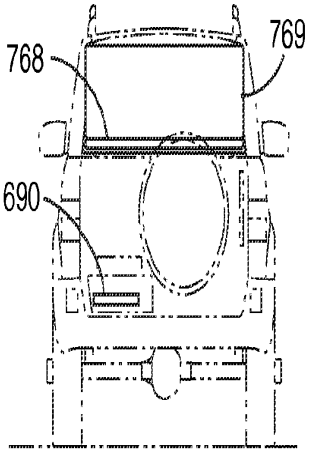


FIG. 9

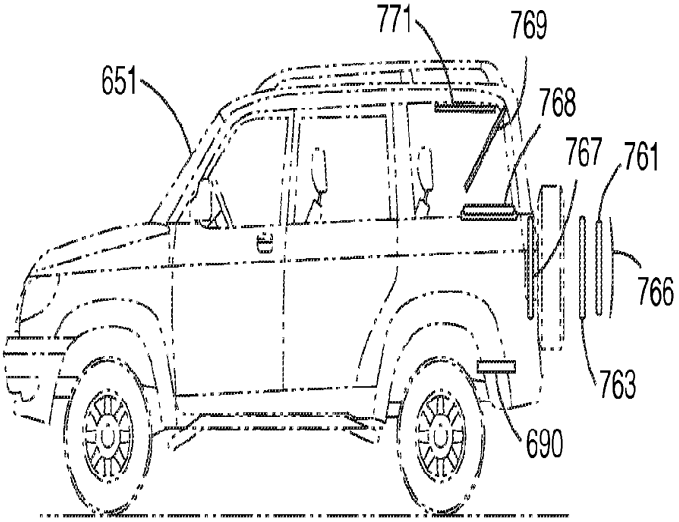


FIG. 10

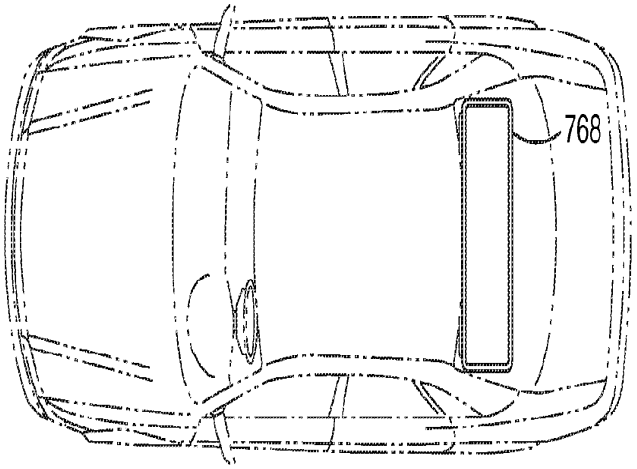


FIG. 12

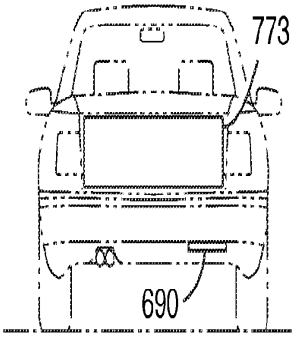


FIG. 11

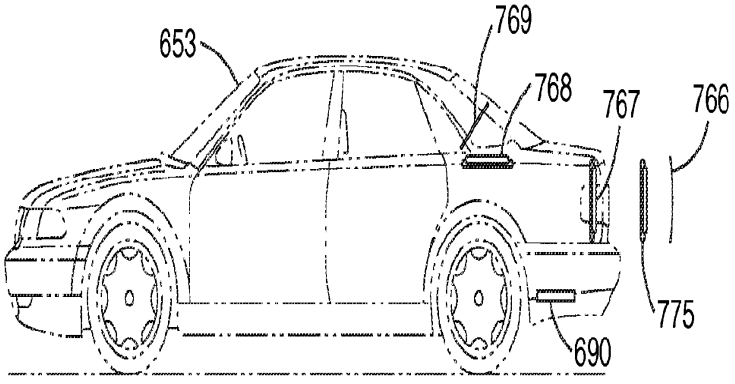


FIG. 13

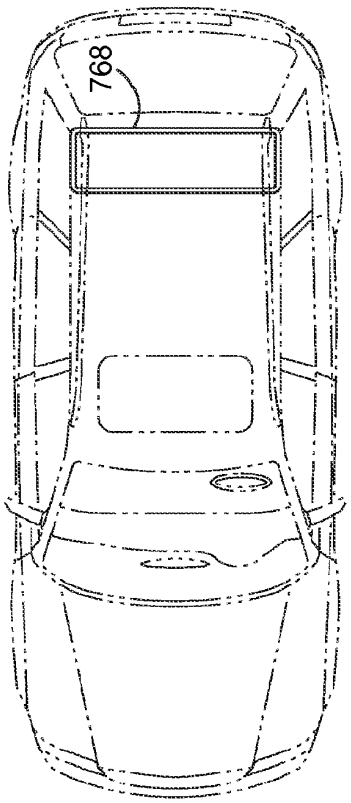


FIG. 15

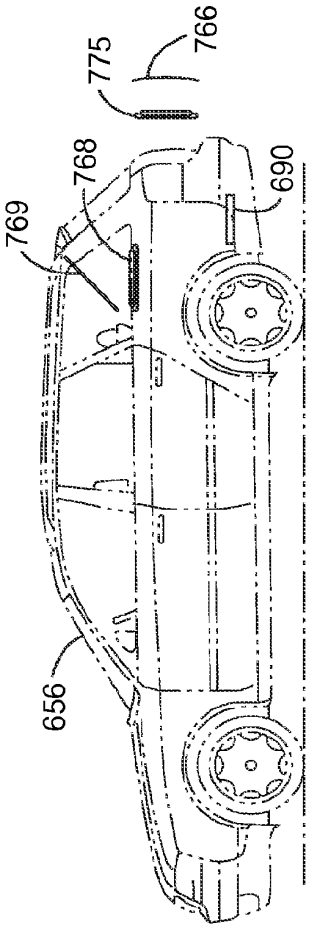


FIG. 16

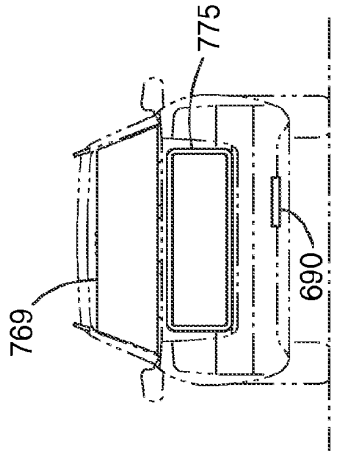


FIG. 14

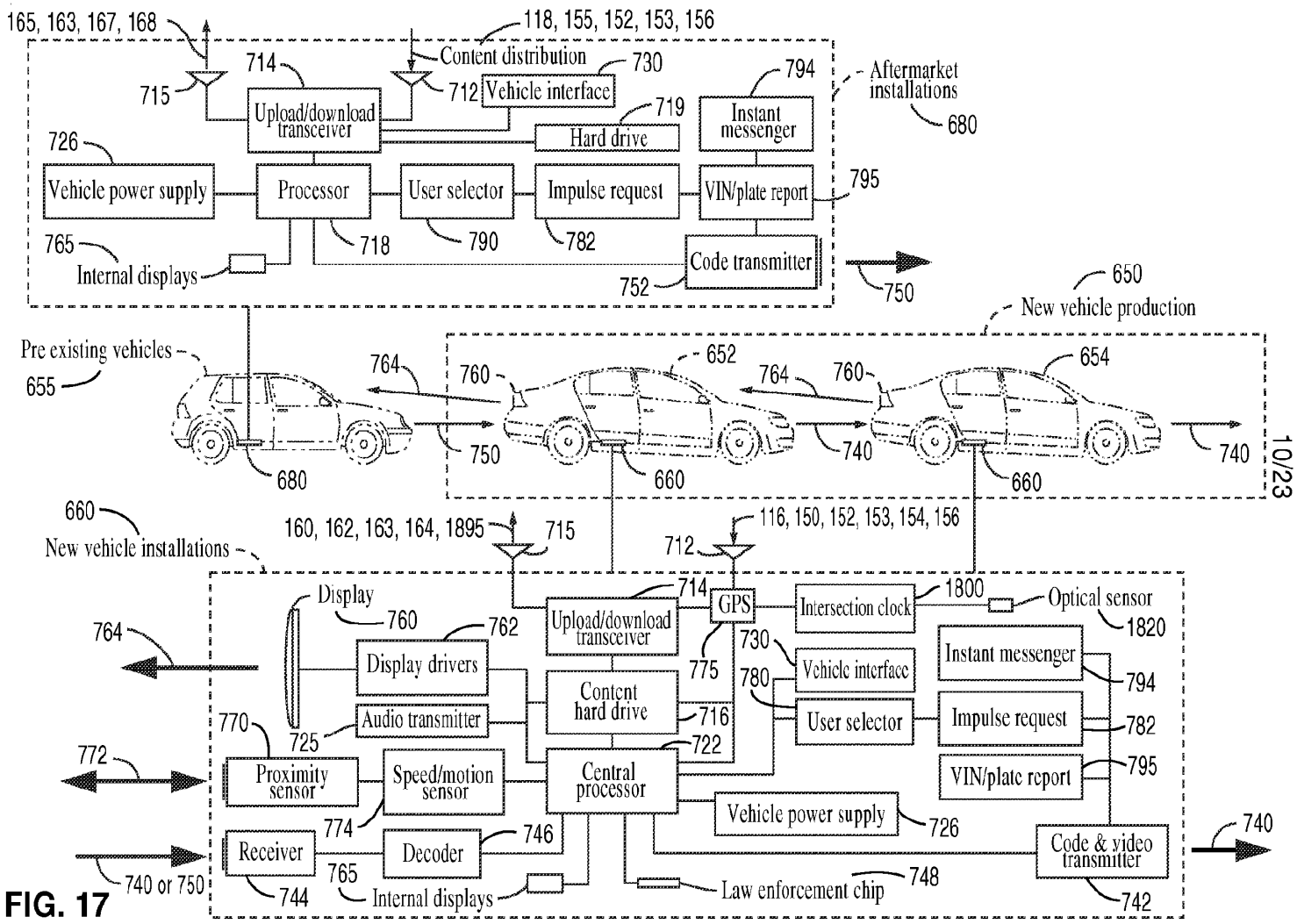

165, 163, 167, 168
118, 155, 152, 153, 156
Content distribution
714
730
794
715
712
Vehicle interface
Upload/download transceiver
719
Instant messenger
Aftermarket installations
680
Hard drive
726
Vehicle power supply
Processor
User selector
Impulse request
VIN/plate report
795
765
718
790
782
Internal displays
Code transmitter
752
750
650
New vehicle production
Pre existing vehicles
655
764
760
652
654
750
740
680
660
660
660
New vehicle installations
160, 162, 163, 164, 1895
715
712
116, 150, 152, 153, 154, 156
Display
760
762
714
GPS
1800
Optical sensor
1820
Intersection clock
764
Display drivers
Upload/download transceiver
730
Vehicle interface
Instant messenger
794
775
780
Content hard drive
716
User selector
Impulse request
782
770
725
Audio transmitter
722
772
Proximity sensor
Speed/motion sensor
Central processor
VIN/plate report
795
Vehicle power supply
726
740
774
746
Receiver
Decoder
Code & video transmitter
765
748
740 or 750
744
Internal displays
Law enforcement chip
742

FIG. 17

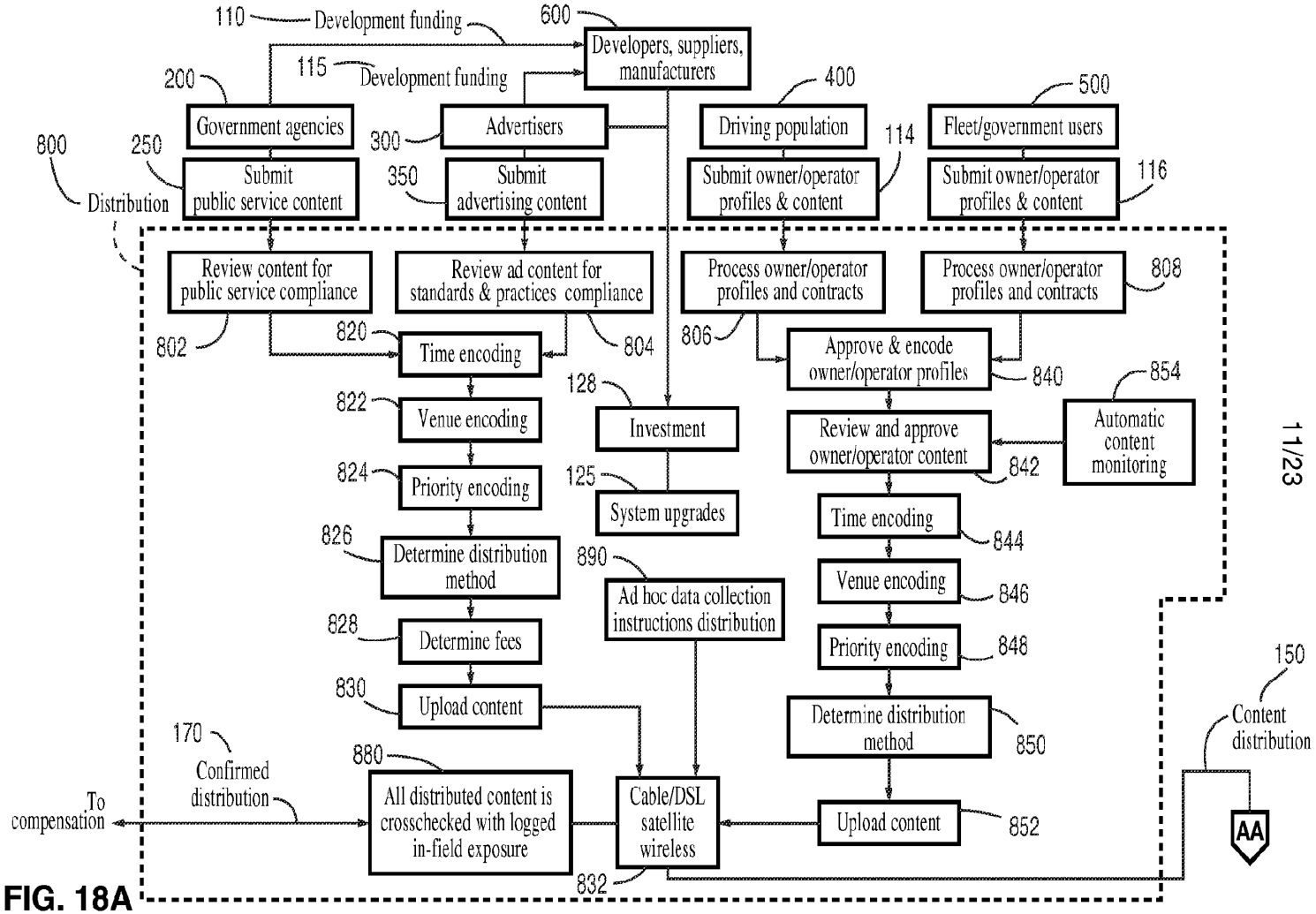

110
Development funding
600
Developers, suppliers, manufacturers
115
Development funding
200
400
500
Government agencies
Advertisers
Driving population
Fleet/government users
800
250
300
114
Distribution
Submit public service content
350
Submit advertising content
Submit owner/operator profiles & content
116
Submit owner/operator profiles & content
Review content for public service compliance
Review ad content for standards & practices compliance
Process owner/operator profiles and contracts
Process owner/operator profiles and contracts
808
802
820
804
806
Time encoding
Approve & encode owner/operator profiles
840
854
128
822
Venue encoding
Investment
Review and approve owner/operator content
Automatic content monitoring
842
824
125
Priority encoding
System upgrades
Time encoding
844
826
890
Determine distribution method
Ad hoc data collection instructions distribution
Venue encoding
846
828
Determine fees
Priority encoding
848
150
830
Upload content
Determine distribution method
850
Content distribution
170
880
Confirmed distribution
To compensation
All distributed content is crosschecked with logged in-field exposure
Cable/DSL satellite wireless
Upload content
852
AA
832

FIG. 18A

11/23

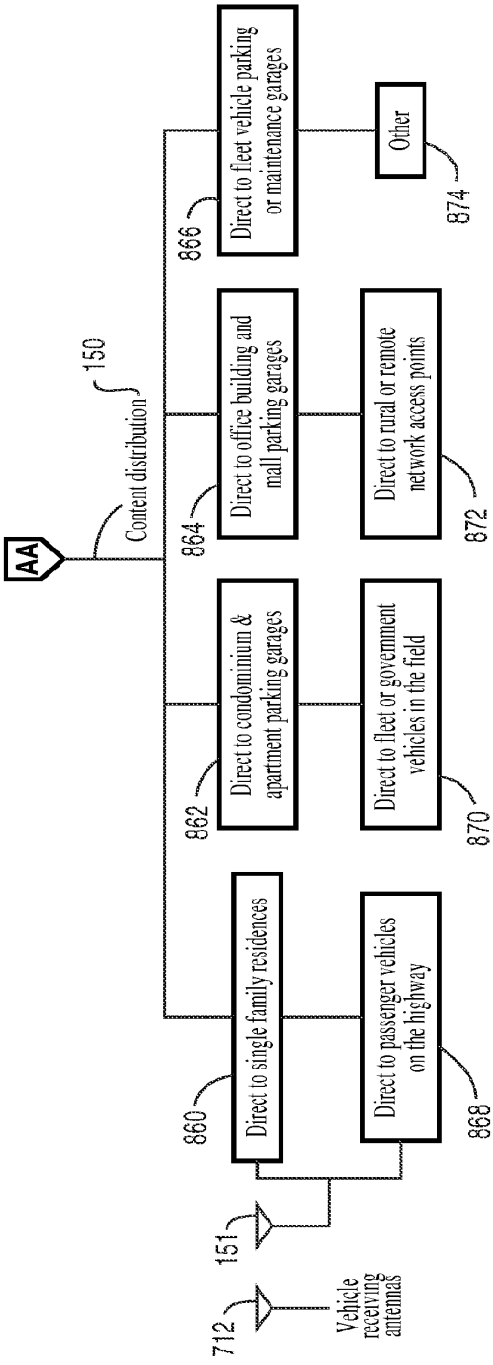


FIG. 18B

IPR2023-01353 Page 01331

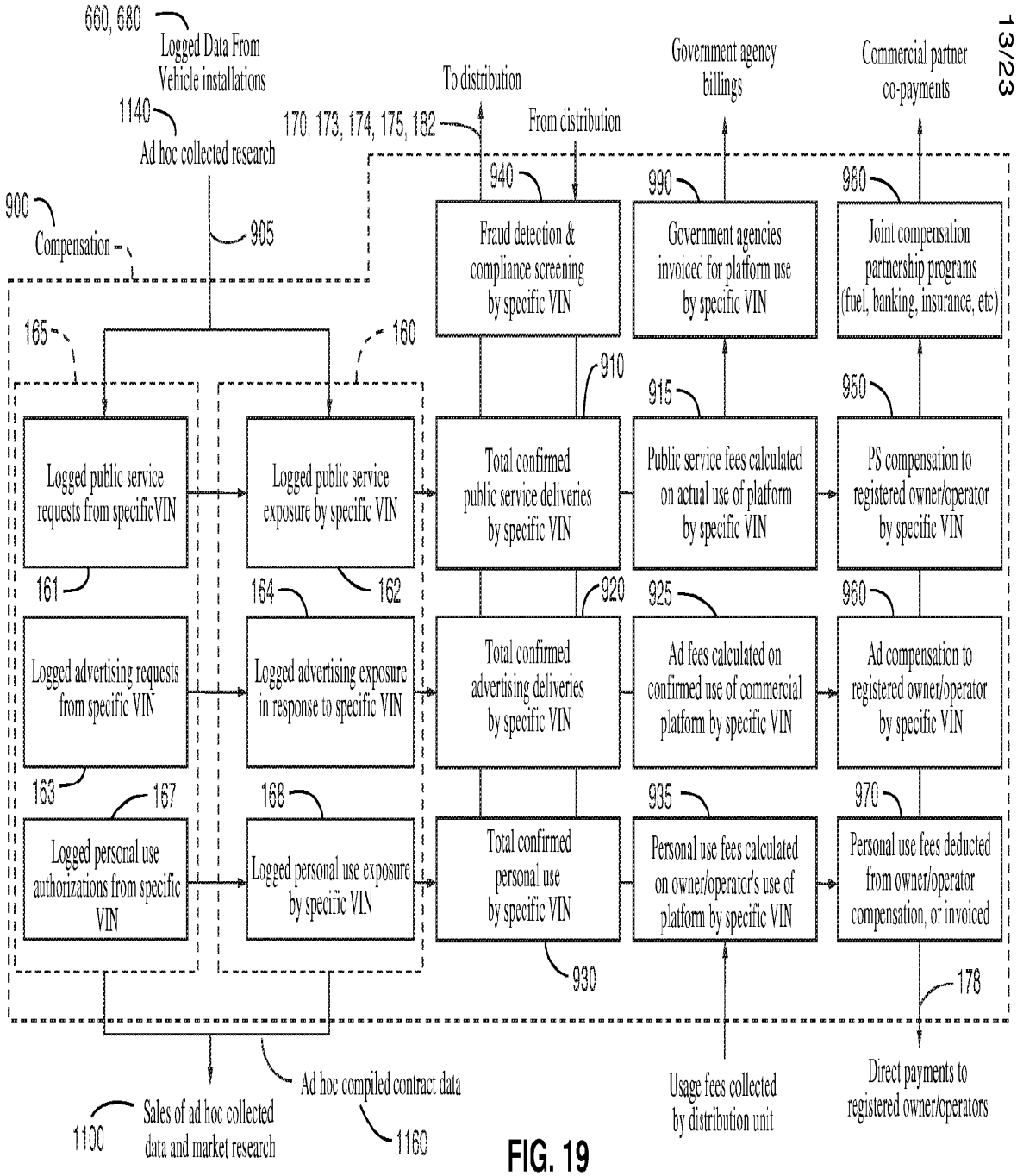

660, 680
Logged Data From Vehicle installations
1140
Ad hoc collected research
900
Compensation
905
165
160
170, 173, 174, 175, 182
To distribution
From distribution
Government agency billings
Commercial partner co-payments
940
Fraud detection & compliance screening by specific VIN
990
Government agencies invoiced for platform use by specific VIN
980
Joint compensation partnership programs (fuel, banking, insurance, etc)
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
164
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
1100
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

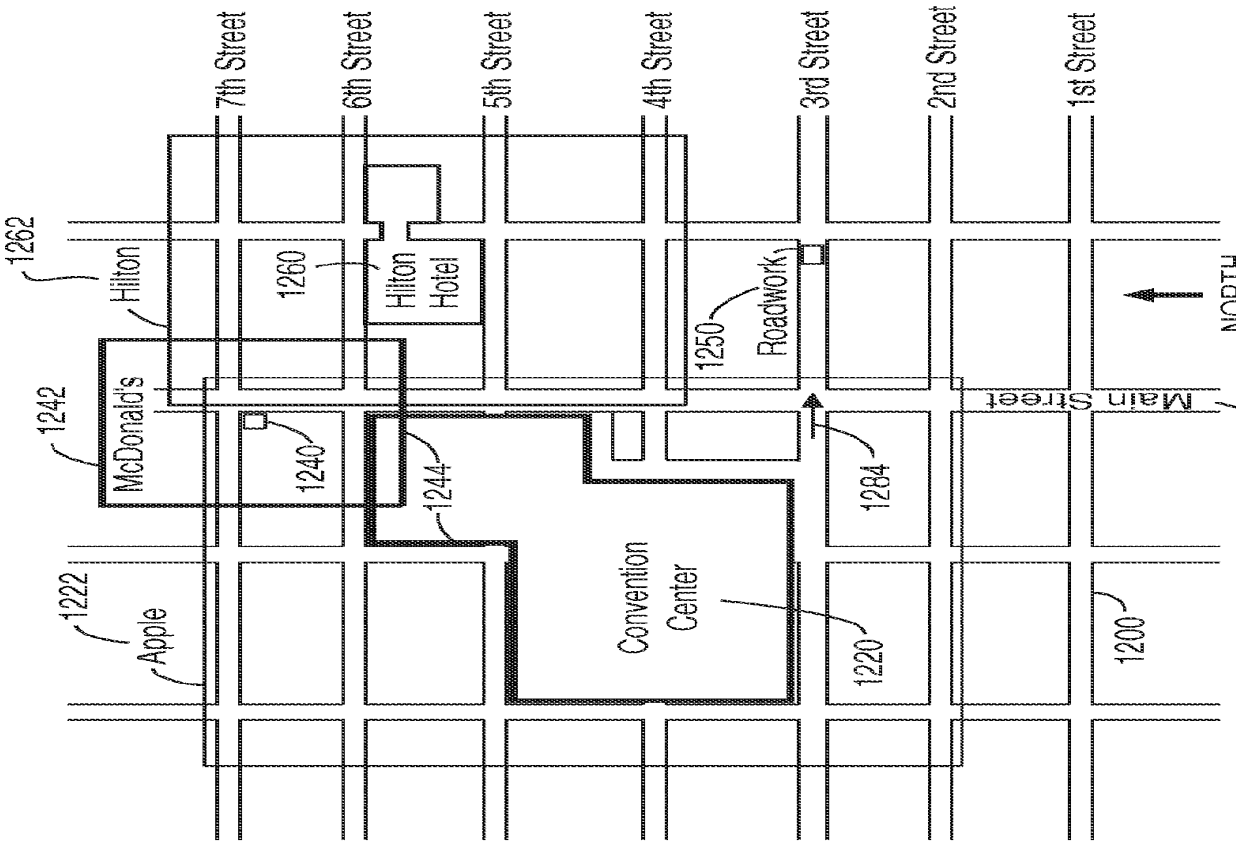


FIG. 28

IPR2023-01353 Page 01335

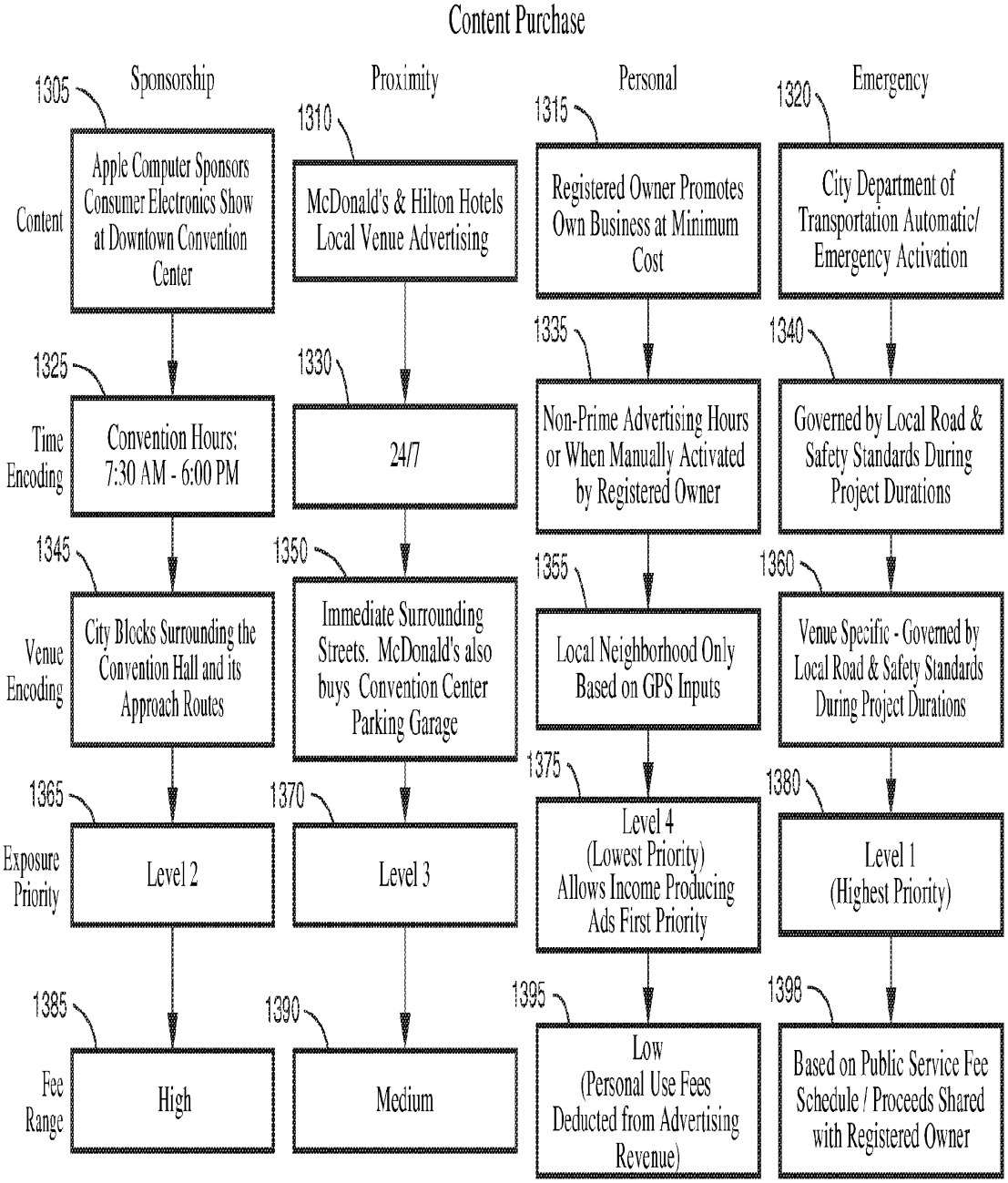

Content Purchase
Sponsorship
Proximity
Personal
Emergency
1305
1310
1315
1320
Content
Apple Computer Sponsors Consumer Electronics Show at Downtown Convention Center
McDonald's & Hilton Hotels Local Venue Advertising
Registered Owner Promotes Own Business at Minimum Cost
City Department of Transportation 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

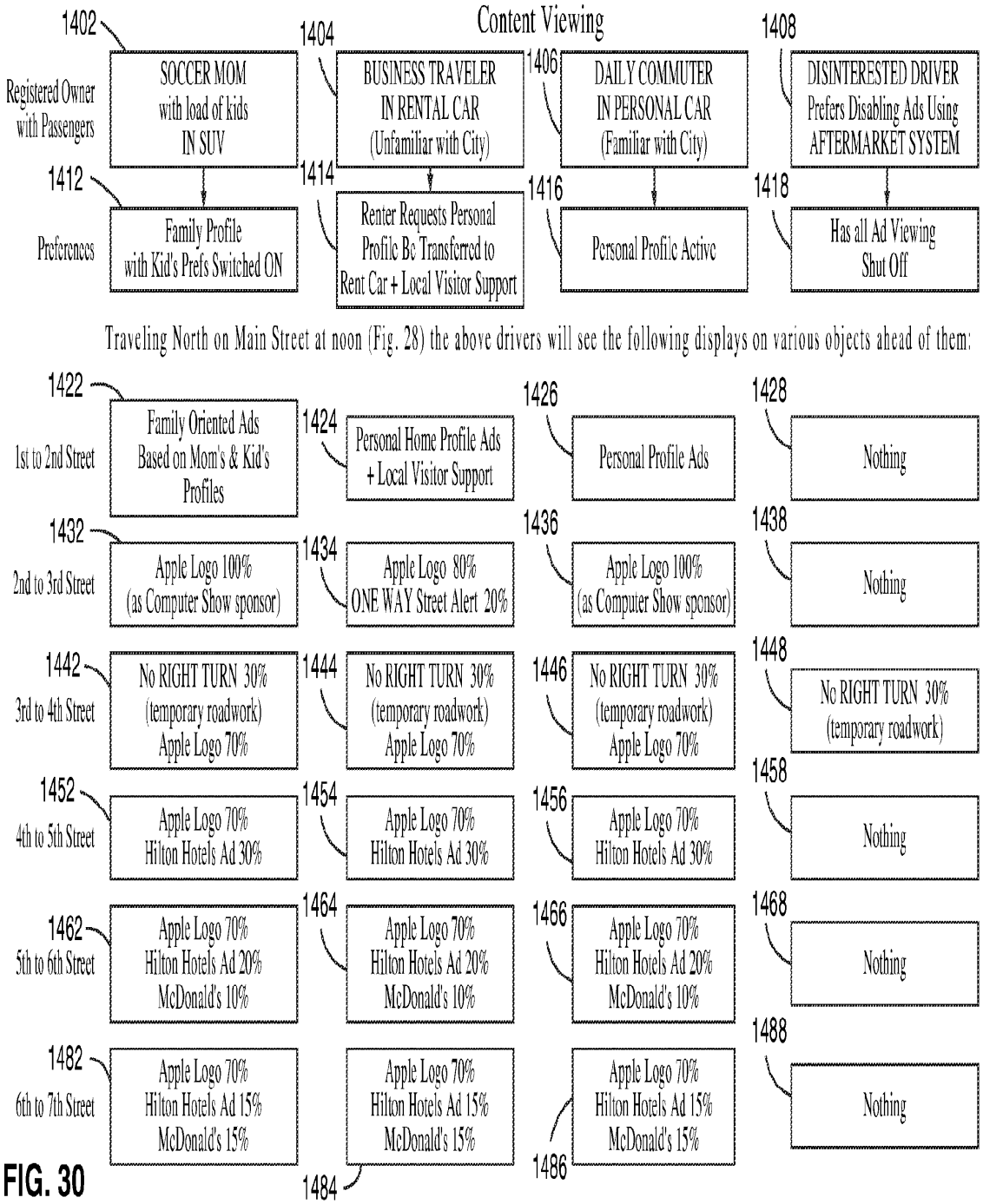

Content Viewing
1402
1404
1406
1408
Registered Owner with Passengers
SOCCER MOM with load of kids IN SUV
BUSINESS TRAVELER IN RENTAL CAR (Unfamiliar with City)
DAILY COMMUTER IN PERSONAL CAR (Familiar with City)
DISINTERESTED DRIVER Prefers Disabling Ads Using AFTERMARKET SYSTEM
1412
1414
1416
1418
Preferences
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

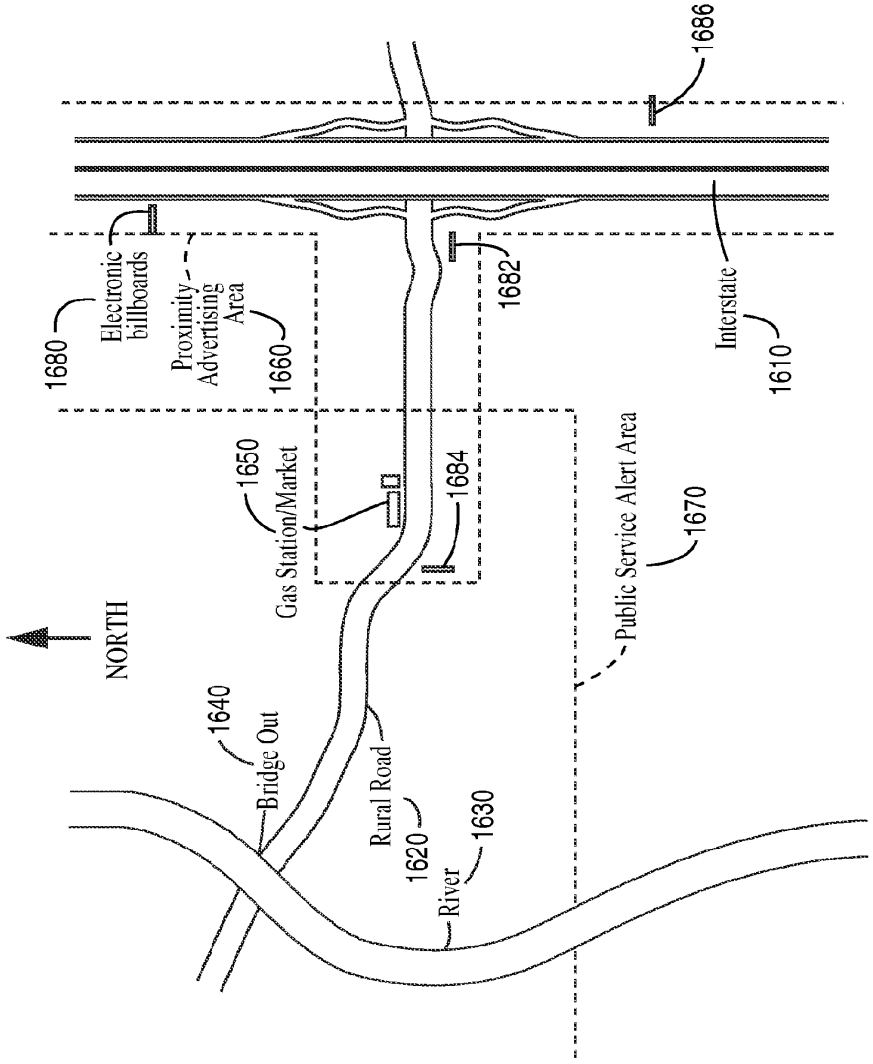


FIG. 32

IPR2023-01353 Page 01338

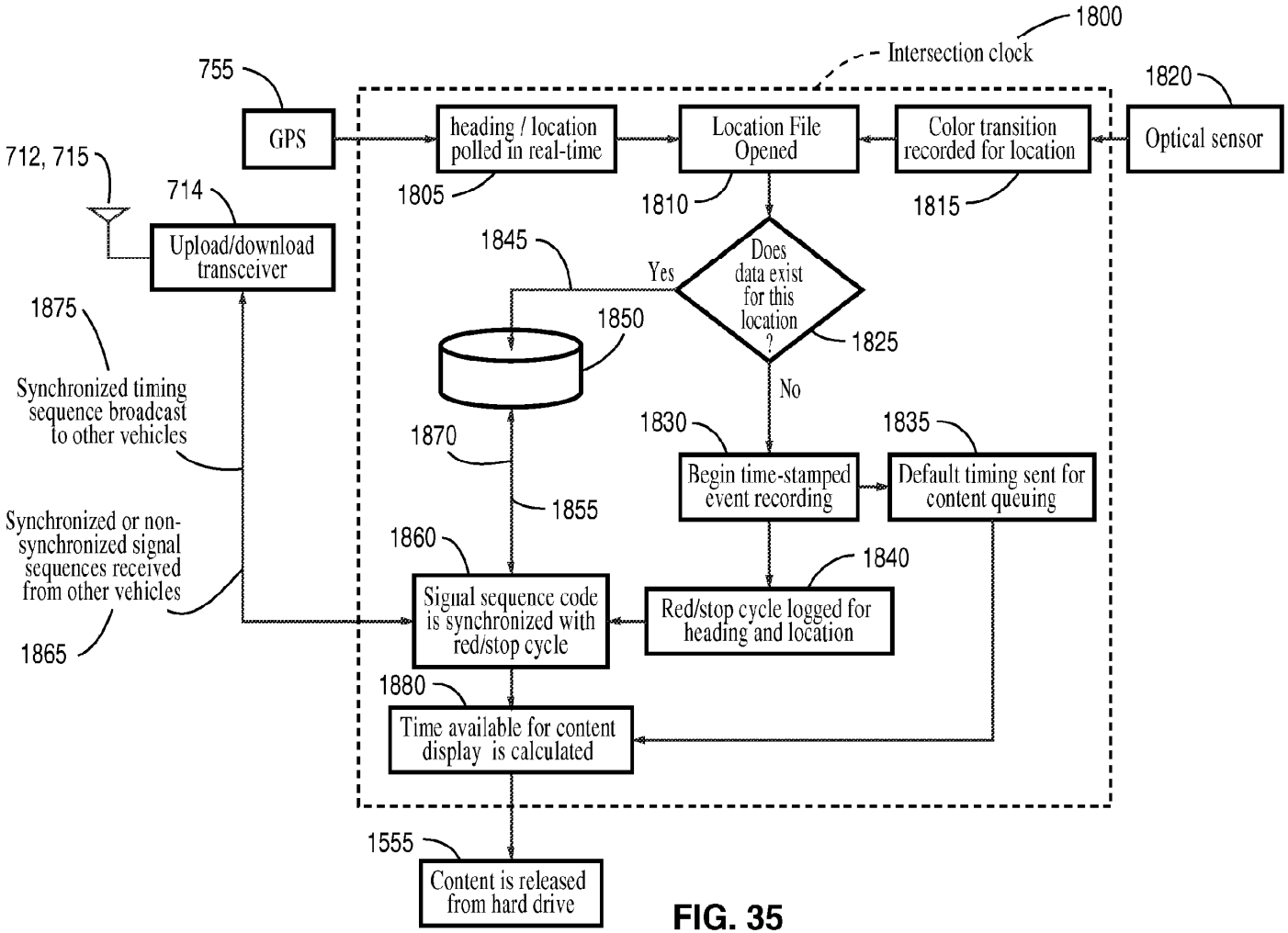

1800
Intersection clock
755
GPS
heading / location polled in real-time
1805
Location File Opened
1810
Color transition recorded for location
1815
1820
Optical sensor
712, 715
714
Upload/download transceiver
1845
Yes
Does data exist for this location ?
1825
No
1850
1875
Synchronized timing sequence broadcast to other vehicles
1870
1855
1830
Begin time-stamped event recording
1835
Default timing sent for content queuing
Synchronized or non-synchronized signal sequences received from other vehicles
1865
1860
Signal sequence code is synchronized with red/stop cycle
1840
Red/stop cycle logged for heading and location
1880
Time available for content display is calculated
1555
Content is released from hard drive

FIG. 35

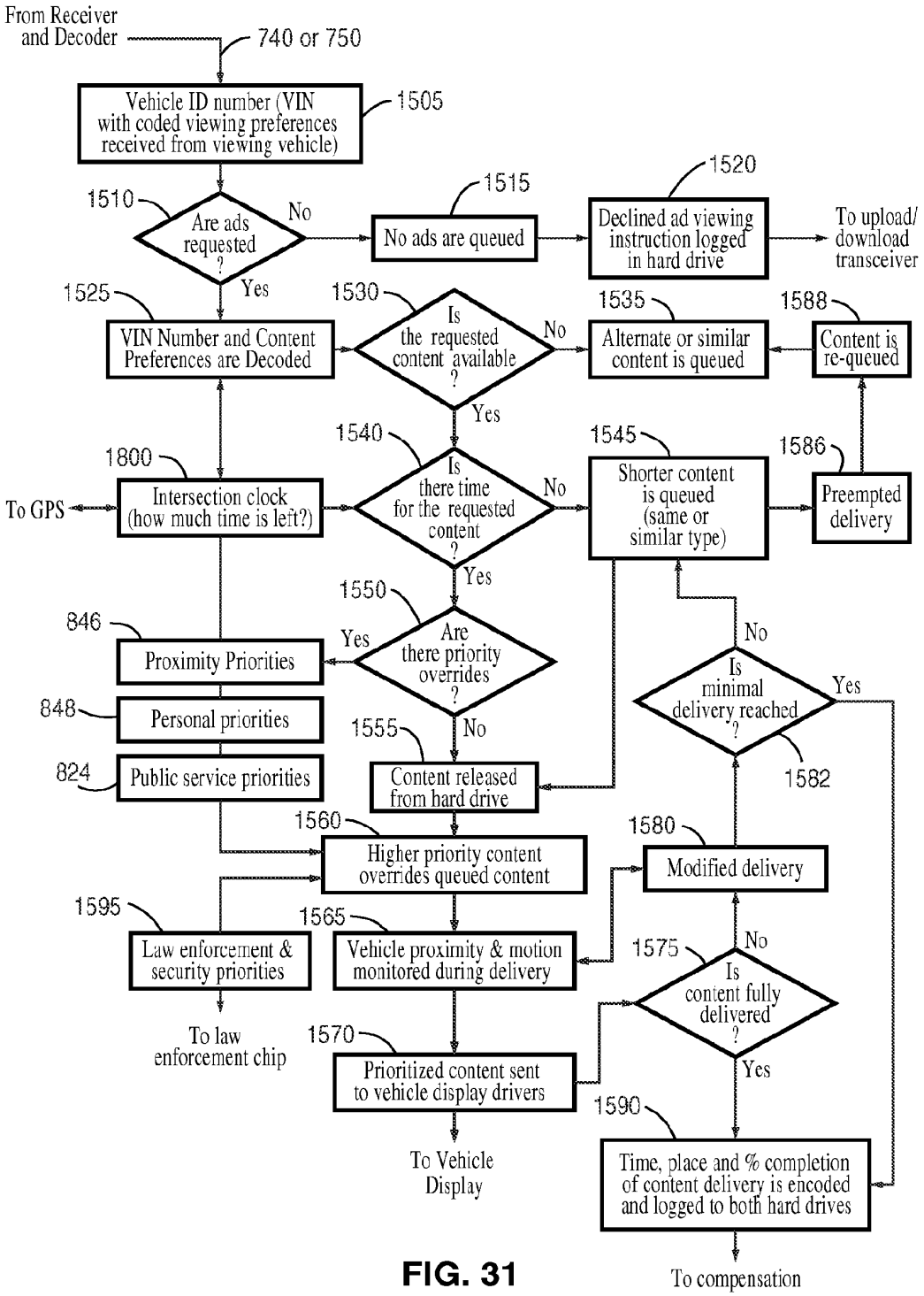

From Receiver and Decoder
740 or 750
Vehicle ID number (VIN with coded viewing preferences received from viewing vehicle)
1505
1510
Are ads requested ?
No
1515
No ads are queued
1520
Declined ad viewing instruction logged in hard drive
To upload/ download transceiver
Yes
1525
VIN Number and Content Preferences 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

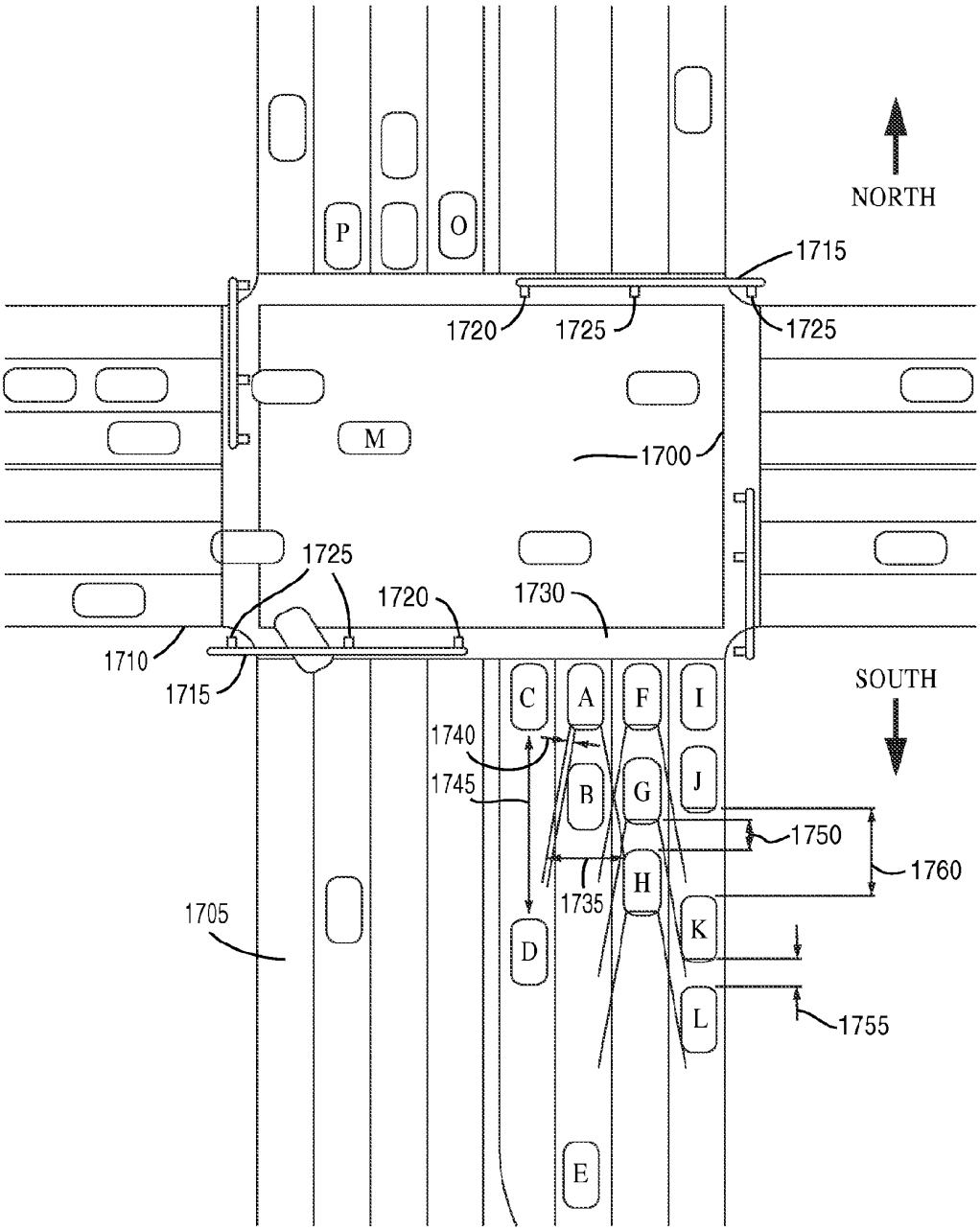

NORTH
SOUTH
P
O
M
1715
1720
1725
1725
1700
1725
1720
1730
1710
1715
C
A
F
I
1740
1745
B
G
J
1750
1760
H
1735
K
1705
D
L
1755
E

FIG. 33

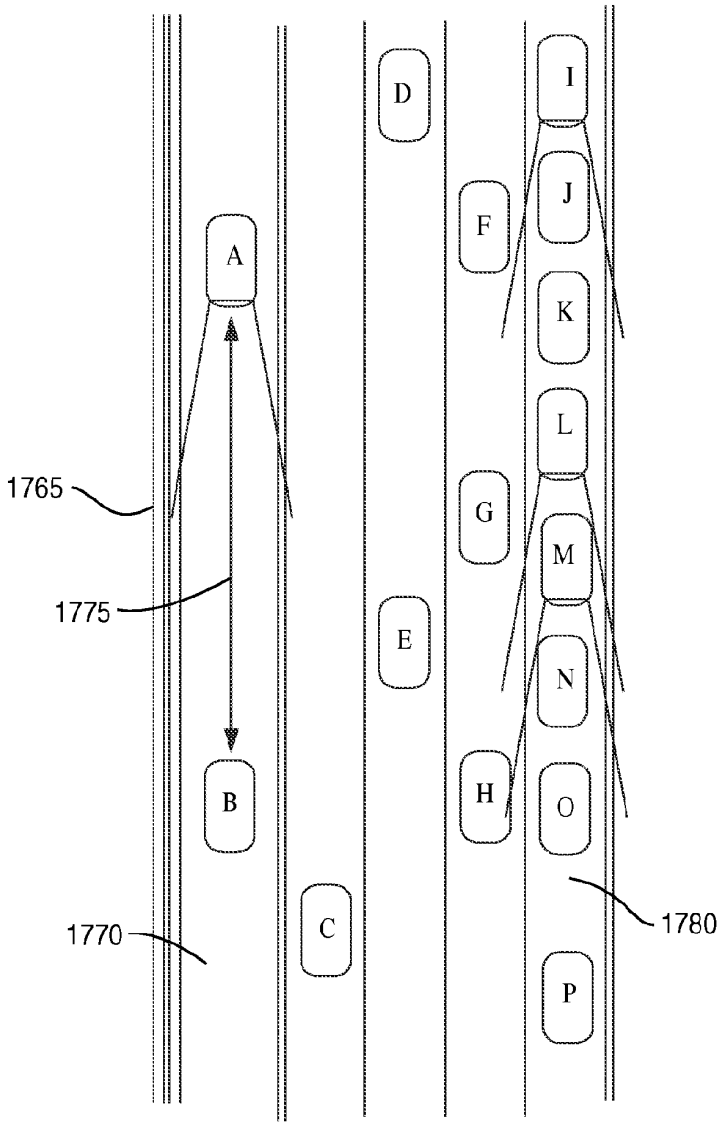


FIG. 34

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

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 007742.00023	Date of mailing *(day/month/year)* 7 November 2013 (07-11-2013)
International application No. PCT/US2013/057502	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 30 August 2013 (30-08-2013)

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.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Facsimile 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 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. 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. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   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 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.

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 VINCI, Rossana Tel: +31 (0)70 340-2812

NOV 12 2013

Form PCT/ISA/220 (July 2010)

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.
007742.00023		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/057502	30 August 2013 (30-08-2013)	22 October 2012 (22-10-2012)
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. 1
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

NOV 12 2013

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/057502

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05) paragraphs [0011], [0017] - [0019]	1-20
X	US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01) column 3, line 38 - column 4, line 32; claims 1-11	1-20

☐ 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 October 2013	07/11/2013

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	Veen, Gerardus

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/057502

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1677484 A2	05-07-2006	CN 1777179 A	24-05-2006
		EP 1677484 A2	05-07-2006
		JP 4914052 B2	11-04-2012
		JP 2006146891 A	08-06-2006
		KR 20060056231 A	24-05-2006
		US 2006129808 A1	15-06-2006
		US 2009172774 A1	02-07-2009
US 6226372 B1	01-05-2001	AU 1950301 A	18-06-2001
		US 6226372 B1	01-05-2001
		US 2001014150 A1	16-08-2001
		WO 0143343 A1	14-06-2001

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/US2013/057502	30.08.2013	22.10.2012

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.

NOV 1 2 2013

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

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 43bis.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 filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

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 in 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	1-20
Inventive step (iS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1 The following documents are referred to:

D1 EP 1 677 484 A2 (MICROSOFT CORP [US]) 5 July 2006 (2006-07-05)

D2 US 6 226 372 B1 (BEEBE TODD [US] ET AL) 1 May 2001 (2001-05-01)

2 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

2.1 In the words of independent claim 1, D1 discloses:

'A method (column 4, line 13), comprising:

at each of one or more packet security gateways (c.4, l.16, 'enforcement engine') associated with a security policy management server (c.4, l.15, 'policy server'):

receiving a dynamic security policy from the security policy management server (c.4, l.16-19);

receiving packets associated with a network protected by each respective packet security gateway; and

performing, on a packet by packet basis, at least one of multiple packet transformation functions specified by the dynamic security policy on the packets (c.4, l.19-20, 'enforcing the security policies'), wherein performing the at least one of multiple packet transformation functions specified by the dynamic security policy on the packets comprises performing at least one packet transformation function other than forwarding or dropping the packets (c.5, l.30-36)'.

Claim 1 is thus not new (Art. 33(2) PCT).

2.2 The same reasoning applies, mutatis mutandis, to independent claims 19 and 20 which are, therefore, also not new.

2.3 Dependent claims 2-18 do not contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding citations in the search report.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

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 007742.00030	Date of mailing *(day/month/year)* 24 June 2014 (24-06-2014)
International application No. PCT/US2014/023286	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 11 March 2014 (11-03-2014)

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.

   Where? 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 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. 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. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   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 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.

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 ROTHENBüCHER, Anita Tel: +31 (0)70 340-9872

JUN 24 2014

BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2010)

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.
007742.00030		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2014/023286	11 March 2014 (11-03-2014)	12 March 2013 (12-03-2013)
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. 2
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] 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 24 2014
BANNER & WITCOFF LTD

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/023286

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 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03) paragraphs [03.7], [0008], [0025] - [0027]	1-20
X	US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12) paragraphs [0054] - [0055]	1-20

☐ 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
13 June 2014	24/06/2014

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	Veen, Gerardus

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/023286

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003123456 A1	03-07-2003	NONE	
US 2007083924 A1	12-04-2007	NONE	

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/US2014/023286	11.03.2014	12.03.2013

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.

JUN 24 2014
BANNER & WITCOFF LTD

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Veen, Gerardus Telephone No. +31 70 340-3811

Form PCT/ISA/237 (Cover Sheet) (July 2009)

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 43bis.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 filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

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 in 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	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

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

The following documents are referred to:

D1 US 2003/123456 A1 (DENZ PETER R [US] ET AL) 3 July 2003 (2003-07-03)

D2 US 2007/083924 A1 (LU HONGQIAN K [US]) 12 April 2007 (2007-04-12)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims 1-20 is not new.

1.1 Independent claim 1 (as far as it is clear, see **Item VIII**) defines a method for filtering a packet, the method having two stages:

1) in the first stage, a first operation ('operator') is performed upon the packet, based on a first header field value;

2) in the second stage, a second operation ('transformation') is performed upon the packet, based on a second header field value.

Moreover, these two steps are interrelated in the sense that the criteria, with which the second header field value is compared during the second stage, are determined during the first stage.

Such a method is also disclosed in D1 (see the passages cited in the search report).

Present claim 1 is thus not new according to Art. 33(2) PCT.

1.2 The same reasoning applies, mutatis mutandis, to independent claims 11 and 20 which are, therefore, also not new.

1.3 Dependent claims 2-10 and 12-19 do not appear to contain any features which, in combination with the features of the claims to which they refer, meet the requirements of the PCT in respect of novelty and inventive step, see D1, D2 and the corresponding references cited in the search report.

1.4 It is further noted that a reasoning based on D2 would lead to very similar conclusions.

Re Item VIII

Certain observations on the international application

2 Claims 1-20 do not meet the requirements of Article 6 PCT for, at least, the following reasons:

- in claim 1, the expressions 'header field' and 'application header field', and especially how they differ from each other, are not clear;

- a similar remark applies to the expressions 'operator' and 'packet transformation function', respectively.

Similar observations apply to independent claims 11 and 20.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

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 007742.00025	Date of mailing *(day/month/year)* 24 March 2014 (24-03-2014) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2013/072566	International filing date *(day/month/year)* 2 December 2013 (02-12-2013)
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.

   Where? 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 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. 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. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   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 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.

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 ROTHENBüCHER, Anita Tel: +31 (0)70 340-9872

RECEIVED
MAR 28 2014
BANNER & WITCOFF, LTD.

Form PCT/ISA/220 (July 2010)

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.
007742.00025		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2013/072566	2 December 2013 (02-12-2013)	11 January 2013 (11-01-2013)
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. 2
      [ ] as suggested by the applicant
      [X] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] 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 28 2014
BANNER & WITCOFF, LTD.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072566

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	EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21) abstract paragraph [0010] paragraph [0022] paragraph [0024] paragraph [0029] paragraph [0040] paragraph [0025] ----- -/--	1-24

[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
14 March 2014	24/03/2014

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	Oliveira, Joel

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072566

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19) abstract page 3, line 14 - line 28 page 4, line 10 - line 11 page 5, line 10 page 5, line 23 - line 32 page 7, line 2 - line 8 page 7, line 30 - page 8, line 8 page 11, line 20 - line 25	1-24
A	US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03) paragraph [0017] paragraph [0021] - paragraph [0022]	1-24

1

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

IPR2023-01353 Page 01363

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/072566

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1313290 A1	21-05-2003	AT 346446 T	15-12-2006
		DE 60216218 T2	08-03-2007
		EP 1313290 A1	21-05-2003
		US 2003097590 A1	22-05-2003
WO 2005046145 A1	19-05-2005	CN 1879361 A	13-12-2006
		EP 1683313 A1	26-07-2006
		JP 4323523 B2	02-09-2009
		JP 2007534219 A	22-11-2007
		US 2005111434 A1	26-05-2005
		WO 2005046145 A1	19-05-2005
US 2011055916 A1	03-03-2011	AU 2010297968 A1	22-03-2012
		EP 2471218 A2	04-07-2012
		US 2011055916 A1	03-03-2011
		US 2014007216 A1	02-01-2014
		WO 2011038420 A2	31-03-2011

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/US2013/072566	02.12.2013	11.01.2013

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 28 2014

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
BANNER & WITCOFF, LTD.
Oliveira, Joel
Telephone No. +31 70 340-3334

Form PCT/ISA/237 (Cover Sheet) (July 2009)

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 43bis.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 filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

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 in 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, 3, 6-9, 11, 13, 14, 17-22, 24
	No:	Claims	1, 4, 5, 10, 12, 15, 16, 23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21)

D2 WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19)

D3 US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims **1, 12 and 23** is not new.

1.1 **D1** discloses a method comprising, at a network protection device **(abstract)**:

receiving a first rule set **(paragraph [0010], column3 lines 4-7)**;

receiving a second rule set **(paragraph [0010], column3 lines 4-7)**;

preprocessing the first rule set and the second rule set **(considered to be implicit from paragraphs [0010], [0013], [0040]: when a new set of rules is made available it must be made certain that they do not contain errors which could stop the filtering of the firewall)**;

configuring the network protection device to process packets in accordance with the first rule set **(paragraph [0010], column3 lines 13-18)**;

receiving packets **(column 6 lines 23-26)**;

processing a first portion of the packets in accordance with the first rule set **(paragraphs [0010], [0020])**;

reconfiguring the network protection device to process packets in accordance with the second rule set **(paragraphs [0010], [0024])**; and

processing a second portion of the packets in accordance with the second rule set **(paragraphs [0010], [0024])**.

1.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus and computer-readable media claims **12 and 23**, which therefore are also considered not new.

1.3 Dependent claims **2-11, 13-22 and 24** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (for claims **4, 5, 10, 15, 16**) and/or inventive step (for claims **2, 3, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 24**) see passages cited in the Search Report.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 313 290 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.05.2003 Bulletin 2003/21

(51) Int Cl.7: **H04L 29/06**

(21) Application number: **02102581.2**

(22) Date of filing: **14.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **19.11.2001 US 988356**

(71) Applicant: **Stonesoft Corporation**
00210 Helsinki (FI)

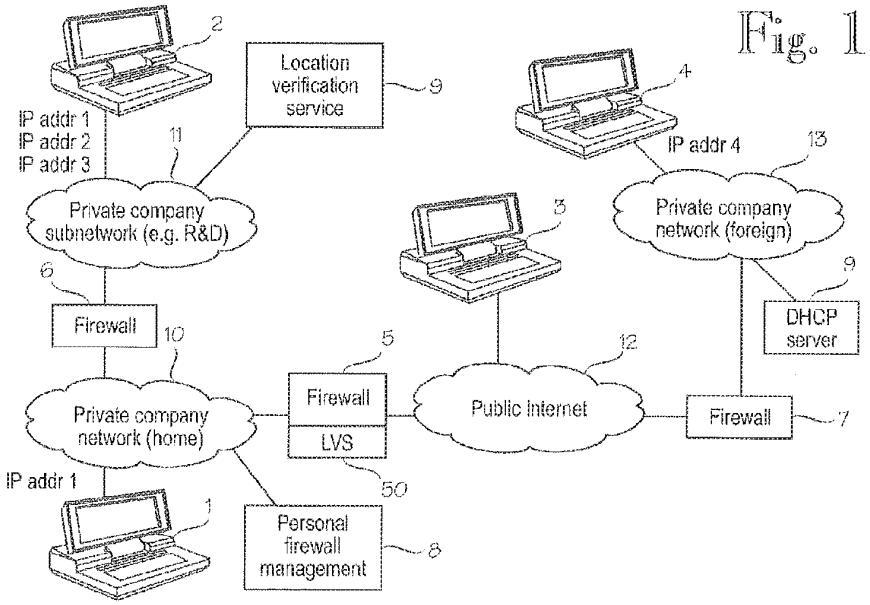
(72) Inventor: **Syvänne, Tuomo**
Fin-01450, Vantaa (FI)

(74) Representative: **Äkräs, Tapio Juhani**
Kolster Oy Ab,P.O. Box 148,
Iso Roobertinkatu 23
00121 Helsinki (FI)

(54) A personal firewall with location dependent functionality

(57) A computer device is provided with a local security mechanism, a personal firewall, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to a home network. The personal firewall is provided with different sets of security rules for the home network and foreign networks. The personal firewall is arranged to detect its current location, i.e. determine to which network it is connected to at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location.

Fig. 1



EP 1 313 290 A1

Printed by Jouve, 75001 PARIS (FR)

Description

Field of the invention

[0001] The present invention relates to network security and, more particularly, to personal firewalls.

Background of the invention

[0002] Traditionally, a firewall is considered as a set of components forming a gateway between two or more networks. Thus, a firewall has been a gateway which operates at the same time as a connector and a separator between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to do the tasks assigned to it. It can be a router, a personal computer (PC), or any other device that can be used for such purposes. Although firewalls are mostly used to connect Local Area Networks (LANs), i.e. internal networks, to the Internet and to protect against attackers or undesired traffic in general, they may also be used to separate and connect different segments of internal network for security purposes. The advantages of having a firewall are numerous. A firewall secures the network and can be used as a tool for monitoring the traffic especially from the outside to the inside of the network guarded by a firewall. Because all traffic intended for the internal network must pass through the firewall, most of the network security actions and policies can be concentrated in this particular point. This is of course a cost and administrative advantage.

[0003] Nowadays, laptop computers and other portable computer devices are widely used. While outside the internal network, the laptop cannot make benefit of the protection provided by the conventional "gateway-type" firewall. Therefore, approaches to improve security of a client located in a foreign network (a public network or an internal network of a foreign organisation) have been proposed. These approaches are based on protecting the laptop itself by means of a local security mechanism, called a personal firewall herein, installed in the laptop (in addition to or instead of a firewall in an internal network, which protects the computers connected to the internal network). The personal firewall may be implemented as software installed in the computer device, or as a separate electronic device connected to the computer device.

[0004] European patent application EP 0 952 715 discloses a firewall security device connected to an external communication port of a computer device. The incoming communications stream to the computer device from e.g. public networks is passed through the firewall security device. The firewall device applies standard security measures, thereby protecting the computer device.

[0005] There is a particular need for such protection by means of a personal firewall if the laptop is allowed to have a remote access, e.g. make a VPN (Virtual Private Network) connection to company network while being connected to a foreign network. In order to improve security of the VPN connections, one prior art solution is to enforce a protection level of a laptop, when a VPN tunnel to a company network is created. This means for example that, during a VPN connection, the IP address forwarding is not allowed, or that any connection attempts to the laptop are denied.

[0006] Clearly this is not enough, since the laptop must be protected as soon as it is connected to a foreign network, not only during a VPN connection. The laptops are often used by non-technical people, which increases the risk of overlooking security aspects. Laptops contain sensitive material, such as customer emails. If a laptop is unprotected, when connected to a foreign network, even for a short period of time, there is a risk of getting infected by a hostile application. Such application can be activated later, when the laptop is connected to an internal network and offer inside help for attacks.

[0007] Thus, there is a need to protect the laptop by means of a personal firewall always when the laptop is connected to a foreign network. However, when the laptop is connected to a company internal network, such personal firewall may unduly prevent some essential traffic. For example, the personal firewall should allow use of a laptop at home (internal) network and access to all services, such as disk-share. In a home network even non-IP protocols are sometimes used. Therefore, it is not feasible to have a personal firewall running at all times, at least not with the same configuration, since the protection needs in an internal network are different from those in a foreign network.

[0008] Some of the current solutions allow changing the set of rules used in the personal firewall, that is, they allow the user of the laptop to use different rule sets when connected to the internal network and when connected to a foreign network. However this is a manual operation. Since manual action is required, there is a high risk that operation is not done. Risk is even higher if the end user does not fully understand the need of a firewall.

Summary of the Invention

[0009] An object of the invention is to improve the security and flexibility of a personal firewall. The object is achieved by the invention disclosed in the attached independent claims. Preferred embodiments are disclosed in the attached dependent claims.

[0010] A computer device which can be connected to a home network (such as an internal network of a company or other organisation where the user is employed) and to a foreign network (such as a public network or an internal network of a foreign organisation) is provided with a local security mechanism, called a personal fire-

EPNSDOCID: <EP 1313290A1_I_>

IPR2023-01353 Page 01370

wall herein, for protecting the computer device from attacks from a foreign network, in addition to or instead of a firewall in the internal network which protects the computer when connected to the internal network. The personal firewall is provided with different sets of security rules, at least one set of rules for the home network and at least one set of rules for foreign networks. In its simplest form, the set of rules for the home network contains no restrictions for the communication or use of service in the home network. The personal firewall is arranged to detect its current location, i.e. to determine the network to which it is connected at each particular moment. The personal firewall activates one of the given sets of security rules according to the detected current location of the computer device, i.e. the personal firewall automatically uses the security rules predefined for the network to which the computer device is connected at each particular moment. Upon detecting a change in the location, the personal firewall immediately adapts to use security rules predefined for the new location. A benefit of the invention is that the protection of a personal firewall is always enabled at the correct level, depending on the current location. On the other hand, when the computer device is located in the home network, a lower level of protection, or no protection at all, can be automatically provided by the personal firewall, so that the communication and services are not unduly restricted in the home network. Thus, the automated location-dependent management of different sets of rules offers optimal protection in different networks, while not unduly restricting operation in the home network.

[0011] The current location of the computer device is preferably determined on the basis of a currently used IP address of the computer device. This is based on the common practice that a computer device has a different IP address, either a fixed address or a dynamic address, in different networks. The IP address can thereby be utilized for identifying the current network and the location of the computer device.

[0012] However, there are situations where the IP address fails to indicate current location of the computer device. Therefore, in an embodiment of the invention, the current location determined on the basis of the current IP address of the computer device is verified by carrying out an additional location verification procedure with a predetermined network element. In a still further embodiment of the invention, availability of said predetermined network element related to the current IP address is checked. The predetermined network element is such that it responses only if the computer device is located in the network in which it is assumed to be on the basis of the current IP address. If the predetermined network element responses and identifies itself properly, the current location determined based on the current IP address is considered to be verified. Otherwise the computer device determines that the current IP address fails to indicate current location of the computer device. The additional verification process makes it even possible to automatically create a secured tunnel, such as a VPN tunnel to a home network even if the computer device uses the same IP address in the current location as in the internal (home) network. The present invention offers benefits even with stand alone personal firewalls wherein the security rules can be defined locally by the user, although the use of these rules is automated and location-dependent. However, more advantages are achieved when the basic invention is used with a central management of personal firewalls.

[0013] According to an aspect of the invention, security rules are defined, updated and distributed centrally by a centralized rule-based server. Especially the updating of the rules is challenging, because the rule updates must be applied as soon as possible, and therefore the process of updating rules in the personal firewalls must be automated. Updating of rules by push method from the centralized rule base server is not a sufficient option in this case. Use of DHCP (Dynamic Host Configuration Protocol), frequent travelling and the fact that at times the laptop may not be connected to any network makes it next to impossible for the centralized management to initiate contacts with the personal firewalls in the computer devices, because there is no way for the centralized management to know the IP address the computer device is using at a given moment. Therefore, according to an aspect of the invention, the personal firewall is configured to periodically query the availability of updated security rules from the centralized management. The queries should only be made, while the computer device is located in the home network, or optionally, when the computer device has a remote access (e.g. VPN connection) to the home network while being located in a foreign network. In other words, also the updating process is dependent on the current location of the computer device in a similar manner as the selection of the active rules, and similar methods can be utilized for determining the current location.

[0014] According to another aspect of the invention, log files containing information of a status and usage of resources of the computer device are handled in a centralized management location. This enables personnel aware of security aspects to verify whether there have been any attacks against the computer device or not. To that end, the personal firewall sends the log files to the central management, such as to a centralized log server, when the computer device is located in the home network. However, when the computer device is disconnected from the home network, the log files are collected and stored locally in the firewall. In order to enable central handling of the log files, the personal firewall transfers the collected log files to the central log server when such is available. This is performed automatically, whenever the computer device is located in, or optionally, connected to the home network. Again, the handling of the log files in the personal firewall is automated and location dependent in a way similar to the selection of active rules, and similar methods can be used for de-

BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01371

termining the current location of the computer device.

[0015] The present invention allows use of a computer device in a home (internal) network and access to all services, such as disc-share, and even use of non-IP protocols, which are often denied in foreign networks.

Brief description of the drawings

[0016] Preferred embodiments of the invention will now be described with reference to the attached drawings, in which

Figure 1 is a schematic block diagram of an exemplary network configuration where the present invention can be applied;
Figure 2 shows an exemplary protocol stack of a computer device containing a personal firewall according to the present invention,
Figure 3 illustrates exemplary selection rules and a security rule basis, and the association therebetween,
Figure 4 is a flow diagram illustrating a location-dependent rule base selection according to an embodiment of the invention;
Figures 5 and 6 are flow diagrams illustrating the location verification procedure according to an embodiment of the invention;
Figures 7 and 8 are flow diagrams illustrating the rule base updating according to an embodiment of the invention; and
Figure 9 is a flow diagram illustrating the handling of log files according to an embodiment of the invention.

Preferred embodiments of the invention

[0017] The present invention can be applied in personal firewalls in any computer device which can be moved and connected to different networks. Typically such devices are portable computer devices, such as laptop computers, PDAs, communicators, smart phones, intelligent telecommunication devices, etc. In the following illustrative embodiments of the invention, a laptop computer is used as an example of suitable computer devices.

[0018] Figure 1 shows a schematic block diagram of an exemplary network configuration. The configuration is shown only to facilitate the understanding and description of the present invention. The present invention is not intended to be restricted to any particular network configuration. Further, in order to improve clarity, only network elements which are somehow involved with the present invention are shown in Figure 1.

[0019] As illustrated in Figure 1, private local networks 10 and 13 are coupled to a public network, such as the Internet 12 via firewalls 5 and 7, respectively. Naturally, the coupling between the private networks and the public Internet 12 may include also routers and Internet service providers (ISPs not shown in Figure 1). As is well known in the art, private networks 10 and 13 may be, for example, company networks, such as local area networks (LANs) which connect users and resources, such as workstations, servers, printers and the like of the company. A private internal network may also consist of several sub-networks separated by internal firewalls. In the exemplary network configuration shown in Figure 1, the private company sub-network 11 is connected via a firewall 6 to the private local network 10. Such a sub-network 11 may be, for example, a dedicated network for a specific department of the organisation, such as the research and development (R&D) department which must have a restrictive access and higher protection level compared with other part of the company network. Sub-networks of the company, such as the local networks of organisation headquarters and branch offices may be interconnected by secure connections, such as virtual private network (VPN).

[0020] As already described above, the firewalls 5, 6 and 7 are gateways which operate at the same time as connectors and separators between the networks in a sense that the firewall keeps track of the traffic that passes through it from one network to another and restricts connections and packets that are defined as unwanted by the administrator of the system. Physically a firewall is a machine with appropriate software to perform the task assigned to it. It can be a router, a personal computer (PC), or whatever that can be used for such purposes.

[0021] However, the firewalls between the networks, or the implementations thereof, are not relevant to the present invention.

[0022] The present invention relates to protecting of the computer device, e.g. laptop itself, by means of a local security mechanism, called a personal firewall herein, installed on the laptop in addition to or instead of a firewall in a private network. The personal firewall may be implemented as software installed and run in the computer device, which is a preferred embodiment, or as a separate electronic device connected to the computer device. In Figure 1, the laptops 1, 2, 3 and 4 illustrate laptops provided with a personal firewall.

[0023] Figure 2 illustrates the basic principle of a personal firewall installed in a laptop. Physical and network layers 200 refer to all protocols and physical connections required for transferring protocol data units (PDUs) of the upper layers. The upper layers 200 include applications and any transmission protocols employed, such as Internet protocol (IP) transmission control protocol (TCP), NetPEUI, IPX, etc. Basically the personal firewall protection layer 201 operates in a manner analogue to a firewall between networks. More particularly, the personal firewall protection layer 201 operates at the same time as a connector and a separator between the underlying layers and the upper layer in a sense that the personal firewall keeps track of the traffic that passes through it from underlying layers to the upper layers, and

EPODOC: <EP_____1313290A1_I_>

IPR2023-01353 Page 01372

vice versa, and restricts connections and packets that are defined as unwanted according to the security rules used. The personal firewall protection layer 201 is implemented or controlled by a personal firewall application 203 run in the laptop. In a preferred embodiment of the invention, the personal firewall application 203 carries out the location detection and the location-dependent functions described below, such as the selection of the active rule base according to the current location of the laptop. However, it should be appreciated that the present invention is not intended to be restricted to any specific practical implementation of the personal firewall.

[0024] In accordance with the principles of the present invention, the personal firewall has different sets of rules for the home network (such as the private company network 10) and foreign network, such as the public Internet 12, or the foreign private network 13, or a network of another department of the company. It is not relevant to the present invention what kind of security rules are applied, but some examples are given in Figure 3. For example, a rule base 301 for the foreign company network may list as allowed connections of protocols: hypertext transfer protocol (http), secured http (Https), domain name service (DNS), single message transfer protocol (SMTP) and a VPN connection with IPsec. In the preferred embodiment of the invention these rules are exclusive, in other words, other protocols and connections are denied and blocked by the personal firewall. For a default network, which may be the public Internet 12, the rule base 302 is similar to the rule base 301, except that the SMTP protocol is no longer allowed. For the home network 10, a rule base 300 is defined. The allowed protocols include, in addition to the http, https and the SMTP, also other transmission protocols, such as NetBEUI and IPX. The rule base 300 also allows a disc-share for predefined servers using NetBIOS. Other protocols and connections are denied. It is also possible that the rule base 300 allows all protocols and connections in the home network. Since the home network is protected by a company firewall, the use of a personal firewall in the home network may be regarded as unnecessary. However, the company firewall gives protection only against attacks from the outside of the home network, and the use of a personal firewall protection may be necessary for protecting against attacks from within the home network.

[0025] The different rule bases could be activated manually by a user. However, according to the basic principle of the present invention, the personal firewall automatically selects and activates the proper rule base according to the current location of the laptop.

[0026] Figure 4 is a flow diagram illustrating the selection of the rule base according to one embodiment of the present invention. The simplest way to determine the current location of the laptop is to do it on the basis of the currently used IP address only. This is possible in the cases where the laptop has a different IP address, either a fixed or a dynamic address, in different networks. As is well known in the art, a part of the IP address identifies the network, and can thus be used for detecting the current network of the laptop. The personal firewall may, for example, contain information on the IP address space of home network, and optionally, foreign networks, or a list of addresses available for the laptop in the home network.

[0027] When the current IP address of the laptop matches to a given address space or a list of addresses of the home network 10, for example, it can be assumed that the laptop is located in the home network 10 and the rule base 300 of the home network 10 is used. Thus, the current IP address is used as a selection rule for activating the rule base 300. However, there is some uncertainty in determining the location based on the current IP address only, and some approaches to overcome this problem are described with reference to further embodiments of the invention below.

[0028] Referring again to the generic flow diagram shown in Figure 4, the current IP address of the laptop is firstly determined in the step 401. The current IP address may be obtained simply by asking for it from the operating system of the laptop by means of using IP configuration routine. The current location of the laptop is monitored constantly, and therefore the personal firewall may be configured to periodically query the current IP address from the operating system. More preferably, the operating system of the laptop may be configured to inform any changes in the IP address to the personal firewall, and therefore a need for query the IP address time-to-time can be avoided. The step 401 may also include verification of the location determined based on the IP address by a verification procedure described below. In step 402, the personal firewall compares the current IP address with the current IP address stored in the personal firewall. If the IP address has not changed, the present active rule base can be maintained. However, if the IP address has changed, the personal firewall checks whether the new IP address matches to any IP address space or IP address belonging to one of the networks on the selection rule list in the personal firewall (step 403). If the new IP address does not belong to any of the networks on the selection rule list, the personal firewall considers the current network an unidentified network, and a default rule base 302 is selected (step 404). If the network cannot be identified and the default rule base must be used, it is normally assumed that the laptop is in a potentially hostile environment, most likely in the public Internet 12. Therefore, the default rule base is typically defined to provide the maximum protection needed. If the new IP address belongs to one of the networks defined on the selection rule list in step 403, it means that the network has been identified and a rule base linked to the identified network (or the corresponding selection rule) is selected and activated (step 405). In the simplest implementation, the selection rules include only the home network of the laptop and the cor-

BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01373

responding IP address space or list of addresses . If the current IP address belongs to the home network, the rule base 300 of the home network 10 is used. Otherwise the rule base 310 for foreign network or the default rule base 302 is used. In a more complicated implementation, there are selection rules (i.e. IP addresses and associated rule bases) also for at least one foreign network and/or different segments of the home network 10.

[0029] In the examples described above there are two or more rule bases which are enabled or disabled on the basis of the current location of the laptop. However, there are also alternative ways to implement different rule bases. One alternative is to provide only one rule base in which the rules are enabled and disabled in different combinations on the basis of the current location of the laptop.

[0030] As noted above, there are situations where the location (the current network) determined on the basis of the current IP address is uncertain, i.e. the IP address fails to indicate the current location of the laptop. If the IP address does not match the current network, use of the Internet protocol (IP) to attack against the laptop is not likely, and one may reason that in that case a personal firewall does not need to be used. However, there is still a possibility that there is an attack using other protocols, such NetBEUI or IPX. By detecting the situation where the IP address of the laptop is not an IP address of the current network, it is possible to block such protocols while in foreign networks. Further, NAT (network address translation) and private IP addresses are frequently used. This means that the same IP address is in use in several networks. In that case it is not enough to trust IP address information only when determining the location of the laptop. It is even possible that while being connected to a hostile network, the DHCP (dynamic host configuration protocol) gives familiar IP address to make it easier to attack the laptop. Basically, the DHCP enables individual computers on a network to connect to a DHCP server, such as the server 9 in Figure 1, and be assigned a dynamic IP address of the current network.

[0031] Thus, according to an aspect of the invention, in addition to the detection of location based on the current IP address described above, a further location verification procedure is carried out with a predetermined network element, which is preferably reachable only from the location to be verified. More generally, the network element is selected in such a way that it responses to the verification request only if the request originates from the location (i.e. the network) to be verified. Preferably, the specific network element is provided with a location verification service supporting the verification according to the invention. The verification procedure requires that the verification method be specified for the personal firewall, preferably at the same time as the different locations are specified. In other words, the methods to verify the location are specified for the personal firewall in the initial configuration, for example. It is also possible that the verification methods are updated or changed by means of the updating procedure described below, in a manner similar to other security rules.

[0032] A generic location verification procedure according to one embodiment of the invention is described with reference to Figures 5 and 6. Firstly, the current location is determined on the basis of the currently used IP address as described above (step 501). Next, the personal firewall selects a predetermined network element that should be available for verification from the determined current location (step 502). Then the personal firewall sends to the selected network element a request to send a response with some data proving the identity of the network element (step 503). Referring now to Figure 6, the verifying network element receives the verification request (step 601) from a personal firewall. Then, either always in response to the verification request or only if predetermined requirements are met, the network element sends the response with the required identity data to the personal firewall (step 602). Referring again to Figure 5, the personal firewall waits for a response (step 504), and if no response is received (preferably within a predetermined period of time), the location determined on the basis of the current IP address is rejected, and the location is determined to be unknown (step 505). In that case, a default location and an associated rule base, such as the rule base 302, can be used.

[0033] However, if the response is received from the network element in the step 504, the personal firewall verifies the identity of the network element on the basis of the received identity data, e.g. by comparing the received identity data with identity data stored in the personal firewall (step 506). If the verification of the identity is unsuccessful (step 507), the procedure proceeds to the step 505 described above. However, if the verification of the identity of the network element is successful, also the location of the laptop determined on the basis of the current IP address has been successfully verified and can be accepted.

[0034] Additionally, it is possible that one IP address is included in more than one selection rule in the personal firewall. In that case, if the verification of the laptop being located in a first network indicated by the current IP address fails, it is checked if the laptop is located in a second network indicated by the current IP address. There are various ways to implement the generic location verification procedure described above. The simplest way to implement the location verification service is to probe some known (known to the personal firewall) element. For example, it is possible to ask the MAC address of the known network element located in the home network and having a known IP address. The network element returns the MAC address in response, and if the AMC address is the one that it is assumed to be (e. g. matches with a MAC address stored in the personal firewall), it is verified that the laptop is located in the home network. If the MAC address is not the correct one, the laptop is determined to be outside the internal

EPNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01374

network.

[0035] One possible implementation is that the location verification service is implemented in such network element in an internal network which can be reached only from inside the internal network. For example, the firewall protecting the internal network, such as firewall 5 in Figure 1, may be configured to discard all connections from outside the internal network to this network element. If the personal firewall is able to reach this specific network element, it is verified that the personal firewall resides inside the internal network. Otherwise the personal firewall resides outside the internal network. There may be a plurality of such location verification services in a plurality of internal networks or sub-networks, and if the personal firewall cannot reach any of them, then it is assumed to be outside this plurality of internal networks or sub-networks.

[0036] The location verification service may be incorporated into the network firewall, such as the location verification service 50 in the firewall 5 in Figure 1. For example, verification requests only from the direction of the internal network (such as home network 10) may be responded by the location verification service 50. This implementation is rather straightforward, since the present firewalls are readily capable of detecting from which direction, that is, from which interface, a data packet is coming from.

[0037] In any case it is preferred that the personal firewall communicates with the location verification service by using some cryptographically strong method, such as public key encryption. For example SSL can be used. The certainty of the location verification can be further improved by setting the TTL (time-to-live) field in the location verification request to a relatively low value, so that the request is capable of reaching only a nearby location verification service. The TTL value is decremented each time the verification request passes through a router connecting different networks or network segments. If the TTL value is set to, for example, a zero value the verification request is not able to pass through a router to a different network or a network segment.

[0038] The use of additional location verification makes it even possible to automatically create a VPN tunnel to the home network even if the current location (a foreign network) is using the same IP address as in the internal network.

[0039] All the embodiments described above are effective both in standalone computers and in centrally managed computers. The central management of personal firewalls enables a uniform protection level in all computer devices using the private network. One feature of the central management is that preferably all of the personal firewalls have essentially similar security rules. It should also be possible to update these. It is preferable that rule updates are applied in the personal firewalls as soon as possible after they have been made in the central management. Because it is not sufficient to rely on the manual updating by the user, the process of updating the rules must be automated. However, distribution of the updated rules by a push transmission from the central management is not a sufficient option in a case where the personal firewalls can move from one network to another. Therefore, according to an aspect of the invention, the personal firewalls are arranged to periodically query the availability of updated rules from the central management. An updating procedure according to one embodiment of the invention is described with reference to Figures 7 and 8.

[0040] Firstly, a personal firewall measures a predetermined updating period, which can be any period of time, preferably one day or a few days (step 701). In step 702, the personal firewall checks whether the updating period has expired, and if not, the procedure returns to the step 701. When the updating period has expired, the personal firewall checks whether the current location of the laptop is in the home network (step 703) or in another subnetwork of the same company. The location determination is preferably based on the methods described above. If the current location is in the home network, the process proceeds directly to the step 705. However, if the current location is not in the home network, the personal firewall waits for the laptop to return to or establish a connection (e.g. VPN) to the home network (step 704), before proceeding to the step 705. In the step 705, the personal firewall sends a rule update query to the central management, such as the personal firewall management server 8 in Figure 1. Referring now to Figure 8, the personal firewall management 8 receives the rule update query from the personal firewall (step 801) and sends updated rules, if there are any, to the personal firewall (step 802). Referring again to Figure 7, the personal firewall checks whether the reply received from the personal firewall management 8 contains rule updatings (step 706), and if not, the process returns to the step 701 to measure the next updating period. However, if rule updatings have been received, the personal firewall updates the relevant rule bases stored in the laptop (step 707).

[0041] It is also preferable that the logs relating to the communication transactions of the laptop are handled in a central location. Since the laptops are frequently disconnected from the home network, logs must be collected locally. In order to enable central handling, the logs must be transferred to a central log server, such as the personal firewall management 8, when such is available. This should take place automatically when the computer device provided with a personal firewall is connected to the home network. Figure 9 illustrates log handling according to one embodiment of the invention.

[0042] Firstly, the personal firewall creates a log file each time the laptop is involved with a communication transaction, such as an Internet session (step 91). Then the personal firewall determines the current location of the laptop, preferably based on the location determining methods described above (steps 92 and 93). If the lo-

EPODOC: <EP_____1313290A1_I_>

IPR2023-01353 Page 01375

cation of the laptop is in the home network or in another subnetwork of the same company, the personal firewall sends the log file to the central log server 8 immediately (step 94). However, if the current location of the laptop is not in the home network, the process proceeds to the step 95, where the log file is stored locally. Similarly, a number of log files is collected locally while the laptop is disconnected from the home network. When the personal firewall next time detects that the computer device is relocated in the home network, it sends the collected log files to the central log server 8. Optionally, the personal firewall may also send the collected log files to the personal firewall management 8 when the laptop has established a (e.g. VPN) connection to the home network.

[0043] It is apparent for those skilled in the art that the illustrative embodiments described are only examples and that various modifications can be made within the scope and spirit of the invention as defined in the appended claims.

Claims

1. A method of controlling a personal firewall in a client computer, said method comprising

providing said personal firewall with at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and

automatically selecting one of said sets of security rules by said personal firewall according to said current location of said client computer.

2. A method according to claim 1, wherein

said step of providing comprises providing said client computer with said set of security rules in form of at least two rule bases,

said step of selecting comprises enabling one of said rule bases at a time according to the current location of said client computer.

3. A method according to claim 1, wherein

said step of providing comprises providing said client computer with said set of security rules in form of one rule base, and

said step of selecting comprises enabling and disabling rules in said one rule base in different combinations according to the current location of said client computer.

4. A method according to claim 1, wherein said step of monitoring comprises

storing in said client computer an IP address space of said home network,

comparing the current IP address of said client computer with said IP address space, and

if the current IP address of said client computer matches said IP address space, determining said personal firewall to be located in said home network.

5. A method according to any one of claims 1, 2 or 3, wherein said step of monitoring comprises

storing in said client computer a list of IP addresses of said home network,

comparing the current IP address of said client computer with said list of IP addresses, and

if the current IP address of said client computer matches one of said addresses on said list, determining said client computer to be located in said home network.

6. A method according to any one of claims 1, 2 or 3, comprising

verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element.

7. A method according to claim 6, wherein said step of verifying comprises

checking availability of said predetermined network element related to the current IP address, said predetermined network element responding only if said client computer is located in the network in which it is assumed to be on the basis of the current IP address,

verifying the current location determined based on said current IP address, if said predetermined network element responses with a specific identity data.

8. A method according to claim 7, wherein said specific identity data is a Media Access Control (MAC) address of said predetermined network element.

9. A method of managing a personal firewall in a client computer, comprising

storing in said personal firewall at least one set of security rules to be used when said client computer is connected to a home network of said client computer, and at least one set of security rules to be used when said client computer is connected to foreign networks,

storing updated sets of security rules, if any, in a centralized unit in said home network of said client computer,

configuring said personal firewall to periodically query the availability of said updated sets of security rules from said centralized rule base server

BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01376

when being located in said home network, or when having a remote access to said home network while being located in a foreign network, and

loading said updated sets of security rules from said centralized rule base server to said personal firewall in response to said query, if such updated sets of security rules are available.

10. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer, and

automatically activating said periodical query, when the current location of said client computer is in said home network.

11. A method according to claim 9, comprising

monitoring the current location of said client computer based on an Internet Protocol (IP) address currently used by said client computer,

sending log files to a centralized log server from said personal firewall, when the current location of said client computer is in said home network, said log files containing information on communication transactions in said client computer,

collecting log files locally at said personal firewall, when the current location of said client computer is not in said home network, and

transferring said locally collected log files from said personal firewall to said centralized log server, when said client computer is connected to said home network.

12. A computer terminal, comprising

a personal firewall provided with at least one set of security rules to be used when said computer terminal is connected to a home network of said computer terminal, and at least one set of security rules to be used when said computer terminal is connected to foreign networks,

said personal firewall having a mechanism monitoring the current location of said computer terminal based on an Internet Protocol (IP) address currently used by said computer terminal, and

said personal firewall having a mechanism automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer terminal.

13. A computer terminal according to claim 12, further comprising

a mechanism verifying the current location determined on the basis of the current IP address of said computer terminal by carrying out a location verification procedure with a predetermined network element.

14. A computer-readable medium, containing a computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

storing at least one set of security rules to be used when said computer device is connected to a home network of said computer device, and at least one set of security rules to be used when said computer device is connected to foreign networks,

monitoring the current location of said computer device based on an Internet Protocol (IP) address currently used by said computer device, and

automatically selecting one of said sets of security rules by said personal firewall according to said current location of said computer device.

15. A computer-readable medium according to claim 14, said personal firewall routine further comprising

verifying the current location determined on the basis of the current IP address of said client computer by carrying out a location verification procedure with a predetermined network element

16. A computer device, comprising a personal firewall routine configured to store security rules for a home network of said computer device, and for foreign networks,

periodically query the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

download said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

17. A computer device according to claim 16, said personal firewall routine being further configured to

activate said periodical query also when said computer device has a remote access to said home network while being located in a foreign network.

18. A computer device, comprising a personal firewall routine configured to

send log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collect log files locally in said computer device, when the current location of said client device is not in said home network,

transfer said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

19. A computer-readable medium, containing computer software which, when executed in a computer de-

EPNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01377

vice, causes the computer device to provide a personal firewall routine comprising

storing security rules for a home network of said computer device, and for foreign networks,

periodically querying the availability of updated security rules from a centralized rule base server in said home network of said computer device when said computer device is located in said home network, and

downloading said updated security rules from said centralized rule base server, if such updated security rules are available in said centralized rule base server.

20. A computer-readable medium, containing computer software which, when executed in a computer device, causes the computer device to provide a personal firewall routine comprising

sending log files to a centralized log server, when a current location of said computer device is in a home network of said computer device, said log files containing information on communication transactions in said computer device,

collecting log files locally in said computer device, when the current location of said client device is not in said home network,

transferring said locally collected log files to said centralized log server, when said computer device is reconnected to said home network.

21. A computer program comprising program code means for performing all the steps of any one of claims 1 to 11 when the program is run on a computer.

BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01378

Fig. 1

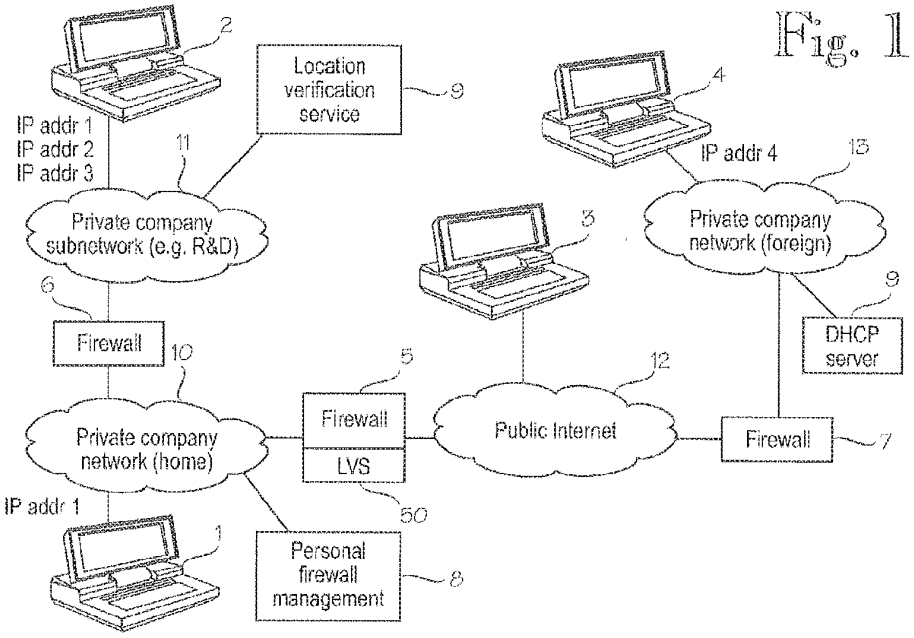


Fig. 2

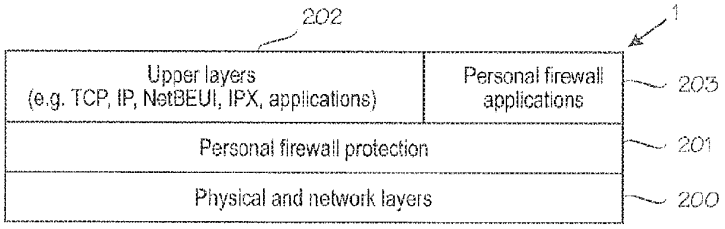
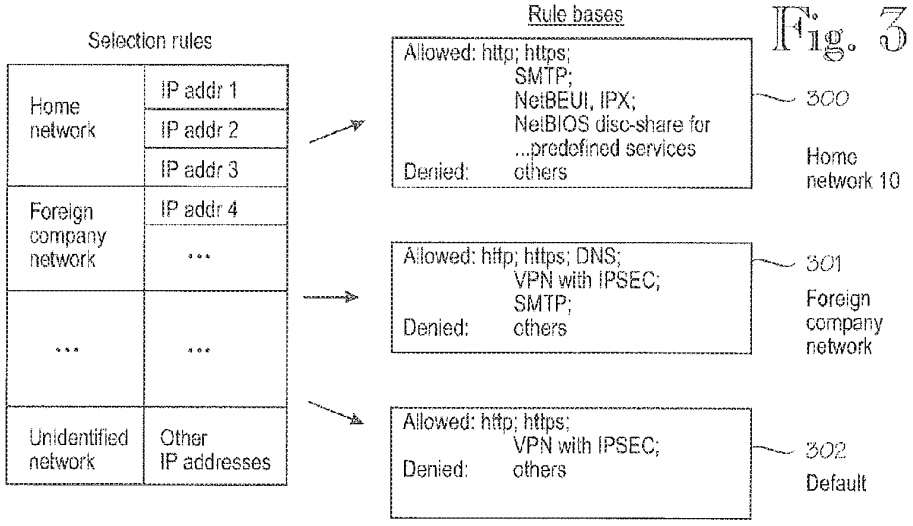


Fig. 3



BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01379

Fig. 4

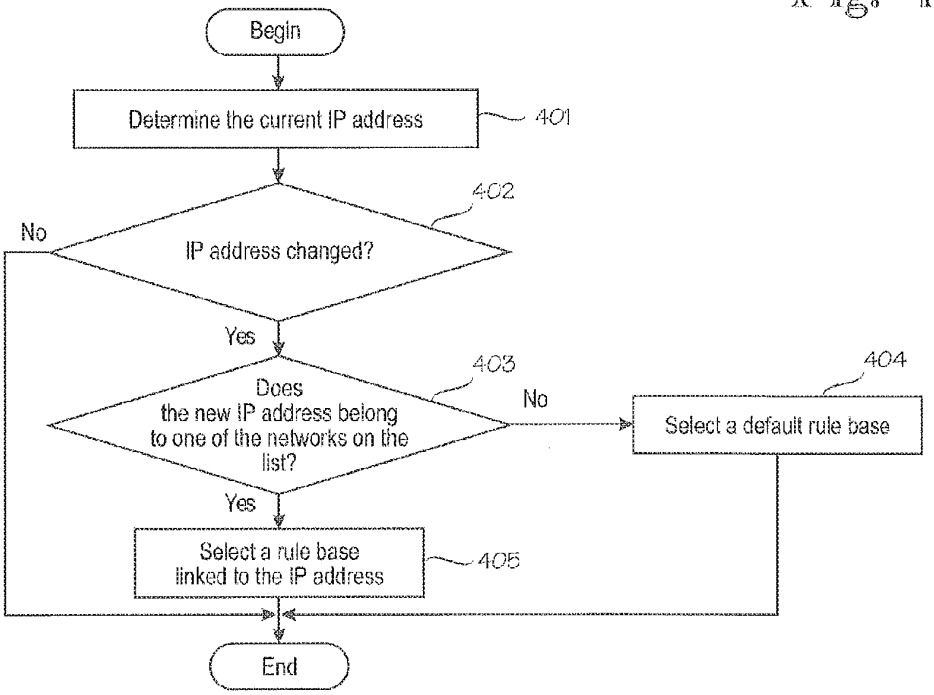
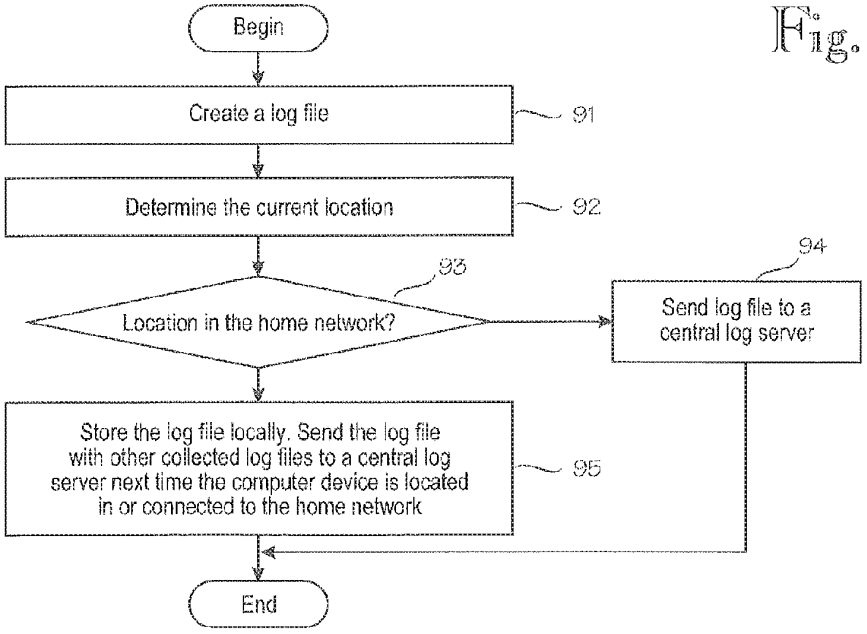


Fig. 9



BNSDOCID: <EP.....1313290A1_I_>

IPR2023-01353 Page 01380

Fig. 5

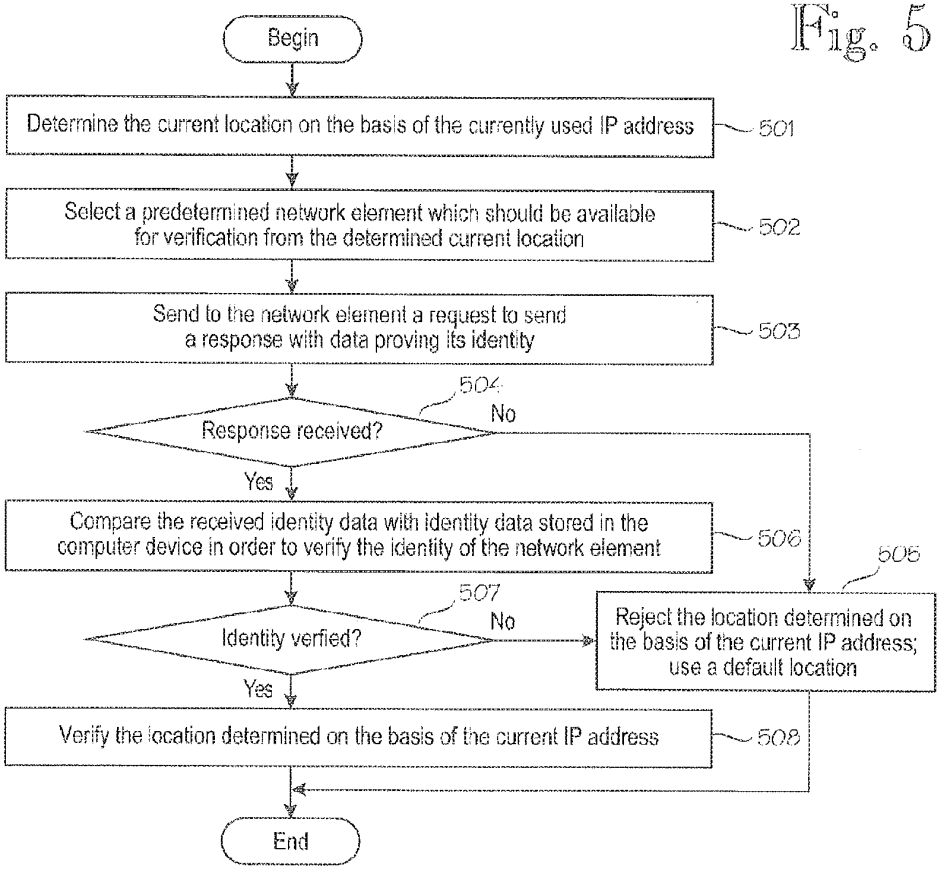


Fig. 6

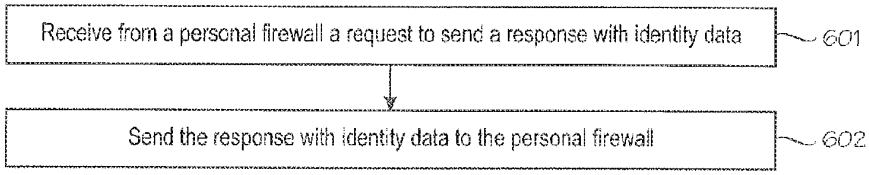
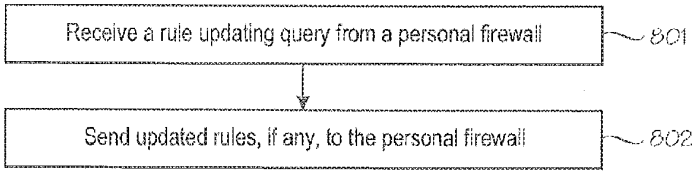


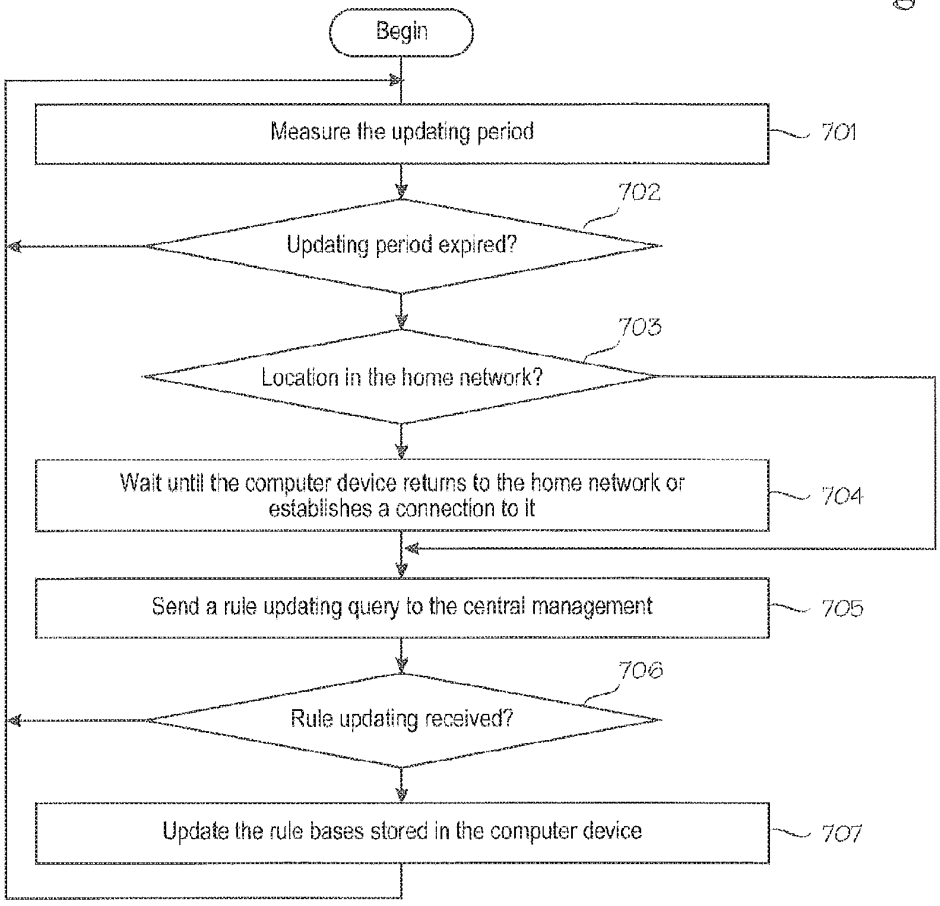
Fig. 8



BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01381

Fig. 7



BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01382

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 10 2581

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	EP 0 854 621 A (AT & T CORP) 22 July 1998 (1998-07-22) * page 4, line 28 - line 47 *	1-21	H04L29/06
A	US 6 158 008 A (OWENS LESLIE DALE ET AL) 5 December 2000 (2000-12-05) * claim 1 *	1-21	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	14 March 2003	Veen, G

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP_____1313290A1_I_>

IPR2023-01353 Page 01383

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 10 2581

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-03-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0854621 A	22-07-1998	US 6233686 B1	15-05-2001
		CA 2226814 A1	17-07-1998
		EP 0854621 A1	22-07-1998
		JP 10229418 A	25-08-1998
US 6158008 A	05-12-2000	WO 9921339 A1	29-04-1999

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

IPR2023-01353 Page 01384

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 May 2005 (19.05.2005)

PCT

(10) International Publication Number
WO 2005/046145 A1

(51) International Patent Classification[7]: H04L 12/56, 12/46

(21) International Application Number: PCT/SE2004/001611

(22) International Filing Date: 5 November 2004 (05.11.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/517,737 6 November 2003 (06.11.2003) US
10/977,724 29 October 2004 (29.10.2004) US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventor: HALEN, Joacim; Anhaltsvägen 8, S-191 40 Sollentuna (SE).

(74) Agent: KARIN BOESTAD et al.; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (SE).

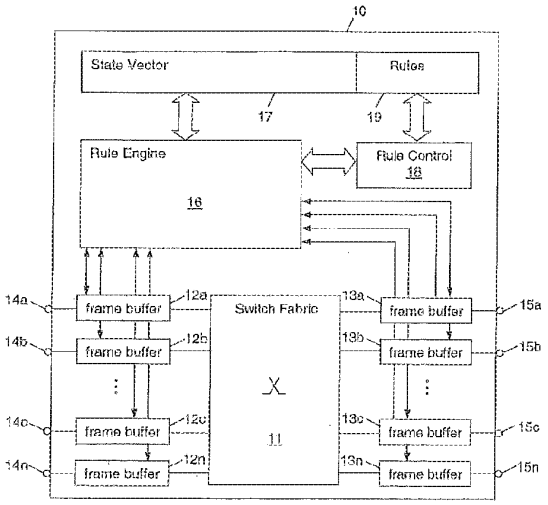
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, 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, LU, MC, 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:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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: ADAPTABLE NETWORK BRIDGE



(57) Abstract: An adaptable network bridge such as an Ethernet bridge (10) includes a Rule Engine (16) that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means (18) for dynamically adding, subtracting, or modifying the switching rules in response to changes in the bridge's state information, or changes in context information. If the bridge includes a plurality of input/output ports (14, 15), the Rule Engine (16) may include a plurality of sets of switching rules, with each set of switching rules being applicable to a different port in the bridge. In this way, different network providers can share the same equipment, but have different network behavior.

WO 2005/046145 A1

ADAPTABLE NETWORK BRIDGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This nonprovisional application claims priority under 35 U.S.C. § 119(e) on U.S. Provisional Application No. 60/517,737 entitled, *Programmable Bridge*, filed November 6, 2003, the disclosure of which is incorporated herein in its entirety.

BACKGROUND OF THE INVENTION

Technical Field of the Invention

The present invention relates generally to digital communication systems. More particularly, and not by way of limitation, the invention is directed to an adaptable network bridge having a Rule Engine that simplifies adapting the bridge to dynamically changing conditions.

Description of Related Art

Ethernet is a layer-2 packet-based transmission protocol that is primarily used in local area networks (LANs). Ethernet is the common name for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 industry specification. Data is transmitted in Ethernet frames. Each frame includes a preamble with 64 bits utilized for synchronization. A Start of Frame Delimiter (SFD), a destination address, a source address, and a length/type identifier follow the preamble. Media Access Control (MAC) client data, together with a Packet Assembler/Disassembler (PAD) may vary in length from 46 to 1500 bytes (octets). A Frame Check Sequence (FCS) adds four more octets. Higher-level protocols reside in the content part of the frame. The frame size is counted from the destination address to the FCS, inclusive, and thus may vary between 64 and 1518 octets, not including a Virtual Local Area Network (VLAN) tag, which adds 4 octets.

Today most packet-based networks are built on Ethernet technology, as it is a cheap and reliable technology with good performance. Ethernet has been used in office networks for a long time and is now used to build Wide Area Networks (WANs) as well as small networks in homes. The communications

IPR2023-01353 Page 01386

industry is now expanding the use of Ethernet to what is called "Public Ethernet" where millions of users are connected in the same network. Unfortunately, Ethernet does not scale to such large networks due to flooding of broadcasted messages. Some solutions have been proposed, but these solutions require modifications to the existing standards if they are to be implemented on standard equipment.

Ethernet bridging is a way to connect networks together to form a larger network. The standard for bridging is ANSI/IEEE 802.1d, which is hereby incorporated by reference herein. A bridge is a way to connect two separate network segments together in a protocol-independent way. Packets are forwarded based on Ethernet address, rather than IP address. Since forwarding is done at Layer 2, all protocols can go transparently through a bridge.

There are basically two approaches to adding new functionality to Ethernet bridges (and other Ethernet equipment as well): standardization thru IEEE, or proprietary solutions, which make the equipment non-standard. Adding new functionality and behavior to IEEE 802.1d MAC bridges, better known as Ethernet switches (or other Ethernet equipment), is a difficult and time-consuming process without any guarantees of success. Each new function must be proposed to and scrutinized by an IEEE standardization group (an existing working group or a new group has to be accepted and established). If one is lucky, the proposed function is accepted and added to the standard. However, since each new function requires a change in the standard, there is reluctance to add new functions. If the proposal is rejected, one is limited to a proprietary solution on non-standard equipment. The members of the standardization groups come from different vendors and other organizations, and although they are supposed to act in the interest of IEEE and the entire community, they may also act on agendas from their own organization/company that might be in conflict with the proposed functionality, thereby turning it down. It should also be noted that if a new function is added to the standard, it is then up to the different vendors to add the standardized functionality. A feature may be standardized but not made mandatory.

The proprietary approach also has its drawbacks. For example,

IPR2023-01353 Page 01387

programmable network processors have been available for some time, and bridges may be purchased off the shelf containing programmable network processors. Proprietary solutions can be implemented on these. However, these network processors are vendor specific, and the solution will only work on that network processor or processor family. The solution will not be portable, and it will not be possible to run it on other vendors' equipment. Additionally, programming a network processor is done at a very low level, basically in assembly language, and the programming model is hard, requiring special skill. It should also be noted that a proprietary solution will make the equipment non-standard, and customers are more reluctant to buy non-standard equipment. There might also be inter-operational problems with other equipment.

SUMMARY OF THE INVENTION

The present invention is an adaptable network bridge having a Rule Engine that simplifies the adaptation of the bridge to dynamically changing conditions related, for example, to network conditions and user context. Simplicity is achieved by specifying how data frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating of rules in the bridge via a protocol. In addition, one bridge may generate or modify rules for loading at another, neighboring, bridge. In a preferred embodiment, the bridge is an Ethernet bridge.

Thus, in one aspect, the invention is directed to an adaptable network bridge that includes a Rule Engine that processes data frames according to a set of switching rules. Each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed. The bridge also includes means for dynamically modifying the switching rules. In particular, the rules may be dynamically loaded and updated, for example, in response to changes in the bridge's state information, or changes in context information. In another embodiment, the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

In one aspect the rules are forced on the switch by external units such as a

IPR2023-01353 Page 01388

Network Management System (NMS).

In a further aspect, a switch generates or modifies rules that are forced on other switches.

In yet another aspect, the invention is directed to a method of processing and switching Ethernet frames in an adaptable Ethernet bridge. The method includes the steps of defining a set of switching rules for the adaptable Ethernet bridge; receiving a given frame in the bridge; determining whether any of the rules are applicable to the given frame; and upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule. The switching rules may be dynamically added, subtracted, or modified, for example, in response to changes in state or context information.

An important aspect of the invention is how the extended state vector can be utilized in new ways in the switching process. The switching process can be controlled and adapted in new ways allowing completely new ways to control networks.

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, the essential features of the invention will be described in detail by showing preferred embodiments, with reference to the figures of the attached drawings.

FIG. 1 is a simplified block diagram of a Rule Engine utilized in the adaptable network bridge of the present invention;

FIG. 2 is a sequence diagram illustrating the steps of a process performed by the Rule Engine; and

FIG. 3 is an illustration of a network of adaptable Ethernet bridges controlled by a Network Management System (NMS).

DETAILED DESCRIPTION OF THE INVENTION

In the following description, for purposes of explanation and not limitation, specific details are set forth, such as particular embodiments, circuits, signal formats etc. in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art that the present invention may be

IPR2023-01353 Page 01389

practiced in other embodiments that depart from these specific details.

In existing Ethernet bridges, there are two identifiable phases in the switching process. In the first phase, parts of the frame header are checked for specific information. For example, the destination address of each frame may be checked against a forwarding table, priority bits, VLAN tags, and the like. In the second phase, different actions are taken within the bridge depending on the result of this check. For example, the frame may be sent to the port pointed to in the forwarding table, or the frame may be sent to all ports except the originating port, and so on. These steps characterize a process in which a frame is put through a filter that selects the action to take. Another important element is that the bridge stores and retrieves information in the form of a simple state vector in a forwarding table (i.e., memory), which the bridge is using in the process. However, the different parts of this process are fixed and may not be altered.

The present invention is based on a generalization of this switching process that adds several new key aspects to switching, enabling new ways of adapting and controlling the switching process as well as new ways to control Ethernet networks. The invention provides an adaptable Ethernet bridge having a Rule Engine that simplifies the addition or modification of functionality within the bridge. One of the purposes of the adaptable bridge is to provide a simple solution whereby anyone with reasonable skill can implement and add new functionality in a standardized way on standard equipment. Simplicity is achieved by specifying how Ethernet frames should be processed and switched in terms of switching rules. Flexibility is achieved by enabling dynamic loading and updating, inspection, and prioritization of rules in bridges via a protocol.

The generalized switching process consists of the Rule Engine processing Ethernet frames by applying the switching rules. A switching rule encapsulates a specific switching behavior that describes the filter and action processes together with the state vector. A switching rule thus consists of three parts:

1) A filter function that can filter any part or parts of a frame. The purpose of the filter is to decide if the rule is applicable to a given frame. In other words, the filter works as a predicate function on frames. In this decision process information in the state vector may be used.

IPR2023-01353 Page 01390

2) An action function that describes how a frame header (or the entire frame) should be transformed and how the frame should be switched, i.e. to which port or ports the frame should be sent. In this process the action function may alter the state vector.

3) A state vector that the filter function and the action function can use in the switching process.

The switching rule can also contain other information such as version, priority specification, vendor information, and the like.

The state vector is an abstraction of several parts:

1) A local memory for a rule or a set of rules where rule-specific data can be stored and altered. Specific "management rules" make it possible to access that data from, for example, a management system.

2) A global bridge memory where bridge-specific data applicable to and accessible by all rules can be stored and altered. One example is the port-forwarding table.

3) Access to a set of bridge resources that can be implemented as library functions. Some examples are a function to retrieve the source port of the frame processed, a function that provides timestamps, counters and timers, and functions that describe the traffic flows and load in the bridge. The invention is not limited to these examples; other functions may be identified by those skilled in the art.

A switching rule describes the types of frames that match the rule and how these frames should be processed (e.g., switched or transformed before switching). Each incoming frame is checked against the set of rules stored in the bridge. If a rule matches, the frame is processed and switched according to the specification in the rule. If no rule matches the frame, a default rule may be utilized, or the frame may be dropped.

With the concept of rules, the switching process is defined as a simple and understandable programming model. Standardizing rule language and making it possible to dynamically load new rules in a bridge also makes it possible to add new functionality, adapting standard equipment to the needs at hand. If some functionality becomes obsolete, that functionality can be removed by removing the

IPR2023-01353 Page 01391

rule or set of rules implementing it.

A powerful extension is to allow different rule sets to be valid for different ports enabling, for example, different network providers to share the same hardware but have different network behavior. Different embodiments of this extension include: a rules control mechanism that selects and prioritizes available rule sets based on port, time of day, load, and the like. Alternatively, this kind of information may be described in the filter functions, and the Rule Engine tries all rules until it finds a match.

Yet another powerful extension is to allow rules that monitor the state vector instead of being matched against Ethernet frames. That is, the filter function monitors the state vector, and when some condition is fulfilled, the action function is invoked. The monitoring process can be implemented by regularly processing these rules in the Rule Engine or in a separate Rule Engine.

Note that allowing the filter and action functions to have access to a state vector that goes beyond the forwarding table provides new and powerful ways to process and switch frames.

FIG. 1 is a simplified block diagram of an exemplary embodiment of the dynamically adaptable network bridge 10 of the present invention. The adaptable bridge includes many of the same components as existing bridges such as switch fabric 11, frame buffers 12a-12n and 13a-13n, and ports 14a-14n and 15a-15n. In addition, however, the adaptable bridge includes a Rule Engine 16, which replaces the implementation of some or all protocols. The adaptable bridge also includes a state vector memory 17 accessible by the Rule Engine, a rule control function 18, and a rules memory 19 accessible by the Rule Engine through the rule control function. Collectively, these new bridge components enable the adaptable bridge to receive and store rules from external units, store a state vector which may be dependent on external sources, and store rules that are imposed on other bridges.

Hybrid designs having both a Rule Engine and some of the protocols of existing bridges may also be implemented. The Rule Engine has processing capabilities, that is, the Rule Engine can (1) apply the filter function to a frame and calculate the result; (2) apply the action function if the rule matches; (3) access

IPR2023-01353 Page 01392

the state vector; and (4) access the other resources of the switch. A frame entering the adaptable bridge through an input port such as port 14a and frame buffer 12a is acted upon by switching rules in the Rule Engine 16, including the filter function, action function, and state vector. The result is a calculated result frame, which is outputted through switch fabric 11, and an appropriate frame buffer and output port such as frame buffer 13a and output port 15a.

The rule control function 18 adds and removes rules dynamically, and orders or prioritizes THE set of rules. The rule control function may be implemented as protocols and secured against unwanted manipulation by using well known techniques intended for that purpose, for example, using digital signatures and encryption. Additionally, the rule control function may include a mechanism to transform (or translate) switching rules in human-readable form to an efficient form understandable by the Rule Engine 16.

The mechanisms to access different bridge resources and state information (i.e., state vectors), mechanisms to access library functions, and a protocol for externally accessing the state information are important parts of the adaptable bridge. The bridge resources and state information may be accessed via, for example, an Application Programming Interface (API). The protocol for externally accessing the state information may be implemented as a set of rules. The state of the bridge can affect switching rules dynamically, that is, a rule can behave differently depending on the current state. For example, frames can be switched differently depending on time of day, traffic pattern, traffic load, and the like. This behavior can also be controlled externally by, for example, a network management system (NMS).

FIG. 2 is a sequence diagram illustrating the steps of a method of processing an Ethernet frame by the Rule Engine 16. The process starts at step 21 and moves to step 22 where, for each incoming Ethernet frame, the port-specific rules associated with the Source Port are merged with the rules shared among all ports of the bridge (this merge can be done in advance by the priority module as a ordered list). The rules in the list are then tested to determine whether the frame matches the rule. This process begins at step 23, where a determination is made whether there are any more rules left to test. If not, and all

IPR2023-01353 Page 01393

the rules have been tested, the frame is dropped at step 24. However, in the case of the first rule, there are rules left to test, so the method moves to step 25 where the filter function of the first rule in the list is applied to the frame. The filter function uses the information found in the frame together with the current state vector to determine whether the frame matches the rule. The filter function is a predicate, so the result at step 26 will be either true (the frame matches the rule) or false (the frame does not match the rule). If the result is false, the rule is discarded at step 27, and the method returns to step 23 where the test is performed on the next rule in the list.

The remainder of the rules are then tested until either no rules are left and the frame is dropped at step 24, or there is a match at step 26, and the method moves to step 28 where the action function of the rule is applied to the frame. The action function may use the library functions, the information in the frame, and the state vector to transform (or modify) the frame. In this process, the action function can use functions to modify the state vector. For example, a counter may be incremented, which counts the number of frames containing a specific high-level protocol coming from the port. At step 29, the action function determines the destination port or ports and sends the (possibly transformed) frame to the determined port or ports. The method then ends at step 30.

Another important aspect of the invention not shown in the sequence diagram is that other resources or modules in the bridge may continuously monitor and change the state vector in parallel. An extended Rule Engine, to the one described, may then invoke rules that, instead of being matched against Ethernet frames, monitor the state vector. When one or more predefined criteria are fulfilled (determined by the filter function), the action function generates new frames containing new rules to be sent to the bridge itself or to nearby bridges altering their behavior.

FIG. 3 is an illustration of a network 35 of adaptable Ethernet bridges controlled by a Network Management System (NMS) 36. The NMS monitors the state in the bridges and issues rules that adapt the behavior of certain bridges accordingly. For example, if $Bridge_{11}$ becomes heavily loaded with traffic, the NMS may issue a rule that will move some traffic from associated bridges (i.e.,

IPR2023-01353 Page 01394

$Bridge_{21}$ – $Bridge_{23}$) to $Bridge_{12}$. For example, the rule may move every third frame or frames carrying a particular protocol to $Bridge_{12}$. Context information may also be added to the state vector, thereby allowing context to influence switching. Context information may contain, but is not limited to, information about traffic load in nearby bridges, forecasts or predictions of expected traffic, and the like. This feature is of particular interest in a mobile environment.

The NMS 36 is shown connected to the network by a dotted line because the adaptable bridges may automatically generate specific context rules and distribute them to nearby bridges as users move around in the network. When bridges automatically generate rules to other bridges (and to themselves), a self-managed network can be implemented in which bridges exchange rules dynamically. This capability can be used, for example, to setup a particular flow-path, distribute traffic during heavy load, or automatically redirect traffic in the case of network failures. For example, if Bridge11 receives a flow of high priority frames when it is already heavily loaded with traffic, it can issue a rule or set of rules to Bridge22 that move the flow to Bridge12 instead.

An Ethernet bridge is working in "wire-speed" and therefore it is desirable that the bridge introduce as little delay as possible. Adding a Rule Engine and basing the switching on rules may increase the delay. However, a number of techniques and mechanisms can be used to make the Rule Engine more efficient:

1) Filter functions can be tested in parallel, and a priority module can select the matching rule with highest priority. These computations can be performed because the filter functions are pure predicates, i.e. they contain no side effects.

2) Filter functions will in most cases be a conjunction (or disjunction) of comparisons. These can be directly mapped onto a pipelined matrix of comparison modules in hardware.

3) A similar pipelined hardware matrix realizing the language constructs used in the action functions can be implemented.

4) Some parts of the state vector, for example library functions reflecting bridge context and resources, can be implemented in hardware such as registers, thereby providing "instant" access to them.

In the preferred embodiment, the rule language used to describe the filter

IPR2023-01353 Page 01395

and action functions is not a general purpose programming language. A programming language should only have the necessary constructs and mechanisms needed to express the solutions to the problems in the specified domain. If the language is too powerful, as a general-purpose language, it is possible to express an infinite loop (accidentally or on purpose) thereby increasing the delay to infinity. The preferred switching rule language, therefore, is a language primarily restricted to the domain of Ethernet switching (layer 2), with language constructs expressing the mechanisms used in the switching process. However, language constructs that are useful for other purposes like network management, constructs related to exchange of new rules, and so on, that are not in conflict with the basic requirements may also be included.

The present invention provides several advantages. The Ethernet standards can be implemented as switching rule sets, and as the standards evolve, the rule sets are updated. These updated rule sets can then easily be loaded into an adaptable network bridge. The rule sets can be vendor-independent and, for example, published by IEEE. Today, each vendor decides which protocols (standards) to support in a bridge, and unless the vendor issues an update whenever the standard is updated, users have to buy a new bridge if they need to follow the new standard.

In the present invention, the "programming language" of rules may be standardized thereby enabling anyone to add new functionality, as a switching rule, to any bridge with a Rule Engine. These rules can then be updated or removed if necessary. A proprietary solution can also be implemented as a rule or set of rules and loaded in any bridge with a Rule Engine. If a user later wants to use another solution, the rule set is simply replaced with a new rule set. It will be much less expensive to implement new functionality because, in most cases, the user only has to write some software in the form of a set of rules.

The present invention also greatly increases flexibility in networks because each bridge can be loaded with its own rule set down to the individual port level. The invention also provides the ability to adapt the functionality on each port based on time, user demands, service agreements, and the like. For example, different operators can share the same physical bridge (network) and provide

IPR2023-01353 Page 01396

different services to their respective users.

Some examples of functionality that can be implemented with switching rules include the following:

1) Broadcast tunnels. It is simple to implement broadcast tunnels necessary for building Public Ethernet Networks.

2) Distributed router functionality added to a set of bridges.

3) Simple firewall functionality.

4) User adapted services on the port level.

5) Authentication and security mechanisms on the port level that are transparent to users.

6) Self-managed networks or semi-self managed networks.

This list is not intended to be exhaustive, and other functions may also be implemented with switching rules and loaded into any adaptable bridge with a Rule Engine.

As shown by the above examples, the state of the dynamically adaptable bridge can be utilized in the switching process to enable entirely new functionality and to provide new ways to use bridges in networks.

Although preferred embodiments of the present invention have been illustrated in the accompanying drawings and described in the foregoing Detailed Description, it is understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications, and substitutions without departing from the scope of the invention. The specification contemplates any all modifications that fall within the scope of the invention defined by the following claims.

IPR2023-01353 Page 01397

WHAT IS CLAIMED IS:

1. A dynamically adaptable network bridge comprising:

a Rule Engine that processes data frames according to a set of switching rules, wherein each switching rule identifies a type of frame to which the rule applies, and how the type of frame is to be processed; and

means for dynamically modifying the switching rules.

2. The dynamically adaptable network bridge of claim 1 wherein the means for dynamically modifying the switching rules includes a protocol for dynamically loading and updating the switching rules.

3. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a filter function for determining whether a given rule is applicable to a given frame.

4. The dynamically adaptable network bridge of claim 3, wherein each switching rule also includes an action function for specifying changes to the given frame's header and how the given frame should be switched.

5. The dynamically adaptable network bridge of claim 1, wherein each switching rule includes a state vector utilized for processing the type of frames to which each rule applies.

6. The dynamically adaptable network bridge of claim 5, wherein the state vector includes an abstraction of a local memory for storing rule-specific data for each switching rule.

7. The dynamically adaptable network bridge of claim 6, wherein specific management rules enable the Rule Engine to access the rule-specific data for each switching rule.

IPR2023-01353 Page 01398

8. The dynamically adaptable network bridge of claim 6, wherein the state vector also includes an abstraction of a global bridge memory for storing bridge-specific data applicable to and accessible by all the switching rules.

9. The dynamically adaptable network bridge of claim 8, wherein the bridge-specific data includes a port-forwarding table.

10. The dynamically adaptable network bridge of claim 8, wherein the state vector also includes a set of library functions that implement bridge resources.

11. The dynamically adaptable network bridge of claim 10, wherein the set of library functions are selected from a group consisting of:

a function that retrieves a source port of a processed frame;
a function that provides timestamps;
a function that describes traffic flows in the bridge; and
a function that indicates the traffic load in the bridge.

12. The dynamically adaptable network bridge of claim 3, wherein the given frame is processed in accordance with the given rule if the filter function determines that the given rule is applicable to the given frame, and the given frame is dropped if the filter function determines that there is no rule applicable to the given frame.

13. The dynamically adaptable network bridge of claim 1, wherein the bridge includes a plurality of input/output ports, and the Rule Engine includes a plurality of sets of switching rules, wherein each set of switching rules is applicable to a different port in the bridge.

14. The dynamically adaptable network bridge of claim 1, wherein the bridge is an Ethernet bridge.

IPR2023-01353 Page 01399

15. The dynamically adaptable network bridge of claim 1, wherein the means for dynamically modifying the switching rules includes a protocol that dynamically adds, subtracts, and modifies the switching rules.

16. The dynamically adaptable network bridge of claim 1, further comprising means for prioritizing rules within the set of switching rules.

17. The dynamically adaptable network bridge of claim 1, further comprising means for accessing state information for the bridge, wherein a given rule causes a given frame to be processed differently when the state information changes.

18. The dynamically adaptable network bridge of claim 17, wherein the given rule processes the given frame differently, depending on traffic load in the bridge.

19. The dynamically adaptable network bridge of claim 17, further comprising a port for receiving rules from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance.

20. The dynamically adaptable network bridge of claim 17, wherein the state information includes context information, wherein a given rule causes a given frame to be processed differently when the context information changes.

21. The dynamically adaptable network bridge of claim 1, wherein the bridge is one of a plurality of adaptable bridges in a network, and the bridge further comprises means for generating specific context rules and distributing the context rules to other adaptable bridges in the network.

IPR2023-01353 Page 01400

22. A method of processing and switching data frames in an adaptable network bridge, said method comprising the steps of:

defining a set of switching rules for the adaptable bridge;

receiving a given frame in the bridge;

determining whether any of the rules are applicable to the given frame; and

upon determining that one of the rules is applicable to the given frame, processing and switching the frame according to the applicable rule.

23. The method of claim 22, further comprising dynamically adding, subtracting, and modifying the switching rules.

24. The method of claim 23, further comprising accessing state information for the bridge, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the state information.

25. The method of claim 24, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

receiving a new or modified switching rule from a Network Management System (NMS), wherein the NMS monitors the state information for a plurality of adaptable bridges in a network, and issues rules that adapt the behavior of the bridge to optimize network performance; and

processing and switching frames according to the new or modified switching rule received from the NMS.

26. The method of claim 24, further comprising adding context information to the state information, wherein the step of dynamically adding, subtracting, and modifying the switching rules is performed in response to a change in the context information.

27. The method of claim 22, wherein the bridge is one of a plurality of adaptable bridges in a network, and the method further comprises the steps of:

generating specific context rules; and

IPR2023-01353 Page 01401

distributing the context rules to other adaptable bridges in the network.

28. The method of claim 22, wherein the bridge is an Ethernet bridge.

5

IPR2023-01353 Page 01402

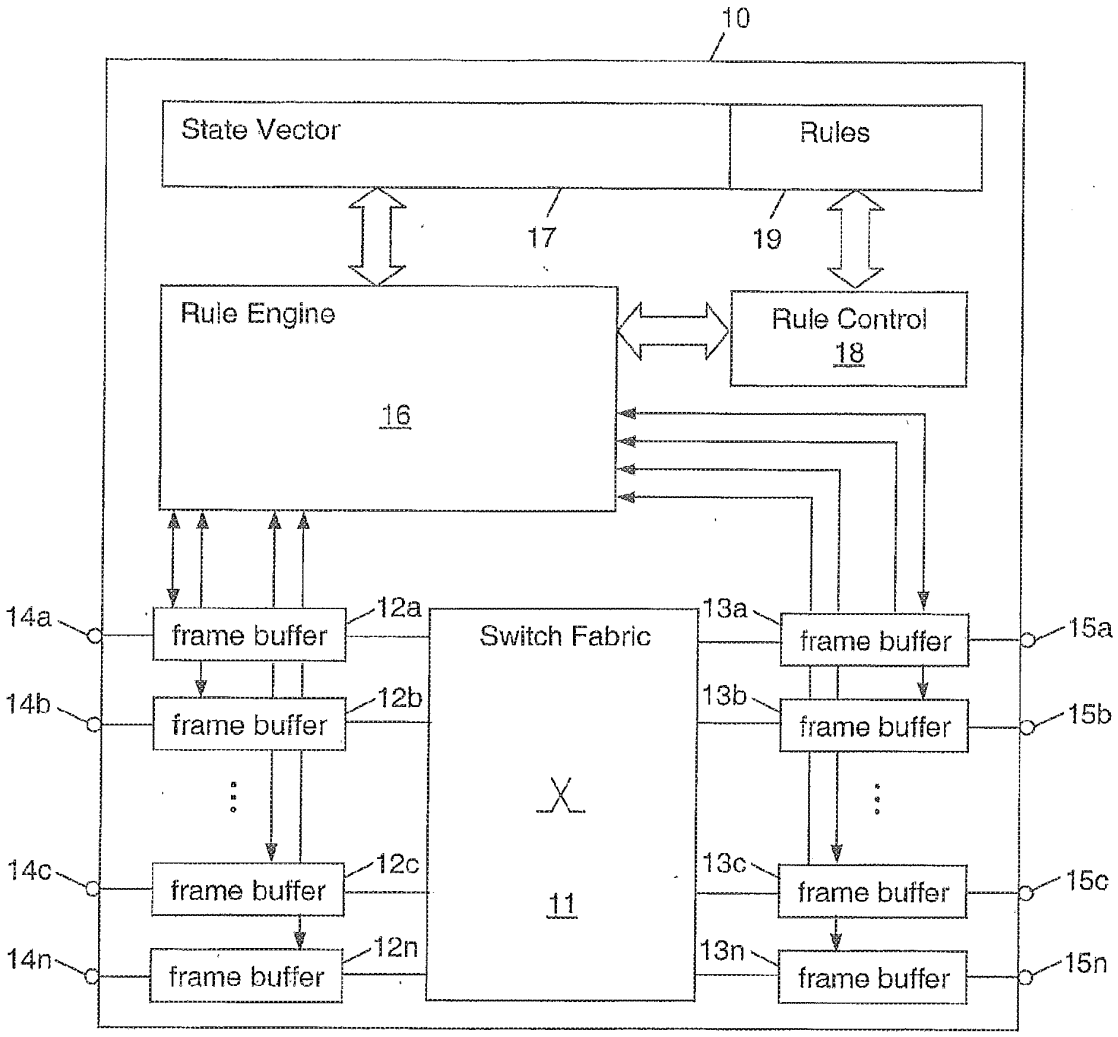


FIG. 1

BNSDOCID: <WO_____2005046145A1_I_>

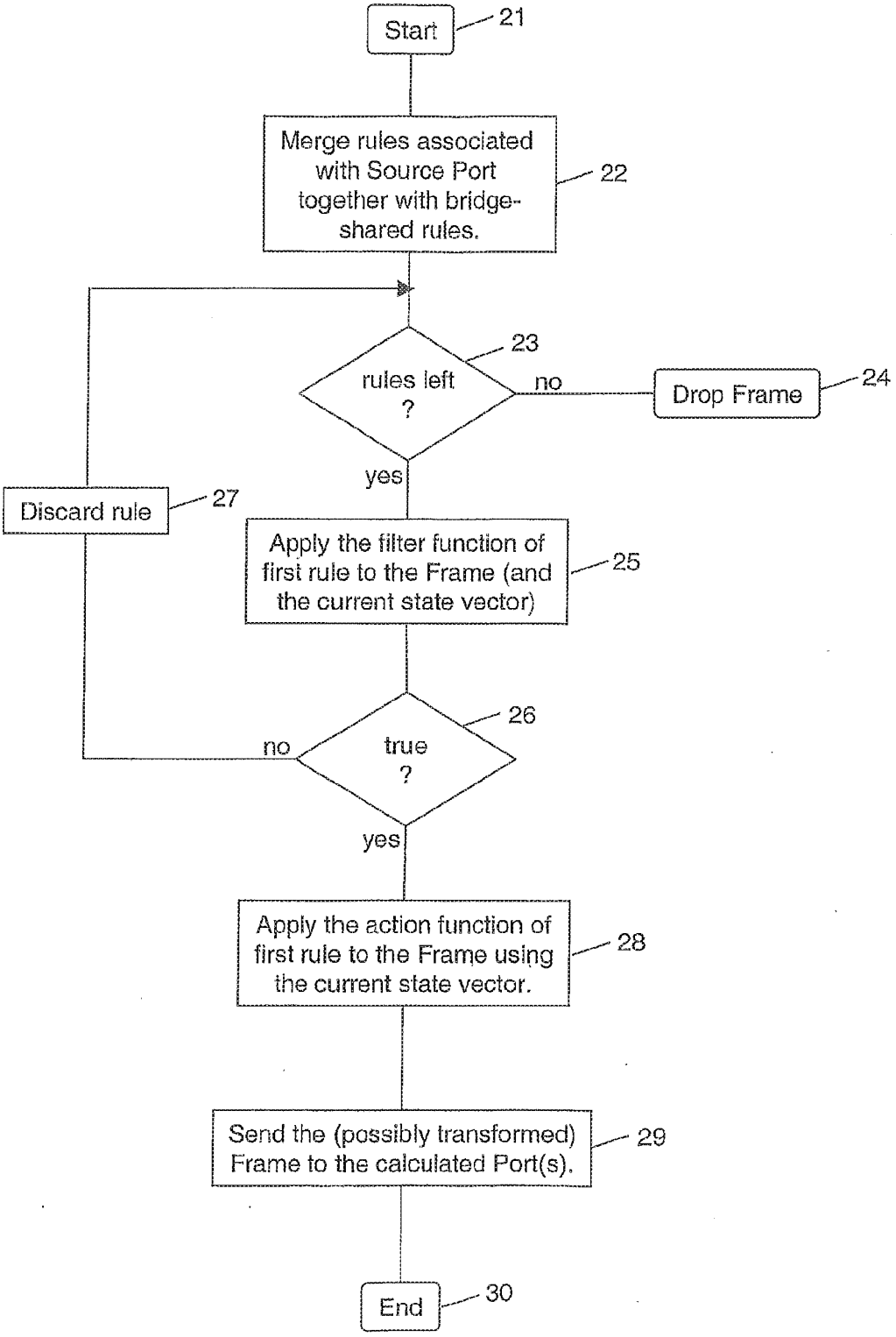


FIG. 2

BNSDOCID: <WO_____2005046145A1_I_>

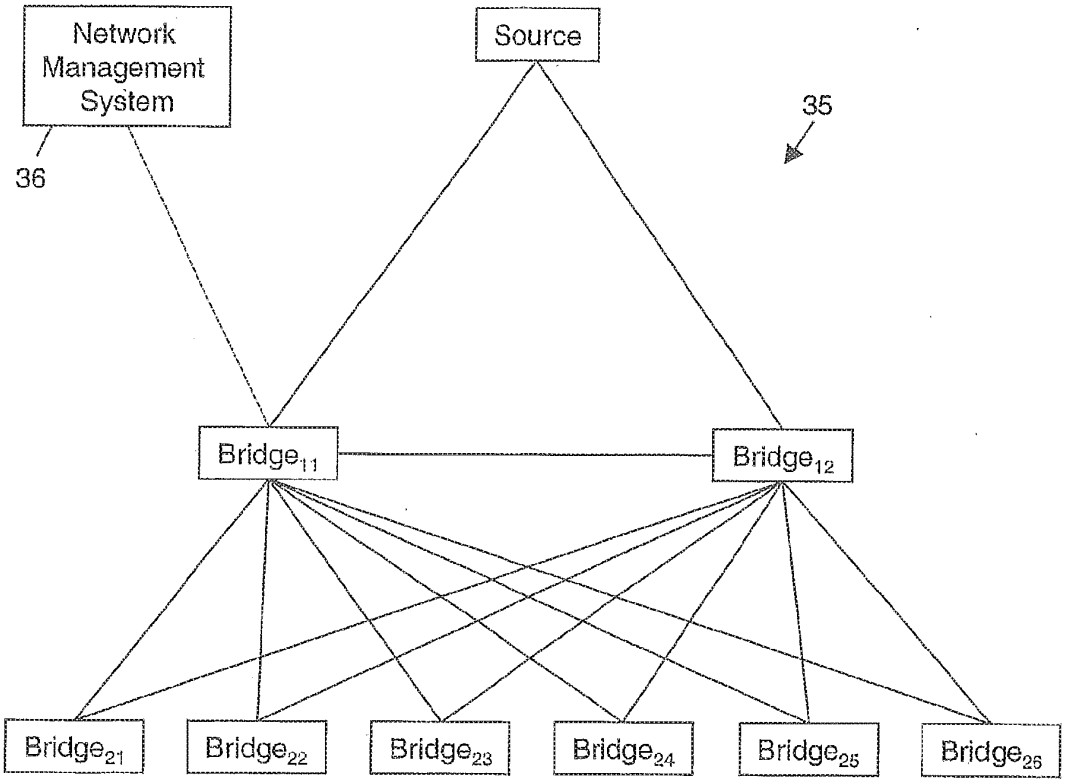


FIG. 3

BNSDOCID: <WO_____2005046145A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
T/SE2004/001611

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/56 H04L12/46

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)
IPC 7 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, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 790 554 A (PITCHER ET AL) 4 August 1998 (1998-08-04) abstract column 1, line 15 - column 1, line 67 column 2, line 39 - column 3, line 25 column 3, line 48 - column 4, line 42 column 4, line 60 - column 8, line 4 column 8, line 24 - column 8, line 26; claims 1,2,14,22,28; figures 2,3 -/---	1-5, 12-20, 22-25, 27,28

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in 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
21 March 2005	31/03/2005

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Todorut, C

Form PCT/ISA/210 (second sheet) (January 2004)

BNSDOCID: <WO_____2005046145A1_I_>

INTERNATIONAL SEARCH REPORT

International Application No
T/SE2004/001611

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 396 493 A (SUGIYAMA ET AL) 7 March 1995 (1995-03-07) abstract column 1, line 63 - column 3, line 11 column 4, line 11 - column 4, line 51 column 5, line 67 - column 6, line 39; claims 1,17; figures 1-4	1-28
X	WO 00/56024 A (BROADCOM CORPORATION; KADAMBI, SHIRI; AMBE, SHEKHAR; KALKUNTE, MOHAN;) 21 September 2000 (2000-09-21) abstract	1-4,22, 23
A	page 53, line 12 - page 65, line 21; claims 1,2	5-21, 24-28
A	US 2003/123387 A1 (JACKSON ANDREW LLOYD 'GB!) 3 July 2003 (2003-07-03) abstract column 1, paragraph 2 - column 1, paragraph 9 column 2, paragraph 16 - column 3, paragraph 25; claims 1,6,9; figure 4	1-28
A	US 5 959 976 A (KUO ET AL) 28 September 1999 (1999-09-28) abstract column 1, line 5 - column 2, line 40 column 3, line 8 - column 3, line 18 column 5, line 56 - column 6, line 10; claim 1; figures 3-5	1-28
A	EP 0 508 886 A (DIGITAL EQUIPMENT CORPORATION) 14 October 1992 (1992-10-14) abstract column 1, line 40 - column 3, line 54 column 4, line 45 - column 5, line 16 column 5, line 55 - column 6, line 53; claims 1,23; figures 5-8	1-28
A	US 5 515 376 A (MURTHY ET AL) 7 May 1996 (1996-05-07) abstract column 6, line 1 - column 9, line 21	1-28

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

BNSDOCID: <WO_____2005040145A1_I_>

IPR2023-01353 Page 01407

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5790554	A	04-08-1998	NONE		
US 5396493	A	07-03-1995	JP	6224918 A	12-08-1994
			KR	9614983 B1	23-10-1996
WO 0056024	A	21-09-2000	US	2001043611 A1	22-11-2001
			AU	3529500 A	04-10-2000
			AU	3752000 A	04-10-2000
			AU	4325800 A	04-10-2000
			EP	1161817 A2	12-12-2001
			EP	1169809 A2	09-01-2002
			EP	1159805 A2	05-12-2001
			WO	0056024 A2	21-09-2000
			WO	0056011 A2	21-09-2000
			WO	0056013 A2	21-09-2000
			US	6707817 B1	16-03-2004
			US	6810037 B1	26-10-2004
			US	6850521 B1	01-02-2005
			US	6707818 B1	16-03-2004
			US	2004174898 A1	09-09-2004
			US	2005047411 A1	03-03-2005
			US	2002039365 A1	04-04-2002
			AU	5442700 A	12-12-2000
			AU	5586400 A	12-12-2000
			AU	5737300 A	31-01-2001
			AU	6334400 A	22-01-2001
			EP	1181791 A1	27-02-2002
			EP	1181792 A1	27-02-2002
			EP	1212867 A2	12-06-2002
			EP	1192767 A2	03-04-2002
			WO	0072533 A1	30-11-2000
			WO	0102965 A2	11-01-2001
			WO	0072531 A1	30-11-2000
			WO	0101724 A2	04-01-2001
			US	2002093974 A1	18-07-2002
			US	2002186705 A1	12-12-2002
			US	6813268 B1	02-11-2004
			US	6735679 B1	11-05-2004
			US	6792500 B1	14-09-2004
			US	6842457 B1	11-01-2005
			US	6430188 B1	06-08-2002
			US	6859454 B1	22-02-2005
			US	2004170176 A1	02-09-2004
			US	2005036488 A1	17-02-2005
			US	2002031090 A1	14-03-2002
US 2003123387	A1	03-07-2003	NONE		
US 5959976	A	28-09-1999	NONE		
EP 0508886	A	14-10-1992	DE	69217103 D1	13-03-1997
			DE	69217103 T2	21-08-1997
			EP	0508886 A1	14-10-1992
			JP	5114905 A	07-05-1993
			US	5515513 A	07-05-1996
US 5515376	A	07-05-1996	EP	0710415 A1	08-05-1996
			JP	3335358 B2	15-10-2002

BNSDOCID: <WO_____2005046145A1_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
/SE2004/001611

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5515376 A		JP 9500774 T	21-01-1997
		WO 9503659 A1	02-02-1995
		US 5610905 A	11-03-1997
		US 6545982 B1	08-04-2003

Form PCT/ISA/210 (patent family annex) (January 2004)

BNSDOCID: <WO_____2005046145A1_I_>

US 20110055916A1

(19) **United States**

(12) **Patent Application Publication**

Ahn

(10) **Pub. No.: US 2011/0055916 A1**

(43) **Pub. Date: Mar. 3, 2011**

(54) **METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ADAPTIVE PACKET FILTERING**

(76) Inventor: **David K. Ahn**, Winston-Salem, NC (US)

(21) Appl. No.: **12/871,806**

(22) Filed: **Aug. 30, 2010**

Related U.S. Application Data

(60) Provisional application No. 61/237,974, filed on Aug. 28, 2009.

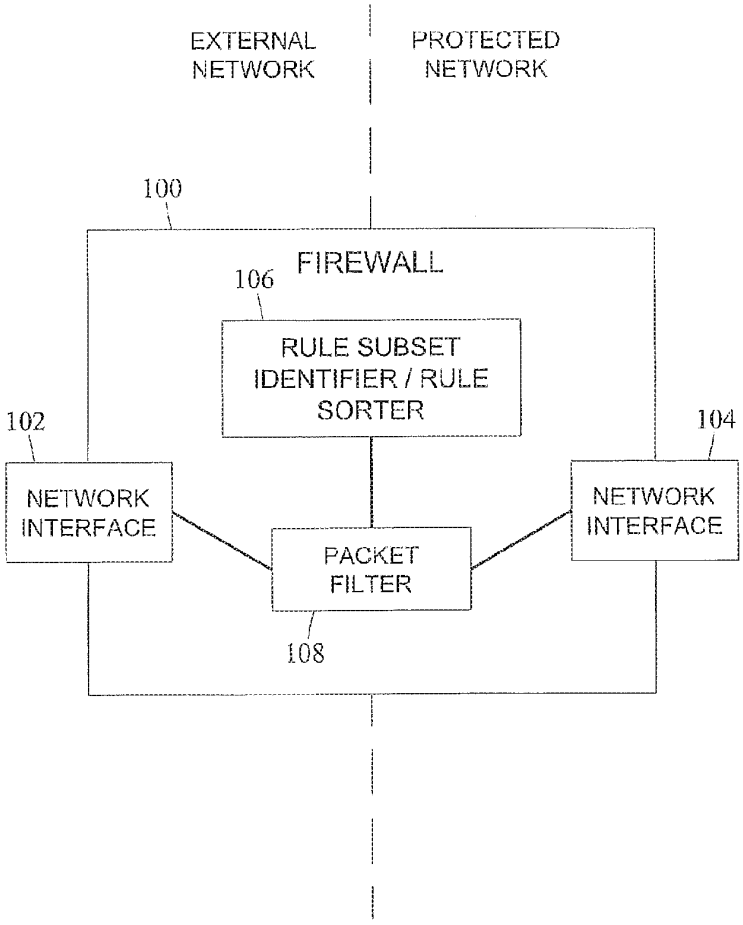
Publication Classification

(51) **Int. Cl.**
G06F 17/00 (2006.01)

(52) **U.S. Cl.** **726/13**

(57) **ABSTRACT**

The subject matter described herein includes methods, systems, and computer readable media for adaptive packet filtering. One method includes identifying at least one subset of rules and an ordered set of firewall packet filtering rules that defines a firewall policy such that the subset contains disjoint rules. Disjoint rules are defined as rules whose order can be changed without changing integrity of the firewall policy. Rules in the subset are sorted to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters. Packets are filtered at the firewall using the sorted rules in the subset by comparing each packet to each of the sorted rules in the subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for packets filtered using the sorted rules in the subset.



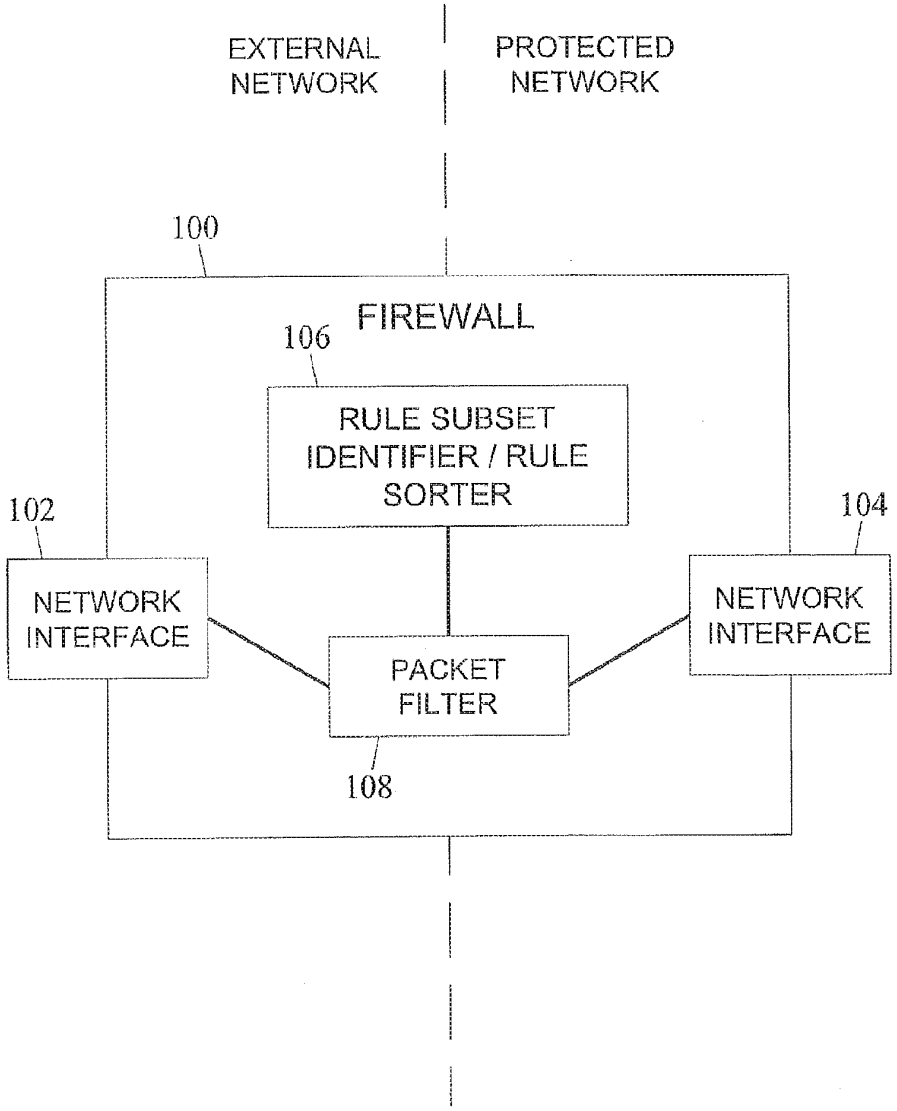


FIG. 1

BNSDCCID: <US____20110055916A1_I_>

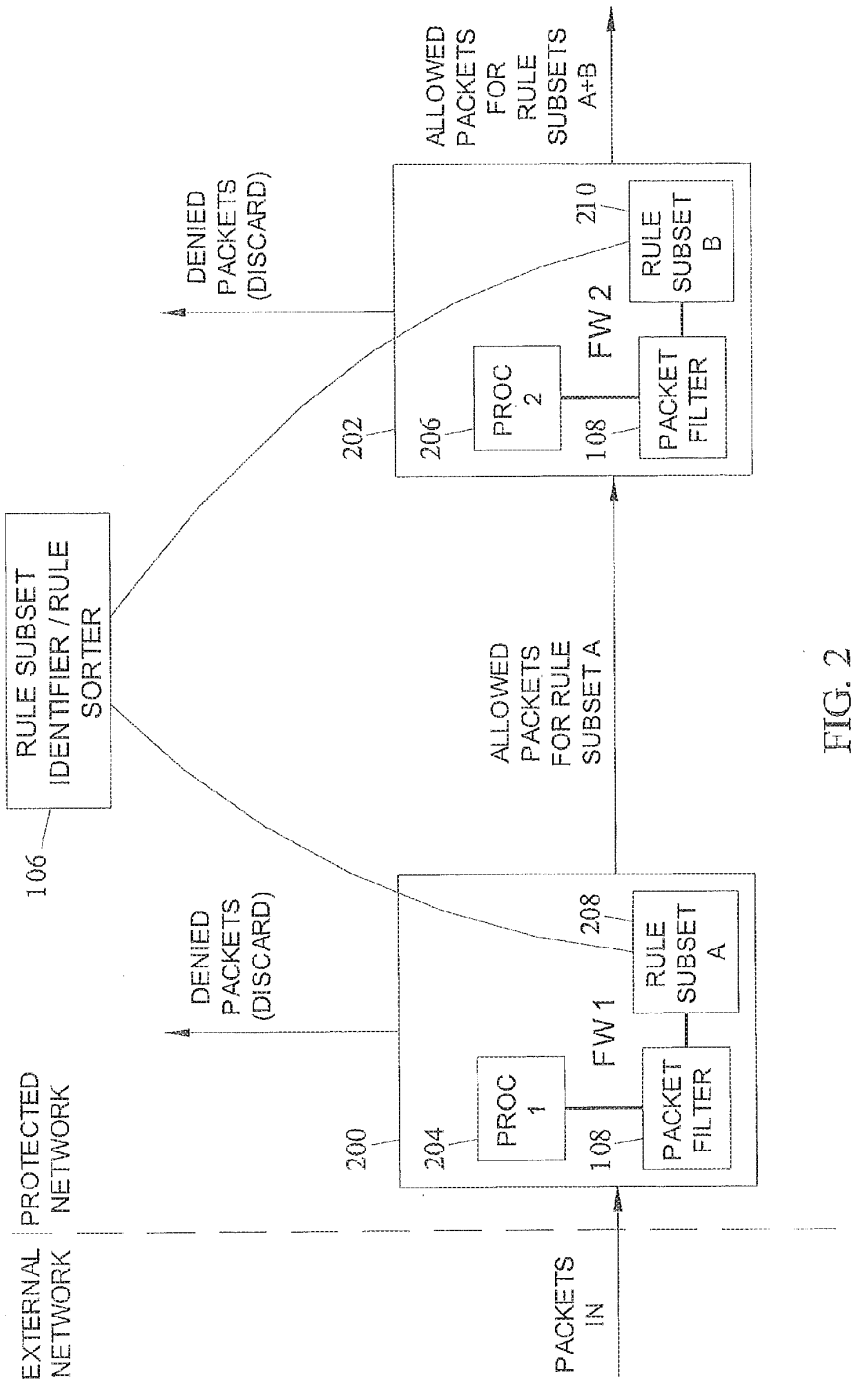


FIG. 2

BNSDOCID: <US____20110055916A1_I_>

IPR2023-01353 Page 01413

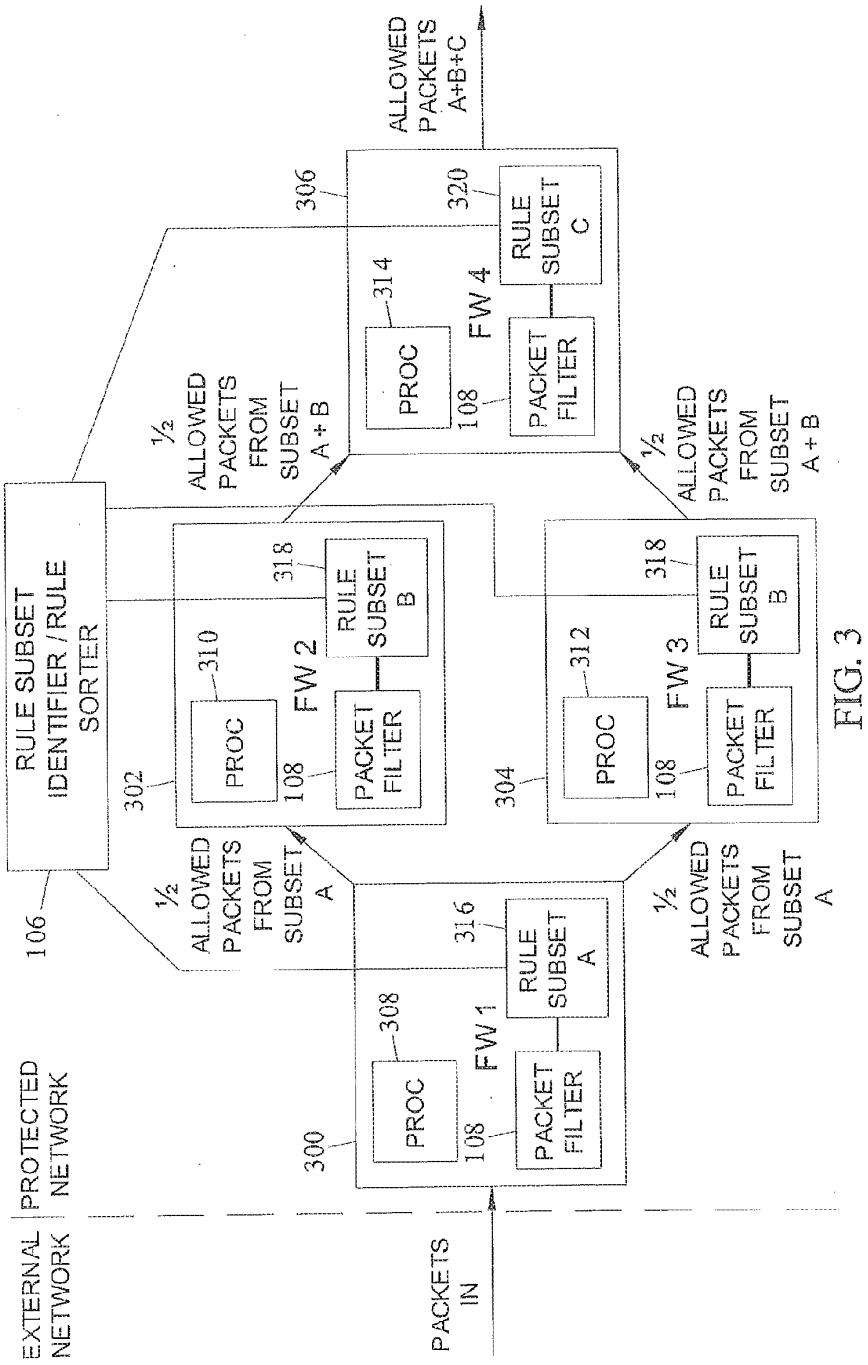


FIG. 3

BNSDOCID: <US____20110055916A1_I_>

IPR2023-01353 Page 01414

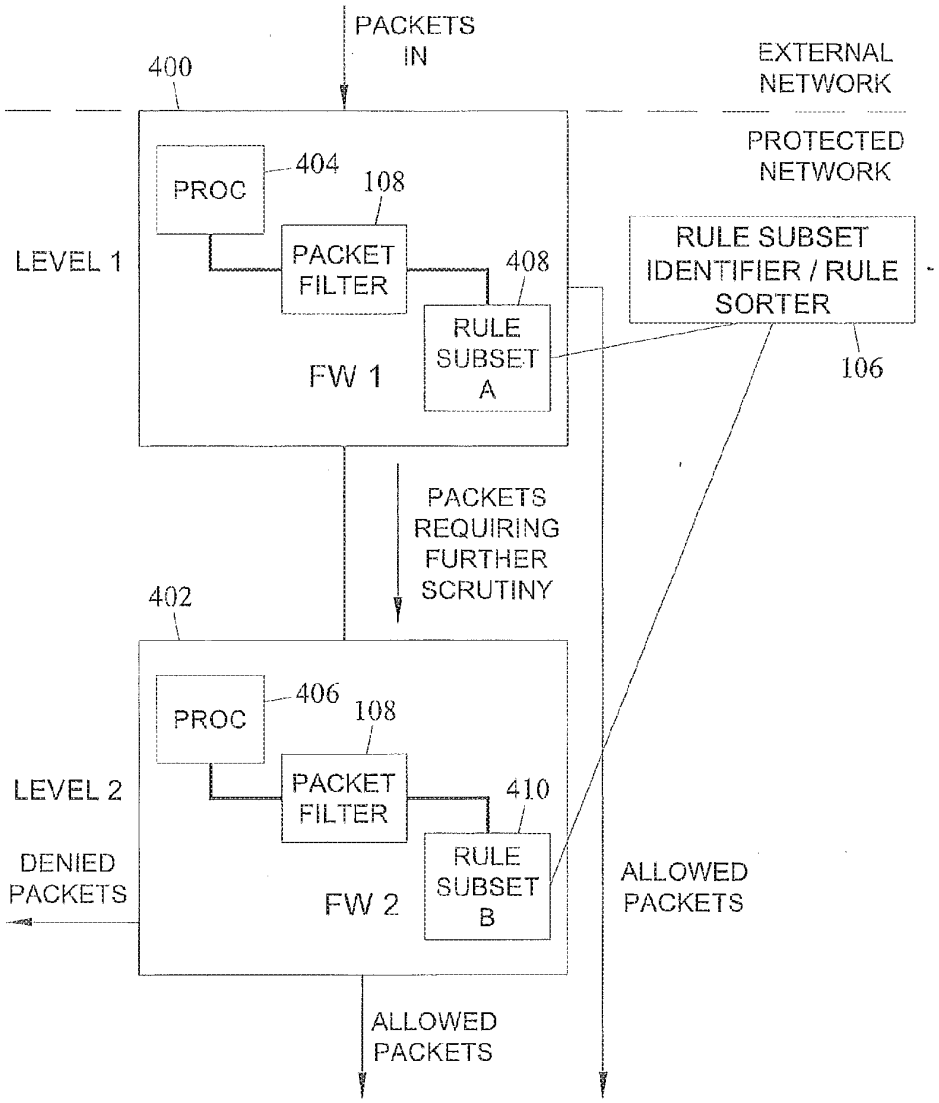


FIG. 4

BNSDCCID: <US____20110055916A1_I_>

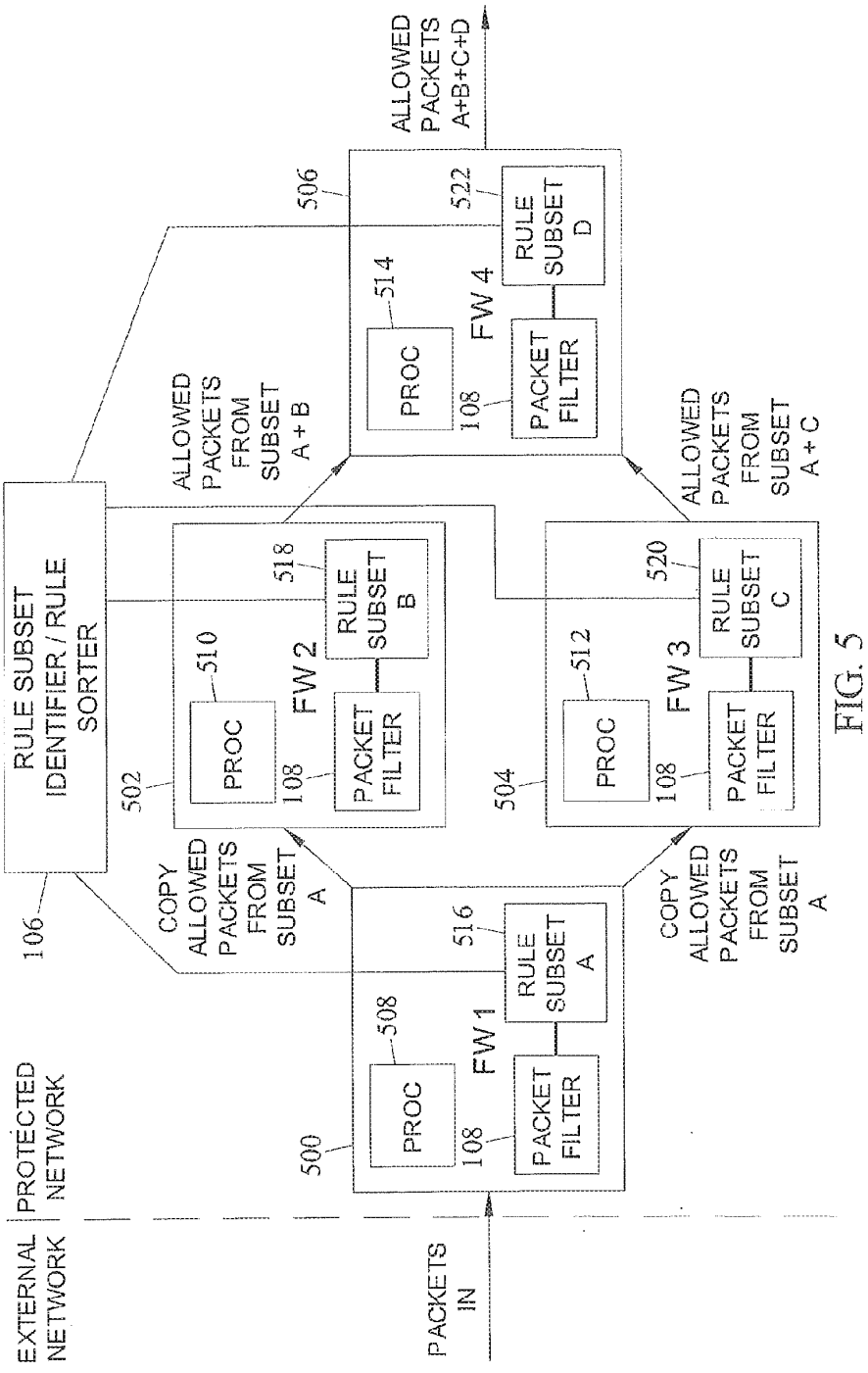


FIG. 5

IPR2023-01353 Page 01416

METHODS, SYSTEMS, AND COMPUTER READABLE MEDIA FOR ADAPTIVE PACKET FILTERING

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/237,974, filed Aug. 28, 2009; the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The subject matter described herein relates to network firewall filtering. More particularly, the subject matter described herein relates to methods, systems, and computer readable media for adaptive packet filtering.

BACKGROUND

[0003] A firewall generally processes a packet against a list of ordered rules to find the first rule match. The list of ordered rules represents an aggregate security policy, and arbitrarily changing the order of the rules can result in a violation of the aggregate security policy. The Wake Forest University (WFU) techniques described in U.S. patent application publication nos. 2006/0248580 and 2006/0195896 provide the methods to optimally reorder the list while preserving the aggregate security policy, thereby improving the performance of the firewall. The WFU techniques also include methods to break apart rules into functionally independent lists containing (groups of) dependent rules such that a function parallel firewall can simultaneously process one packet against multiple lists, which can substantially improve the performance of the firewall. However, these improvements provided by WFU techniques can be dwarfed by the performance degradation as the number of rules in the list becomes very large.

[0004] A key reason for the lack of scalability of most firewall implementations is due to the common use of linear search algorithms for comparing packets against a list of rules. In the worst case, a packet is matched at the last N^{th} rule in the list, so it must also be compared against all N−1 prior rules for a total of N comparisons. This poses a computational resource problem when the size of N is very large on a single processing node (including when such nodes are arranged in a data-, function-, hierarchical- or hybrid-parallel system), where the time required for processing each packet can quickly increase latency and reduce throughput to unacceptable levels. In fact, the WFU techniques provide good results in part because the reordering of, or the reduction in size of, rules on each processing node allows for a larger percentage of the total rules to reside in each processor's cache(s), which then substantially increases their performance relative to when only a small portion of those rules are cached.

[0005] The problem of searching firewall rule sets is well understood and highly researched, and there are some published techniques for sub-linear (substantially faster than linear) techniques applicable to firewall rules. However, these sub-linear techniques generally involve changing the underlying representation of rules. Examples of such an approach might be to use a graph, tric- or tree-like structure instead of a list to represent a set of rules, which would allow a match to be determined using tree search algorithms by traversing down the graph, trie or tree (see E. Fulp, Trie-Based Policy Representations for Network Firewalls, Proceedings of the IEEE International Symposium on Computer Communications, 2005 and Al-Shaer et al., Modeling and Management of Firewall Policies, IEEE Transactions on Network and Service Management, 2004). These approaches have potential but can add complexity or limitations that may reduce their practical usefulness in a commercial high performance firewall product.

SUMMARY

[0006] Adaptive packet filtering (APF), a set of techniques for processing firewall rules and packets, is described herein. APF offers improved processing performance compared to the WFU techniques in most cases, and can be combined with the WFU techniques or other parallel, pipelining and optimization techniques to achieve even greater performance.

[0007] The subject matter described herein includes methods, systems, and computer readable media for adaptive packet filtering. One method includes identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the subset contains disjoint rules. Disjoint rules are defined as rules whose order can be changed without changing the integrity of the firewall policy. Rules in the subset are sorted to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters. Packets are filtered at the firewall using the sorted rules in the subset by using binary search, interpolated search, informed search, or hash lookup search algorithms to compare each packet to the sorted rules in the subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for packets filtered using the sorted rules in the subset.

[0008] The subject matter described herein for adaptive packet filtering can be implemented in a non-transitory computer readable medium having stored thereon executable instructions that when executed by the processor of a computer control the computer to perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include chip memory devices, disk memory devices, programmable logic devices and application specific integrated circuits. In addition, a computer readable medium that implements a subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

[0009] Further, the subject matter described herein for adaptive packet filtering can be implemented on a particular machine, such as a network firewall including one or more network interfaces for receiving packets and packet filtering hardware and software for optimizing rules as described herein and for filtering packets using the optimized arrangement of rules.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Preferred embodiments of the subject matter described herein will now be described with reference to the accompanying drawings of which:

[0011] FIG. 1 is a block diagram of a system for adaptive packet filtering according to an embodiment of the subject matter described herein;

IPR2023-01353 Page 01417

[0012] FIG. **2** is a block diagram of application of the present subject matter to a pipelined processing approach according to an embodiment of the subject matter described herein;

[0013] FIG. **3** is a block diagram illustrating application of the present subject matter to a combination of pipelined and data parallel processing approaches according to an embodiment of the subject matter described herein; and

[0014] FIG. **4** is a block diagram illustrating application of the present subject matter to a short-circuiting pipelined processing approach according to an embodiment of the subject matter described herein; and

[0015] FIG. **5** is a block diagram illustrating application of the present subject matter to a combination of pipelined and function parallel processing approaches according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

[0016] Methods, systems, and computer readable media for adaptive packet filtering are disclosed. FIG. **1** is a block diagram illustrating an exemplary system for adaptive packet filtering according to an embodiment of the subject matter described herein. Referring to FIG. **1**, a firewall **100** may function at the boundary between an external network and a protected network. Firewall **100** may include one or more network interfaces **102** for receiving packets from the external network. Firewall **100** may also include one or more network interfaces **104** for transmitting allowed packets to the protective network. In one implementation, firewall **100** may filter Internet protocol (IP) packets based on a combination of source and destination addresses in the IP headers of the packets. However, the subject matter described herein is not limited to filtering any particular protocol. Any packet network protocol with parameters for which firewall filtering rules can be defined is intended to be within the scope of the subject matter described herein.

[0017] As used herein, the term "firewall" includes any network security device or system of devices that inspects network traffic data that originates, terminates, or traverses the device system in any capacity and compares that traffic data (headers, payload, raw bits, etc.) to a set of one or more rules, signatures, or conditions, either inline (i.e., in real time) or offline (i.e., capture and replay of the traffic data). The term "firewall" is also intended to include an intrusion detection device that analyzes network traffic in real time or historically to detect the presence of intrusion events in a network. The term "firewall" is also intended to include a deep packet inspection device that analyzes network traffic in real time or historically to detect the presence of certain packet content in a network.

[0018] Firewall **100** includes a firewall rule subset identifier/rule sorter **106** for identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing the firewall policy. Firewall rule subset identifier/rule sorter **106** may sort the rules in the subset or subsets to statistically decrease the number of comparison that will be applied to each packet that the firewall encounters. Exemplary methods for grouping and sorting rules will be described below.

[0019] Although in the example illustrated in FIG. **1** rule subset identifier/rule sorter **106** is illustrated as a component of firewall **100**, the subject matter described herein is not limited to such an implementation. Rule subset identifier/rule sorter **106** can be implemented on any computing platform capable of sorting firewall rules using the methods described herein, and the sorted rule set can be provided to firewall **100** through any suitable means, such as communication over a network. In one implementation, rule subset identifier/rule sorter **106** may be implemented on a management platform separate from firewall **100**.

[0020] Firewall **100** further includes a packet filter **108** for filtering packets at the firewall using the rules in the subset by using binary search, interpolated search, informed search, hash lookup search algorithms, or other sub-linear algorithms to compare each packet to each of the sorted rules in the subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in the subset.

[0021] Once the subsets of disjoint rules have been identified by rule subset identifier/rule sorter **106**, the rule subsets can be distributed across plural firewall processors in order to improve packet filtering efficiency. FIG. **2** is a block diagram illustrating an exemplary pipelined approach where rules and different subsets are distributed across plural firewall processors for processing packets in a pipelined manner. Referring to FIG. **2**, firewalls **200** and **202** each include separate processors **204** and **206** for executing packet filters **108**. In this example, rule subset identifier/rule sorter **106** identifies two rule subsets, subset A **208** and subset B **210**. The rules within each subset **208** and **210** are disjoint and sorted to statistically decrease the number of comparisons that will be applied to each packet using the methods described herein. However, the rules in subset B **210** are dependent on the rules in rule subset A **208**. Accordingly, rule subset identifier/rule sorter **106** distributes the rule across firewall processors **204** such that the rules in rule subset A **208** are applied before the rules in rule subset B **210**. Because the rules in different subsets are distributed across plural processors in a pipeline manner, packet filtering efficiency is improved over a single-processor approach because the different processors can simultaneously apply rules to different packets. In the example illustrated in FIG. **2**, packets that pass the filtering of rule subset A **208** are processed by processor **206**, which applies rule subset B **210**, at the same time that processor **204** applies rule subset A to new incoming packets.

[0022] In yet another embodiment, rule subset identifier/rule sorter **106** may distribute the grouped, sorted rules across firewall processors such that a combination of pipelined and data parallel processing techniques are used. FIG. **3** illustrates an example where firewalls **300**, **302**, **304**, and **306** each include separate processors **308**, **310**, **312**, and **314** for applying their respective packet filters. In the illustrated example, rule subset identifier/rule sorter **106** distributes rule subset A **316** to firewall **300**, rule subset B **318** to firewalls **302** and **304**, and rule subset C **320** to firewall **306**. The rules within each subset A, B and C are disjoint. The rules in subset B are dependent upon the rules in subset A. The rules in subset C are dependent upon the rules in subsets A and B.

[0023] In operation, packets entering firewall **300** are filtered using rule subset A **316**. The packets that are allowed by rule subset A **316** are divided between firewalls **302** and **304** such that the application of the rules in rule subset B **318** to different packets is performed in parallel. This is referred to as a data parallel approach. The packets that pass the filtering by rule subset B **318** are passed to firewall **306** for application of

IPR2023-01353 Page 01418

the rules in rule subset C **320**. Accordingly, FIG. **3** illustrates an example where the rule subsets that are identified and sorted by rule subset identifier/rule sorter **106** are distributed across the firewall processors for a combination of pipelined and data parallel processing.

[0024] In yet another embodiment, the rules subsets that are identified and in which the rules are sorted using rule subset identifier/rule sorter **106** may be distributed across firewall processors in a short-circuiting pipelined manner. FIG. **4** is an example of short-circuiting pipelined filtering using rule subsets that are identified and sorted by rule subset identifier/rule sorter **106**. Referring to FIG. **4**, a first firewall **400** and a second firewall **402**, respectively including processors **404** and **406**, filter packets using packet filters **108**. In the illustrated example, packet filter **108** uses rule subset A **408** and packet filter **108** uses rule subset B **410**. Rule subsets A and B **408** and **410** may respectively implement different levels of a firewall hierarchy such that packets that pass the filtering by rule subset A **408** are allowed into the protected network. Packets that are identified by rule subset A **408** is requiring further filtering are distributed to rule subset B **410** for that filtering. Thus, rule subset identifier/rule sorter **106** can also be used with short-circuiting pipelined firewall techniques without departing from the scope of the subject matter described herein.

[0025] In yet another embodiment, rule subset identifier/rule sorter **106** may distribute the grouped, sorted rules across firewall processors such that a combination of pipelined and function parallel processing techniques are used. FIG. **5** illustrates an example where firewalls **500**, **502**, **504**, and **506** each include separate processors **508**, **510**, **512**, and **514** for applying their respective packet filters. In the illustrated example, rule subset identifier/rule sorter **106** distributes rule subset A **516** to firewall **500**, rule subset B **518** to firewalls **502**, and rule subset C **520** to firewall **504**, and rule subset D **522** to firewall **506**. The rules within each subset A, B, C and D are disjoint. The rules in subset B and C are dependent upon the rules in subset A. The rules in subset D are dependent upon the rules in subsets A, B and C.

[0026] In operation, packets entering firewall **500** are filtered using rule subset A **516**. The packets that are allowed by rule subset A **516** are copied to both firewalls **502** and **504** such that the application of the rules in rule subsets B **518** and C **520** to the packets is performed in parallel. This is referred to as a function parallel approach. The packets that pass the filtering by rule subsets B **518** and C **520** are passed to firewall **506** for application of the rules in rule subset D **522**. Accordingly, FIG. **5** illustrates an example where the rule subsets that are identified and sorted by rule subset identifier/rule sorter **106** are distributed across the firewall processors for a combination of pipelined and function parallel processing.

TECHNIQUE

[0027] APF analyzes and orders the list of firewall rules in-place to contain functionally dependent groups, where each group contains a subset of rules that are disjoint, dependent or both, without substantially changing the underlying representation of rules and while preserving the aggregate security policy. APF then uses varying criteria to sort each group containing disjoint rules, then uses sub-linear search algorithms when comparing packets against the rules within that group. APF uses linear search algorithms when comparing packets within a group containing dependent rules or when otherwise appropriate. A detailed computational complexity analysis of APF would need to be completed. However, on average, it is hypothesized that only O(log(N)) comparisons would be needed to process a rule list of size N. In the theoretical best case when all rules are disjoint, this translates to about 20 comparisons (instead of 1,000,000) for a list of N=1,000,000 rules and about 30 comparisons for a list of N=1,000,000,000 rules. In the worst case when all rules are dependent, APF performs the same as linear search firewall cores. In practice, APF should process a packet against a very large list of rules (N=millions) in the same amount of time that other techniques can process against a very small list (N=hundreds, or thousands). APF does not inherently use parallel techniques; therefore, it can be combined with WFU techniques or other parallel/pipelining techniques to increase performance.

[0028] The following table shows preliminary results comparing a single linear search firewall) with a single APF core as the number of rules is increased.

	linear firewall core		APF core	
N = # rules in the core	PPS = packets per second at max throughput with 0 loss	Latency in microseconds at max throughput with 0 loss	PPS = packets per second at max throughput with 0 loss	Latency in microseconds at max throughput with 0 loss
1	844,595	12.3	811,688	12.3
10	730,994	11.9	765,871	12.3
100	314,861	13.9	718,391	12.0
1,000	29,357	44.6	683,060	12.0
10,000	930	1,112.4	464,684	12.0
100,000	Fail	Fail	292,740	17.4
1,000,000			252,525	14.3
10,000,000			132,556	18.6

DETAILED TECHNIQUE

[0029] This section describes an exemplary algorithm for implementing the subject matter described herein.

[0030] A firewall rule is defined as an n-tuple criteria and an associated action for matching packets. For example, a 5-tuple rule that matches Internet Protocol version 4 (IPv4) packets might consist of 5 IPv4 header fields (source address, source port, destination address, destination port and protocol) and an action (allow, deny), and might specify the rule R1 as:

IPR2023-01353 Page 01419

Rule	Source Addr	Source Port	Dest Addr	Dest Port	Protocol	Action
R1	192.168.1.1	12345	10.1.1.1	80	TCP	DENY

[0031] A firewall rule set is defined as an ordered list of n rules R1, R2, R3, . . . , Rn where the i in Ri is the index of the rule in the list. Packets that traverse the firewall are checked against each rule in the rule set until the first matching rule is found and its associated action is applied. An example rule set is S1 which contains:

Rule	Source Addr	Source Port	Dest Addr	Dest Port	Protocol	Action
R1	192.168.1.1	12345	10.1.1.1	80	TCP	DENY
R2	192.168.2.2	ANY	10.2.2.2	25	TCP	ALLOW
R3	192.168.3.3	ANY	10.3.3.3	53	UDP	ALLOW
R4	ANY	ANY	10.1.1.1	ANY	ANY	ALLOW
R5	ANY	ANY	ANY	ANY	ANY	DENY

An example TCP packet from source 192.168.4.4 port 54321 to destination 10.1.1.1 port 80 would be checked against but not match R1, R2 and R3; would be checked against and match R4 and be allowed; and, would not be checked against R5 because R4 was the first matching rule.

[0032] A firewall security policy is defined as the set of all possible packets that can traverse the firewall along with their specified outcomes as defined by the rule set. Changing the rules in a rule set usually results in a change of its security policy.

[0033] Within a rule set, a firewall rule is dependent on another rule if swapping the order of the two rules results in a change in the security policy of the rule set. Otherwise, the two rules are disjoint if swapping the order does not result in a change the security policy. For example, in rule set S1 above, rules R1 and R4 are dependent because placing R4 ahead of R1 would render R1 ineffective, thereby changing the security policy. Rules R1 and R2 are disjoint because placing R2 ahead of R1 does not change the security policy.

[0034] A permutation of a rule set is defined as a new rule set which contains the same rules as the original rule set, but which lists a different ordering of the rules from the original rule set without changing the original security policy. For example, in the rule set S1 above, swapping the order of the disjoint rules R1 and R2 would result in a permutation rule set S1':

Rule	Source Addr	Source Port	Dest Addr	Dest Port	Protocol	Action
R2	192.168.2.2	ANY	10.2.2.2	25	TCP	ALLOW
R1	192.168.1.1	12345	10.1.1.1	80	TCP	DENY
R3	192.168.3.3	ANY	10.3.3.3	53	UDP	ALLOW
R4	ANY	ANY	10.1.1.1	ANY	ANY	ALLOW
R5	ANY	ANY	ANY	ANY	ANY	DENY

[0035] Two rules are spatially disjoint if they are disjoint and their corresponding tuples are either identical or do not overlap. For example, in the rule set S1 above, rules R1 and R2 are disjoint but not spatially disjoint because the source ports 12345 and ANY overlap. However, rules R2 and R3 are both disjoint and spatially disjoint because the source ports ANY and ANY are identical, and the other 4 tuples do not overlap. (Other examples follow.)

[0036] A transform function is an algorithm that can be applied to a rule to create a sortable key for that rule, which can then be used to sort the rules by their keys using a key comparison function. For example, the transform function Tfn could concatenate the tuples of a rule into a bit array that is interpreted as a large integer, and a corresponding comparison function Cfn could be a simple integer comparison function. (Other examples follow.)

[0037] A rule subset is defined as an ordered grouping of one or more rules within a rule set. For example, in rule set S1 above, the rule subsets might be:

Subset	Rules
T1	R1, R2, R3
T2	R4
T3	R5

[0038] A rule group is defined as a rule subset with a group type (dependent, disjoint), transform function, comparison function, and a search algorithm hint (linear, sub-linear). The group type can be dependent if the group contains dependent rules, or can be disjoint if the group strictly contains disjoint rules. For example, the rule set S1 above might contain the following disjoint rule group:

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R1, R2, R3	Tfn	Cfn	Sub-linear

[0039] A rule set may be partitioned into a list of ordered rule groups such that the security policy of the rule set is not changed when each rule group is decomposed in the listed order. This partitioning is accomplished by applying a rule subset identification method to a given rule set. An example of such a method is:

[0040] 1. For a given rule set S containing n rules R1, R2, . . . , Rn:

[0041] a. Create a new empty disjoint rule group Gj (initially G1) in S.

[0042] b. Place the first ungrouped rule Ri (initially R1) into Gj.

[0043] c. For each remaining ungrouped rule Ri in S:

[0044] i. If Ri is disjoint from rules in Gj and placing Ri into Gj does not modify the security policy of S, then place Ri into Gj.

[0045] ii. Otherwise, leave Ri ungrouped.

[0046] d. If S contains ungrouped rules, then go to step 1.a.

[0047] 2. The rule set S now contains m disjoint rule groups G1, G2, G3, . . . , Gm which group together the n (possibly reordered) rules R1, R2, . . . , Rn.

Applying the above method to rule set S1 might result in its partitioning into the following list of disjoint ordered rule groups:

IPR2023-01353 Page 01420

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R1, R2, R3			Linear
G2	Disjoint	R4			Linear
G3	Disjoint	R5			Linear

Decomposing the disjoint rule groups would result in G1, G2, G3={R1, R2, R3}, {R4}, {R5}=R1, R2, R3, R4, R5=S1.

[0048] A partitioned rule set containing disjoint rule groups may then be sorted by applying a transform function to each rule within each disjoint group to derive a sortable key for each rule. Then, the rules may be reordered within their disjoint groups using their sortable keys. The resulting sorted groups may be searched using sub-linear searching algorithms. An example of the sorting method is:

[0049] 1. For each disjoint group Gj in rule set S:

[0050] a. For each rule Ri in Gj:

[0051] i. Apply Transform Tfn to Ri to derive a sortable key Ki.

[0052] b. Sort the rules in Gj using the comparison function Cfn on the sortable keys K.

[0053] 3. The rule set S now contains m sorted disjoint rule groups G1, G2, G3, . . . , Gm.

Applying the above method to the partitioned rule set S1 might result in a new permutation rule set S1' that contains the following list of sorted rule groups where the ordering of rules within G1 might change from R1, R2, R3 to R3, R1, R2:

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R3, R1, R2	Tfn	Cfn	Sub-linear
G2	Disjoint	R4	Tfn	Cfn	Sub-linear
G3	Disjoint	R5	Tfn	Cfn	Sub-linear

[0054] The permutated rule set containing disjoint rule groups may be consolidated to reduce the number of groups that contain a rule count at or below a certain threshold, such as 1 rule, by merging two or more consecutive disjoint groups into a larger dependent group that may be searched using linear searching algorithms. An example of the consolidation method is:

[0055] 1. For each group Gj in rule set S:

[0056] a. If the sum of the number of rules in Gj and its subsequent group Gj+1 is less than or equal to a specified threshold (e.g. 1), then the two groups are merged, their rules are concatenated, and the group type is set to dependent.

[0057] 2. The rule set S now contains m or fewer rule groups of both dependent and disjoint types.

Applying the above method to the permuted rule set S1' might merge the disjoint group G3 into G2:

Group	Group Type	Rules	Transform Fn	Comparison Fn	Hint
G1	Disjoint	R3, R1, R2	Tfn	Cfn	Sub-linear
G2	Dependent	R4, R5	(none)	(none)	Linear

[0058] The APF packet filtering method matches packets against a given rule set by sequentially iterating over each of the ordered rule groups, then performing the specified sub-linear or linear search within each group. An example of a rule filtering method is:

[0059] 1. For each packet that traverses the firewall:

[0060] b. For each group Gj in rule set S:

[0061] i. If Gj is a dependent group, then perform linear search within that group until there is a first rule match.

[0062] ii. If Gj is a disjoint group:

[0063] 1. Apply transform T to the packet to derive a lookup key K.

[0064] 2. Use the comparison function C and sub-linear search within the group until there is a first rule match on key K.

[0065] iii. If there is a first rule match, then process the packet according to its specified action. Otherwise, continue to the next group Gj+1.

ADDITIONAL NOTES

[0066] The primary purpose of the partitioning of rules is to create rule groups that, in aggregate, enable the fastest possible searching of each packet against the rules in the rule set. In most cases, the optimal partitioning should be the grouping of maximal subsets of spatially disjoint rules. However, in some cases where these disjoint groups are small (e.g. less than 10 rules), consolidating the disjoint groups into a single larger group containing rules that are ordered using other criteria (such as hit probabilities or hardware cache friendliness) and employing linear or interpolated search algorithms may improve performance. A critical concept is the flexibility to organize the rules within the rule set in different ways that enable the use of the most efficient and applicable search algorithm that is available that accounts for the hardware capabilities, which is the motivation behind the term "adaptive" in Adaptive Packet Filtering.

[0067] Rule sets may be partitioned, sorted and consolidated in-place.

[0068] When partitioning a rule set into rule groups, each disjoint group should generally contain the maximal subsets of disjoint rules in order to reduce the number of disjoint groups in the rule set.

[0069] When partitioning a rule set into rule groups and/or sorting those groups, the transform and comparison functions may be different for each rule group.

[0070] When partitioning a rule set into rule groups and/or sorting those groups, the algorithms may account for the hit probabilities of each rule and the aggregate hit probabilities of each group.

[0071] When filtering packets, the search performed within any given rule group may employ the fastest available search algorithm applicable to that group even if it may be different from the specified search algorithm hint.

[0072] When filtering packets, a sub-linear binary search within a disjoint rule group may account for hit probabilities at each pivot so that each recursion could maximize the probability of a rule match.

[0073] When filtering packets, a constant-time search within a disjoint rule group is possible by defining a

IPR2023-01353 Page 01421

hashing function as the transform function such that the hash values for all rules within a group are unique within that group.

Examples

[0074] This section provides examples of the following items described in the algorithm in the previous section.

1) Example of the rule breakup
2) Example of transform function
3) Definition of rule representation
4) Difference between sub-linear and linear
5) Explanation of disjoint rules

1) Examples of the Rule Breakup

[0075] Define

[0076] S1={R1, R2, R3, R4, R5)

and

[0077] R1=from 1.2.3.4 to 3.4.5.6 deny
[0078] R2=from 2.3.4.5 to 4.5.6.7 allow
[0079] R3=from 3.4.5.6 to 5.6.7.8 allow
[0080] R4=from *.*.*.* to 3.4.5.6 allow
[0081] R5=from *.*.*.* to *.*.*.* deny

[0082] Then S1' contains 3 groups of disjoint rules:

[0083] S1'={G1, G2, G3)
[0084] G1={R1, R2, R3)
[0085] G2={R4)
[0086] G3={R5)

[0087] Or, S1' can contain 2 groups of disjoint and dependent rules:

[0088] S1'={G1, G2)
[0089] G1={R1, R2, R3), disjoint, sub-linear
[0090] G2={R4, R5), dependent, linear

or

[0091] Define

[0092] S2={R1, R2, R3, R4, R5, R6, R7, R8, R9)

and

[0093] R1=from 1.2.3.4 to 3.4.5.6 deny
[0094] R2=from 2.3.4.5 to 4.5.6.7 allow
[0095] R3=from 1.2.3.4 to 4.5.6.7 deny
[0096] R4=from 1.*.*.* to *.*.*.* allow
[0097] R5=from 3.4.5.6 to 5.6.7.8 deny
[0098] R6=from 2.*.*.* to *.*.*.* deny
[0099] R7=from *.*.*.* to 3.4.5.6 allow
[0100] R8=from *.*.*.* to 5.6.7.8 allow
[0101] R9=from *.*.*.* to *.*.*.* deny

[0102] Then S2' contains 4 groups of "spatially disjoint" rules:

[0103] S2'={G1, G2, G3, G4)
[0104] G1={R1, R2, R3, R5)
[0105] G2={R4, R6)
[0106] G3={R7, R8)
[0107] G4={R9)

[0108] Or, S2' can contain 2 groups of disjoint and dependent rules:

[0109] S2'={G1, G2)
[0110] G1={R1, R2, R3, R5), disjoint, sub-linear
[0111] G2={R4, R6, R7, R8, R9), dependent, linear

2) Example of Transform Function

[0112] A rule R usually consists of an N-tuple, most basically a 3-tuple such as "from 1.2.3.4 to 3.4.5.6 deny"

[0113] tuple a=source IP address, e.g. "1.2.3.4"
[0114] tuple b=destination IP address, e.g. "3.4.5.6"
[0115] tuple c=action, e.g. "deny"

[0116] Each of these tuples have underlying scalar integer/bit vector representation, so in the above example:

[0117] source IP address="1.2.3.4"=32 bit integer 0016909060

[0118] destination IP address="3.4.5.6"=32 bit integer 0050595078

[0119] action="deny"=8 bit integer 000

[0120] One possible transform function is a transform to scalar key which concatenates the digits of each of the tuples into a large integer value:

[0121] T(a, b, c)=abc

[0122] T(1.2.3.4, 3.4.5.6, deny)=0016909060 0050595078 000=001690906000050595078000

[0123] Another possible transform function is a transform to scalar key which concatenates the bits of each of the tuples into a large integer/bit vector:

[0124] a=1.2.3.
4=00000001000000100000001100000100 (32 bits)

[0125] b=3.4.5.
6=00000011000001000000010100000110 (32 bits)

[0126] c=0=00000000 (8 bits)

T(a, b, c)=abc=000000010000001000000011000001000000001100000100000001010000110000000000

[0127] Another possible transform function is an identity function (i.e. transformation function that does not do anything), then defining a multi-dimensional comparison function for sorting purposes. An example of this is a comparison function that is radix-based for each tuple, which would essentially result in a rule set that is radix sorted by each tuple.

[0128] Note that the transform function must convert the rule into a sortable key, which does not necessarily have to be a scalar key (i.e. it can be a multi-dimensional key that uses a multi-dimensional comparison function for sorting).

3) Definition of Rule Representation.

[0129] Rule representation is the way a rule and a rule set are conceptually represented in software. The most common representation of a rule is as an N-tuple object or structure that simply holds all the tuples together:

```
struct rule {
    unsigned char ip_proto;
    unsigned int ip_src_addr;
    unsigned int ip_dst_addr;
    unsigned short ip_src_port;
    unsigned short ip_dst_port;
    ...
    unsigned char action;
};
```

[0130] The most common representation of a rule set is an array or linked list that hold the rules in a fixed order, and allows for iteration forwards and backwards in the array or list.

[0131] Example of Array:

memory location	0	1	2	3	4	5	6	7	8
value	R1	R2	R3	R4	R5	R6	R7	R8	R9

IPR2023-01353 Page 01422

[0132] Example of Linked List:

[0133] An alternate rule representation is to hold the rule and rule set in a trie or other graph structure. An example of this is described in "Balancing Trie-Based Policy Representations for Network Firewalls." Stephen J. Tarsa and Errin W. Fulp. Proceedings of the IEEE International Symposium on Computer Communications, 2006

[0134] Another alternate rule set representation is a hierarchical one as described in OPTWALL, described in Acharya et al., "OPTWALL: A Hierarchical Traffic-Ware Firewall," available at:

http://www.isoc.org/isoc/conferences/ndss/07/papers/OPTWALL.pdf,

where rule sets are broken down into mutually exclusive rule subsets which are arranged in a hierarchical order. Despite some similarities in terminology, OPTWALL and APF are different. For example, APF does not change the underlying rule or rule set representation. It simply reorders the rules in place and keeps track of the beginning and ending rules in each subset T externally from the rule or rule set. For example, say that a given rule is a standard structure and the rule set is an array form so that the rule set contains the following in the computer's memory:

[0135] Rule set S:

Location	0	1	2	3	4	5	6	7	8
value	R1	R2	R3	R4	R5	R6	R7	R8	R9

[0136] Suppose that the above rule set S can be divided into subsets containing disjoint rules:

[0137] T1=R2, R9, R1, R3

[0138] T2=R5, R7

[0139] T3=R2, R4, R8

so that

[0140] S'=T1, T2, T3=R2, R9, R1, R3, R5, R7, R2, R4, R8

[0141] Then the order of the rules in memory can be changed in place:

[0142] Rule set S':

location	0	1	2	3	4	5	6	7	8
value	R2	R9	R1	R3	R5	R7	R2	R4	R8
		---------				---		-------		
	T1				T2		T3		

[0143] The memory ranges for T1 (0-3), T2 (4-5) and T3 (6-8) are stored outside of the rule and rule set data structures.

4) Difference Between Linear and Sub-Linear.

[0144] A linear algorithm is one whose computational time increases linearly as the size of the set is increased. The best example of this is when looking up a word in a dictionary. If the dictionary is unsorted, then the order of the words would be arbitrary. Therefore, when looking up the word "zebra," one could start from the beginning and search until the end to find it. If the dictionary contains 1,000 entries, you would need to examine all 1,000 words in the worst case.

[0145] A sub-linear algorithm is one whose computational time increases sub-linearly as the size of the set is increased. In the above example, if the dictionary were sorted alphabetically, then one could still use a linear search by starting from the beginning and searching until the end to find "zebra." However, one could also use a sub-linear binary search algorithm by looking in the middle of the dictionary, then seeing if the middle entry comes alphabetically before or after (or is equal), then recursively selecting the middle of the appropriate half again and again to find the word "zebra." Since at each recursion ½ of the remaining words are eliminated, it would take about $\log_2$ (1,000) or about 10 examinations to find the entry in the worst case.

[0146] Another example of a sub-linear algorithm is hashing. Suppose that the above dictionary contains only 5 letter words. If we define a hash function that sums the alphabet order of each letter in the word (z=26, e=05, b=02, r=18, a=01), then hash("zebra")=26+05+02+18+01=52. The computer could have an array containing all the words in the dictionary where each word's position in the array is the hash value of the word (subject to collisions). In the above example, the array's 52nd position would have the word "zebra," so it would take only 1 comparison to determine a match without collision. This hash technique can be selectively used in APF.

5) Explanation of Disjoint Rules.

[0147] A rule R1 is "disjoint" from another rule R2 if their positions in the rule set S can be exchanged without altering the overall security policy. An example of this is rule set S containing:

[0148] R1=from 1.*.*.* to 2.3.4.5 deny

[0149] R2=from 1.2.3.4 to 1.2.3.4 allow

has the same security policy as rule set S' containing:

[0150] R2=from 1.2.3.4 to 1.2.3.4 allow

[0151] R1=from 1.*.*.* to 2.3.4.5 deny

because P=P'; therefore, R1 and R2 are disjoint.

[0152] The technique set forth above does not explain the concept of "spatially disjoint" rules. This is important if the transform function T cannot account for overlapping tuple values, which can be very common in practical settings.

[0153] A rule R1 is "spatially disjoint" from another rule R2 if they are "disjoint" and their corresponding tuples do not unevenly overlap (must be exactly equal, or do not overlap at all). In the above example, R1 and R2 are disjoint but not spatially disjoint because the first tuple of R1 (1.*.*.*) and R2 (1.2.3.4) are not equal but do overlap, i.e. the value of 1.2.3.4 would match the first tuple of both R1 and R2. An example of spatially disjoint rules are:

[0154] R3=from 1.2.3.4 to 3.4.5.6 deny

[0155] R4=from 2.3.4.5 to 3.4.5.6 allow

[0156] Here, the first tuple of R1 (1.2.3.4) and the first tuple of R2 (2.3.4.5) do not overlap, the second tuple of R1 (3.4.5.6) and R2 (3.4.5.6) are equal, and the >> third tuple of R1 (deny) and R2 (allow) do not overlap.

[0157] The importance of "spatially disjoint" rules is dependent upon the definition of a transform function T, so it may be possible to define T such that rules need not be "spatially disjoint" so long as rules are "disjoint."

[0158] The disclosure of each of the publications referenced herein is hereby incorporated by reference in its entirety.

[0159] It will be understood that various details of the presently disclosed subject matter may be changed without departing from the scope of the presently disclosed subject

IPR2023-01353 Page 01423

matter. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

What is claimed is:

1. A method for adaptive packet filtering, the method comprising:

identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the at least one subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing the integrity of the firewall policy;

sorting the rules in the at least one subset to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters; and

filtering packets at the firewall using the sorted rules in the at least one subset by comparing each packet to each of the sorted rules in the at least one subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in at least one subset.

2. The method of claim 1 comprising, for the disjoint rules within the at least one subset, identifying spatially disjoint rules and grouping the spatially disjoint rules together within the at least one subset and wherein sorting the rules includes sorting the rules within each of the spatially disjoint groupings.

3. The method of claim 1 comprising identifying at least another subset of rules in the ordered set of firewall rules that are non-disjoint and refraining from sorting the rules in the at least another subset and wherein filtering the packets includes filtering the packets using the sorted, disjoint rules and the non-sorted, non-disjoint rules, thereby achieving sub-linear searching for the sorted, disjoint rules and achieving linear searching for the non-sorted, non-disjoint rules.

4. The method of claim 1 wherein sorting the rules includes applying a transform function to each rule in the at least one subset to compute a sortable key for each of the rules and sorting the rules according to the keys.

5. The method of claim 1 wherein sorting the rules includes sorting the rules according to hit probabilities.

6. The method of claim 1 wherein sorting the rules includes sorting the rules in a binary search tree.

7. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using a binary search algorithm.

8. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using an interpolated search algorithm.

9. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using an informed search algorithm.

10. The method of claim 1 wherein filtering packets by comparing each packet to the sorted rules includes comparing each packet to the sorted rules using a hash lookup algorithm.

11. The method of claim 1 wherein each rule includes an IP source address and an IP destination address.

12. The method of claim 1 wherein the firewall includes a plurality of processors, the at least one subset comprises a plurality of subsets and further comprising distributing the subsets across the plurality of processors to implement at least one of pipelined processing, data parallel processing, and function parallel processing.

13. The method of claim 12 wherein the firewall implements a combination of pipelined and function parallel processing.

14. The method of claim 12 wherein the firewall implements a combination of pipelined and data parallel processing.

15. The method of claim 12 wherein the firewall implements a combination of pipelined, function parallel, and data parallel processing.

16. A system for adaptive packet filtering, the system comprising:

a firewall rule subset identifier/rule sorter for identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the at least one subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing integrity of the firewall policy, and for sorting the rules in the at least one subset to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters; and

a packet filter for filtering packets at the firewall using the sorted rules in the at least one subset by comparing each packet to each of the sorted rules in the at least one subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in at least one subset.

17. The system of claim 16 comprising, for the disjoint rules within the at least one subset, the firewall rule subset identifier/rule sorter identifies spatially disjoint rules and groups the spatially disjoint rules together within the at least one subset and wherein the firewall rule subset identifier/rule sorter the rules within each of the spatially disjoint groupings.

18. The system of claim 16 wherein the firewall rule subset identifier/rule sorter identifies at least another subset of rules in the ordered set of firewall rules that are non-disjoint and refrains from sorting the rules in the at least another subset and wherein the firewall packet filter filters the packets using the sorted, disjoint rules and the non-sorted, non-disjoint rules, thereby achieving sub-linear searching for the sorted, disjoint rules and achieving linear searching for the non-sorted, non-disjoint rules.

19. The system of claim 16 wherein the firewall rule subset identifier/rule sorter applies a transform function to each rule in the at least one subset to compute a sortable key for each of the rules and sorting the rules according to the keys.

20. The system of claim 16 wherein the firewall rule subset identifier/rule sorter sorts the rules includes sorting the rules according to hit probabilities.

21. The system of claim 16 wherein the firewall rule subset identifier/rule sorter sorts the rules includes sorting the rules in a binary search tree.

22. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using a binary search algorithm.

23. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using an interpolated search algorithm.

IPR2023-01353 Page 01424

24. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using an informed search algorithm.

25. The system of claim 16 wherein the packet filter compares each packet to the sorted rules using a hash lookup algorithm.

26. The system of claim 16 wherein each rule includes an IP source address and an IP destination address.

27. The system of claim 16 wherein the firewall includes a plurality of processors, the at least one subset comprises a plurality of subsets and further comprising distributing the subsets across the plurality of processors to implement at least one of pipelined processing, data parallel processing, and function parallel processing.

28. The system of claim 27 wherein the firewall implements a combination of pipelined and function parallel processing.

29. The system of claim 27 wherein the firewall implements a combination of pipelined and data parallel processing.

30. The system of claim 27 wherein the firewall implements a combination of pipelined, data parallel, and function parallel processing.

31. A non-transitory computer readable medium having stored thereon on executable instructions that when implemented by a processor of a computer controls the computer to perform steps comprising:

identifying at least one subset of rules in an ordered set of firewall packet filtering rules that defines a firewall policy such that the at least one subset contains disjoint rules, where disjoint rules are defined as rules whose order can be changed without changing integrity of the firewall policy;

sorting the rules in the at least one subset to statistically decrease the number of comparisons that will be applied to each packet that a firewall encounters; and

filtering packets at the firewall using the sorted rules in the at least one subset by comparing each packet to each of the sorted rules in the at least one subset until the packet is allowed or denied and ceasing the comparing for the packet in response to the packet being allowed or denied and thereby achieving sub-linear searching for the packets filtered using the sorted rules in at least one subset.

* * * * *

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
Wright, Bradley C.
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)

Applicant's or agent's file reference 007742.00031	Date of mailing *(day/month/year)* 26 June 2014 (26-06-2014)
International application No. PCT/US2014/027723	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 14 March 2014 (14-03-2014)

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.

   Where? 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 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. 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. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   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 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.

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 GOTTAR, Chantal Tel: +49 (0)89 2399-3203

RECEIVED
JUL 07 2014
BANNER & WITCOFF LTD

Form PCT/ISA/220 (July 2010)

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.
007742.00031		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2014/027723	14 March 2014 (14-03-2014)	15 March 2013 (15-03-2013)
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. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] 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
JUL 07 2014
BANNER & WITCOFF LTD

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2014/027723

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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02) figures 1-4 paragraph [0002] - paragraph [0027] paragraph [0037] - paragraph [0042] paragraph [0046] - paragraph [0058] ----- -/--	1-20

[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
13 June 2014	26/06/2014

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	Olaechea, Javier

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06] the whole document	1-20
A	EP 2 385 676 A1 (ALCATEL LUCENT [FR]; INST TELECOM TELECOM BRETAGNE [FR]) 9 November 2011 (2011-11-09) paragraph [0044] - paragraph [0059]	1-20
A	EP 2 498 442 A1 (OPENET TELECOM LTD [IE]) 12 September 2012 (2012-09-12) paragraph [0053] - paragraph [0079]	1-20
A	Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12] the whole document	1-20
A	US 2010/011434 A1 (KAY RONY [US]) 14 January 2010 (2010-01-14) paragraph [0034] - paragraph [0045]	1-20

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2014/027723

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006048142 A1	02-03-2006	NONE	
EP 2385676 A1	09-11-2011	CN 102934122 A	13-02-2013
		EP 2385676 A1	09-11-2011
		JP 2013525927 A	20-06-2013
		KR 20130005301 A	15-01-2013
		US 2013111548 A1	02-05-2013
		WO 2011138417 A1	10-11-2011
EP 2498442 A1	12-09-2012	EP 2498442 A1	12-09-2012
		US 2012233656 A1	13-09-2012
US 2010011434 A1	14-01-2010	NONE	

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

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/US2014/027723	14.03.2014	15.03.2013

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
JUL 01 2014
BANNER & WITCOFF LTD

Name and mailing address of the ISA:
European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0
Fax: +49 89 2399 - 4465

Date of completion of this opinion
see form PCT/ISA/210

Authorized Officer
Olaechea, Javier
Telephone No. +49 89 2399-8233

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 43bis.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 filed or furnished:

   a. (means)

      ☐ on paper

      ☐ in electronic form

   b. (time)

      ☐ in the international application as filed

      ☐ together with the international application in electronic form

      ☐ subsequently to this Authority for the purposes of search

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 in 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	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	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

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 document:

D1 US 2006/048142 A1 (ROESE JOHN J [US] ET AL) 2 March 2006 (2006-03-02)

D2 Sean Moore: "SBIR Case Study: Centripetal Networks Subtitle: How CNI Leveraged DHS S&T SBIR Funding to Launch a Successful Cyber Security Company Cyber Security Division 2012 Principal Investigators' Meeting 10-October-2012", , 10 October 2012 (2012-10-10), XP055122227, Retrieved from the Internet: URL:http://www.dhs.gov/sites/default/files/publications/csd-day-2-04-sbir-centripetal-price.pdf [retrieved on 2014-06-06]

D3 Cisco: "Control Plane Policing Implementation Best Practices", , 13 March 2013 (2013-03-13), XP002725728, Retrieved from the Internet: URL:https://web.archive.org/web/20130313135143/http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html [retrieved on 2014-06-12]

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claims 1, 11 and 16 is not new in the sense of Article 33(2) PCT.

2.1 The document D1 discloses (the references in parentheses applying to this document) in terms of claim 1:

A method, comprising:

at a computing platform comprising at least one processor, memory, and communication interface (*network device in Figures 1 and 2*):

receiving, via the communication interface, a plurality of packets (paragraph 55; *traffic is received by the network device*);
responsive to a determination that an overload condition has occurred in one or more networks associated with the computing platform, applying, by the processor and to at least some of the plurality of packets, a first group of packet-filtering rules that comprises at least one five-tuple indicating a first set of packets that should be allowed to continue toward their respective destinations, wherein applying the first group of packet-filtering rules includes allowing at least a first portion of the plurality of packets that fall within the first set of packets to continue toward their respective destinations (paragraphs 24, 56 and table in pages 9-10; *in response to an attack trigger, a rule set is activated by the network device, said rule set including disabling all traffic excluding the management traffic, RR1*); and

responsive to a determination that the overload condition has been mitigated to a first degree, applying, to at least some of the plurality of packets, a second group of packet-filtering rules that comprises at least one five-tuple indicating a second set of packets that should be allowed to continue toward their respective destinations, wherein applying the second group of packet-filtering rules includes allowing at least a second portion of the plurality of packets that fall within the second set of packets to continue toward their respective destinations, and wherein the second group of packet-filtering rules is less restrictive than the first group of packet-filtering rules (paragraph 24; *upon detection of a new triggering condition, a less restrictive set of filtering rules is implemented by the networking device*).

Since all the features of claim 1 are known in combination from document D1, the subject-matter of claim 1 is not new (Article 33(2) PCT). Therefore, claim 1 is not allowable (Article 33(1) PCT).

2.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 11 and 16, which therefore are also considered not new (Article 33(2) PCT).

2.3 Furthermore, it is noted that the disclosure of document D2 (see page 4) would also render the subject-matter of claims 1, 11 and 16 not new or at least not inventive.

3 None of the dependent claims 2-10, 12-15 and 17-20 contain additional features which lead the subject-matter to be both new and inventive (see documents D1-D3 and the corresponding passages cited in the search report).

Re Item VII

Certain defects in the international application

The independent claims are not in the two-part form in accordance with Rule 6.3(b) PCT, which in the present case would be appropriate, with those features known in combination from the prior art being placed in the preamble (Rule 6.3(b)(i) PCT) and with the remaining features being included in the characterising part (Rule 6.3(b)(ii) PCT).

The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

The description is not in conformity with the claims as required by Rule 5.1(a)(iii) PCT.

Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1-D3 is not mentioned in the description, nor are these documents identified therein.

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.
1743/2 PCT		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2010/054520	**28 OCTOBER 2010 (28.10.2010)**	28 AUGUST 2009 (28.08.2009)

Applicant

GREAT WALL SYSTEMS et al

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.

☐ 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 :
      ☒ 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,**
   ☒ 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,**
   ☒ 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. **1**
      ☒ as suggested by the applicant.
      ☐ as selected by this Authority, because the applicant failed to suggest a figure.
      ☐ as selected by this Authority, because this figure better characterizes the invention.
   b. ☐ none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2010/054520

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/22(2006.01)i, H04L 12/26(2006.01)i, H04L 12/56(2006.01)i, H04L 29/06(2006.01)i

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 12/22; G06F 15/16; H04L 9/00; G06F 9/00; H04L 12/56

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: firewall, filter, rule, policy

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6098172 A1 (MICHAEL JOHN COSS et al.) 01 August 2000 See figures 5A, 5B and their corresponding explanation.	1-31
A	US 2006-0070122 A1 (STEVEN MICHAEL BELLOVIN) 30 March 2006 See paragraphs [0007], [0049]-[0055].	1-31
A	US 2005-0010765 A1 (BRIAN D. SWANDER et al.) 13 January 2005 See figures 9, 10.	1-31
A	KR 10-2001-0079361 A (S.W. KIM) 22 August 2001 See abstract and figure 2.	1-31

☐ 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 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
26 APRIL 2011 (26.04.2011)	**27 APRIL 2011 (27.04.2011)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Cheongsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	CHUN, DAE NYUNG Telephone No. 82-42-481-5991

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2010/054520

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6098172 A1	01.08.2000	EP 0909073 A2	14.04.1999
		JP 03-298832 B2	19.04.2002
		JP 11-167537 A	22.06.1999
		JP 2002-215478 A	02.08.2002
		JP 2009-295187 A	17.12.2009
		JP 3298832 B2	08.07.2002
US 2006-0070122 A1	30.03.2006	US 7051365 B1	23.05.2006
US 2005-0010765 A1	13.01.2005	CN 1574791 A	02.02.2005
		EP 1484886 A2	08.12.2004
		JP 2004-364315 A	24.12.2004
		KR 10-2004-0110981 A	31.12.2004
		US 2007-0204154 A1	30.08.2007
		US 7308711 B2	11.12.2007
		US 7761708 B2	20.07.2010
KR 10-2001-0079361 A	22.08.2001	None	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREGORY A. HUNT
JENKINS, WILSON, TAYLOR & HUNT, P.A.
SUITE 1200 UNIVERSITY TOWER
3100 TOWER BOULEVARD
DURHAM, NC 27707

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	03 JUL 2008
Applicant's or agent's file reference 1498/3/2 PCT	**FOR FURTHER ACTION** See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US06/11291	28 March 2006 (28.03.2006)	28 March 2005 (28.03.2005)

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

IPC: **H04L 9/00**(2006.01),**G06F 9/00,15/16/17/00,15/18**(2006.01)
USPC: 726/1,11,25;713/163,166

Applicant

WAKE FOREST UNIVERSITY

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 or 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 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 notified 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.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	24 June 2008 (24.06.2008)	Ayaz Sheikh DEBORAH A. THOMAS PARALEGAL SPECIALIST Telephone No. 571-272-3000

Form PCT/ISA/237 (cover sheet) (April 2007)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US06/11291

Box No. I Basis of this 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. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

4. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US06/11291

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)	Claims 1-41	YES
	Claims NONE	NO
Inventive step (IS)	Claims 1-41	YES
	Claims NONE	NO
Industrial applicability (IA)	Claims 1-41	YES
	Claims NONE	NO

2. Citations and explanations:

Claims 1-41 meet the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest optimization of firewall policy management for intrusion detection and intrusion prevention while maintaining the integrity of the original policy. Prior art does not teach a heuristic to order firewall rules the reduces average number of comparison by calculating a probability indication a likelihood of receiving a packet matching the rule sorted in order of non-increasing probability while maintaining the integrity of firewall policy.

Claims 1-41 meet the criteria set out in PCT Article 33 (4) because the subject matter claimed can be made or used in industry.

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:
GREGORY A. HUNT
JENKINS, WILSON & TAYLOR, P.A.
SUITE 1400 UNIVERSITY TOWER
3100 TOWER BOULEVARD
DURHAM, NC 27707

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing *(day/month/year)*	11 SEP 2006
Applicant's or agent's file reference 1498/3/3 PCT	FOR FURTHER ACTION See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US05/47008	22 December 2005 (22.12.2005)	22 December 2004 (22.12.2004)

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

IPC: **G06F 17/00**(2006.01) G06F 17/00(2006.01)
USPC: 726/14

Applicant

WAKE FOREST UNIVERSITY

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 or 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 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 notified 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.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US	Date of completion of this opinion	Authorized officer
Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	16 August 2006 (16.08.2006)	Nasser G Moazzami Telephone No. 571-272-2100

Form PCT/ISA/237 (cover sheet) (April 2005)

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/47008

Box No. I Basis of this 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. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

☐ a sequence listing

☐ table(s) related to the sequence listing

b. format of material

☐ on paper

☐ in electronic form

c. time of filing/furnishing

☐ contained in the international application as filed.

☐ filed together with the international application in electronic form.

☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US05/47008

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)	Claims NONE	YES
	Claims 1-52	NO
Inventive step (IS)	Claims NONE	YES
	Claims 1-52	NO
Industrial applicability (IA)	Claims 1-52	YES
	Claims NONE	NO

2. Citations and explanations:

Please See Continuation Sheet

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:
Claims 1-52 lack novelty under PCT Article 33(2) as being anticipated by Xu (U.S. Patent Pub. No. 2002/0038339 A1).

Regarding claims 1 and 31, Xu teaches a function-parallel firewall/system comprising:
a first firewall node for filtering received packets using a first portion of a rule set including a plurality of rules, the first portion including less than all of the rules in the rule set (figure 13, reference number 1361); and
at least one second firewall node for filtering packets using a second portion of the rule set, the second portion including at least one rule in the rule set that is not present in the first portion (figure 13, reference number 1362),
wherein the first and second portions together include all of the rules in the rule set (paragraph 0170).

Regarding claim 2, Xu teaches wherein the first and second portions respectively include rules present in first and second levels of a firewall hierarchy (figure 9E).

Regarding claim 3, Xu teaches wherein the first and second firewall nodes are connected to each other such that the rules in the first level are applied to received packets before the rules in the second level (paragraph 0092).

Regarding claim 4, Xu teaches wherein the first firewall node is adapted to forward packets that pass one of the rules in the first portion to an internal network in a manner that bypasses the second firewall node (paragraph 0122).

Regarding claim 5, Xu teaches wherein the first firewall node is adapted to discard packets that fail one of the rules in the first portion (paragraph 0171).

Regarding claim 6, Xu teaches wherein the rules in the second portion are more processor-intensive than the rules in the first portion (paragraph 0170).

Regarding claim 7, Xu teaches comprising:
a packet distributor for replicating each packet to the first and second firewall nodes (figure 13, reference number 1390); and
a gate machine for collecting results of applying the first and second portions of the rule set to each packet from the first and second firewall nodes and for making a forwarding decision based on the results (figure 13, reference number 1300).

Supplemental Box
In case the space in any of the preceding boxes is not sufficient.

Regarding claim 8, Xu teaches wherein each of the first and second firewall nodes is adapted to process the packets in a pipelined manner and wherein the gate machine is adapted to maintain state information for multiple packets simultaneously (paragraph 0168).

Regarding claim 9, Xu teaches wherein the gate machine is adapted to signal the second firewall node when processing of a packet is no longer needed due to matching of the packet with one of the rules used by the first firewall node (paragraph 0119).

Regarding claim 10, Xu teaches wherein the first and second firewall nodes implement rules of the same hierarchical level (figure 9E).

Regarding claim 11, Xu teaches wherein at least one of the rules in the first portion is present in the second portion to provide redundancy (paragraph 0177).

Regarding claims 12 and 22, Xu teaches wherein the first and second firewall nodes are configured to implement a gateless design wherein the rules are distributed among the first and second firewall nodes such that for any given packet, one of the first and second firewall nodes will accept the packet and the other of the first and second firewall nodes will deny the packet (paragraph 0201).

Regarding claim 13, Xu teaches wherein the first and second firewall nodes are implemented on different physical machines (figure 13, reference number 1361, 1362, and 1363).

Regarding claim 14, Xu teaches wherein the first and second firewall nodes are implemented on different processors in the same machine (paragraph 0244).

Regarding claims 15 and 28, Xu teaches wherein the first and second firewall nodes are adapted to simultaneously process copies of the same packets (figure 12, reference number 1261-1263).

Regarding claims 16, 24, 32, and 36, Xu teaches wherein the rule set includes firewall rules for filtering packets based on packet headers (paragraph 0091).

Regarding claims 17, 25, 33, and 37, Xu teaches wherein the rule set includes intrusion detection rules for filtering packets based on packet payloads (paragraph 0091).

Regarding claims 18, 26, 34, and 38, Xu teaches wherein the rule set includes intrusion protection rules for filtering packets based on a combination of packet headers and packet payloads (paragraph 0091).

Regarding claim 19, Xu teaches a stateful function-parallel firewall system comprising:
a first function-parallel firewall subsystem including a plurality of firewall nodes implementing a first rule set for filtering packets arriving in a network, wherein the first function-parallel firewall subsystem includes at least first and second firewall nodes respectively implementing first and second portions of the first rule set, the first portion including at least one rule that is not present in the second portion (figure 13, reference number 1361 and figure 8, INBOUND PACKETS); and
a second function-parallel firewall sub-system including a second set of firewall nodes implementing a second rule set for filtering packets departing from the network, wherein the second function-parallel firewall subsystem includes at least third and fourth firewall nodes, the third and fourth firewall nodes implementing first and second portions of the second rule set, the first portion of the second rule set including at least one rule that is not present in the second portion of the second rule set, wherein the first and second function-parallel firewall subsystems share state information regarding connections established through the first and second sets of firewall nodes (figure 13, reference number 1362 and figure 8, OUTBOUND PACKETS).

Regarding claim 20, Xu teaches comprising a database node coupled to the first and second function-parallel firewall subsystems, wherein the database node stores the state information, wherein the first set of firewall nodes obtains state information regarding connections established through the second set of firewall nodes from the database node, and wherein the second set of firewall nodes obtains state information regarding connections established through the first set of firewall nodes from the database node (figure 14, reference number 1471-1473).

Regarding claim 21, Xu teaches wherein the first and second sets of firewall nodes store copies of the state information maintained by the database node (paragraph 0014).

Regarding claim 23, Xu teaches wherein the firewall nodes of the first subsystem are adapted to simultaneously process copies of the same packets arriving in the network and wherein the firewall nodes in the second subsystem are adapted to simultaneously process copies of packets departing from the network (figure 12, reference number 1261-1263).

Regarding claim 27, Xu teaches a firewall grid comprising:
a plurality of firewall nodes being physically connected to each other via a network for filtering packets (figure 12, reference

Supplemental Box
In case **the space in any of the preceding boxes is not sufficient.**

number 1261, 1262, and 1263); and
a controller for controlling logical connections between the firewall nodes, wherein the controller is adapted to configure the firewall nodes in a logical firewall hierarchy without changing physical connections between the firewall nodes (paragraph 0165-0167).

Regarding claim 29, Xu teaches wherein the logical firewall hierarchy comprises a function-parallel hierarchy where individual firewall nodes implement different portions of a rule set (figure 13, reference number 1361-1363).

Regarding claim 30, Xu teaches wherein the controller is adapted to detect congestion at a first level in the firewall hierarchy and is adapted to reconfigure the logical connections between the firewall nodes to add a firewall node from another level in the firewall hierarchy to the level at which congestion was detected (figure 17).

Regarding claims 35 and 50, Xu teaches a method/computer program product for controlling access to a network based on a set of packet filtering rules distributed in a function-parallel manner, the method comprising:
distributing packet filtering rules of a rule set among a plurality of different nodes in a function-parallel manner so that at least some of the different nodes implement different portions of the rule set (figure 13, reference number 1361-1363);
replicating packets to each of the nodes (paragraph 0168); and
applying the rules to filter the packets (paragraph 0170).

Regarding claim 39, Xu teaches comprising, receiving a first packet at a first node, determining whether the packet matches a first rule implemented by the first node, and, in response to determining that a match occurs, notifying the other nodes of the match (paragraph 0119).

Regarding claim 40, Xu teaches comprising, at the other nodes, ceasing processing of the first packet (paragraph 0119).

Regarding claims 41 and 51, Xu teaches a method/computer program product for distributing rules in a function-parallel firewall, the method comprising:
defining a rule set for a function-parallel firewall (paragraph 0168);
assigning rules in the rule set to nodes and branches in a trie data structure, wherein each node in the trie data structure corresponds to a data field and each branch represents a value for each data field to be compared to values in corresponding fields in received packets (figure 13, reference number 1361-1363 and paragraph 0170); and
pruning the trie data structure in a manner that preserves ordering of the rules in the rule set (figure 20, deleting certain entries in 2091, 2092, and 2093).

Regarding claim 42, Xu teaches wherein pruning the trie data structure includes pushing a rule to its descendants and deleting the original rule (figure 20, deleting entries in 2091-2093).

Regarding claim 43, Xu teaches comprising reducing the depth of the trie using level reordering (paragraph 0246).

Regarding claim 44, Xu teaches wherein assigning rules in the rule set to nodes and branches in the trie data structure includes assigning rules requiring longer processing time to lower levels in the trie (paragraph 0170).

Regarding claims 45 and 52, Xu teaches a method/computer program product for assigning rules to a plurality of firewall nodes, the method comprising:
assigning packet filtering rules to nodes in a directed acyclical graph (DAG) (paragraph 0168);
representing relationships between rules by edges in the DAG (figure 9E); and
distributing the rules among a plurality of firewall nodes using the DAG such that different firewall nodes implement different rules and such that relationships between the rules specified in the DAG are preserved (figure 13, reference number 1361-1363 and paragraph 0170).

Regarding claim 46, Xu teaches wherein distributing the rules among a plurality of firewall nodes using the DAG includes distributing the rules such that intersecting accept rules are not present in more than one firewall node (figure 9E, rules that overlap are blacked out).

Regarding claim 47, Xu teaches wherein distributing the rules among a plurality of firewall nodes using the DAG includes distributing the rules such that the edges to not span multiple firewall nodes (figure 9E, rules that overlap are blacked out).

Regarding claim 48, Xu teaches wherein distributing the rules among a plurality of firewall nodes using the DAG includes replicating deny rules in each of the firewall nodes (paragraph 0177).

Regarding claim 49, Xu teaches comprising eliminating a deny rule implemented by a first firewall node in response to determining that the deny rule for the first firewall node includes no inbound edges and outbound edges from the first deny rule terminate only in a superset deny rule (paragraph 0177).

Doc Code: PA..

Document Description: Power of Attorney

PTO/AIA/82B(07-12)
Approved for use through 11/30/2014. OMB 0651-0035
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.

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in the attached transmittal letter.

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent): 22907

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A or equivalent):

Name	Registration Number	Name	Registration Number

Please recognize or change the correspondence address for the application identified in the attached transmittal letter to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant:

☐ Inventor or Joint Inventor

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor

☒ Assignee or Person to Whom the Inventor is Under an Obligation to Assign

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document)

SIGNATURE of Applicant for Patent

Signature		Date	July 19 2013
Name	Steven Rogers	Telephone	(571) 252-5082
Title and Company	Chief Executive Officer, Centripetal Networks, Inc.		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms for more than one signature, see below *.

☒ *Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. 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 1.11 and 1.14. This collection is estimated to take 3 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.

FILTERING NETWORK DATA TRANSFERS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation of and claims priority to U.S. Patent Application Serial No. 14/625,486, filed on February 18, 2015, and entitled "FILTERING NETWORK DATA TRANSFERS," which is a continuation of U.S. Patent Application Serial No. 13/795,822, filed on March 12, 2013, now U.S. Patent No. 9,124,552, and entitled "FILTERING NETWORK DATA TRANSFERS." The disclosures of these two priority applications are incorporated by reference herein in their entirety and made part hereof.

BACKGROUND

[0002] The TCP/IP network protocols (*e.g.*, the Transmission Control Protocol (TCP) and the Internet Protocol (IP)) were designed to build large, resilient, reliable, and robust networks. Such protocols, however, were not originally designed with security in mind. Subsequent developments have extended such protocols to provide for secure communication between peers (*e.g.*, Internet Protocol Security (IPsec)), but the networks themselves remain vulnerable to attack (*e.g.*, Distributed Denial-of-Service (DDoS) attacks, phishing attacks, and the like).

[0003] A category of cyber attack known as exfiltrations (*e.g.*, stealing sensitive data or credentials via the Internet) has proven to be especially difficult for conventional cyber defense systems to prevent. A first cause is that many exfiltrations are facilitated by using popular network data transfer protocols, such as the Hypertext Transfer Protocol (HTTP) used by the World Wide Web, that often appear to an observer (*e.g.*, a conventional cyber defense system) as normal network behavior. A second cause is that typical network trust models, such as those used by network firewalls, interpret exfiltrations as trusted operations. A third cause is that human users often knowingly or unknowingly engage in network activities that are vulnerable to attack. A fourth cause is the general inability of conventional cyber defense systems to scale sufficiently to counter a cyber threat; for example, with respect to traffic volumes, network link speeds, network performance (*e.g.*, latency and packet loss requirements), network usage policy enforcement, etc. Accordingly, many cyber attacks (*e.g.*, DDoS attacks and exfiltrations) leverage Internet-scale

characteristics to achieve their goals. Moreover, beyond those enumerated here, there are other causes for the failure of conventional, state-of-the-art cyber defense systems to prevent cyber attacks, such as exfiltrations.

SUMMARY

[0004] The following presents a simplified summary in order to provide a basic understanding of some aspects of the disclosure. It is neither intended to identify key or critical elements of the disclosure nor to delineate the scope of the disclosure. The following summary merely presents some concepts in a simplified form as a prelude to the detailed description below.

[0005] Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.

[0006] In some embodiments, a network packet filter may be located at a boundary between a secured network and an unsecured network (*e.g.*, the Internet). The filter may observe packets traversing the network link between the secured network and the unsecured network. The filter may be capable of comparing certain packet header information (*e.g.*, source and destination IP address(s), source and destination port(s), and protocol type(s)) with one or more packet filtering rules, which may define a network usage policy or network security policy. One or more of the rules may be associated with an operator that may be applied to a packet that matches one or more criteria specified by the rule.

[0007] Such packet filters may implement at least two operators: an identity operator, which may allow the packet to continue towards its destination, and a null operator which may prevent, or block, the packet from continuing towards its destination. In some embodiments, the network packet filter may implement one or more additional operators having the capability to determine

if a packet contains an application-level header that specifies a particular method associated with a data transfer protocol; and, if so, whether to apply an identity operator or null operator to the packet. To distinguish a network packet filter that implements said additional operators from network packet filters that do not, a network packet filter that implements such additional operators will be referred to hereinafter as a packet security gateway (PSG).

[0008] For example, such an operator may be able to perform one or more of the following functions: (1) determine if an IP packet traversing a boundary contains an HTTP packet (*e.g.*, an application-level HTTP packet) that specifies one or more specific HTTP methods (*e.g.*, GET, PUT, POST, etc.), and (2) allow the packet (*e.g.*, if a GET method is specified), or block the packet (*e.g.*, if a PUT or POST method is specified). One or more administrators of the secured network may associate such an operator with one or more rules in a network security policy in order to enforce, via the PSG, a Web usage policy that may, for example, allow users to surf (*e.g.*, GET) to one or more web sites attached to the Internet, but may prevent such user(s) from one or more of writing (*e.g.*, PUT) data files or posting (*e.g.*, POST) forms to one or more web sites. For example, administrator(s) may utilize such functionality to prevent one or more exfiltrations (*e.g.*, file transfers containing sensitive information, posting of login credentials (usernames and passwords), etc.) to network nodes (*e.g.*, web sites) that they may not trust.

[0009] Other details and features will be described in the sections that follow.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present disclosure is pointed out with particularity in the appended claims. Features of the disclosure will become more apparent upon a review of this disclosure in its entirety, including the drawing figures provided herewith.

[0011] Some features herein are illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings, in which like reference numerals refer to similar elements.

[0012] FIG. 1 illustrates an exemplary network environment in which one or more aspects of the disclosure may be implemented.

[0013] FIG. 2 illustrates an exemplary packet security gateway.

[0014] FIG. 3 illustrates an exemplary dynamic security policy with operators that filter on data transfer protocol, or application-layer protocol, header information.

[0015] FIG. 4 illustrates an exemplary method for protecting a secured network by enforcing one or more network usage policies or network security policies.

DETAILED DESCRIPTION

[0016] In the following description of various illustrative embodiments, reference is made to the accompanying drawings, which form a part hereof, and in which is shown, by way of illustration, various embodiments in which aspects of the disclosure may be practiced. It is to be understood that other embodiments may be utilized, and structural and functional modifications may be made, without departing from the scope of the present disclosure.

[0017] Various connections between elements are discussed in the following description. These connections are general and, unless specified otherwise, may be direct or indirect, wired or wireless, physical or logical. In this respect, the specification is not intended to be limiting.

[0018] FIG. 1 illustrates an exemplary network environment **100** in which one or more aspects of the disclosure may be implemented. Referring to FIG. 1, network **102** may function as an interconnect between networks **104**, **106**, and **108**. For example, network **102** may be the public Internet, or some other large TCP/IP network functioning as an interconnect between one or more Local Area Networks (LANs) or Wide-Area Networks (WANs), (*e.g.*, the Non-classified Internet Protocol (IP) Router Network (NIPRNet), operated by the United States Defense Information Systems Agency (DISA)). Networks **104**, **106**, and **108** may be LANs or WANs operated by or otherwise associated with various organizations (*e.g.*, one or more commercial enterprises, companies, universities, military commands, government agencies, or cyber criminal organizations).

[0019] For example, a geographically distributed commercial enterprise X may own and operate networks **104** and **106**, and use network **102** (*e.g.*, the Internet) to interconnect networks **104** and **106**, and to access other networks (*e.g.*, other networks not owned or operated by enterprise X) attached to network **102**. One or more computing devices (*e.g.*, workstations, servers, etc.) of enterprise X may be attached to network **104** or **106**. Network **108** may be owned

and operated by a cyber criminal organization Z, which may attempt to steal information (*e.g.*, sensitive data) from enterprise X, for example, via network **102**. Members of organization Z may attach one or more computing devices (*e.g.*, workstations or servers) to network **108**, and may use these workstation(s) or server(s) to attack or collect data from one or more networks affiliated with enterprise X (*e.g.*, network **104** or **106**).

[0020] As used herein, a packet security gateway (PSG) may include one or more computing devices configured to receive packets, and apply one or more filters or operators, including an identity (*e.g.*, allow) or null (*e.g.*, block) operator, to the packets. In some embodiments, a packet security gateway may be configured to apply one or more additional operators as described herein. As used herein, a security policy management server may include one or more computing devices configured to communicate a dynamic security policy to a packet security gateway. In some embodiments, a security policy management server may be configured to perform one or more additional functions as described herein. As used herein, a dynamic security policy may include one or more rules, messages, instructions, files, data structures, or the like specifying criteria corresponding to one or more packets and may identify one or more operators to be applied to packets corresponding to the specified criteria. In some embodiments, a dynamic security policy may specify one or more additional parameters as described herein.

[0021] Network environment **100** may include one or more packet security gateways and one or more security policy management servers. For example, network environment **100** may include packet security gateways **110** and **112**, and security policy management server **114**. One or more security policy management servers may be associated with a protected network. For example, networks **104** and **106** may each be distinct LANs associated with a common enterprise X, and may each form part of a protected or secured network associated with security policy management server **114**. Enterprise X may desire to prevent cyber attacks (*e.g.*, exfiltrations) from one or more of its networks (*e.g.*, network **104** or **106**). Accordingly, it may locate one or more packet security gateways at each boundary between its networks and one or more public interconnect networks (*e.g.*, network **102**), which may be utilized by a cyber criminal, such as organization Z, to attempt to remotely access its networks (*e.g.*, network **104** or **106**), and which may, for example, potentially be used to attempt to transfer data from one or more of its networks (*e.g.*, network **104** or **106**) to one or more networks affiliated with organization Z (*e.g.*, network **108**). For example, packet

security gateway **110** may protect network **104** from one or more cyber attacks (*e.g.*, exfiltrations) mediated by network **102** (*e.g.*, the Internet), and packet security gateway **112** may protect network **106** from one or more cyber attacks (*e.g.*, exfiltrations) mediated by network **102**.

[0022] As will be described in greater detail below, each of one or more packet security gateways associated with a security policy management server may be configured to receive a dynamic security policy from a security policy management server, receive packets associated with a network protected by the packet security gateway, and perform one or more operations specified by the dynamic security policy on the packets. For example, each of packet security gateways **110** and **112** may be configured to receive a dynamic security policy from security policy management server **114**. Each of packet security gateways **110** and **112** may also be configured to receive packets associated with networks **104**, **106**, or **108**. Each of packet security gateways **110** and **112** may further be configured to apply one or more rules or operators specified by the dynamic security policy received from security policy management server **114** to packets associated with networks **104**, **106**, or **108**.

[0023] FIG. 2 illustrates an exemplary packet security gateway according to one or more aspects of the disclosure. Referring to FIG. 2, as indicated above, packet security gateway **110** may be located at network boundary **202** between networks **104** and **102**. Packet security gateway **110** may include one or more processors **204**, memory **206**, network interfaces **208** and **210**, packet filter **212**, and management interface **214**. Processor(s) **204**, memory **206**, network interfaces **208** and **210**, packet filter **212**, and management interface **214** may be interconnected via data bus **216**. Network interface **208** may connect packet security gateway **110** to network **104**. Similarly, network interface **210** may connect packet security gateway **110** to network **102**. Memory **206** may include one or more program modules that when executed by processor(s) **204**, may configure packet security gateway **110** to perform one or more of various functions described herein.

[0024] Packet security gateway **110** may be configured to receive a dynamic security policy from security policy management server **114**. For example, packet security gateway **110** may receive dynamic security policy **218** from security policy management server **114** via management interface **214** (*e.g.*, via out-of-band signaling) or network interface **208** (*e.g.*, via in-band signaling). Packet security gateway **110** may include one or more packet filters or packet discriminators, or logic for implementing one or more packet filters or packet discriminators. For

example, packet security gateway **110** may include packet filter **212**, which may be configured to examine information associated with packets received by packet security gateway **110** and forward such packets to one or more of operators **220**, **222**, or **224** based on the examined information. For example, packet filter **212** may examine information associated with packets received by packet security gateway **110** (*e.g.*, packets received from network **104** via network interface **208**) and forward the packets to one or more of operators **220**, **222**, or **224** based on the examined information.

[0025] As will be described in greater detail below, dynamic security policy **218** may include one or more rules and the configuration of packet filter **212** may be based on one or more of the rules included in dynamic security policy **218**. For example, dynamic security policy **218** may include one or more rules specifying that packets having specified information should be forwarded to operator **220**, that packets having different specified information should be forwarded to operator **222**, and that all other packets should be forwarded to operator **224**. Operators **220**, **222**, and **224** may be configured to perform one or more functions on packets they receive from packet filter **212**. For example, one or more of operators **220**, **222**, or **224** may be configured to forward packets received from packet filter **212** into network **102**, forward packets received from packet filter **212** to an IPsec stack (not illustrated) having an IPsec security association corresponding to the packets, or drop packets received from packet filter **212**. In some embodiments, one or more of operators **220**, **222**, or **224** may be configured to drop packets by sending the packets to a local "infinite sink" (*e.g.*, the /dev/null device file in a UNIX/LINUX system).

[0026] FIG. 3 illustrates an exemplary dynamic security policy in accordance with one or more embodiments. Referring to FIG. 3, dynamic security policy **218** may include rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, 6 **312**, and 7 **314**. Each of these rules may specify criteria and one or more operators that may be applied to packets associated with (*e.g.*, matching) the specified criteria. The specified criteria may take the form of a five-tuple, which may, for example, comprise one or more values selected from, packet header information, specifying a protocol type of the data section of an IP packet (*e.g.*, TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or one or more other protocols), one or more source IP addresses, one or more source port values, one or more destination IP addresses, and one or more destination ports.

[0027] For example, rule 1 **302** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port 22 (*e.g.*, associated with the Secure Shell (SSH) protocol) should have an ALLOW operator (*e.g.*, an identity operator) applied to them. Similarly, rule 2 **304** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port 25 (*e.g.*, associated with the Simple Mail Transfer Protocol (SMTP)) should have an ALLOW operator applied to them.

[0028] Rule 3 **306** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port 110 (*e.g.*, associated with Post Office Protocol version 3 (POP3)) should have an ALLOW operator applied to them.

[0029] Rule 4 **308** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port 143 (*e.g.*, associated with the Internet Message Access Protocol (IMAP)) should have an ALLOW operator applied to them.

[0030] Rule 5 **310** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210, having any source port, destined for an IP address that begins with 140.212, and destined for port 443 (*e.g.*, associated with the port for the Hypertext Transfer Protocol Secure (HTTPS) protocol) should have a specified Transport Layer Security (TLS) protocol (*e.g.*, REQUIRE-TLS 1.1-1.2) operator (as described in greater detail below) applied to them.

[0031] Rule 7 **314** may be a "wildcard" rule and may apply a BLOCK operator (*e.g.*, a null operator which "drops" any packets it is applied to) to any packets that do not match the criteria of any of Rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, or 6 **312** (*e.g.*, when rules 1 **302**, 2 **304**, 3 **306**, 4 **308**, 5 **310**, 6 **312**, and 7 **314** are applied to packets in a linear fashion).

[0032] As described above with respect to FIG. 1, networks **104** and **106** may be owned or operated by enterprise X. Enterprise X may have allocated IPv4 addresses 140.210.0.0/16 to network **104**, and IPv4 addresses 140.212.0.0/16 to network **106**. Enterprise X may have loaded

PSG **110** with dynamic security policy **218**, and may utilize PSG **110** to enforce one or more network security policies embodied in one or more rules of dynamic security policy **218** to restrict network communications between networks **104** and **106** (*e.g.*, to secure system logins, e-mail, encrypted web sessions, and the like). For example, based on standard usage of ports, rule 1 **302** may allow any hosts attached to network **104** to conduct Secure Shell (SSH) sessions (*e.g.*, system logins) with any hosts attached to network **106**; rule 2 **304** may allow any e-mail servers attached to network **104** to conduct SMTP sessions (*e.g.*, e-mail transfer sessions) with any e-mail servers attached to network **106**; rule 3 **306** and rule 4 **308**, may respectively allow e-mail clients attached to network **104** to conduct POP3 and IMAP sessions (*e.g.*, e-mail download sessions into a webmail browser application) with any e-mail servers attached to network **106**; and rule 5 **310** may allow web browsers attached to network **104** to conduct HTTPS sessions (*e.g.*, secure web sessions) with any web servers attached to network **106**, but may, as described in greater detail below, utilize the REQUIRE-TLS-1.1-1.2 operator to ensure that only HTTPS secure web sessions using version 1.1 or 1.2 of the Transport Layer Security (TLS) protocol to secure such HTTPS sessions are allowed (*e.g.*, because the popular TLS version 1.0 protocol has a known security vulnerability that attackers may exploit to decrypt HTTPS sessions).

[0033] Rule 6 **312** may specify that IP packets containing one or more TCP packets, originating from a source IP address that begins with 140.210., having any source port, destined for an IP address that begins with 200.214, and destined for port 80 (*e.g.*, associated with the HTTP protocol) should have an HTTP-EXFIL operator applied to them. As described in greater detail below, an HTTP-EXFIL operator may allow HTTP packets containing a GET method, but may block HTTP packets containing other HTTP methods (*e.g.*, PUT, POST, CONNECT, etc.). Such an operator may thus allow a web browser to "surf the web" (*e.g.*, download web pages hosted by web servers), but may prevent the web browser from writing files to a web server (*e.g.*, using the PUT method), posting forms (*e.g.*, forms that might contain login credentials, such as usernames or passwords) to a web server (*e.g.*, using the POST method), or otherwise communicating with a web server (*e.g.*, using any HTTP method except GET). Because attackers may often use HTTP PUT or POST methods to exfiltrate sensitive data, operators such as HTTP-EXFIL may be used to stop such exfiltrations.

[0034] Returning to the example described above, organization Z may own or operate network **108**, and may have allocated network IP addresses 214.0.0.0/8 to network **108**. Enterprise X may not have a business relationship with organization Z, and may therefore not consider network **108** to be trusted. While enterprise X could simply block all communications to networks that are owned or operated by organizations it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet. Enterprise X's employees, therefore, could not freely surf the Web, which may restrict the employees' ability to conduct business on behalf of enterprise X. By enforcing sets of rules similar to rule 6 **312** that may apply operators like or similar to HTTP-EXFIL, enterprise X may enable its employees to freely surf the web and conduct company business, but may prevent one or more cyber attacks (*e.g.*, HTTP-mediated exfiltrations).

[0035] One function of operators like HTTP-EXFIL and REQUIRE-TLS-1.1-1.2 may be to inspect fields in the headers of application packets contained in IP packets, determine field values, and depending on the field values, decide to allow, block, or otherwise apply a packet transformation function (*e.g.*, encapsulate the packet into a tunnel, alter one or more header field values, etc.) to the packets. The logic for this function may be executed by one or more of operators **220**, **222**, or **224**. The logic may be developed in a high-level programming language such as C. An example of such programmatic logic, written in pseudocode, for the HTTP-EXFIL operator, is as follows:

[0036]
```
Operator HTTP-EXFIL(ip-packet):
        Inspect app-pkt(ip-packet) match GET return ALLOW;
        Inspect app-pkt(ip-packet) match POST return BLOCK;
        Inspect app-pkt(ip-packet) match PUT return BLOCK;
        Inspect app-pkt(ip-packet) match DELETE return BLOCK;
        Inspect app-pkt(ip-packet) match CONNECT return BLOCK;
        Return BLOCK;
End Operator HTTP-EXFIL;
```

[0037] Referring to the above-example, Operator HTTP-EXFIL may accept as input an IP packet that matches a rule, such as rule 6 **312** of dynamic security policy **218**. If the application packet contained in the IP packet is an HTTP packet, the value of the HTTP method field in the HTTP packet header may be compared to the values that encode the GET, POST, PUT, DELETE,

and CONNECT methods. If a match is found, then the HTTP-EXFIL operator may return either ALLOW or BLOCK, depending on the method value. If no match is found, then the HTTP-EXFIL operator may return BLOCK.

[0038] An example of programmatic logic, written in pseudocode, for a REQUIRE-TLS-1.1-1.2 operator is provided below. The REQUIRE-TLS-1.1-1.2 operator may be associated with filter rules for HTTPS sessions, such as rule 5 **310** of dynamic security policy **218**. HTTPS may be used to encrypt HTTP sessions. HTTPS is not a protocol *per se*, but rather the result of layering the HTTP protocol on top of the TLS protocol. For an HTTPS session composed of IP packets, the application packets contained in the IP packets may be TLS Record Protocol packets. The header fields of TLS Record Protocol packets may not be encrypted. One of the header fields may contain a value indicating the TLS version.

[0039] Exemplary programmatic logic for a REQUIRE-TLS-1.1-1.2 operator, written in pseudocode, is as follows:

[0040]
```
Operator REQUIRE-TLS-1.1-1.2(ip-packet):
        Inspect app-pkt(ip-packet) match 1.0 return BLOCK;
        Inspect app-pkt(ip-packet) match 1.1 return ALLOW;
        Inspect app-pkt(ip-packet) match 1.2 return ALLOW;
        Return BLOCK;
End Operator REQUIRE-TLS-1.1-1.2;
```

[0041] Referring to the above-example, Operator REQUIRE-TLS-1.1-1.2 may accept as input an IP packet that matches a rule, such as rule 5 **310** of dynamic security policy **218**. If the application packet contained in the IP packet is a TLS Record Protocol packet, the value of the version field in the TLS Record Protocol packet header may be compared to the values that encode version numbers 1.0, 1.1, and 1.2. If a match is found, then the REQUIRE-TLS-1.1-1.2 operator may return either ALLOW or BLOCK, depending on the version number value. If no match is found, then the REQUIRE-TLS-1.1-1.2 operator may return BLOCK.

[0042] The filtering process described herein may be viewed as having two (2) stages: A first stage in which the "5-tuple" of IP packet header field values and transport protocol (*e.g.,* TCP, UDP, etc.) packet header field values may be filtered; and, a second stage in which application

packet header field values may be filtered (*e.g.*, by applying operator logic similar to that described above). Conceptually, the first stage may determine if the network policy allows any communications between the resources identified in the 5-tuple rule; if so, the second stage may determine if the policy allows the specific method or type of communication (*e.g.*, file read, file write, encrypted communication, etc.) between the resources. Such a method may, however, be used in other conceptual models.

[0043] The methods described above may be modified to achieve different functionality and may be extended to other data transfer protocols or to other application-layer protocols. These methods may provide network administrators with capabilities to enforce network usage policies and network security policies that have capabilities and functionalities beyond those described above. For example, these methods may provide network administrators with capabilities to prevent exfiltrations that are mediated by other data transfer protocols besides HTTP and HTTPS. Examples of such protocols include File Transfer Protocol (FTP) and messaging protocols such as eXtensible Messaging and Presence Protocol (XMPP). Moreover, new network applications may emerge in the future which may use new data transfer protocols or application-layer protocols to which the present methods may be applied. These methods may also be used for purposes other than network policy enforcement and exfiltration prevention. For example, it may be useful for a packet filter to rapidly detect if an IP packet contains a Real-time Transport Protocol (RTP) application packet used to deliver audio or video information (*e.g.*, if a cyber attack based on RTP has yet to be discovered, network administrators may choose to not process RTP packets through the cyber security defense systems that may be protecting their networks).

[0044] FIG. 4 illustrates an exemplary method for protecting a secured network in accordance with one or more embodiments of the present disclosure. The steps may be performed at one or more packet security gateways associated with a security policy management server. For example, each of packet security gateways **110** and **112** may be associated with security policy management server **114**, and the steps may be performed at packet security gateway **110** or **112**. At step **400**, packets may be received. For example, packet security gateway **110** may receive packets from network **104** via network interface **208** that are destined for network **106**. At step **402**, a determination may be made as to whether a portion of the received packets have packet header field values corresponding to a packet filtering rule. For example, a determination may be made

as to whether a portion of the packets received from network **104** have packet header field values (*e.g.*, one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to rule 5 **310**. At step **404**, responsive to determining that one or more of the portion of received packets have packet header field values corresponding to the packet filtering rule, an operator specified by the packet filtering rule may be applied to the portion of the received packets. For example, the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** may be applied to the portion of the received packets.

[0045] At step **406**, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator. For example, a determination may be made as to whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (*e.g.*, application header field values corresponding to TLS version 1.1 or 1.2). At step **408**, responsive to determining that one or more of the portion of received packets have application header field values corresponding to one or more application header field criteria specified by the operator, a packet transformation function specified by the operator may be applied to the one or more of the portion of the received packets. For example, an ALLOW packet transformation function specified by the REQUIRE TLS-1.1-1.2 operator may be applied to the one or more of the portion of the received packets having application header field values corresponding to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (*e.g.*, each of the one or more of the portion of the received packets may be allowed to continue toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (*e.g.*, one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

[0046] Returning to step **406**, a determination may be made as to whether one or more application header field values of one or more of the portion of the received packets correspond to one or more application header field criteria specified by the operator. For example, a determination may be made as to whether one or more of the portion of the received packets have application header field values corresponding to one or more application header field criteria of

the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (*e.g.*, application header field values corresponding to TLS version 1.1 or 1.2). Responsive to determining that one or more of the portion of received packets have application header field values that do not correspond to one or more application header field criteria specified by the operator, one or more additional packet filtering rules may be applied to the one or more of the portion of the received packets. For example, rule 7 **314** may be applied to the one or more of the portion of the received packets having application header field values that do not correspond to one or more application header field criteria of the REQUIRE TLS-1.1-1.2 operator specified by rule 5 **310** (*e.g.*, each of the one or more of the portion of the received packets may be blocked from continuing toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (*e.g.*, one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

[0047] Returning to step **402**, a determination may be made as to whether a portion of the received packets have packet header field values corresponding to a packet-filtering rule. For example, a determination may be made as to whether a portion of the packets received from network **104** have packet header field values (*e.g.*, one or more of one or more data section protocols, one or more source IP addresses, one or more source ports, one or more destination IP addresses, or one or more destination ports) corresponding to rule 5 **310**. Responsive to determining that the portion of received packets have packet header field values that do not correspond to the packet filtering rule, one or more additional packet filtering rules may be applied to the one or more of the portion of the received packets. For example, rule 7 **314** may be applied to the portion of received packets that do not have packet header field values that correspond to rule 5 **310** (*e.g.*, each of the portion of the received packets may be blocked from continuing toward their respective destinations). The method may then return to step **400** and await receipt of one or more additional packets (*e.g.*, one or more additional packets from network **104** received via network interface **208** that are destined for network **106**).

[0048] The functions and steps described herein may be embodied in computer-usable data or computer-executable instructions, such as in one or more program modules, executed by one or more computers or other devices to perform one or more functions described herein. 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 various embodiments. 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. Particular data structures may be used to more effectively implement one or more aspects of the disclosure, and such data structures are contemplated to be within the scope of computer executable instructions and computer-usable data described herein.

[0049] Although not required, one of ordinary skill in the art will appreciate that various aspects described herein may be embodied as a method, an apparatus, or as one or more computer-readable media storing computer-executable instructions. Accordingly, those aspects may take the form of an entirely hardware embodiment, an entirely software embodiment, an entirely firmware embodiment, or an embodiment combining software, hardware, and firmware aspects in any combination.

[0050] As described herein, the various methods and acts may be operative across one or more computing devices and one or more networks. The functionality may be distributed in any manner, or may be located in a single computing device (*e.g.*, a server, a client computer, etc.).

[0051] Aspects of the disclosure have been described in terms of illustrative embodiments thereof. Numerous other embodiments, modifications, and variations within the scope and spirit of the appended claims will occur to persons of ordinary skill in the art from a review of this disclosure. For example, one of ordinary skill in the art will appreciate that the steps illustrated in the illustrative figures may be performed in other than the recited order, and that one or more steps illustrated may be optional.

CLAIMS

What is claimed is:

1. A method comprising:

receiving, by a computing system and from a computing device located in a first network, a plurality of packets, wherein the plurality of packets comprises a first portion of packets and a second portion of packets;

responsive to a determination by the computing system that the first portion of packets comprises data corresponding to criteria specified by one or more packet-filtering rules configured to prevent a particular type of data transfer from the first network to a second network, wherein the data indicates that the first portion of packets is destined for the second network:

applying, by the computing system and to each packet in the first portion of packets, a first operator, specified by the one or more packet-filtering rules, configured to drop packets associated with the particular type of data transfer; and

dropping, by the computing system, each packet in first portion of packets; and

responsive to a determination by the computing system that the second portion of packets comprises data that does not correspond to the criteria, wherein the data indicates that the second portion of packets is destined for a third network:

applying, by the computing system and to each packet in the second portion of packets, and without applying the one or more packet-filtering rules configured to prevent the particular type of data transfer from the first network to the second network, a second operator configured to forward packets not associated with the particular type of data transfer toward the third network; and

forwarding, by the computing system, each packet in the second portion of packets toward the third network.

ABSTRACT

Aspects of this disclosure relate to filtering network data transfers. In some variations, multiple packets may be received. A determination may be made that a portion of the packets have packet header field values corresponding to a packet filtering rule. Responsive to such a determination, an operator specified by the packet filtering rule may be applied to the portion of packets having the packet header field values corresponding to the packet filtering rule. A further determination may be made that one or more of the portion of the packets have one or more application header field values corresponding to one or more application header field criteria specified by the operator. Responsive to such a determination, at least one packet transformation function specified by the operator may be applied to the one or more of the portion of the packets.

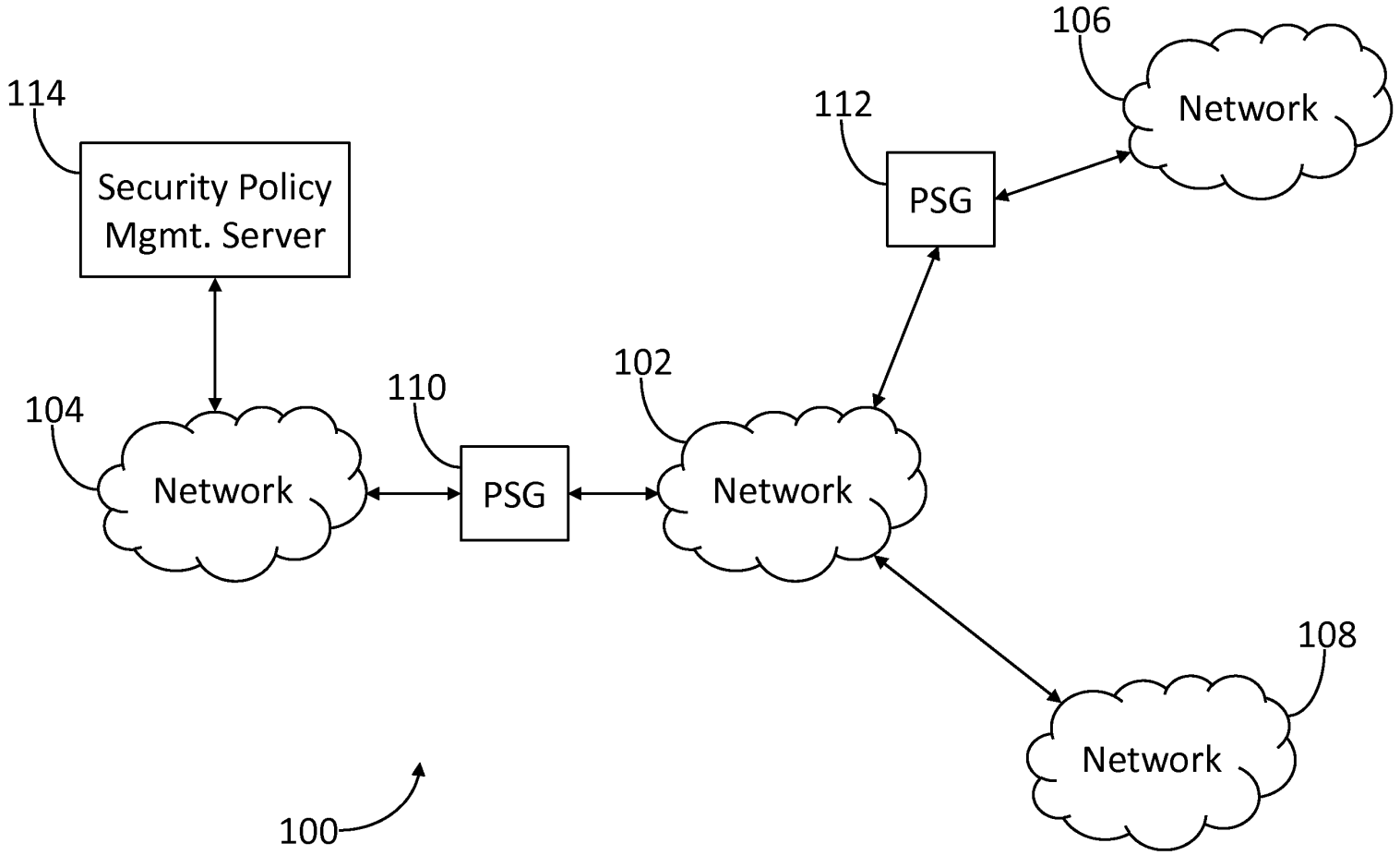

114
Security Policy
Mgmt. Server
106
Network
112
PSG
104
Network
110
PSG
102
Network
108
Network
100

FIG. 1

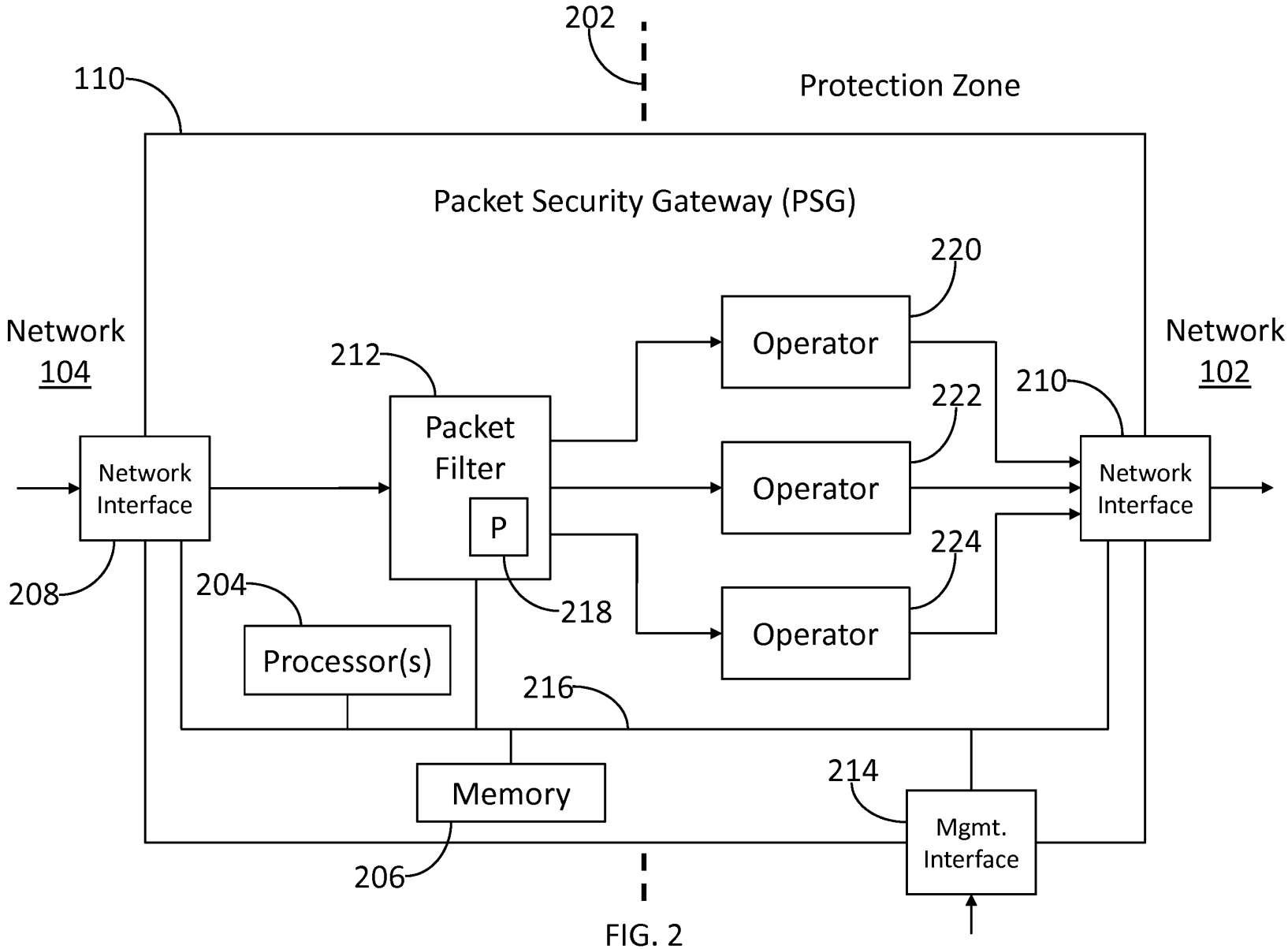
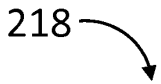

202
Protection Zone
110
Packet Security Gateway (PSG)
220
Network
104
212
Operator
Network
102
210
222
Packet
Filter
Network
Interface
Operator
Network
Interface
P
224
208
204
218
Processor(s)
Operator
216
Memory
214
Mgmt.
Interface
206

FIG. 2



Five-tuple

Rule #	IP Protocol	Source IP Address	Source Port	Destination IP Address	Destination Port	Operator
1 (302)	TCP	140.210.*	*	140.212.*	22	ALLOW
2 (304)	TCP	140.210.*	*	140.212.*	25	ALLOW
3 (306)	TCP	140.210.*	*	140.212.*	110	ALLOW
4 (308)	TCP	140.210.*	*	140.212.*	143	ALLOW
5 (310)	TCP	140.210.*	*	140.212.*	443	REQUIRE-TLS-1.1-1.2
6 (312)	TCP	140.210.*	*	214.*	80	HTTP-EXFIL
7 (314)	*	*	*	*	*	BLOCK

FIG. 3

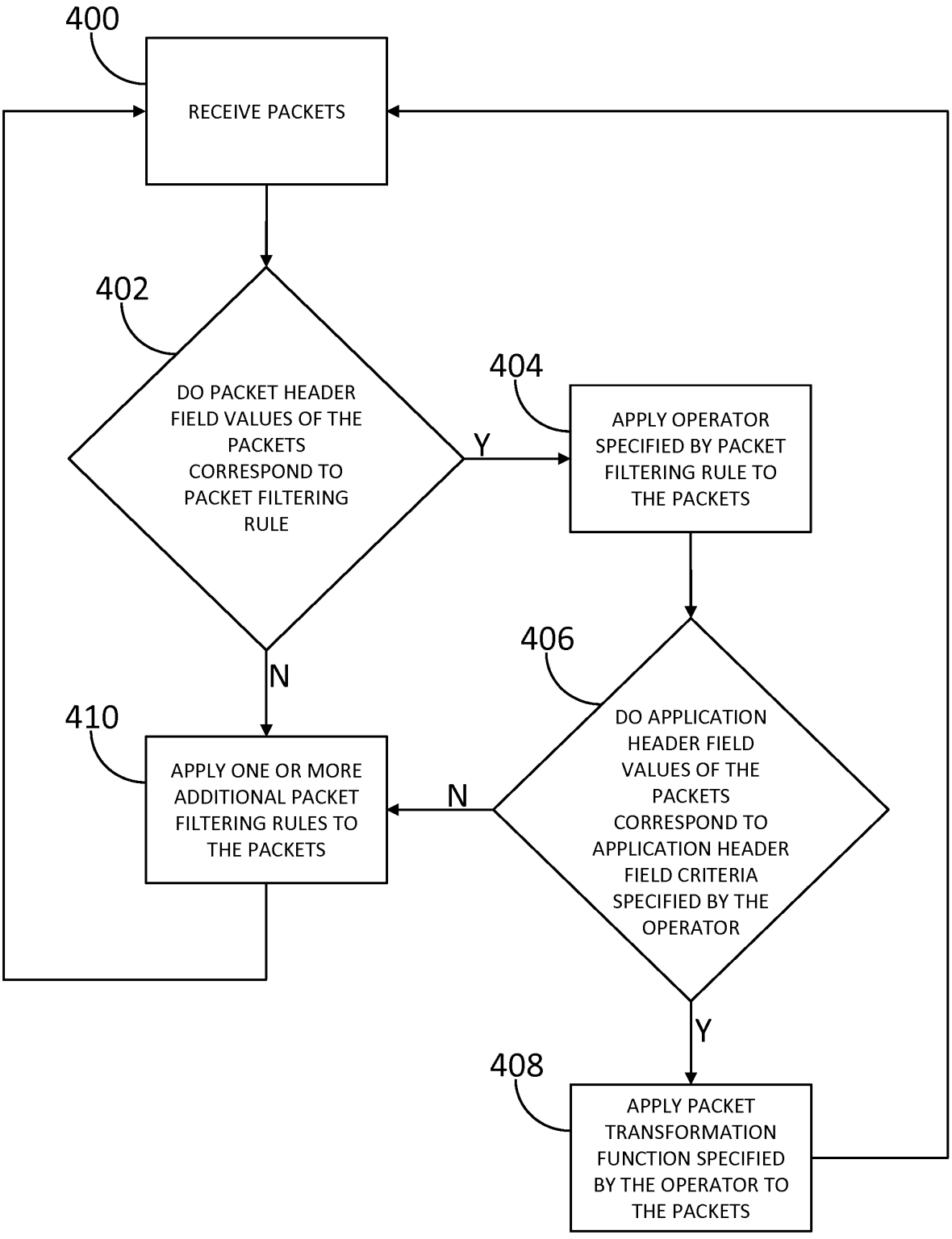

400
RECEIVE PACKETS
402
DO PACKET HEADER FIELD VALUES OF THE PACKETS CORRESPOND TO PACKET FILTERING RULE
Y
404
APPLY OPERATOR SPECIFIED BY PACKET FILTERING RULE TO THE PACKETS
N
406
DO APPLICATION HEADER FIELD VALUES OF THE PACKETS CORRESPOND TO APPLICATION HEADER FIELD CRITERIA SPECIFIED BY THE OPERATOR
N
410
APPLY ONE OR MORE ADDITIONAL PACKET FILTERING RULES TO THE PACKETS
Y
408
APPLY PACKET TRANSFORMATION FUNCTION SPECIFIED BY THE OPERATOR TO THE PACKETS

FIG. 4

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	FILTERING NETWORK DATA TRANSFERS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____ filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Sean Moore Date (Optional): 12-MARCH-2013

Signature: Sean Moore

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1.11 and 1.14. This collection is estimated to take 1 minute 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.

Electronic Acknowledgement Receipt

EFS ID:	29408628
Application Number:	15614956
International Application Number:	
Confirmation Number:	9334
Title of Invention:	FILTERING NETWORK DATA TRANSFERS
First Named Inventor/Applicant Name:	Sean Moore
Customer Number:	22907
Filer:	Bradley C. Wright/Holly Parker
Filer Authorized By:	Bradley C. Wright
Attorney Docket Number:	007742.00091\US
Receipt Date:	06-JUN-2017
Filing Date:	
Time Stamp:	13:57:48
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	Application Data Sheet	Application_Data_Sheet_Fillable_PDF_18554656.pdf	1822537 d91bfcaf4a00e939f6b08733025e0549aee33359	no	8

Warnings:

Information:					
2	Power of Attorney	POA_or_Authorization_of_Agent_18554941.pdf	16594 030eaaffa2e5748c9972d06f5d3930c0d059d9cd	no	1
Warnings:					
Information:					
3	Non Patent Literature	12871806_17748741.pdf	114514 a2c06b74ce562b85ec3c311b441b4dac68e23a60	no	3
Warnings:					
Information:					
4	Non Patent Literature	12871806_17748734.pdf	245205 61c594a1c82e88ac4bd5d5a245b0f5a2f4879713	no	3
Warnings:					
Information:					
5	Non Patent Literature	12871806_17748766.pdf	282709 389e10afbd02afbfcc755285dd4bda35484710a3	no	4
Warnings:					
Information:					
6	Non Patent Literature	12871806_17748764.pdf	108988 d96beeb8b5e3d9e49b59799b7caefc7e504f61d8	no	3
Warnings:					
Information:					
7	Non Patent Literature	12871806_17748760.pdf	2533792 45ea01d4b457774a01670e82e8a04ecd358d5db1	no	62
Warnings:					
Information:					
8	Non Patent Literature	12871806_17748773.pdf	48581 9eef5fc00a34cc7e354f17b4d82fc48b3cdb54f7	no	1
Warnings:					
Information:					

9	Non Patent Literature	12871806_17750290.pdf	436983 dcf36d568d3932bafc15b58fc4fe86344a11e88d	no	15
Warnings:					
Information:					
10	Non Patent Literature	12871806_17750237.pdf	1206684 0044a226d9c011010f6d8ecf62b589c51a6611e1	no	27
Warnings:					
Information:					
11	Non Patent Literature	12871806_17750240.pdf	637605 57627bd99c5d17db648705cbc74e424bf87acfc8	no	21
Warnings:					
Information:					
12	Non Patent Literature	12871806_17750245.pdf	607940 e3193f3218896730ca77045b69d11f333eb71489	no	20
Warnings:					
Information:					
13	Non Patent Literature	12871806_17750248.pdf	659756 aa9de2722748dd0111873f944e94c2f1ba9de19d	no	10
Warnings:					
Information:					
14	Non Patent Literature	12871806_17750229.pdf	238710 8c34046e74fcbd728967753cd8a303b7c952903d	no	6
Warnings:					
Information:					
15	Non Patent Literature	12871806_17750226.pdf	160790 2e0bf87d22fa9e1e6fc994dc8d5eb4440f2921a6	no	3
Warnings:					
Information:					

16	Non Patent Literature	12871806_17750235.pdf	121567 96ad7b5996c3eac66a9ec1489d78ab155c57da3f	no	2
Warnings:					
Information:					
17	Non Patent Literature	12871806_17750279.pdf	891534 83d6eb67909e68839fe14d24cdfd2300f76b215d	no	27
Warnings:					
Information:					
18	Non Patent Literature	12871806_17750277.pdf	918733 eca7ef41a2f4fd1439ea36b27914b8c2c7394e2d	no	28
Warnings:					
Information:					
19	Non Patent Literature	ISA_Comm_dated_07-10-2015_17791693.PDF	817142 58a34465de3fc4cd92bdd252aee97f5d82d82c11	no	6
Warnings:					
Information:					
20	Non Patent Literature	WO2014109843_17791444.PDF	162757 16cf49e3c80078bbf4f33b610ab92b79e059e538	no	5
Warnings:					
Information:					
21	Non Patent Literature	Corr_from_WIPO__-_N__of_Transmittal_of_the_International_Search_Report_17713511.PDF	8618992 3d1c384aa26e1d72a68822e3e4c8bd9f2de5249f	no	126
Warnings:					
Information:					
22	Non Patent Literature	WO2015160567_1_17791384.PDF	160557 1346e81c72ffbe833f253dba3f32fbd5e6062dff	no	6
Warnings:					
Information:					

23	Non Patent Literature	WO2014065943_17791450.PDF	162288 bc6a1f77e76eb307f25c54939ac6af2fade146dd	no	5
Warnings:					
Information:					
24	Non Patent Literature	WO2014164713_17791454.PDF	178111 ec7002ab21a04ce6e2a91f328421cb594c9ef236	no	6
Warnings:					
Information:					
25	Non Patent Literature	WO2014143673_17791459.PDF	238193 5c30981f29a53e5331a157b4d76afe6316810c92	no	7
Warnings:					
Information:					
26	Non Patent Literature	Statement_17761124.pdf	66900 0c2d5d1785db2e8352fd788df77b2eb9cd7979e4	no	1
Warnings:					
Information:					
27	Non Patent Literature	Final_Rejection__1449_17645159.pdf	2839706 a8a9e7d43df581cbe3ff549c6bb5d8f0996c4060	no	68
Warnings:					
Information:					
28	Non Patent Literature	Non-Final_Rejection__892__1449_17737382.pdf	1405925 31cf56d4367545d6e32c691c7085e75f5b184ae0	no	36
Warnings:					
Information:					
29	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__INTVSUMEX__892__1449_17820023.pdf	1978709 4d4e3f669e324489b5cc5e9526926f72d6499efd	no	50
Warnings:					
Information:					

30	Non Patent Literature	AU_2013_372879_1st_report_17844165.PDF	180230 0db14b50d6b54fb780bc134451640ce58c5b8f84	no	3
Warnings:					
Information:					
31	Non Patent Literature	Final_Rejection__892__1449_17836139.pdf	2221034 630c07a4f486c227bd2b154764c1d52922647ed1	no	59
Warnings:					
Information:					
32	Non Patent Literature	Non-Final_Rejection__892__1449_17854388.pdf	3543506 a1ebec4955cf4c5d0cddd8921df2403ac8cbd49b	no	88
Warnings:					
Information:					
33	Non Patent Literature	Non-Final_Rejection__1449_17863955.pdf	1980426 cc2fae7e71b3f218bf284f104b06ea34ced4be21	no	59
Warnings:					
Information:					
34	Non Patent Literature	Non-Final_Rejection__892__1449_17907654.pdf	3501971 596402d50d623fd856dc9e75f0b2e46796297687	no	86
Warnings:					
Information:					
35	Non Patent Literature	AU2014249055OA_17930089.PDF	131541 2c1fd926dd8411ad1cff21014df6bf3f90176215	no	3
Warnings:					
Information:					
36	Non Patent Literature	AU2014228257OA_17930107.PDF	114304 7ec5e241c75e7cf6e0e9496d6097111f08feb5bd	no	2
Warnings:					
Information:					

37	Non Patent Literature	17920268_1_17936575.pdf	154479 327c57ef9aaf24c59b40ae7d298d36d2ea40f261	no	3
Warnings:					
Information:					
38	Non Patent Literature	17949695_1_17954003.pdf	91536 4f342d662e17ef4b0f97d50d89ea43a15f098bd2	no	4
Warnings:					
Information:					
39	Non Patent Literature	Examination_report_1107_17971763.PDF	233390 ea2ab8ea9b22be899b5e4a32d079f436a8187228	no	7
Warnings:					
Information:					
40	Non Patent Literature	Non-Final_Rejection__892__1449_17967478.pdf	1156475 3e4da35c3cb92b86749ebdf8db80e0da3f494217	no	36
Warnings:					
Information:					
41	Non Patent Literature	AUFirstEXam_17988909.pdf	265946 b205b9fb42ea35b902bd6fa3d3f1032d26b65832	no	3
Warnings:					
Information:					
42	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__INTVSUMEX__892__1449_18076047.pdf	1537046 d8a8ad44e3593cdfa76b2c0fdf963036e70bdeb1	no	38
Warnings:					
Information:					
43	Non Patent Literature	OTT01-7836061-v1-PAT_83577W-1_Corr_from_PTO_-_Office_Action_18087198.PDF	282227 53790041ea1a9ccf9b6b0c734e50b101b9b12690	no	4
Warnings:					
Information:					

44	Non Patent Literature	OTT01_-7838337-v1-PAT_83380W-1_Corr_to_PTO_-_Office_Action_18096434.PDF	393438 83111a6b651a98ad89407303a2fc324f521b e058	no	6
Warnings:					
Information:					
45	Non Patent Literature	OTT01_-7861591-v1-PAT_83575W-1_Corr_from_PTO_-_Office_Action_18101654.PDF	285929 c87d715164459l9f7dfca6a0e1dd62aa55e1 463a	no	5
Warnings:					
Information:					
46	Non Patent Literature	18105700_1_18116178.pdf	1041266 9b9dace0d9e37e051b27e2662c18d1d91f3 11243	no	30
Warnings:					
Information:					
47	Non Patent Literature	Non-Final_Rejection__892__1449_18140604.pdf	1584757 a988730b4239ed429a4344dc8b1ddd5c65 372a63	no	42
Warnings:					
Information:					
48	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__1449_18158549.pdf	695760 461671807412c0444aa64839e61ec957956 0a367	no	14
Warnings:					
Information:					
49	Non Patent Literature	14698560_18178105.pdf	607977 4554608d6aeb135ec747c12682f1efe32009 1e51	no	6
Warnings:					
Information:					
50	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__1449_18260634.pdf	618186 c096dbb16fe1eb240566458b09f75d6cb1c bc3b1	no	11
Warnings:					
Information:					

51	Non Patent Literature	Notice_of_Allowance_and_Fees_Due_PTOL-85__1449_18267002.pdf	599424 0b2c0b642ad7a9989fab20f9bf3f01260918d1b5	no	13
Warnings:					
Information:					
52	Non Patent Literature	Non-Final_Rejection__892__1449_18421167.pdf	2205864 d095bc1e87e7d1f9ace363a034b7f0af5e71ea6b	no	58
Warnings:					
Information:					
53	Non Patent Literature	Corr_from_WIPO_-_-_Notification_of_Transmittal_of_The_International_Search_Report__18522354.pdf	658968 635a0e3688a652b4c29d20455c11d91ba6d754cb	no	13
Warnings:					
Information:					
54	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF_1_of_3_18554771.pdf	1042411 3f784462d5fe87b8725720625e038bbf844785b7	no	24
Warnings:					
Information:					
55	Power of Attorney	Centripetal_POA_18554686.PDF	184376 21c73e74c207437bda0e0eb884e1e57c7f141552	no	1
Warnings:					
Information:					
56		00091_Specification_18554942.pdf	79566 a0fd3b11294f4ee00e5cd7eac3ef99a2acfb75c6	yes	17

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Specification	1	15
Claims	16	16
Abstract	17	17

Warnings:

Information:					
57	Drawings-only black and white line drawings	Drawings_as_filed_in_parent_00774200035_18554324.PDF	58272 f5cc78f8e4a42d0ca56b049e922e7bd1f4fc7f06	no	4
Warnings:					
Information:					
58	Oath or Declaration filed	Declaration_as_filed_in_parent_00774200035_18554319.PDF	540936 5581ca43c958b2065f43ada121a61402dd4afdae	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	53673743	

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/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2:

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 — Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Sean		Moore	

Residence Information (Select One) ● US Residency Non US Residency Active US Military Service

City	Hollis	State/Province	NH	Country of Residence	US

Mailing Address of Inventor:

Address 1	c/o Centripetal Networks, Inc.
Address 2	2251 Corporate Park Drive, Suite 150

City	Herndon	State/Province	VA
Postal Code	20171	**Country**	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. — Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	22907		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	FILTERING NETWORK DATA TRANSFERS		
Attorney Docket Number	007742.00091\US	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	4	**Suggested Figure for Publication (if any)**	

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	● Customer Number	US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	22907		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing benefit claim information in the Application Data Sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the "Application Number" field blank.

Prior Application Status: Patented — Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
	Continuation of	14/625486	2015-02-18	9686193	2017-06-20

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14/625486	Continuation of	13/795822	2013-03-12	9124552	2015-09-01

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX)[i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country[i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

● Assignee	Legal Representative under 35 U.S.C. 117	Joint Inventor
Person to whom the inventor is obligated to assign.	Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:

If the Applicant is an Organization check here. ☒

Organization Name	Centripetal Networks, Inc.		
Mailing Address Information For Applicant:			
Address 1	2251 Corporate Park Drive		
Address 2	Suite 150		
City	Herndon	**State/Province**	VA
Country	US	Postal Code	20171
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication. An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e.g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Bradley C. Wright/			Date (YYYY-MM-DD)	2017-06-06
First Name	Bradley	Last Name	Wright	Registration Number	38,061

Additional Signature may be generated within this form by selecting the Add button. Add

PTO/AIA/14 (11-15)
Approved for use through 04/30/2017. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	007742.00091\US
	Application Number	
Title of Invention	FILTERING NETWORK DATA TRANSFERS	

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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 records.

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 CooperationTreaty.

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.

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	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\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	6226372		2001-05-01	Beebe et al.	
	2	7721084		2010-05-18	Salminen et al.	
	3	7684400		2010-03-23	Govindarajan et al.	
	4	7539186		2009-05-26	Aerrabotu et al.	
	5	7710885		2010-05-04	Ilnicki et al.	
	6	8856926		2014-10-07	Narayanaswamy et al.	
	7	6611875		2003-08-26	Chopra et al.	
	8	8806638		2014-08-12	Mani	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	31	9160713	B2	2015-10-13	Moore	
	32	9094445	B2	2015-07-28	Moore et al.	
	33	9137205	B2	2015-09-15	Rogers et al.	
	34	7215637	B1	2007-05-08	Ferguson et al.	
	35	8176561	B1	2012-05-08	Hurst et al.	
	36	8117655	B2	2012-02-14	Spielman	
	37	6147976	A	2000-11-14	Shand et al.	
	38	7610621	B2	2009-10-27	Turley et al.	
	39	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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	1	20030123456	A1	2003-07-03	Denz et al.	
	2	20070083924	A1	2007-04-12	Lu	
	3	20060195896		2006-08-31	Fulp et al.	
	4	20060248580		2006-11-02	Fulp et al.	
	5	20060048142		2006-03-02	Roese et al.	
	6	20100011434		2010-01-14	Kay	
	7	20120113987	A1	2012-05-10	Riddoch et al.	
	8	20110270956	A1	2011-11-03	McDysan et al.	
	9	20100211678	A1	2010-08-19	McDysan et al.	
	10	20050117576		2005-06-02	McDysan et al.	
	11	20040151155	A1	2004-08-05	Jouppi	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	12	20030212900	A1	2003-11-13	Liu et al.	
	13	20030188192	A1	2003-10-02	Tang et al.	
	14	20120264443	A1	2012-10-18	Ng et al.	
	15	20130059527	A1	2013-03-07	HASESAKA et al.	
	16	20010039624		2001-11-08	Kellum	
	17	20030035370	A1	2003-02-20	Brustoloni, Jose	
	18	20030142681		2003-07-31	Chen et al.	
	19	20030145225		2003-07-31	Bruton et al.	
	20	20050138204		2005-06-23	Iyer et al.	
	21	20050141537		2005-06-30	Kumar et al.	
	22	20060212572		2006-09-21	Afek et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	23	20080072307		2008-03-20	Maes	
	24	20100082811		2010-04-01	Van Der Merwe et al.	
	25	20100296441		2010-11-25	Barkan	
	26	20110088092		2011-04-14	Nguyen et al.	
	27	20080005795	A1	2008-01-03	Acharya et al.	
	28	20090172800	A1	2009-07-02	WOOL	
	29	20030097590	A1	2003-05-22	Syvanne	
	30	20090328219	A1	2009-12-31	Narayanaswamy	
	31	20120240135	A1	2012-09-20	Risbood et al.	
	32	20120314617	A1	2012-12-13	Erichsen et al.	
	33	20040088542	A1	2004-05-06	Daude et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	34	20080235755	A1	2008-09-25	Blaisdell et al.	
	35	20100132027	A1	2010-05-27	Ou	
	36	20110055916	A1	2011-03-03	Ahn	
	37	20020016858	A1	2002-02-07	Sawada et al.	
	38	20060262798	A1	2006-11-23	Joshi et al.	
	39	20080043739	A1	2008-02-21	SUH et al.	
	40	20080279196	A1	2008-11-13	Friskney et al.	
	41	20130254766	A1	2013-09-26	Zuo et al.	
	42	20030154297	A1	2003-08-14	Suzuki et al.	
	43	20060114899	A1	2006-06-01	Toumura et al.	
	44	20120331543	A1	2012-12-27	Bostrom et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	45	20110185055	A1	2011-07-28	NAPPIER et al.	
	46	20060070122	A1	2006-03-30	Bellovin	
	47	20050010765	A1	2005-01-13	Swander et al.	
	48	20020198981	A1	2002-12-26	Corl et al.	
	49	20090138938	A1	2009-05-28	Harrison et al.	
	50	20060104202	A1	2006-05-18	Reiner	
	51	20050229246	A1	2005-10-13	Rajagopal et al.	
	52	20040177139	A1	2004-09-09	Schuba et al.	
	53	20040010712	A1	2004-01-15	Hui et al.	
	54	20030120622	A1	2003-06-26	Nurmela et al.	
	55	20080301765	A1	2008-12-04	Nicol et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	56	20050251570	A1	2005-11-10	Heasman et al.	
	57	20050183140	A1	2005-08-18	Goddard	
	58	20050125697	A1	2005-06-09	Tahara	
	59	20040193943	A1	2004-09-30	Angelino et al.	
	60	20020165949	A1	2002-11-07	Na et al.	
	61	20020038339	A1	2002-03-28	Xu	
	62	20050114704	A1	2005-05-26	Swander	
	63	20100268799	A1	2010-10-21	Maestas	
	64	20110055923	A1	2011-03-03	Thomas	
	65	20100303240	A1	2010-12-02	Beachem et al.	
	66	20100199346	A1	2010-08-05	Ling et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	67	20100011433	A1	2010-01-14	HARRISON et al.	
	68	20080077705	A1	2008-03-27	Li et al.	
	69	20050286522	A1	2005-12-29	Paddon et al.	
	70	20040205360	A1	2004-10-14	Norton et al.	
	71	20140366132	A1	2014-12-11	Stiansen et al.	
	72	20130061294	A1	2013-03-07	Kenworthy	
	73	20100242098	A1	2010-09-23	Kenworthy	
	74	20070240208	A1	2007-10-11	Yu et al.	
	75	20060146879	A1	2006-07-06	Anthias et al.	
	76	20060136987	A1	2006-06-22	Okuda	
	77	20020049899	A1	2002-04-25	Kenworthy	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	78	20140281030	A1	2014-09-18	Cui et al.	
	79	20040073655	A1	2004-04-15	Kan et al.	
	80	20150237012	A1	2015-08-20	Moore	
	81	20150304354	A1	2015-10-22	Rogers et al.	
	82	20140115654	A1	2014-04-24	Rogers et al.	
	83	20140201123	A1	2014-07-17	Ahn et al.	
	84	20140283004	A1	2014-09-18	Moore	
	85	20140283030	A1	2014-09-18	Moore et al.	
	86	20080229415	A1	2008-09-18	Kapoor et al.	
	87	20140215574	A1	2014-07-31	Erb et al.	
	88	20010039579	A1	2001-11-08	TRCKA et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	89	20030105976	A1	2003-06-05	Copeland	
	90	20030154399	A1	2003-08-14	Zuk et al.	
	91	20040250124	A1	2004-12-09	Chesla et al.	
	92	20060053491	A1	2006-03-09	Khuti et al.	
	93	20060137009	A1	2006-06-22	Chesla	
	94	20070211644	A1	2007-09-13	Ottamalika et al.	
	95	20100095367	A1	2010-04-15	Narayanaswamy	
	96	20130117852	A1	2013-05-09	Stute	
	97	20140075510	A1	2014-03-13	Sonoda et al.	
	98	20150334125	A1	2015-11-19	BARTOS et al.	
	99	20120106354	A1	2012-05-03	Pleshek et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	100	20110185055	A1	2011-07-28	NAPPIER et al.	
	101	20130047020	A1	2013-02-21	Hershko et al.	
	102	20090240698	A1	2009-09-24	Shukla et al.	
	103	20040098511	A1	2004-05-20	Lin et al.	
	104	20100232445	A1	2010-09-16	Bellovin	
	105	20130305311	A1	2013-11-14	Puttaswamy Naga et al.	
	106	20020186683	A1	2002-12-12	Buck et al.	
	107	20090222877	A1	2009-09-03	Diehl et al.	
	108	20100107240	A1	2010-04-29	Thaler et al.	
	109	20040093513	A1	2004-05-13	Cantrell et al.	
	110	20120023576	A1	2012-01-26	Sorensen et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	111	20080163333	A1	2008-07-03	Kasralikar	
	112	20020164962	A1	2002-11-07	Mankins et al.	
	113	20050024189	A1	2005-02-03	Weber	
	114	20110141900	A1	2011-06-16	Jayawardena et al.	
	115	20050138353	A1	2005-06-23	Spies et al.	
	116	20040199629	A1	2004-10-07	Bomer et al.	
	117	20150350229	A1	2015-12-03	Mitchell	
	118	20050108557	A1	2005-05-19	Kayo et al.	
	119	20150373043	A1	2015-12-24	Wang 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]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	1	1677484	EP	A2	2006-07-05	Microsoft Corp		
	2	1313290	EP	A1	2003-05-21	Stonesoft Corp		
	3	2005046145	WO	A1	2005-05-19	Ericsson Telefon Ab L M		
	4	2385676	EP	A1	2011-11-09	Alcatel Lucent		
	5	2498442	EP	A1	2012-09-12	Openet Telecom Ltd		
	6	20010079361	KR	A	2001-08-22	Kim, Sang Wook		
	7	1006701	EP	A2	2000-06-07	Lucent Technologies Inc		
	8	2006105093	WO	A2	2006-10-05	Univ Wake Forest		
	9	2006093557	WO	A2	2006-09-08	Univ Wake Forest		
	10	2005328336	AU	B2	2011-09-15	Univ Wake Forest		
	11	2011038420	WO	A2	2011-03-31	Great Wall Systems		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	12	1484884	EP	A2	2004-12-08	Microsoft Corp		
	13	2006230171	AU	B2	2012-06-21	Univ Wake Forest		
	14	1864226	EP	B1	2013-05-15	Univ Wake Forest		
	15	2600236	CA	A1	2006-10-05	Univ Wake Forest		
	16	2012146265	WO	A1	2012-11-01	Voipfuture Gmbh		
	17	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.	T5
	1	Copy of ISR for PCT/US2013/057502, dated November 7, 2013.	
	2	International Search Report off International Application No. PCT/US2014/023286, dated June 24, 2014.	
	3	ISR off International Application No. PCT/US2013/072566, dated March 24, 2014.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	4	ISR off International Application No. PCT/US2014/027723, dated June 26, 2014.	
	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>	
	6	Reumann, John; "Adaptive Packet Filters"; IEEE, 2001, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI	
	7	Greenwald, Michael; "Designing an Academic Firewall: Policy, Practice, and Experience with SURF"; IEEE, Proceedings of SNDSS, 1996.	
	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.	
	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.	
	10	John Kindervag; "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", Forrester Research Inc.; Novermber 5, 2010, pps: 1-26.	
	11	Palo Alto Networks; "Designing A Zero Trust Network With Next-Generation Firewalls"; pps. 1-10; last viewed on October 21, 2012.	
	12	2016 Jan 11 - (US) Non Final Rejection - App 14/698,560	
	13	2011 Apr 27 - (WO) International Search Report and Written Opinion - App PCT/US2010/054520	
	14	2011 Mar 04 - (US) Notice of Allowance - App 11/316,331	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	15	2011 Mar 03 - (EP) Communication Pursuant to Rules 70(2) and 70a(2) - App 06758213.0	
	16	2011 Feb 14 - (EP) Search Report - App 06758213.0	
	17	Fulp, Errin: "Errin Fulp," XP002618346, www.cs.wfu.edu/fulp/ewfPub.html, pgs. 1-5 (Copyright 2010)	
	18	2010 Sept 30 - (US) Office Action - App 11/390,976	
	19	2010 Sept 10 - (AU) Office Action - App 2006230171	
	20	2010 Aug 20 - (AU) Office Action - App 2005328336	
	21	2010 Jun 23 - (US) Final Rejection - App 11/316,331	
	22	2010 Apr 29 - (US) Interview Summary - App 11/390,976	
	23	2010 Mar 26 - (US) Final Rejection - App 11/390,976	
	24	2009 Sept 14 (US) Office Action - App 11/316,331	
	25	2009 Jun 24 - (US) Office Action - App 11/390,976	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	26	2008 Jul 03 - (WO) Written Opinion of the International Searching Authority - App PCT/US06/11291	
	27	2007 Aug 31 - (EP) Communication Pursuant to Rules 109 and 110 - App 05857614.1	
	28	Acharya et al, "OPTWALL: A Hierarchical Traffic-Aware Firewall," Department of Computer Science, Telecommunications Program, University of Pittsburgh, pgs. 1-11 (2007)	
	29	2006 Sept 11 - (WO) Written Opinion of the International Searching Authority - App PCT/US05/47008	
	30	Tarsa et al., "Balancing Trie-Based Policy representations for Network Firewalls," Department of Computer Science, Wake Forest University, pgs. 1-6 (2006)	
	31	Fulp, "Trie-Based Policy Representations for Network Firewalls," Proceedings of the IEEE International Symposium on Computer Communications (2005)	
	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	
	33	E. Fulp et al., "Network Firewall Policy Tries", Technical Report, Computer Science Department, Wake Forest University, 2004	
	34	E. Al-Shaer et al., "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, 1(1): 2004	
	35	E.W. Fulp, "Firewall Architectures for High Speed Networks", U.S. Department of Energy Grant Application, Funded September 2003	
	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	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	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	
	38	M. Christiansen et al., "Using IDDsfor Packet Filtering", Technical Report, BRICS, October 2002	
	39	Lee et al., "Development Framework for Firewall Processors," IEEE, pgs. 352-355 (2002)	
	40	L. Qui et al., "Fast Firewall Implementations for Software and Hardware-Based Routers", Proceedings of ACM Sigmetrics, June 2001	
	41	D. Eppstein et al., "Internet Packet Filter Management and Rectangle Geometry", Proceedings of the Symposium on Discrete Algorithms, 827-835, 2001	
	42	E. Fulp, "Preventing Denial of Service Attacks on Quality of Service", Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II, 2001	
	43	S. Goddard et al., "An Unavailability Analysis of Firewall Sandwich Configurations", Proceedings of the 6th IEEE Symposium on High Assurance Systems Engineering, 2001	
	44	G.V. Rooij, "Real Stateful TCP Packet Filtering in IP Filter", Proceedings of the 10th USENIX Security Symposium, 2001	
	45	P. Warkhede et al., "Fast Packet Classification for Two-Dimensional Conflict-Free Filters", Proceedings of IEEE INFOCOM, 1434-1443, 2001	
	46	D. Decasper et al., "Router Plugins: A Software Architecture for Next-Generation Routers", IEEE/ACM Transactions on Networking, 8(1): February 2000	
	47	A. Feldmann et al., "Tradeoffs for Packet Classification", Proceedings of the IEEE INFOCOM, 397-413, 2000	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\US

	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	
	49	A. Hari et al., "Detecting and Resolving Packet Filter Conflicts", Proceedings of IEEE INFOCOM, 1203-1212, 2000	
	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		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	
	Filing Date	
	First Named Inventor	Sean Moore
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	007742.00091\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)	2017-06-06
Name/Print	Bradley C. Wright	Registration Number	38,061

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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Not Yet Assigned
Filing Date	Concurrently Herewith
First Named Inventor	Sean Moore
Title	FILTERING NETWORK DATA TRANSFERS
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	007742.00091\US

SIGNATURE of Applicant or Patent Practitioner

Signature	/Bradley C. Wright/	Date (Optional)	June 6, 2017
Name	Bradley C. Wright	Registration Number	38,061
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)	Centripetal Networks, Inc.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

[X] *Total of 1 forms are submitted.

18554683

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:
Wright, Bradley C.
BANNER & WITCOFF, LTD.
1100 13th Street, N.W. Suite 1200
Washington, DC 20005-4051
ETATS-UNIS D'AMERIQUE

INVITATION TO PAY ADDITIONAL FEES AND, WHERE APPLICABLE, PROTEST FEE

(PCT Article 17(3)(a) and Rule 40.1 and 40.2(e))

Applicant's or agent's file reference 007742.00043	Date of mailing *(day/month/year)* 10 July 2015 (10-07-2015)
International application No. PCT/US2015/024691	**PAYMENT DUE** within **ONE MONTH** from the above date of mailing
Applicant CENTRIPETAL NETWORKS, INC.	International filing date *(day/month/year)* 7 April 2015 (07-04-2015)

1. This International Searching Authority

(i) considers that there are 3 *(number of)* inventions claimed in the international application covered by the claims indicated on an extra sheet:

(ii) therefore considers that **the international application does not comply with the requirements of unity of invention** (Rules 13.1, 13.2 and 13.3) for the reasons indicated on an extra sheet:

(iii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:

see extra sheet

(iv) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid.

2. Consequently, the applicant is hereby **invited to pay**, within the time limit indicated above, the amount indicated below:

EUR 1.875,00	x	2	=	EUR 3.750,00
Fee per additional invention		number of additional inventions		currency/total amount of additional fees

3. The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest**, i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive, where applicable, subject to the payment of a protest fee.

Where the applicant pays additional fees under protest, the applicant is hereby invited, within the time limit indicated above, to pay a protest fee (Rule 40.2(e)) in the amount of EUR 865,00 *(currency/amount)*

Where the applicant has not, within the time limit indicated above, paid the required protest fee, the protest will be considered not to have been made and the International Searching Authority will so declare.

4. [ ] Claim(s) Nos. _____ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

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	BARRIO BARANANO, Ainhoa Tel: +49 (0)89 2399-8621

RECEIVED
JUL 21 2015
BANNER & WITCOFF LTD

Form PCT/ISA/206 (April 2005)
Registered Mail

INVITATION TO PAY ADDITIONAL FEES

International application No.
PCT/US2015/024691

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-9

A method for packet filtering based on application-layer packet header information

---

2. claims: 10-18

A method for selective packet digest logging

---

3. claims: 19, 20

A method for security policy update and management

The lack of unity becomes apparent a posteriori, i.e. for the following reasoning document D1 (US20060136987) is taken into account. From this prior art document what is known is a method comprising a security policy management server ("the controller 13 provides the identifying rule and the processing rule" in paragraph [0093]; "the controller may delete from the identifying rule/processing rule setting table the identifying rule and the processing rule which have not been accessed for a predetermined time." in paragraph [0036]) as claimed in claim 1. These features are the only features common to all the groups of inventions.
With the reference to the prior art document D1:
The third group yields the potential special technical feature of receiving, by a security policy management server and from a computing device, a security update comprising a set of network addresses; updating, one or more rules; receiving, from a different computing device, a security update comprising a different set of network addresses; determining that the different set of network addresses includes at least a portion of network addresses included in the set of network addresses; and responsive to that identifying the at least a portion of network addresses included in the set of network addresses, at least one of the one or more rules stored in the memory that specifies a range of network addresses comprising the at least a portion of network addresses; and updating the at least one of the one or more rules to include one or more other network addresses included in the different set of network addresses, hence solving the objective problem of how to manage security policies based on information received from different sources comprising overlapping network addresses.
Moreover, the first and second invention have further common features, which are also disclosed in document D1 as shown in the following. From document D1 what is further known is:
receiving ("receive the identifying rule and the processing rule from another communication apparatus" in paragraph [0040]), by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server ("the controller 13 provides the identifying rule and the processing rule" in paragraph [0093]; "while the notifying destination of the notifying

message (identifying rule and the processing rule) 740 is made the router 100C in FIG. 8, the gateway apparatus, a switch, and a management system (not shown) may be made a notifying destination." in paragraph [0095]), a dynamic security policy ("receive the identifying rule and the processing rule from another communication apparatus" in paragraph [0040]; "the controller may delete from the identifying rule/processing rule setting table the identifying rule and the processing rule which have not been accessed for a predetermined time." in paragraph [0036]) that includes at least one rule specifying a packet transformation function to be performed on packets
receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway ("received packet" in the abstract);
identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets ("identify a protocol type of a communication packet transmitted/received by a device" in paragraph [0028]); and
performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets ("to automatically set the processing rule of the packet" in paragraph [0028]; "the processing policy may include a policy concerning at least one of a service quality class, filtering, and routing of the packet." in paragraph [0029]) as claimed in claim 1. These features are the only features common to the first two groups of inventions.
With the reference to the prior art document D1:
The first group yields the potential special technical feature of using application-layer packet-header information as the packet identification at the gateway, hence solving the objective problem of how to improve the scalability issues in high resolution filtering.
The second group yields the potential special technical feature of using a packet digest logging function to the identified packets, hence solving the objective problem of how to enable security awareness information in a network.
Consequently, neither the objective problems underlying the subjects of the three claimed inventions, nor the solutions as defined by the special technical features described allow for the link of a common inventive concept to be established between said inventions in the meaning of Rule 13.2 PCT. In conclusion, the three groups of claims are not linked by a single general inventive concept. The application hence does not meet the requirements of unity of invention as defined in Rule 13.1 PCT.

Annex to Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS OF THE PARTIAL INTERNATIONAL SEARCH

International Application No
PCT/US2015/024691

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
see 'Invitation to pay additional fees'
2. This communication is not the international search report which will be established according to Article 18 and Rule 43.

3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.

4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/136987 A1 (OKUDA MASATO [JP]) 22 June 2006 (2006-06-22) paragraph [0028] - paragraph [0030]; figures 1,21 paragraphs [0033], [0036], [0040], [0093], [0095], [0135]	1-9
X	US 2007/240208 A1 (YU MING-CHE [TW] ET AL) 11 October 2007 (2007-10-11) abstract paragraphs [0021], [0024] - paragraph [0026] paragraph [0033] - paragraph [0036] paragraph [0039] - paragraph [0040]	1-9
A	US 2006/146879 A1 (ANTHIAS TEFCROS [US] ET AL) 6 July 2006 (2006-07-06) paragraph [0074] - paragraph [0076] paragraph [0112] - paragraph [0119] paragraphs [0207], [0208], [0240]	1-9
A	US 8 306 994 B2 (KENWORTHY STACY [US]) 6 November 2012 (2012-11-06) abstract; figures 4,6 column 2 - column 4 column 6 - column 9	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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

1

Form PCT/ISA/206 (Annex, first sheet) (July 1992, reprint January 2004)

Patent Family Annex

Information on patent family members

International Application No
PCT/US2015/024691

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006136987 A1	22-06-2006	JP 2006174350 A	29-06-2006
		US 2006136987 A1	22-06-2006
US 2007240208 A1	11-10-2007	NONE	
US 2006146879 A1	06-07-2006	CN 101099345 A	02-01-2008
		EP 1834453 A2	19-09-2007
		US 2006146879 A1	06-07-2006
		WO 2006073740 A2	13-07-2006
US 8306994 B2	06-11-2012	US 6317837 B1	13-11-2001
		US 2002049899 A1	25-04-2002
		US 2010242098 A1	23-09-2010
		US 2013061294 A1	07-03-2013

European Patent Organisation

Account details

N° 3 338 800 00 (BLZ 700 800 00)
Commerzbank
Promenadeplatz 7
D-80273 München
SWIFT Code: DRESDEFF700
IBAN: DE20 7008 0000 0333 880000
BIC: DRESDEFF

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44*bis*)

Applicant's or agent's file reference 007742.00025	**FOR FURTHER ACTION**	See item 4 below
International application No. PCT/US2013/072566	International filing date *(day/month/year)* 02 December 2013 (02.12.2013)	Priority date *(day/month/year)* 11 January 2013 (11.01.2013)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant CENTRIPETAL NETWORKS, INC.		

1. This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 *bis*.1(a).

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.

3. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	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 Article 35(2) with regard to novelty, inventive step or 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

4. The International Bureau will communicate this report to designated Offices in accordance with Rules 44*bis*.3(c) and 93*bis*.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44*bis* .2).

	Date of issuance of this report 14 July 2015 (14.07.2015)
The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Authorized officer Simin Baharlou e-mail: pt09.pct@wipo.int

Form PCT/IB/373 (January 2004)

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/US2013/072566	02.12.2013	11.01.2013

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.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016	see form PCT/ISA/210	Oliveira, Joel Telephone No. +31 70 340-3334

Form PCT/ISA/237 (Cover Sheet) (July 2009)

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 43bis.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 filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

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 in 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, 3, 6-9, 11, 13, 14, 17-22, 24
	No:	Claims	1, 4, 5, 10, 12, 15, 16, 23
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-24
Industrial applicability (IA)	Yes:	Claims	1-24
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 EP 1 313 290 A1 (STONESOFT CORP [FI]) 21 May 2003 (2003-05-21)

D2 WO 2005/046145 A1 (ERICSSON TELEFON AB L M [SE]) 19 May 2005 (2005-05-19)

D3 US 2011/055916 A1 (AHN DAVID K [US]) 3 March 2011 (2011-03-03)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claims **1, 12 and 23** is not new.

1.1 **D1** discloses a method comprising, at a network protection device **(abstract)**:

receiving a first rule set **(paragraph [0010], column3 lines 4-7)**;

receiving a second rule set **(paragraph [0010], column3 lines 4-7)**;

preprocessing the first rule set and the second rule set **(considered to be implicit from paragraphs [0010], [0013], [0040]: when a new set of rules is made available it must be made certain that they do not contain errors which could stop the filtering of the firewall)**;

configuring the network protection device to process packets in accordance with the first rule set **(paragraph [0010], column3 lines 13-18)**;

receiving packets **(column 6 lines 23-26)**;

processing a first portion of the packets in accordance with the first rule set **(paragraphs [0010], [0020])**;

reconfiguring the network protection device to process packets in accordance with the second rule set **(paragraphs [0010], [0024])**; and

processing a second portion of the packets in accordance with the second rule set **(paragraphs [0010], [0024])**.

1.2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent apparatus and computer-readable media claims **12 and 23**, which therefore are also considered not new.

1.3 Dependent claims **2-11, 13-22 and 24** do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty (for claims **4, 5, 10, 15, 16**) and/or inventive step (for claims **2, 3, 6, 7, 8, 9, 11, 13, 14, 17, 18, 19, 20, 21, 22, 24)** see passages cited in the Search Report.

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)* 28 January 2016 (28-01-2016)
Applicant's or agent's file reference 007742.00064	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2015/062691	International filing date *(day/month/year)* 25 November 2015 (25-11-2015)
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 FINNIE, Alistair Tel: +49 (0)89 2399-8251 FEB 8 - 2016

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.
007742.00064		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2015/062691	25 November 2015 (25-11-2015)	10 February 2015 (10-02-2015)
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. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/062691

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L12/701 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, 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 2014/281030 A1 (CUI LIANG [CN] ET AL) 18 September 2014 (2014-09-18) paragraph [0002] - paragraph [0003] paragraph [0004] paragraph [0034] paragraph [0046] - paragraph [0048] paragraph [0053] -----	1-25
X	US 2004/073655 A1 (KAN CHAO [US] ET AL) 15 April 2004 (2004-04-15)	1,24,25
A	paragraph [0006] paragraph [0037] -----	2-23
A	WO 2012/146265 A1 (VOIPFUTURE GMBH [DE]; SCHOLZ HENDRIK [DE]; WALLBAUM MICHAEL [DE]; KRUE) 1 November 2012 (2012-11-01) abstract -----	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
21 January 2016	28/01/2016

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	Pais Gonçalves, A

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/062691

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2014281030 A1	18-09-2014	NONE	
US 2004073655 A1	15-04-2004	EP 1418705 A2	12-05-2004
		US 2004073655 A1	15-04-2004
WO 2012146265 A1	01-11-2012	CA 2834168 A1	01-11-2012
		EP 2702740 A1	05-03-2014
		US 2014089504 A1	27-03-2014
		WO 2012146265 A1	01-11-2012

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/US2015/062691

TITLE: CORRELATING PACKETS IN COMMUNICATIONS NETWORKS

APPLICANT: CENTRIPETAL NETWORKS, INC.

IPC CLASSIFICATION: H04L12/701, H04L12/26

EXAMINER: Pais Gonçalves, A

CONSULTED DATABASES: WPI, EPODOC

CLASSIFICATION SYMBOLS DEFINING EXTENT OF THE SEARCH:

IPC:

CPC: H04L45/00, H04L43/00

FI/F-TERMS:

KEYWORDS OR OTHER ELEMENTS FEATURING THE INVENTION:

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/US2015/062691	25.11.2015	10.02.2015

International Patent Classification (IPC) or both national classification and IPC
INV. H04L12/701 H04L12/26

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.

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	Pais Gonçalves, A 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	1-25
	No:	Claims	
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

Reference is made to the following documents:

D1 US 2014/281030 A1 (CUI LIANG [CN] ET AL) 18 September 2014 (2014-09-18)

D2 US 2004/073655 A1 (KAN CHAO [US] ET AL) 15 April 2004 (2004-04-15)

section VIII

1 Claims 1, 24 and 25 do not fulfil the requirements of Article 6 PCT for the following reasons:

1.1 In the claims it is not clear what is meant by the expression "data identifying the host", how such data is determined or the purpose of generating and transmitting said data.

1.2 According to the description, it seems that this data is used to identify which packets are associated with a particular flow or session. However, this is not clear from the wording of the claims.

1.3 In addition, the desired scope of protection of independent claim 25 is not clearly defined due to the wording "one or more".

section V

2 Assuming the interpretation indicated in point 1.2 above, it seems that claim 1 would be directed to a method of monitoring packets received by a network device and packets transmitted by the device and correlating them in order to determined that the packets are associated with a flow.

2.1 Such a method is already known from the disclosure of D1, see e.g. [0002] to [0004] or D2, see e.g. [0037].

2.2 The only apparent distinguishing feature between claim 1 and e.g. D1 could be that the network device and the host are located in different networks.

2.3 However, such distinguishing feature is a simple modification of the basic concept disclosed in D1 lying within the general design competence of a person skilled in the art who would consider such measure to be at least implicitly disclosed in D1, see e.g. figures 7 and 10A.

2.4 In addition, these arguments are also valid for independent Claim 24, which contains the same combination of features as claim 1 in terms of an apparatus claim, i.e. the apparatus (system) for carrying out the method of claim 1.

2.5 Said arguments are also valid for independent claim 25 which is directed to computer-readable media comprising instructions essentially to carry out the method of claim 1.

2.6 Therefore, the subject-matter of Claims 1, 24 and 25 does not involve an **inventive step**, Article 33 (1), (3) PCT.

2.7 The additional features of the dependent claims seem to relate to minor design details and/or implementation measures, which are known or directly derivable from the above-referred documents or constitute normal practice of a person skilled in the art. These claims thus, either alone or in combination, do not seem to add anything new or of inventive significance to any of the previously-referred claims, see passages indicated in the search report.

section VII

3 Having regard to the above objections, it is not clear at present which part of the application could serve as a basis for a new and inventive subject-matter.

4 Should the Applicant nevertheless regard some particular matter of the application as having an inventive contribution over the prior art, then an independent claim relating to such subject-matter should be filed. The Applicant is also requested to indicate in the letter of reply the difference of said subject-matter vis-à-vis the state of the art and the significance thereof.

4.1 The above-cited documents D1 and D2 should be acknowledged and briefly discussed in the opening part of the description, Rule 5.1 (a) (ii) PCT, making clear any inventive contribution of the claimed invention over the prior art.

4.2 The independent claims should be drafted in a two-part form, having in their pre-characterizing part all features known from D1 (refer to point 2 above), Rule 6.3 (b) (ii) PCT.

4.3 The opening part of the description should be modified to bring it into agreement with the amended claim, Rule 5.1(a)(iii) PCT, if required.

4.4 The claims should include reference signs relating to the features referred to therein, Rule 6.2 (b) PCT.

US 20140281030A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2014/0281030 A1**

(43) **Pub. Date: Sep. 18, 2014**

Cui et al.

(54) **VIRTUAL NETWORK FLOW MONITORING**

(71) Applicant: **VMWARE, INC.**, Palo Alto, CA (US)

(72) Inventors: **Liang Cui**, Beijing (CN); **Wei Zhang**, Beijing (CN); **Jingchun Jason Jiang**, Beijing (CN); **Caixia Jiang**, Beijing (CN)

(73) Assignee: **VMWARE, INC.**, Palo Alto, CA (US)

(21) Appl. No.: **13/831,685**

(22) Filed: **Mar. 15, 2013**

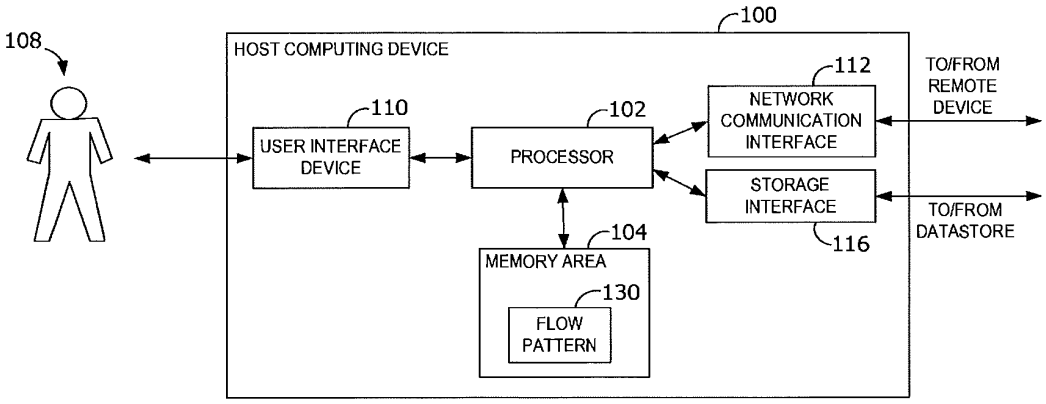
Publication Classification

(51) **Int. Cl.**
H04L 12/717 (2006.01)

(52) **U.S. Cl.**
CPC *H04L 45/42* (2013.01)
USPC **709/244**

(57) **ABSTRACT**

Embodiments perform end-to-end virtual network flow monitoring in a virtual datacenter and provide differentiated views to users based on user role. A target flow pattern describing data packets of interest is distributed to a plurality of applications managing VMs in the virtual datacenter, such as hosts, virtual gateways, and other virtual network applications. Each of the applications monitors data packets routed by the application by comparing the data packets to the flow pattern and selectively collecting context data describing the data packets. The context data collected by the applications is aggregated at a remote server for analysis and reporting.



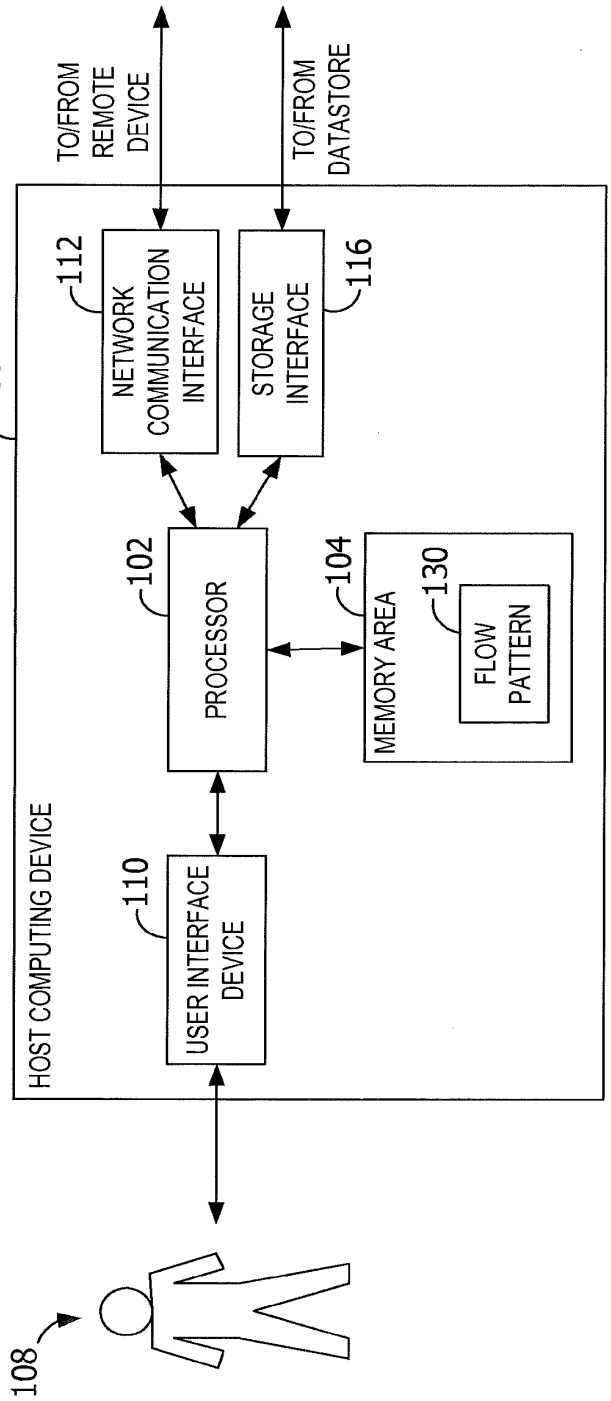

TO/FROM REMOTE DEVICE
TO/FROM DATASTORE
100
112
NETWORK COMMUNICATION INTERFACE
116
STORAGE INTERFACE
102
PROCESSOR
104
MEMORY AREA
130
FLOW PATTERN
110
USER INTERFACE DEVICE
HOST COMPUTING DEVICE
108

FIG. 1

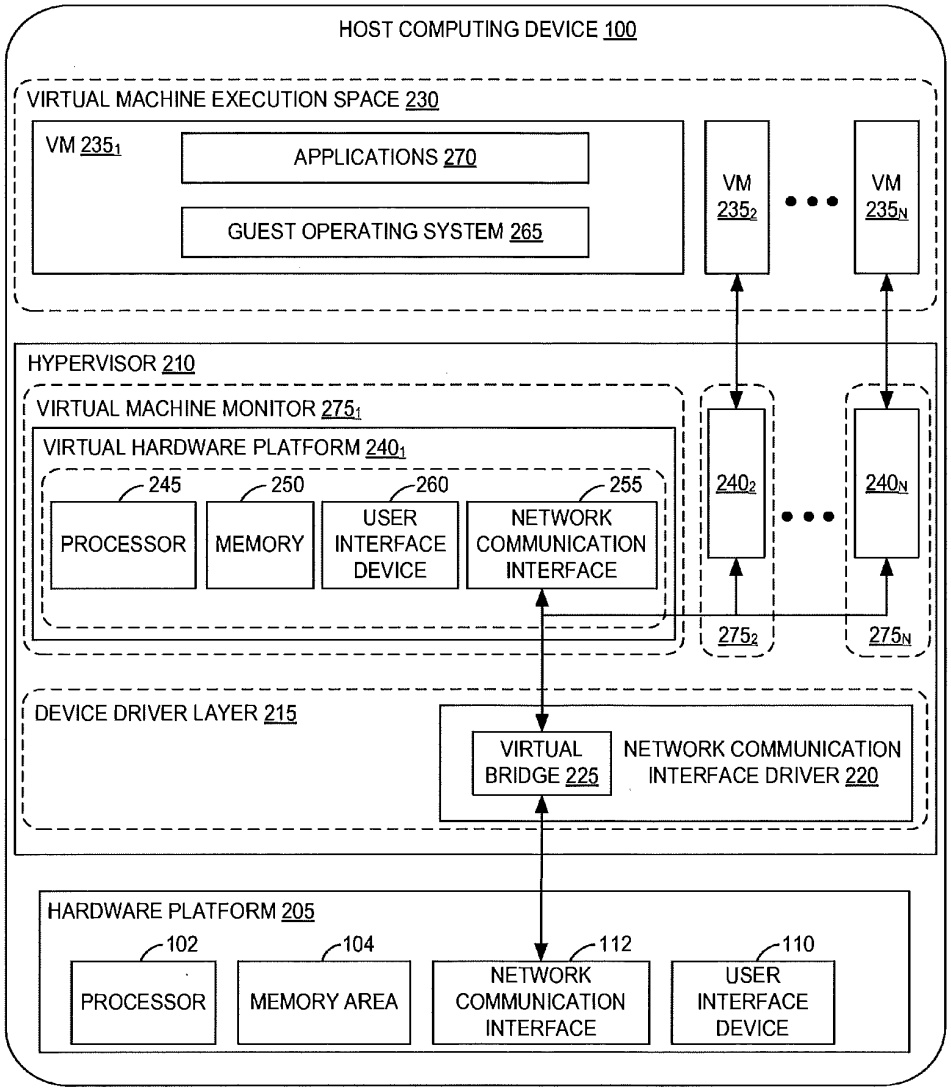


FIG. 2

BNSDOCID: <US____20140281030A1_I_>

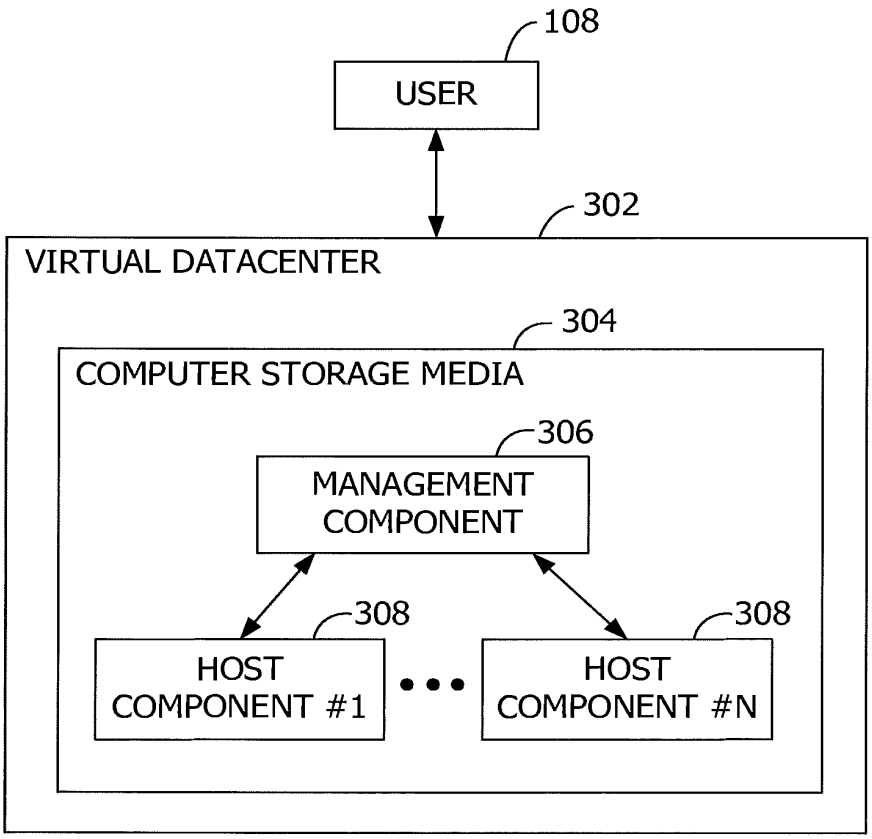

108
USER
302
VIRTUAL DATACENTER
304
COMPUTER STORAGE MEDIA
306
MANAGEMENT COMPONENT
308
HOST COMPONENT #1
308
HOST COMPONENT #N

FIG. 3

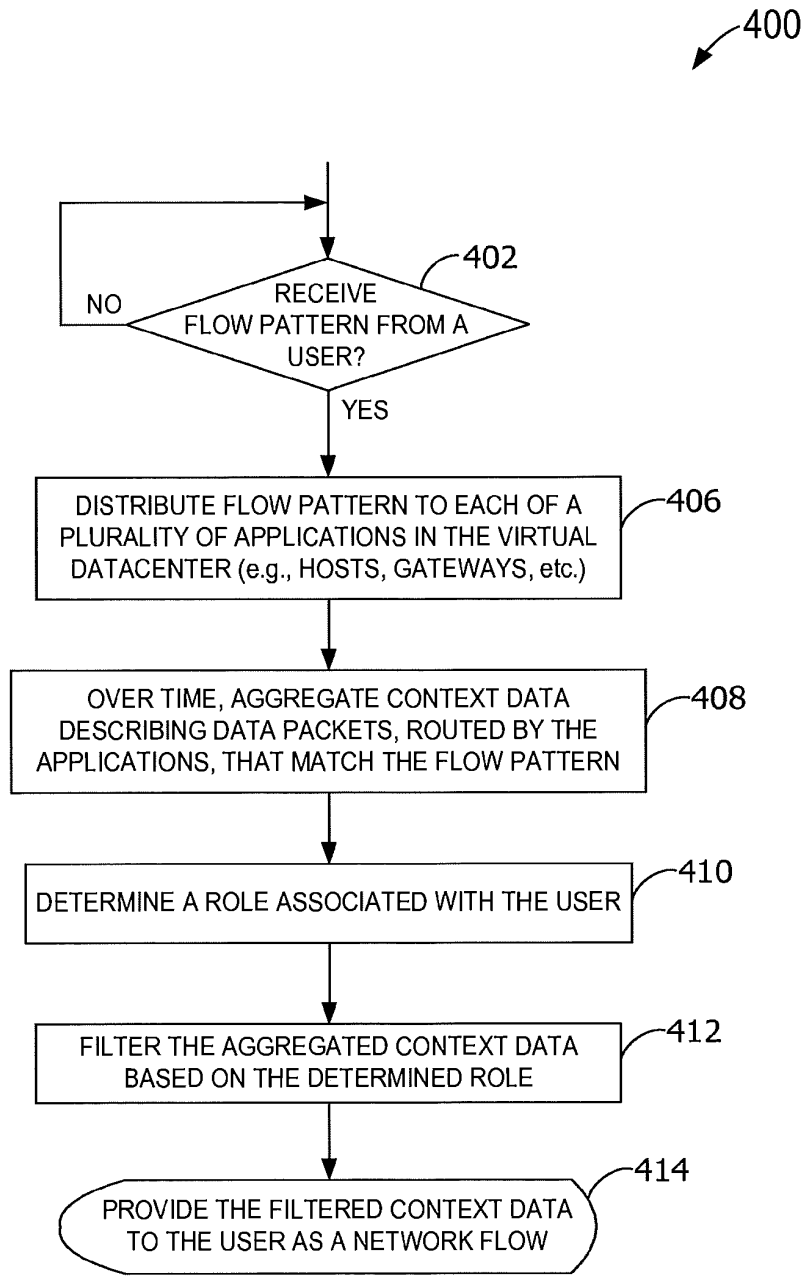


FIG. 4

BNSDOCID: <US____20140281030A1_I_>

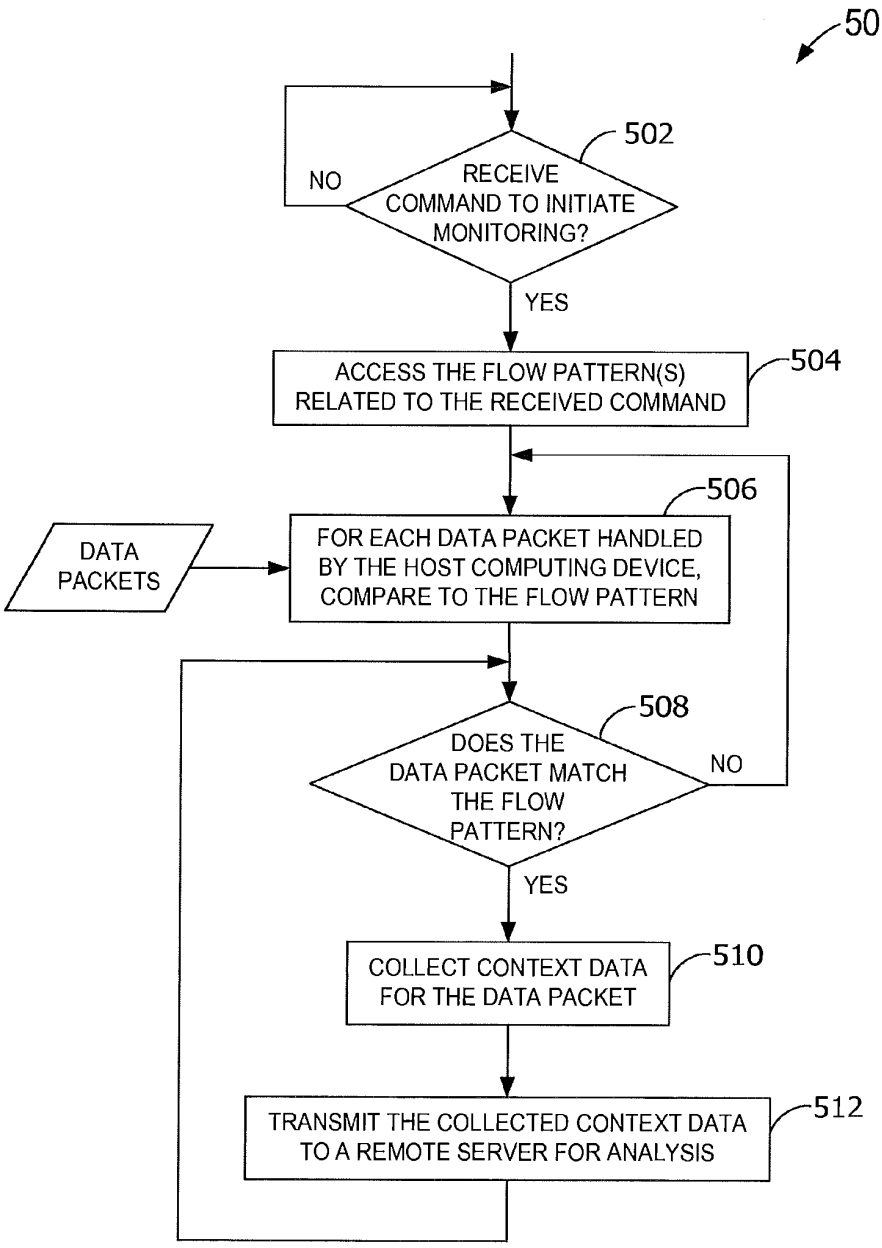

500
502
RECEIVE COMMAND TO INITIATE MONITORING?
NO
YES
504
ACCESS THE FLOW PATTERN(S) RELATED TO THE RECEIVED COMMAND
506
DATA PACKETS
FOR EACH DATA PACKET HANDLED BY THE HOST COMPUTING DEVICE, COMPARE TO THE FLOW PATTERN
508
DOES THE DATA PACKET MATCH THE FLOW PATTERN?
NO
YES
510
COLLECT CONTEXT DATA FOR THE DATA PACKET
512
TRANSMIT THE COLLECTED CONTEXT DATA TO A REMOTE SERVER FOR ANALYSIS

FIG. 5

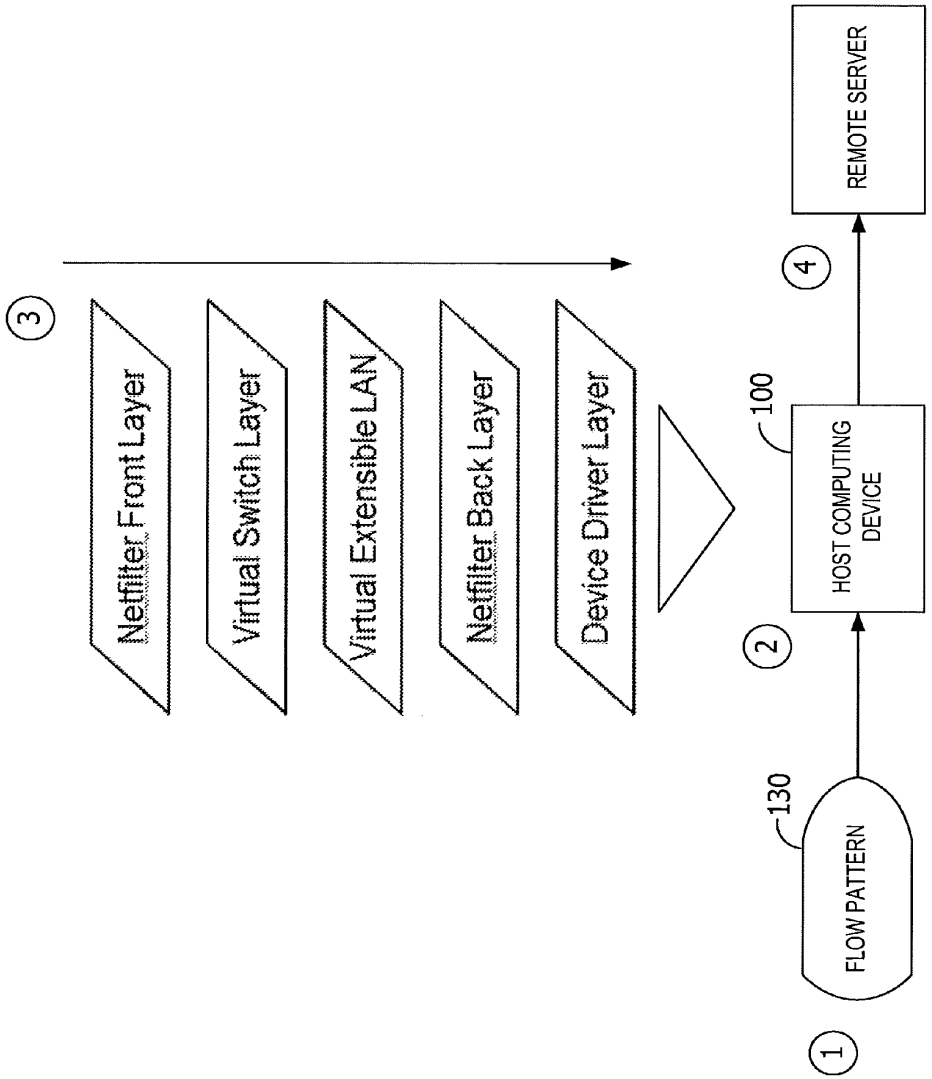

REMOTE SERVER
4
HOST COMPUTING DEVICE
100
2
FLOW PATTERN
130
1
3
Netfilter Front Layer
Virtual Switch Layer
Virtual Extensible LAN
Netfilter Back Layer
Device Driver Layer

FIG. 6

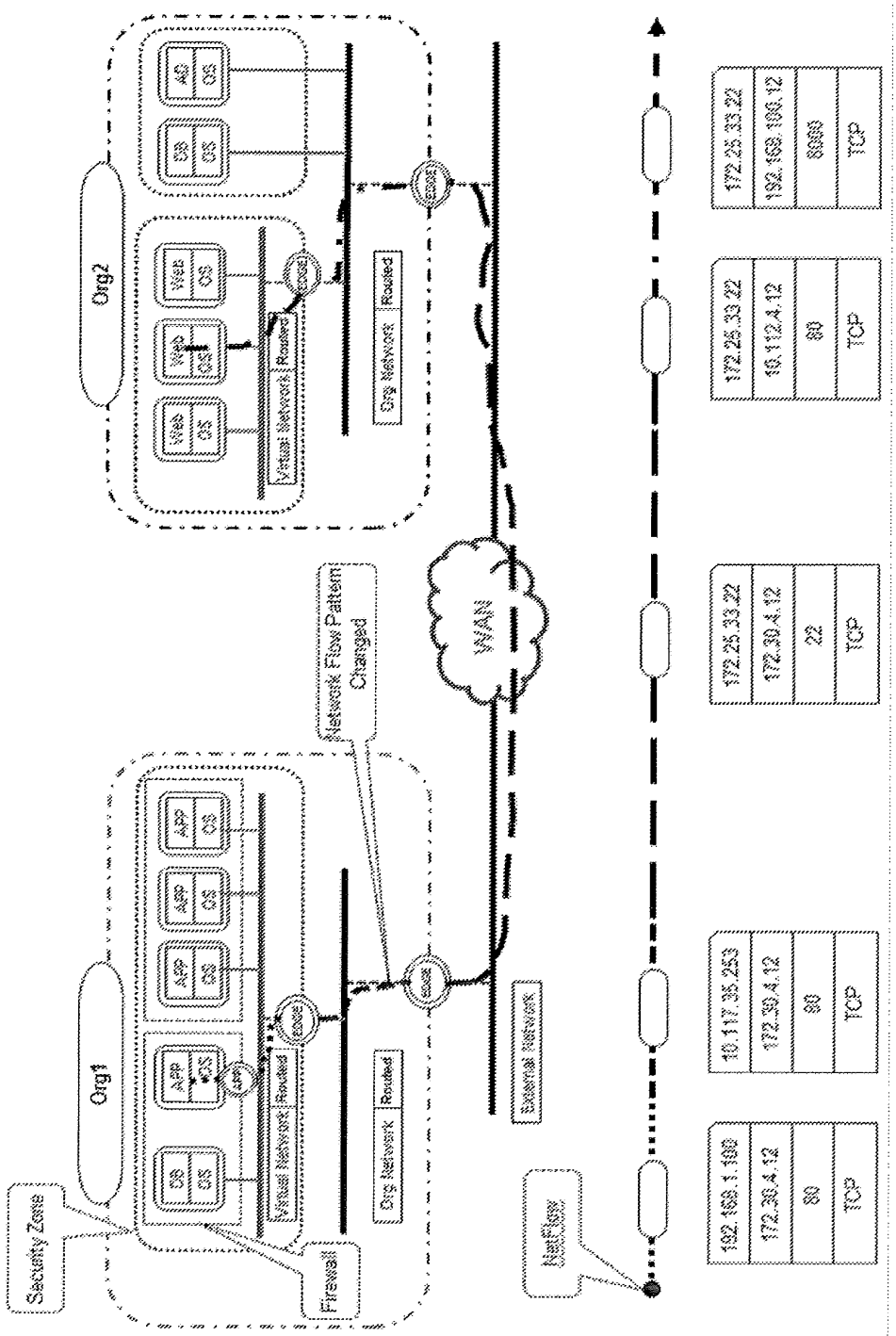


FIG. 7

BNSDOCID: <US____20140281030A1_I_>

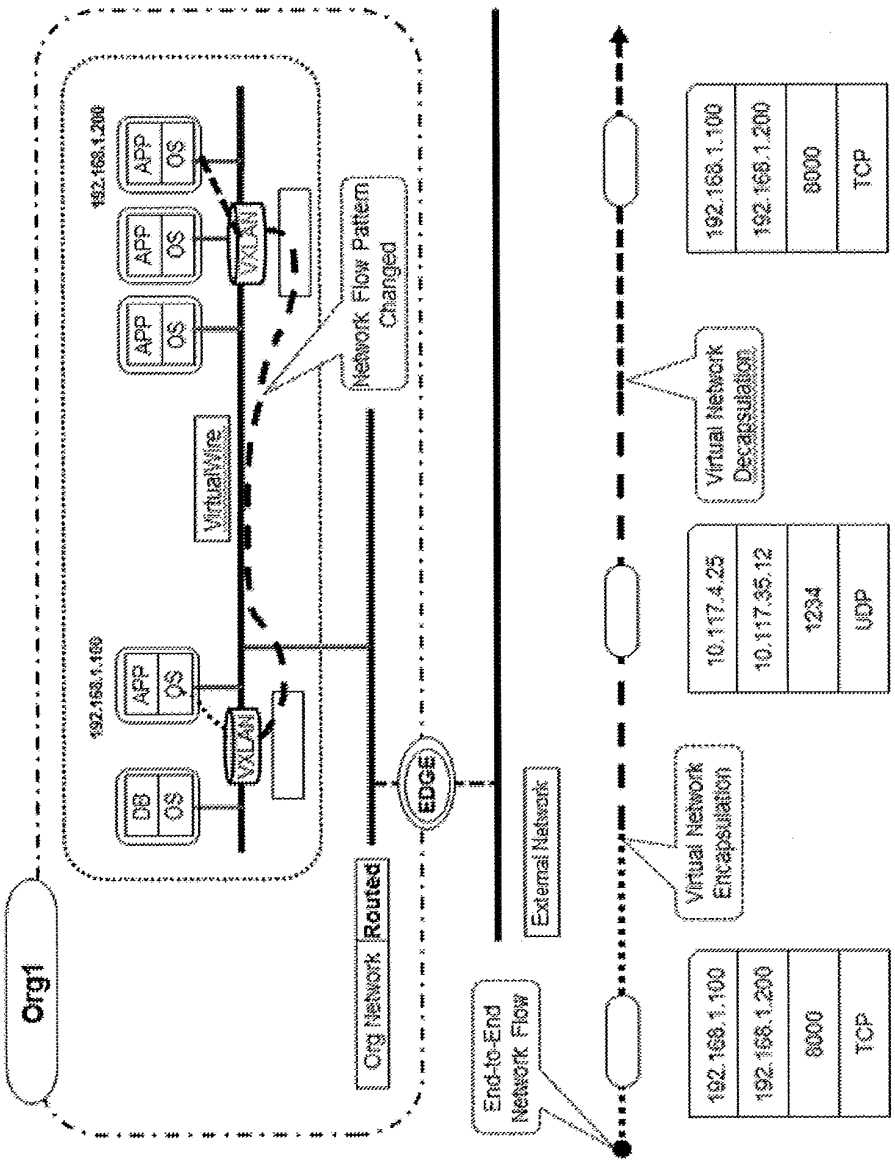

Org1
Org Network
Routed
EDGE
External Network
End-to-End Network Flow
Virtual Network Encapsulation
Virtual Network Decapsulation
Network Flow Pattern Changed
VirtualWire
VXLAN
VXLAN
192.168.1.100
192.168.1.200
8000
TCP
10.117.4.25
10.117.35.12
1234
UDP
192.168.1.100
192.168.1.200
8000
TCP
APP
OS
DB
OS

FIG. 8

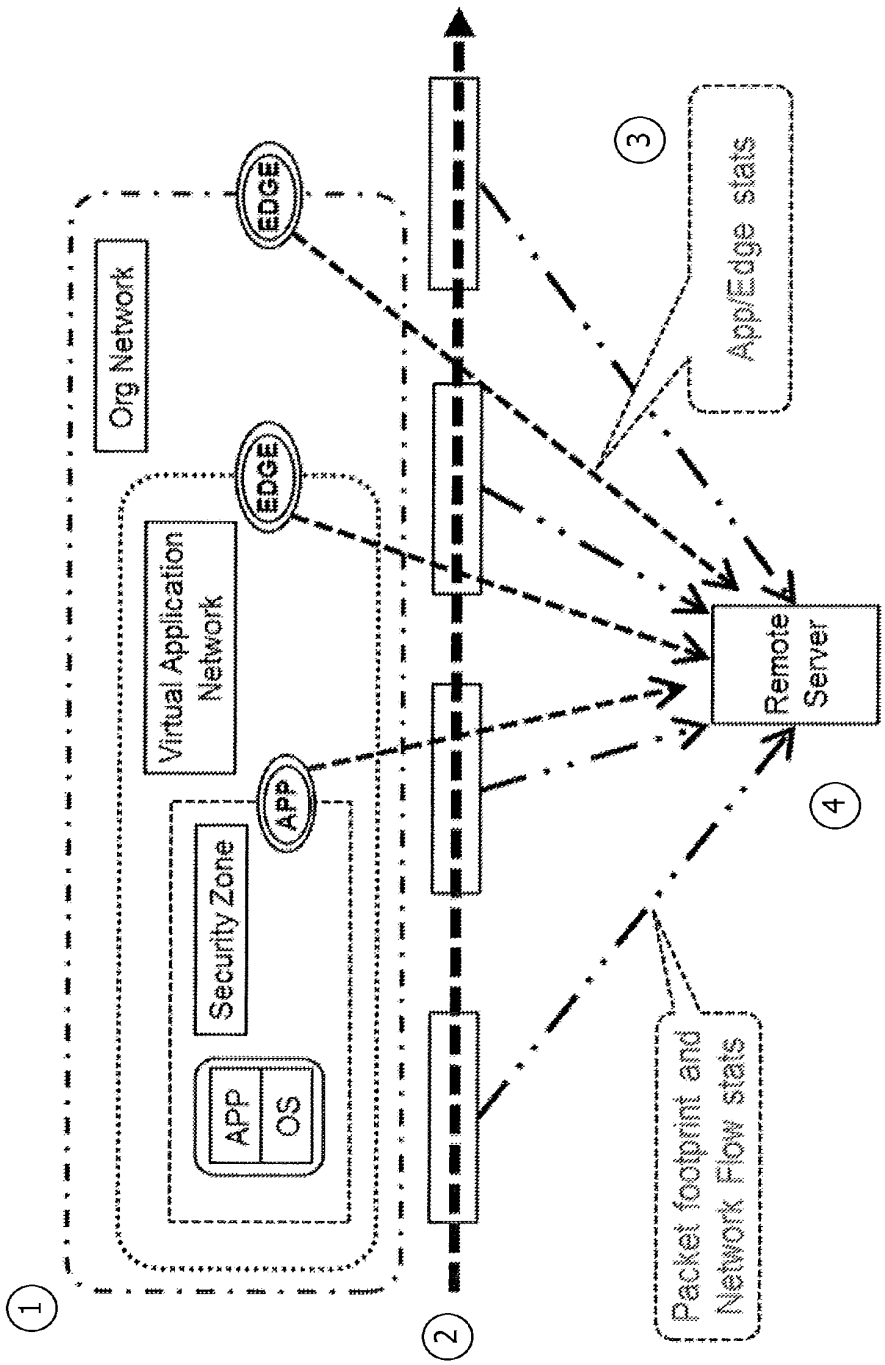

Org Network
EDGE
EDGE
Virtual Application Network
APP
Security Zone
APP
OS
Remote Server
App/Edge stats
Packet footprint and Network Flow stats
1
2
3
4

FIG. 9

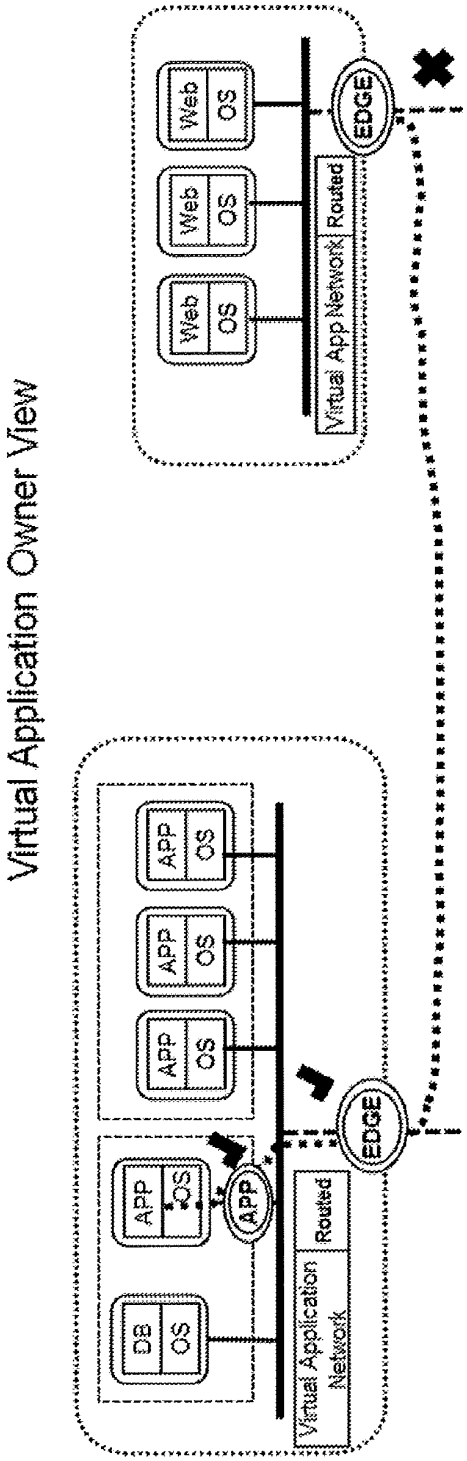

Virtual Application Owner View
Web
OS
Web
OS
Web
OS
Virtual App Network
Routed
EDGE
APP
OS
APP
OS
APP
OS
APP
OS
APP
DB
OS
Virtual Application Network
Routed
EDGE

FIG. 10A

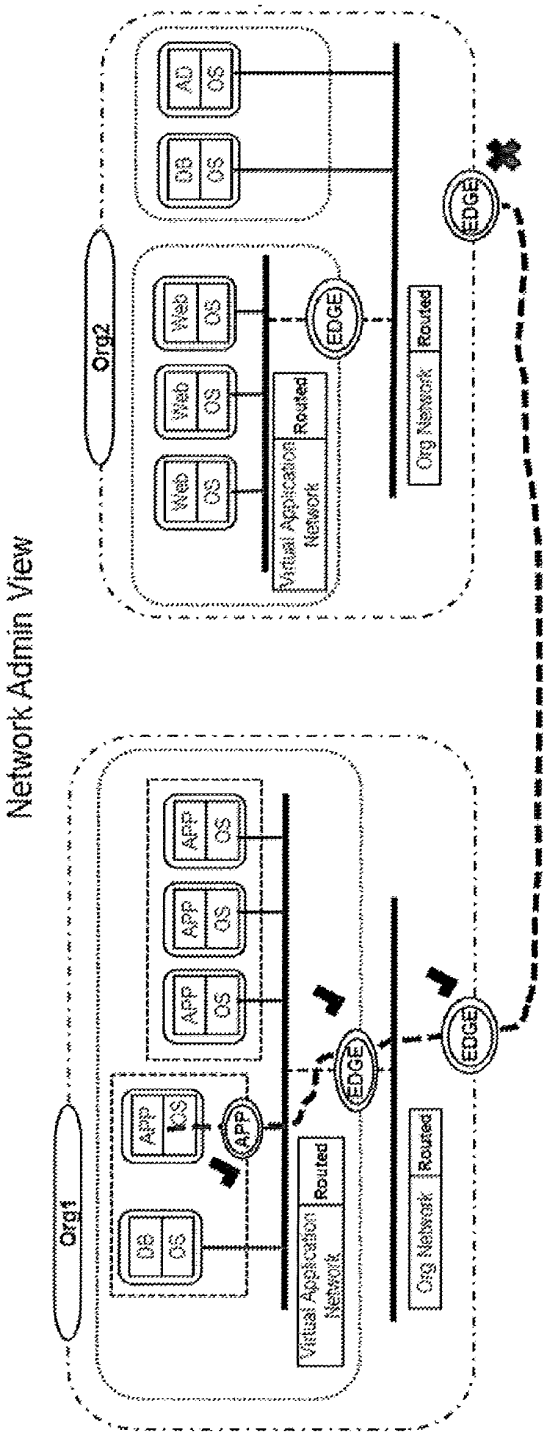

Network Admin View
Org1
Org2
AD
OS
DB
OS
Web
OS
Web
OS
Web
OS
APP
OS
APP
OS
APP
OS
APP
OS
APP
OS
DB
OS
EDGE
EDGE
EDGE
EDGE
Routed
Routed
Routed
Routed
Virtual Application Network
Virtual Application Network
Org Network
Org Network

FIG. 10B

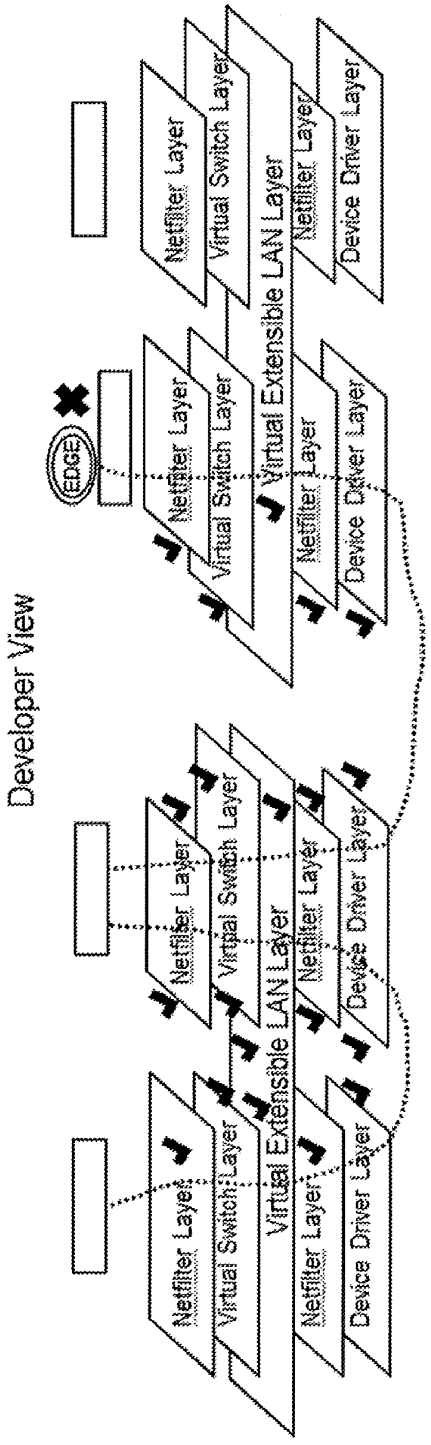


FIG. 10C

BNSDOCID: <US____20140281030A1_I_>

IPR2023-01353 Page 01548

VIRTUAL NETWORK FLOW MONITORING

BACKGROUND

[0001] With the increased use of cloud computing and virtualization technologies, virtual datacenter architectures have grown in scale and complexity. In some instances, thousands of virtual machines (VMs) act as hosts, virtual gateways, and other network appliances to implement complex virtual networks. Troubleshooting network problems in such virtualized environments is difficult with existing monitoring systems that are not adapted to operate in cloud computing environments. Further, some virtual datacenters have multiple management and data path layers on top of the physical network infrastructure. For example, a data path may have a network interface card layer, a local area network encapsulation layer, a virtual network appliance layer, an input/output layer, and so on. Further, there may be logical network concepts such as a virtual network, an organization network, zone, endpoint, and so on. Because some of these layers and logical network concepts do not correspond to traditional physical infrastructure, some of the existing monitoring systems are in capable of identifying the source of network problems in virtualized environments.

[0002] Some existing monitoring systems provide packet-based probing by sending probe packets along the data path to identify physical network connectivity issues. Such systems, however, fail to present a high-level logical view to users, fail to provide network flow-based monitoring, and fail to provide detailed flow information within hosts. Further, the probe packets typically terminate at virtual gateways within the virtual datacenter due to security policies. In addition, such systems have a high resource cost (e.g., processing, memory, latency, etc.) by collecting all network traffic going through routers and switches.

[0003] Other existing systems focus on recording packet information within a single host, but these systems fail to provide end-to-end network flow monitoring along the entire network data path.

SUMMARY

[0004] One or more embodiments described herein provide end-to-end virtual network flow monitoring in a virtual datacenter having a plurality of virtual machines (VMs). In some embodiments, the virtual datacenter distributes a flow pattern to a plurality of applications managing the VMs. For example, the applications are associated with host computing devices, virtual gateways, and other network applications. The flow pattern describes data packets of interest to a user. Each of the applications monitors data packets routed by the application by, for example, comparing the data packets to the flow pattern. For each of the routed data packets that match the flow pattern, applications collect context data describing the data packet and transmit the collected context data to a remote server. In this manner, the virtual datacenter aggregates, from the plurality of applications routing data packets, context data for the data packets that match the flow pattern. The virtual datacenter filters the aggregated context data based on a role associated with the user. The filtered context data is presented to the user.

[0005] This summary introduces a selection of concepts that are described in more detail below. This summary is not intended to identify essential features, nor to limit in any way the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] FIG. **1** is a block diagram of an exemplary host computing device.

[0007] FIG. **2** is a block diagram of virtual machines that are instantiated on a computing device, such as the host computing device shown in FIG. **1**.

[0008] FIG. **3** is a block diagram of components associated with a virtual datacenter.

[0009] FIG. **4** is a flowchart of an exemplary method performed by the virtual datacenter to initiate flow monitoring in virtual networks in the virtual datacenter.

[0010] FIG. **5** is a flowchart of an exemplary method performed by a host computing device, or other entity managing virtual machines, to monitor data packets and collect context data for selected data packets.

[0011] FIG. **6** is a block diagram illustrating exemplary flow monitoring in a stack in a host computing device.

[0012] FIG. **7** is a block diagram illustrating exemplary end-to-end flow monitoring between two organizations.

[0013] FIG. **8** is a block diagram illustrating exemplary end-to-end flow monitoring with network encapsulation.

[0014] FIG. **9** is a block diagram illustrating exemplary flow monitoring at virtual gateways.

[0015] FIGS. **10**A, **10**B, and **10**C are block diagrams illustrating exemplary filtering of flow information based on user role.

[0016] Corresponding reference characters indicate corresponding parts throughout the drawings.

DETAILED DESCRIPTION

[0017] Embodiments described herein provide a virtual network tracing and monitoring system that identifies and selectively monitors network flows, based on a target flow pattern **130**, end-to-end across a virtual network path in a virtual datacenter **302**. In addition to tracing the network flow within hosts, aspects of the disclosure leverage knowledge of virtual datacenter **302** infrastructure to identify, and enable tracing across, logical network edges or other boundaries (e.g., virtual network edges, organization network edges, zones, etc.) along the virtual network path. In some embodiments, virtual network appliances selectively produce a "footprint" of context data for data packets matching flow pattern **130** (e.g., provided by a user **108**). The context data is aggregated at a remote server for analysis and reporting.

[0018] Aspects of the disclosure further enable different users **108** to troubleshoot and identify the source of network issues in different levels within virtual datacenter **302**. In particular, the aggregated context data is filtered or otherwise mined based on different user roles to generate different virtual network monitoring views for presentation to the users **108**. This enables the different users **108** to identify the source of network issues within virtual datacenter **302** according their goals and knowledge levels.

[0019] Accordingly, aspects of the disclosure trace and selectively collect context data for data packets along the entire virtual network data path, including across multiple processing layers. Further, the tracing may occur periodically, intermittently, and/or on-demand, with a reduced negative impact on performance and traffic flooding relative to existing systems due at least to the selectively monitoring. For example, the network traffic is monitored without generating ping messages. As such, aspects of the disclosure provide a consistent, user-differentiated, one-stop troubleshooting and

reporting experience to users **108**. For example, different users **108** can troubleshoot network issues by operating on the same management workflow and user interface, without accessing lower level infrastructure information.

[0020] An example of a virtualized environment is next described.

[0021] FIG. **1** is a block diagram of an exemplary host computing device **100**. Host computing device **100** includes a processor **102** for executing instructions. In some embodiments, executable instructions are stored in a memory area **104**. Memory area **104** is any device allowing information, such as executable instructions and/or other data, to be stored and retrieved. For example, memory area **104** may include one or more random access memory (RAM) modules, flash memory modules, hard disks, solid state disks, and/or optical disks.

[0022] As described further herein, memory **104** stores at least one of flow pattern **130** for use in monitoring data packets.

[0023] Host computing device **100** may include a user interface device **110** for receiving data from user **108** and/or for presenting data to user **108**. User **108** may interact indirectly with host computing device **100** via another computing device such as VMware's vCenter Server or other management device. User interface device **110** may include, for example, a keyboard, a pointing device, a mouse, a stylus, a touch sensitive panel (e.g., a touch pad or a touch screen), a gyroscope, an accelerometer, a position detector, and/or an audio input device. In some embodiments, user interface device **110** operates to receive data from user **108**, while another device (e.g., a presentation device) operates to present data to user **108**. In other embodiments, user interface device **110** has a single component, such as a touch screen, that functions to both output data to user **108** and receive data from user **108**. In such embodiments, user interface device **110** operates as a presentation device for presenting information to user **108**. In such embodiments, user interface device **110** represents any component capable of conveying information to user **108**. For example, user interface device **110** may include, without limitation, a display device (e.g., a liquid crystal display (LCD), organic light emitting diode (OLED) display, or "electronic ink" display) and/or an audio output device (e.g., a speaker or headphones). In some embodiments, user interface device **110** includes an output adapter, such as a video adapter and/or an audio adapter. An output adapter is operatively coupled to processor **102** and configured to be operatively coupled to an output device, such as a display device or an audio output device.

[0024] Host computing device **100** also includes a network communication interface **112**, which enables host computing device **100** to communicate with a remote device (e.g., another computing device) via a communication medium, such as a wired or wireless packet network. For example, host computing device **100** may transmit and/or receive data via network communication interface **112**. User interface device **110** and/or network communication interface **112** may be referred to collectively as an input interface and may be configured to receive information from user **108**.

[0025] Host computing device **100** further includes a storage interface **116** that enables host computing device **100** to communicate with one or more datastores, which store virtual disk images, software applications, and/or any other data suitable for use with the methods described herein. In exemplary embodiments, storage interface **116** couples host computing device **100** to a storage area network (SAN) (e.g., a Fibre Channel network) and/or to a network-attached storage (NAS) system (e.g., via a packet network). The storage interface **116** may be integrated with network communication interface **112**.

[0026] FIG. **2** depicts a block diagram of virtual machines 235_1, 235_2 . . . 235_N that are instantiated on host computing device **100**. Host computing device **100** includes a hardware platform **205**, such as an x86 architecture platform. Hardware platform **205** may include processor **102**, memory area **104**, network communication interface **112**, user interface device **110**, and other input/output (I/O) devices, such as a presentation device **106** (shown in FIG. **1**). A virtualization software layer, also referred to hereinafter as a hypervisor **210**, is installed on top of hardware platform **205**.

[0027] The virtualization software layer supports a virtual machine execution space **230** within which multiple virtual machines (VMs 235_1-235_N) may be concurrently instantiated and executed. Hypervisor **210** includes a device driver layer **215**, and maps physical resources of hardware platform **205** (e.g., processor **102**, memory area **104**, network communication interface **112**, and/or user interface device **110**) to "virtual" resources of each of VMs 235_1-235_N such that each of VMs 235_1-235_N has its own virtual hardware platform (e.g., a corresponding one of virtual hardware platforms 240_1-240_N), each virtual hardware platform having its own emulated hardware (such as a processor **245**, a memory **250**, a network communication interface **255**, a user interface device **260** and other emulated I/O devices in VM 235_1). Hypervisor **210** may manage (e.g., monitor, initiate, and/or terminate) execution of VMs 235_1-235_N according to policies associated with hypervisor **210**, such as a policy specifying that VMs 235_1-235_N are to be automatically restarted upon unexpected termination and/or upon initialization of hypervisor **210**. In addition, or alternatively, hypervisor **210** may manage execution VMs 235_1-235_N based on requests received from a device other than host computing device **100**. For example, hypervisor **210** may receive an execution instruction specifying the initiation of execution of first VM 235_1 from a management device via network communication interface **112** and execute the execution instruction to initiate execution of first VM 235_1.

[0028] In some embodiments, memory **250** in first virtual hardware platform 240_1 includes a virtual disk that is associated with or "mapped to" one or more virtual disk images stored on a disk (e.g., a hard disk or solid state disk) of host computing device **100**. The virtual disk image represents a file system (e.g., a hierarchy of directories and files) used by first VM 235_1 in a single file or in a plurality of files, each of which includes a portion of the file system. In addition, or alternatively, virtual disk images may be stored on one or more remote computing devices **100**, such as in a storage area network (SAN) configuration. In such embodiments, any quantity of virtual disk images may be stored by the remote computing devices **100**.

[0029] Device driver layer **215** includes, for example, a communication interface driver **220** that interacts with network communication interface **112** to receive and transmit data from, for example, a local area network (LAN) connected to host computing device **100**. Communication interface driver **220** also includes a virtual bridge **225** that simulates the broadcasting of data packets in a physical network received from one communication interface (e.g., network communication interface **112**) to other communication interfaces (e.g., the virtual communication interfaces of VMs

235_1-235_N). Each virtual communication interface for each VM 235_1-235_N, such as network communication interface **255** for first VM 235_1, may be assigned a unique virtual Media Access Control (MAC) address that enables virtual bridge **225** to simulate the forwarding of incoming data packets from network communication interface **112**. In an embodiment, network communication interface **112** is an Ethernet adapter that is configured in "promiscuous mode" such that all Ethernet packets that it receives (rather than just Ethernet packets addressed to its own physical MAC address) are passed to virtual bridge **225**, which, in turn, is able to further forward the Ethernet packets to VMs 235_1-235_N. This configuration enables an Ethernet packet that has a virtual MAC address as its destination address to properly reach the VM in host computing device **100** with a virtual communication interface that corresponds to such virtual MAC address.

[0030] Virtual hardware platform 240_1 may function as an equivalent of a standard x86 hardware architecture such that any x86-compatible desktop operating system (e.g., Microsoft WINDOWS brand operating system, LINUX brand operating system, SOLARIS brand operating system, NETWARE, or FREEBSD) may be installed as guest operating system (OS) 265 in order to execute applications **270** for an instantiated VM, such as first VM 235_1. Virtual hardware platforms 240_1-240_N may be considered to be part of virtual machine monitors (VMM) 275_1-275_N that implement virtual system support to coordinate operations between hypervisor **210** and corresponding VMs 235_1-235_N. Those with ordinary skill in the art will recognize that the various terms, layers, and categorizations used to describe the virtualization components in FIG. **2** may be referred to differently without departing from their functionality or the spirit or scope of the disclosure. For example, virtual hardware platforms 240_1-240_N may also be considered to be separate from VMMs 275_1-275_N, VMMs 275_1-275_N may be considered to be separate from hypervisor **210**. One example of hypervisor **210** that may be used in an embodiment of the disclosure is included as a component in VMware's ESX brand software, which is commercially available from VMware, Inc.

[0031] In some embodiments, host computing device **100** represents any device executing instructions (e.g., as application programs, operating system functionality, or both) to implement the operations and functionality described herein. For example, one or more of host computing devices **100** execute instructions to implement the operations illustrated in FIG. **4** and/or FIG. **5**. Host computing device **100** may include any computing device or processing unit. For example, host computing device **100** may represent a group of processing units or other computing devices, such as in a cloud computing configuration.

[0032] Processor **102** includes any quantity of processing units, and is programmed to execute computer-executable instructions for implementing aspects of the disclosure. The instructions may be performed by processor **102** or by multiple processors executing within host computing device **100**, or performed by a processor external to host computing device **100** (e.g., another processor available within virtual datacenter **302**). In some embodiments, processor **102** is programmed to execute instructions such as those illustrated in the figures.

[0033] Memory area **104** includes any quantity of computer-readable media associated with or accessible by host computing device **100** or other entity within virtual datacenter **302**. Memory area **104**, or portions thereof, may be internal to host computing device **100**, external to host computing device **100**, or both.

[0034] FIG. **3** is a block diagram of components associated with virtual datacenter **302**. In the example of FIG. **3**, user **108** interacts with virtual datacenter **302**. User **108** may be classified, categorized, or typed based on a role, employment title, and/or interests of user **108**. For example, user **108** includes, but is not limited to, an administrator of virtual datacenter **302**, an owner of a virtual application, a developer, and/or other user involved with virtual datacenter **302**. In some embodiments, the amount and content of flow monitoring and/or tracing data (e.g., collected context data describing data packets) is dependent on the type, category, role, or classification of user **108**.

[0035] As shown in FIG. **3**, virtual datacenter **302** includes one or more computer storage media **304**, such as memory area **104** in some embodiments. Computer storage media **304** store components that, when executed by a processor such as processor **102**, perform various operations. The components illustrated in FIG. **3** include a management component **306** communicating with each of a plurality of host components **308**, such as host component #1 through host component #N.

[0036] The functionality associated with management component **306** is described below with reference to FIG. **4**. In some embodiments, this functionality is implemented by a cloud operating system, a cloud application, a virtual datacenter operating system, a virtual datacenter application, and/or other logic or code supporting an environment having a plurality of VMs executing therein. An example of a cloud operating system includes VMware's vSphere brand software, while an example of a virtual datacenter operation system and/or application includes VMware's vCloud Director software.

[0037] Further, the functionality associated with host components **308** is described below with reference to FIG. **5**. In some embodiments, this functionality is implemented by a virtualization layer such as hypervisor **210**. For example, each of host components **308** manages a plurality of VMs.

[0038] FIG. **4** is a flowchart of an exemplary method **400** performed by virtual datacenter **302** to initiate flow monitoring in virtual networks in virtual datacenter **302**. For example, one or more of the operations illustrated in FIG. **4** may be performed by management component **306** illustrated in FIG. **3**. However, while method **400** is described with reference to execution by virtual datacenter **302** (shown in FIG. **3**), it is contemplated that method **400** may be performed by any computing device, application, and/or other entity. For example, method **400** may be performed by host computing device **100**.

[0039] At **402**, virtual datacenter **302** checks whether flow pattern **130** has been received from user **108**. For example, flow pattern **130** may be received or identified as part of a request from user **108** to initiate virtual network flow monitoring. Flow pattern **130** describes characteristics of data packets of interest to user **108**. The characteristics relate to the content and/or structure of the data packets. In some embodiments, an exemplary flow pattern **130** includes a source address and a destination address. Flow pattern **130** may include other data such as user-defined keys, a protocol type, and/or other data. Exemplary protocol types include, but are not limited to, a transmission control protocol (TCP) and/or a user datagram protocol (UDP). In some embodiments, flow pattern **130** identifies a source Internet Protocol (IP) address,