



US 20080301776A1

(19) **United States**(12) **Patent Application Publication**
Weatherford(10) **Pub. No.: US 2008/0301776 A1**(43) **Pub. Date: Dec. 4, 2008**(54) **SYSTEM METHOD FOR PROVIDING
SECURE ACCESS TO A COMMUNICATIONS
NETWORK****Publication Classification**(51) **Int. Cl.**
G06F 21/00 (2006.01)(52) **U.S. Cl.** **726/3**(57) **ABSTRACT**

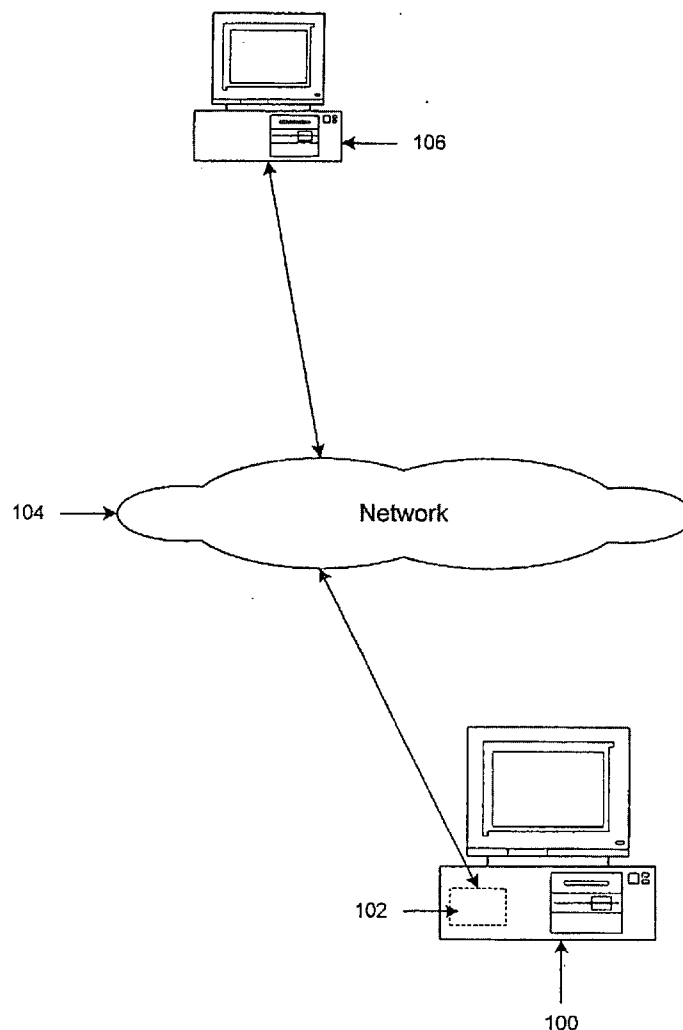
A system and method for providing secure access to a telecommunications network system. In one embodiment, a cellular device produces a communication session key and utilizes an index and corresponding timing intervals previously provided by the network to the cellular device. The session key is divided into multiple segments that are placed into separate data packets. The data packets, separated by the timing intervals, are sent to the network where a comparison is made between the information in the data packets and the time intervals between the data packets. The timing intervals between the data packets must match an identical set of time intervals stored in the network and if so, the network assembles the data packets to provide a session key for secure communications between the network and the access device.

(76) Inventor: **Sidney L. Weatherford,**
Richardson, TX (US)

Correspondence Address:
Sidney L. Weatherford
1006 Rainbow Drive
Richardson, TX 75081 (US)

(21) Appl. No.: **12/218,010**(22) Filed: **Jul. 10, 2008****Related U.S. Application Data**

(63) Continuation-in-part of application No. 11/607,764, filed on Dec. 1, 2006, which is a continuation-in-part of application No. 09/783,049, filed on Feb. 14, 2001, now Pat. No. 7,043,640.



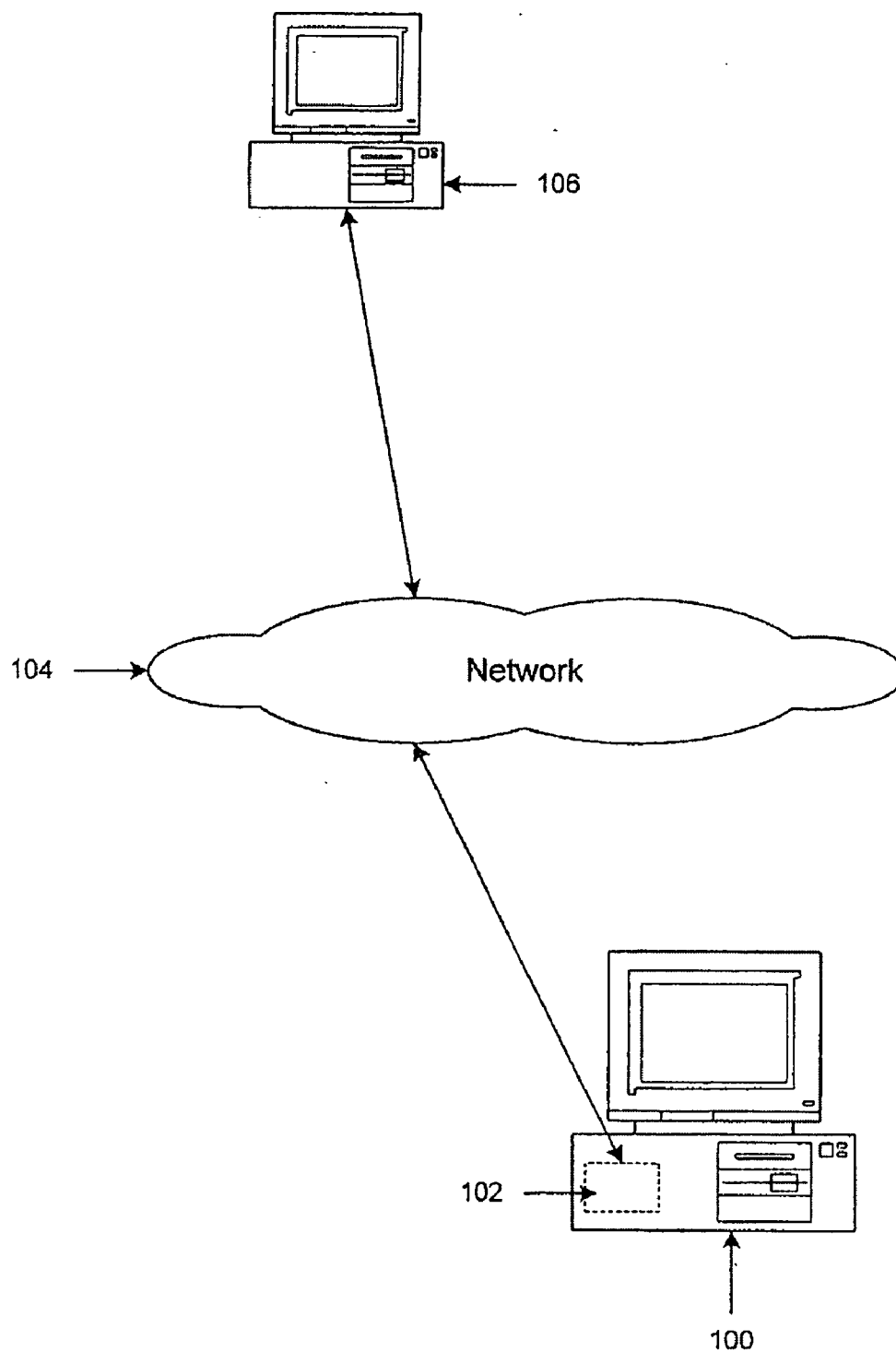


FIGURE 1

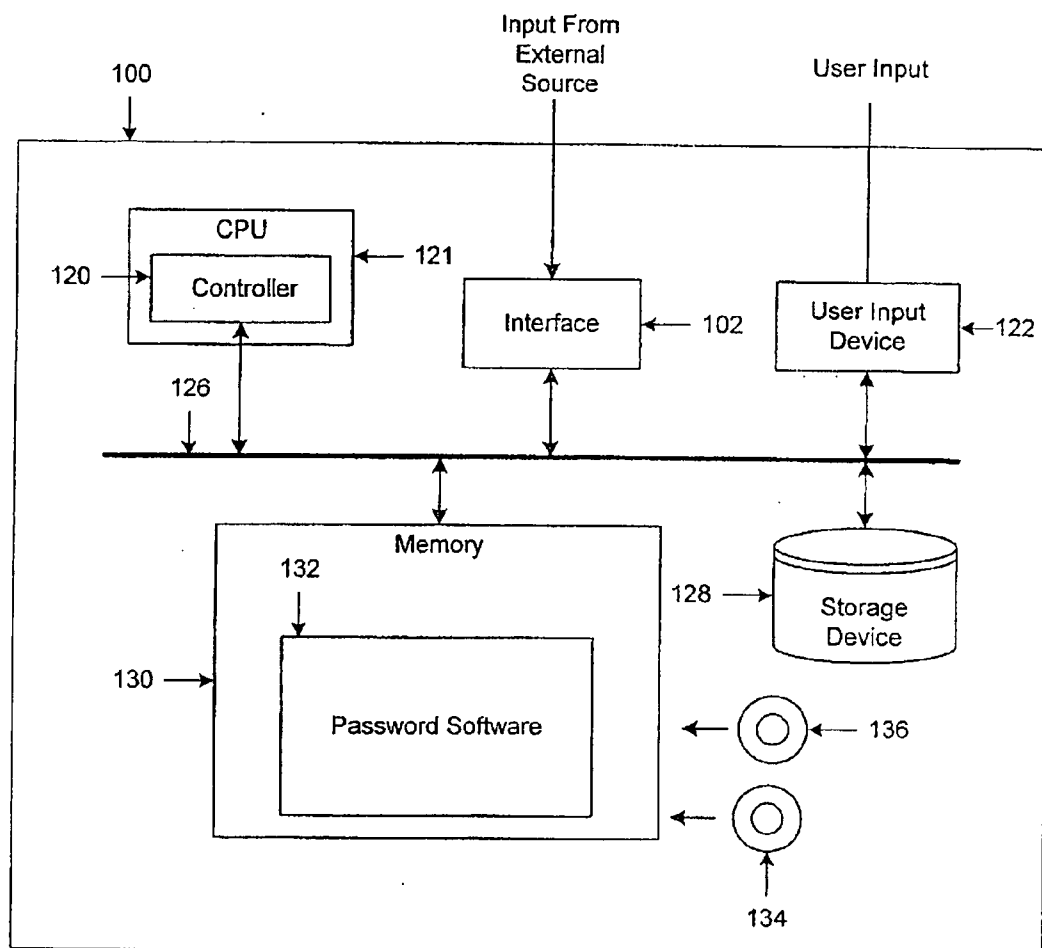


FIGURE 1A

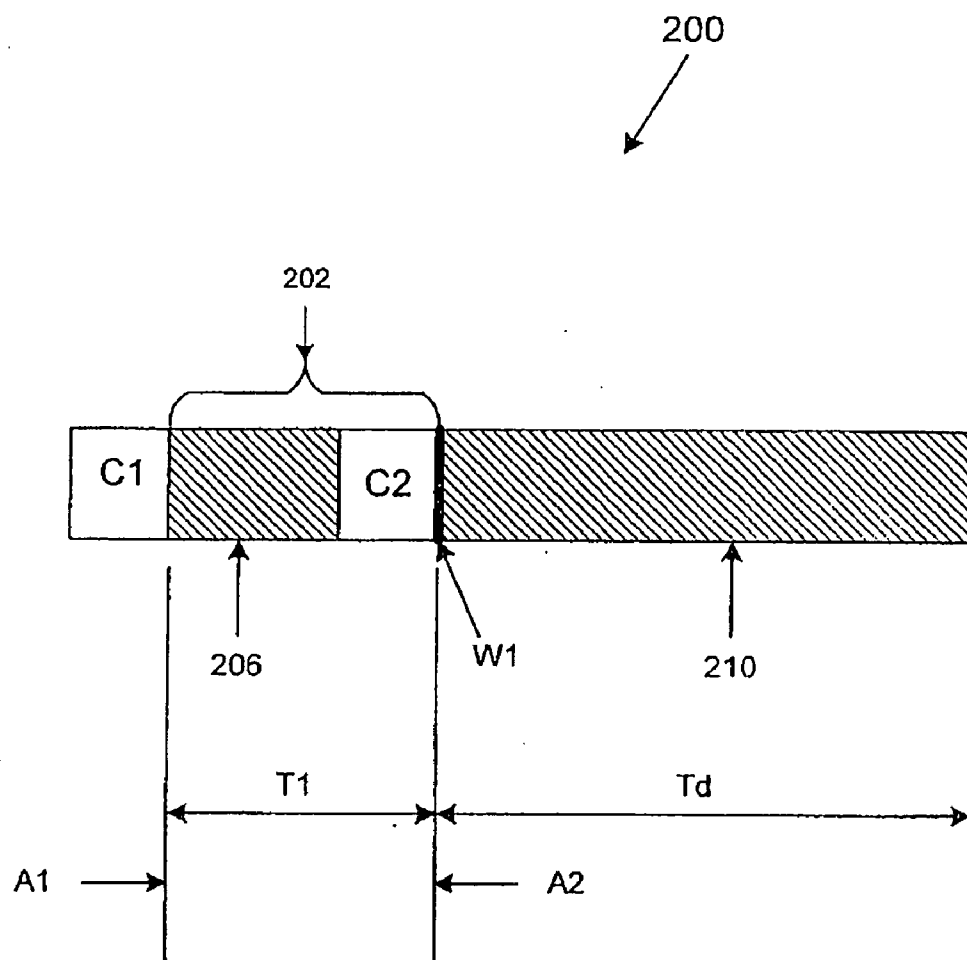


FIGURE 2A

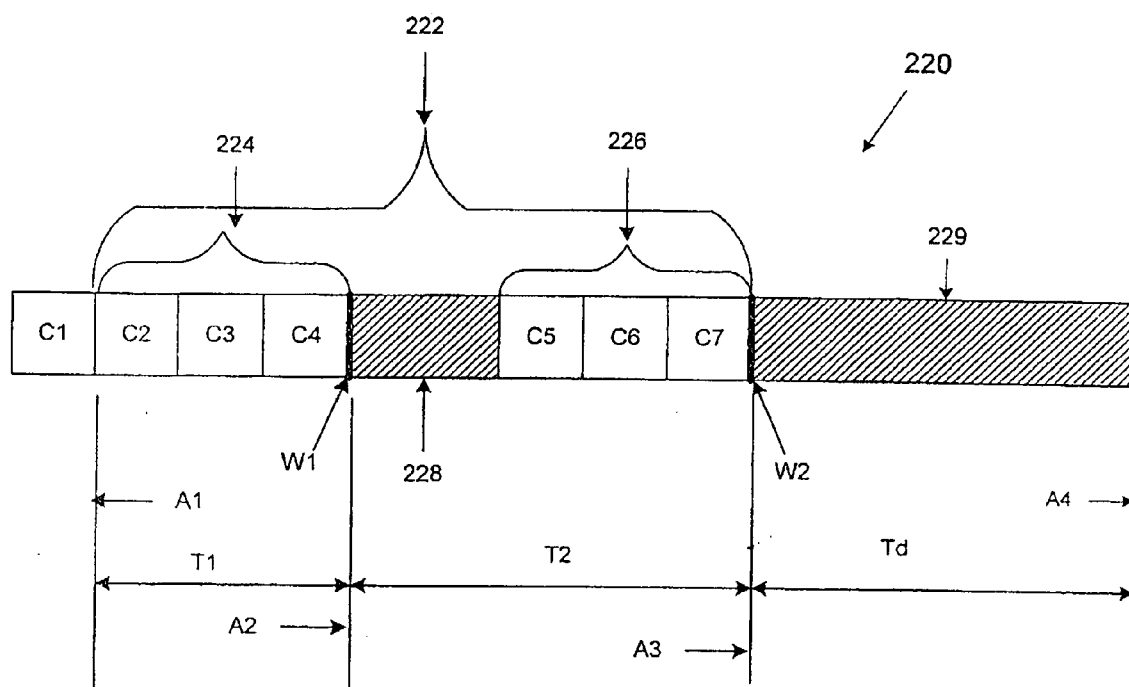


FIGURE 2B

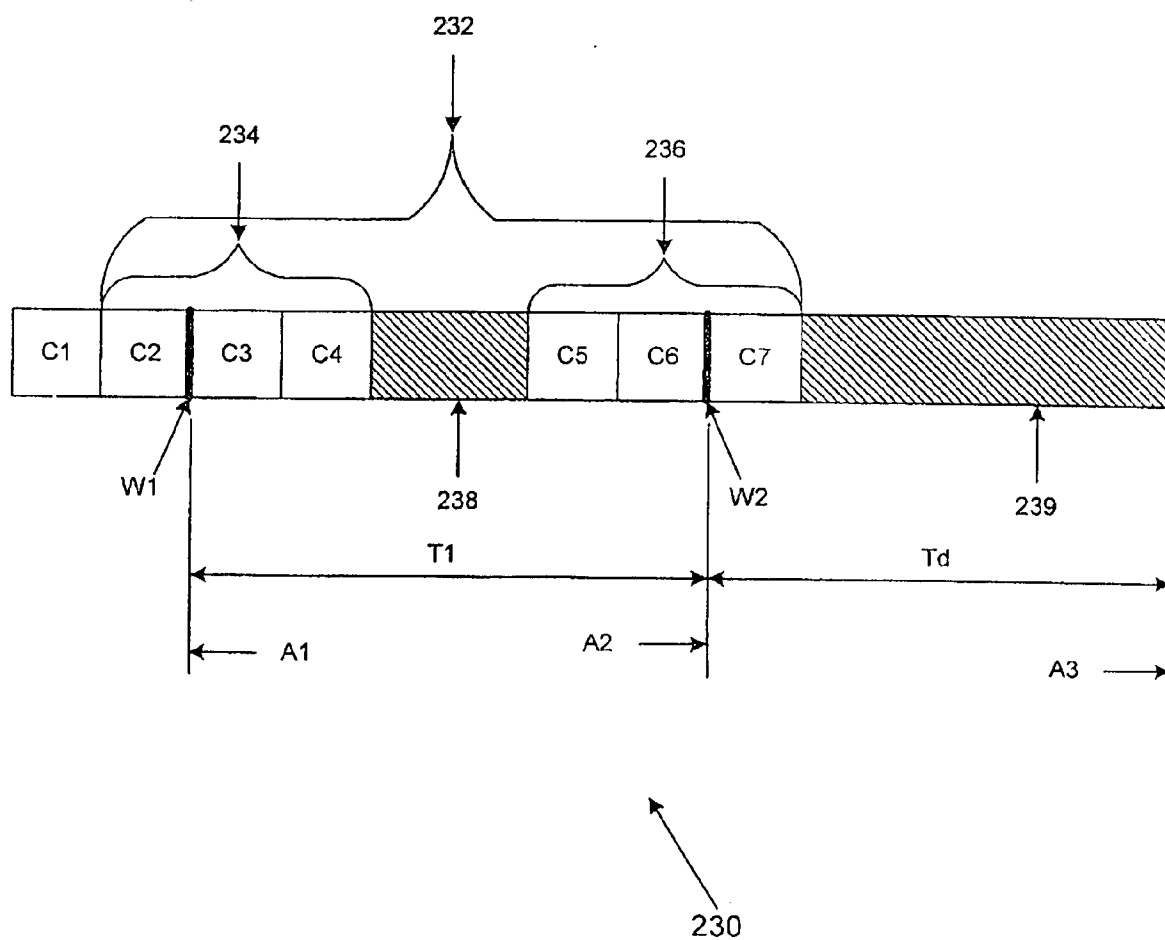


FIGURE 2C

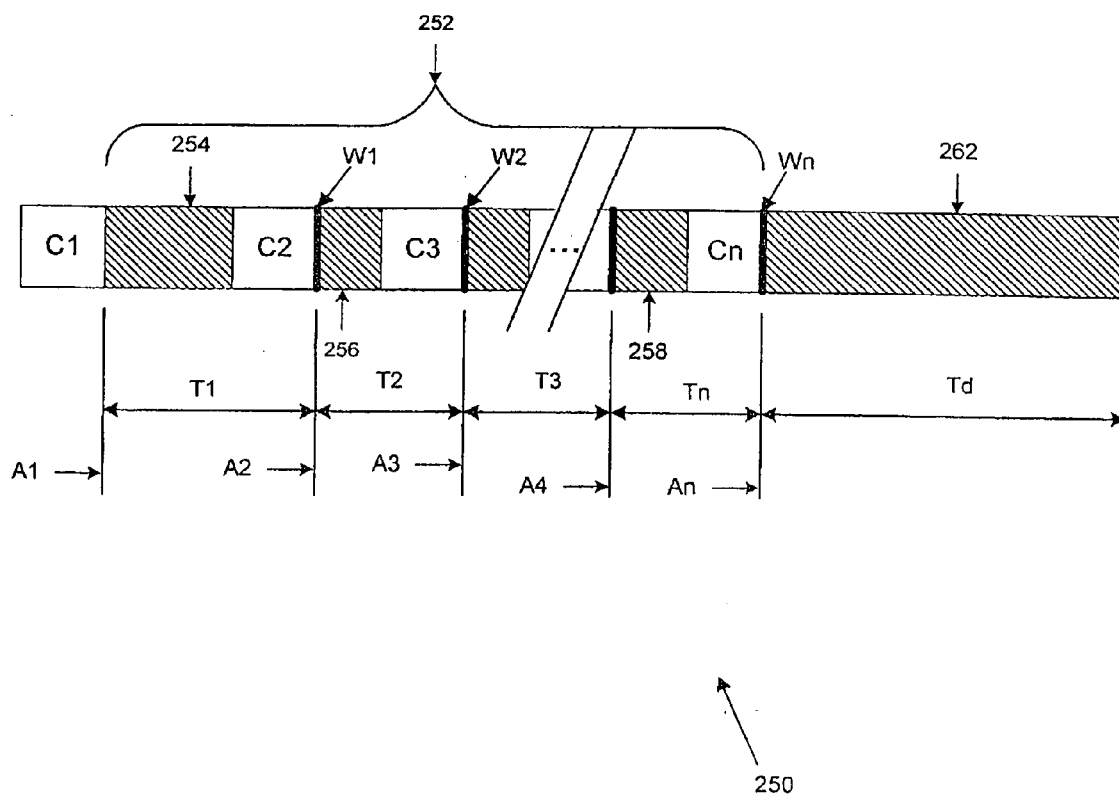


FIGURE 2D

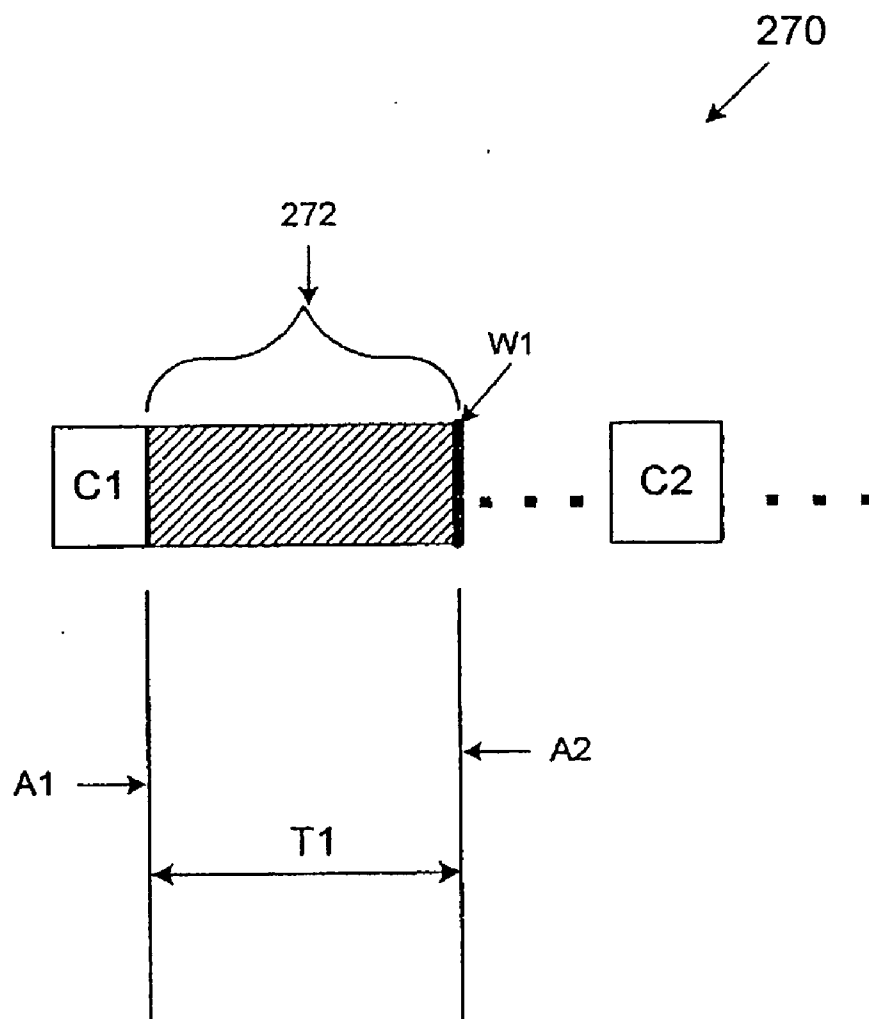


FIGURE 2E

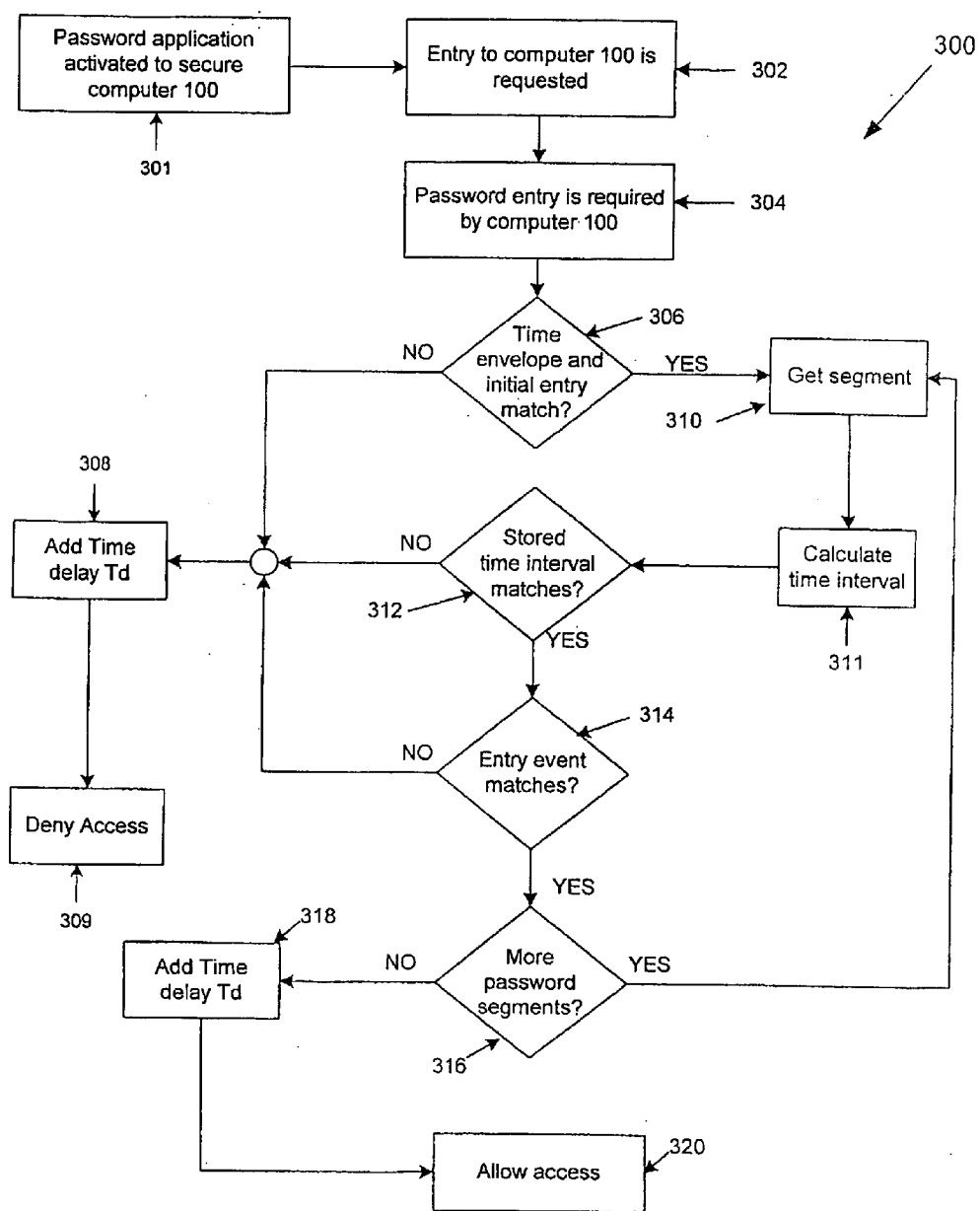


FIGURE 3

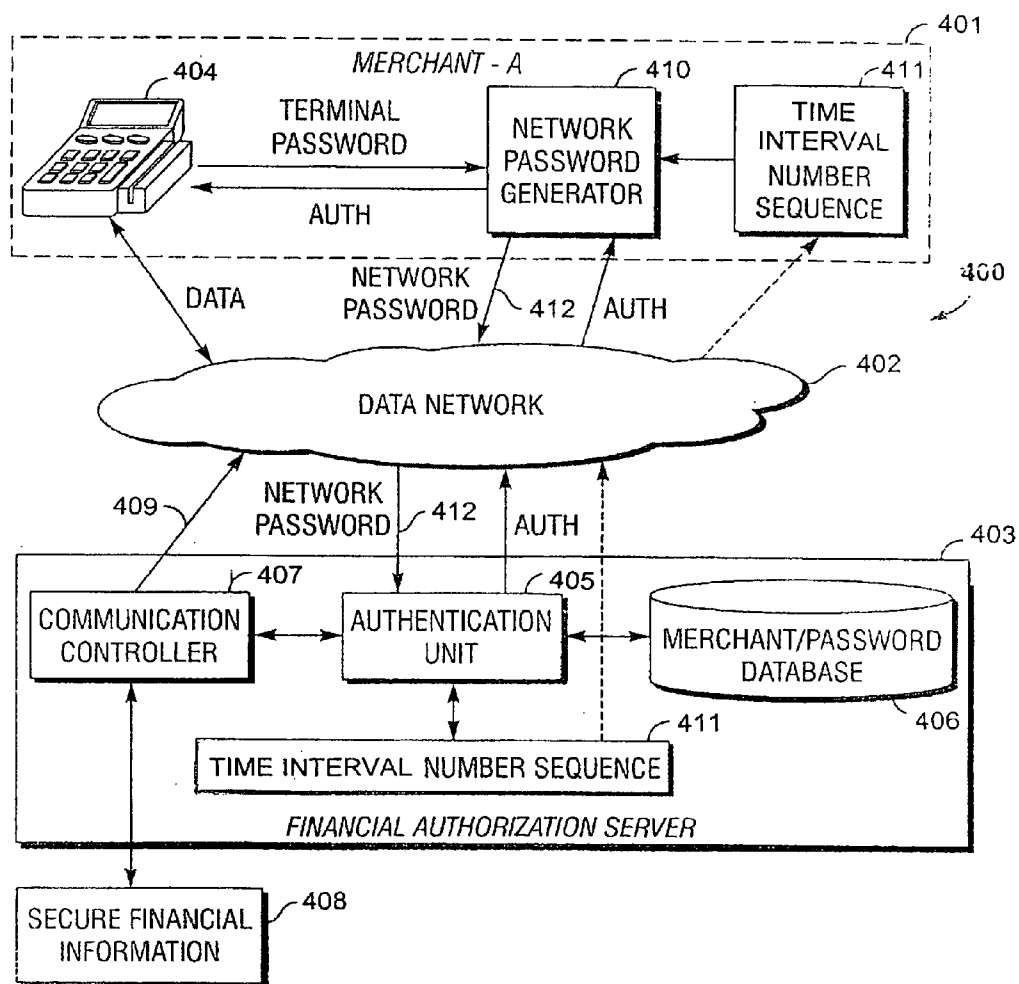


FIGURE 4

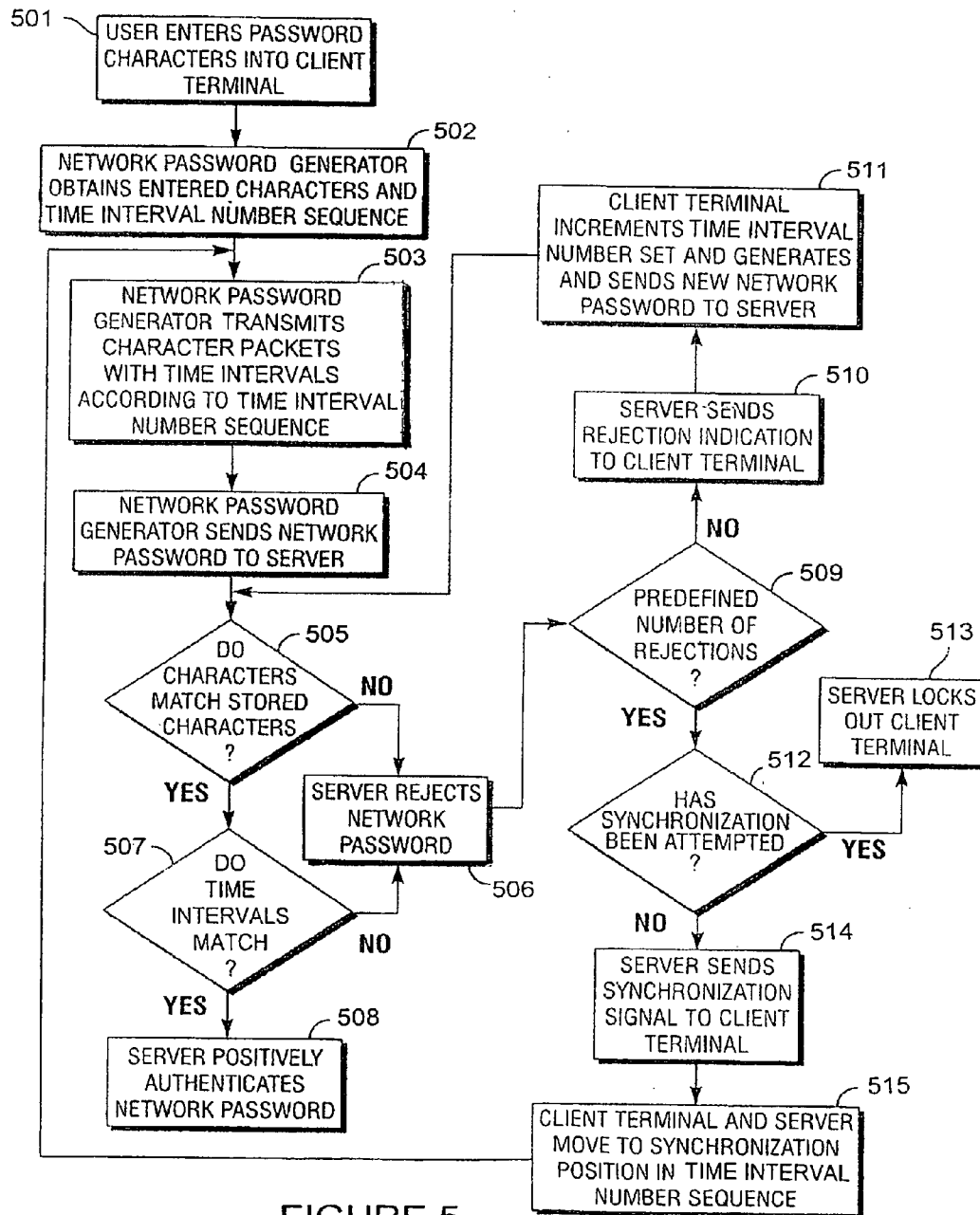


FIGURE 5

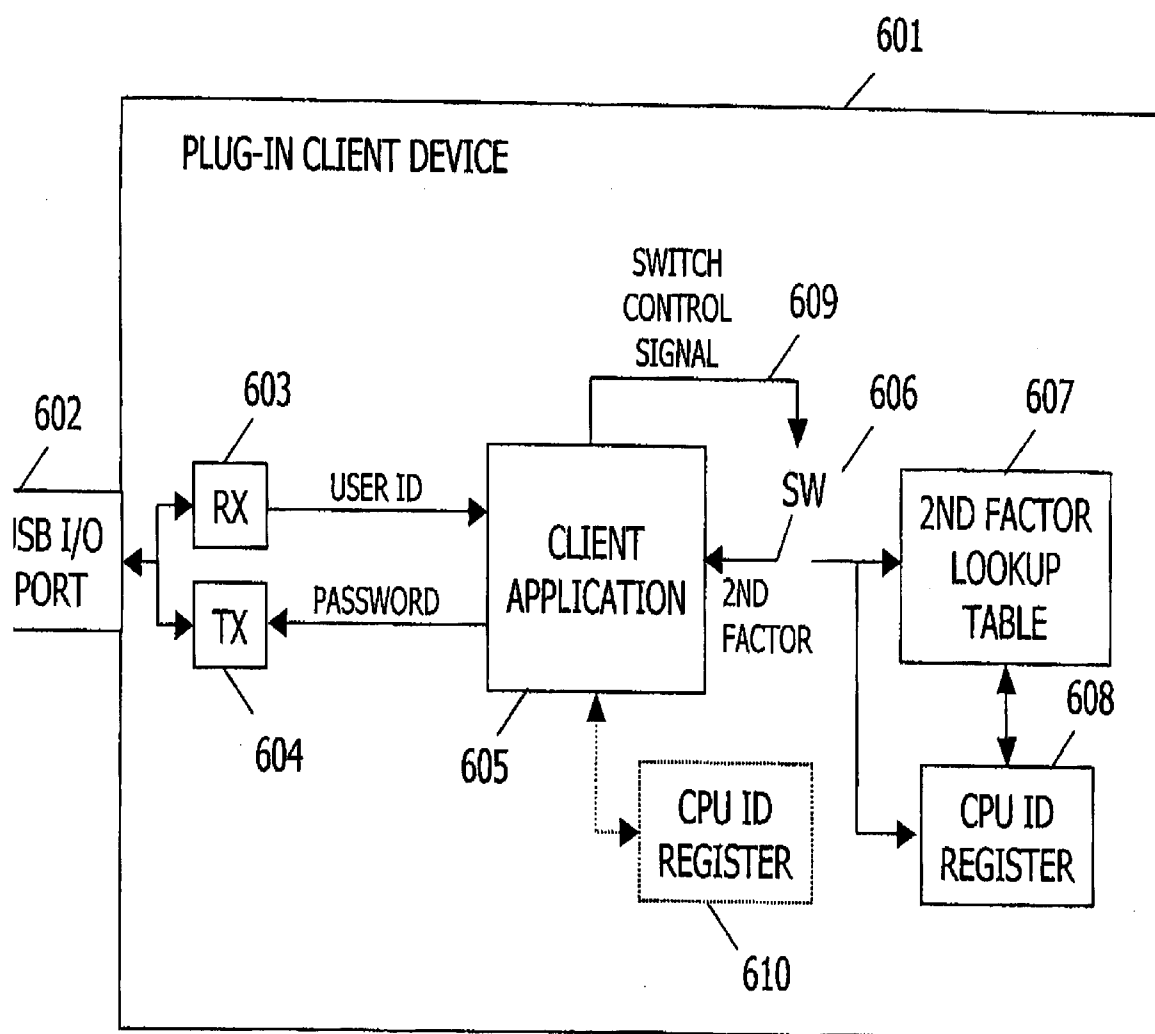


FIGURE 6

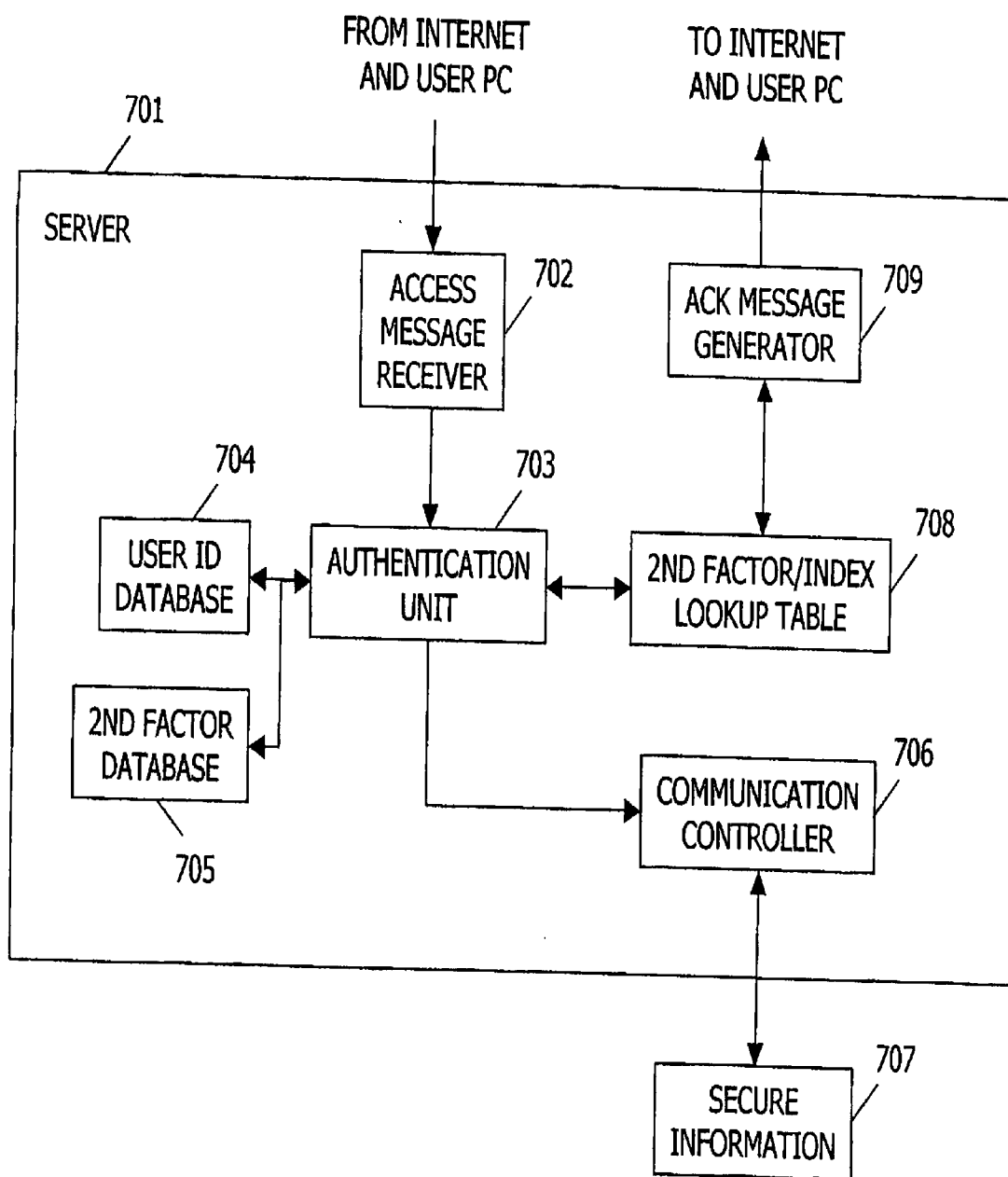


FIGURE 7

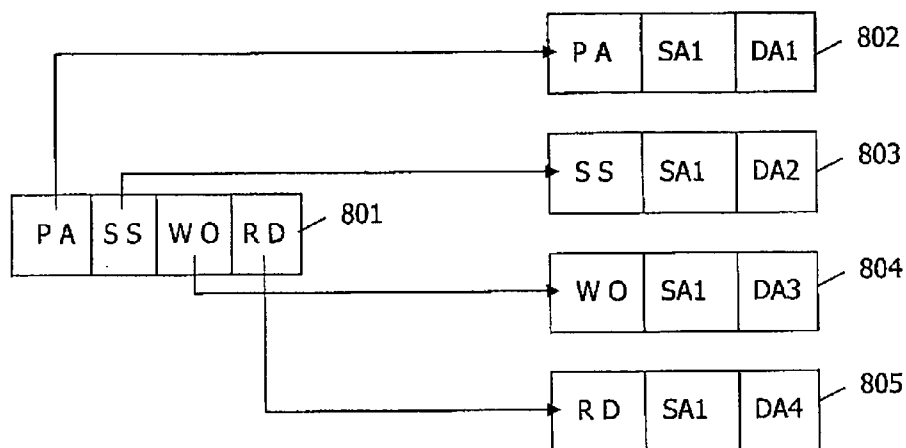


FIGURE 8

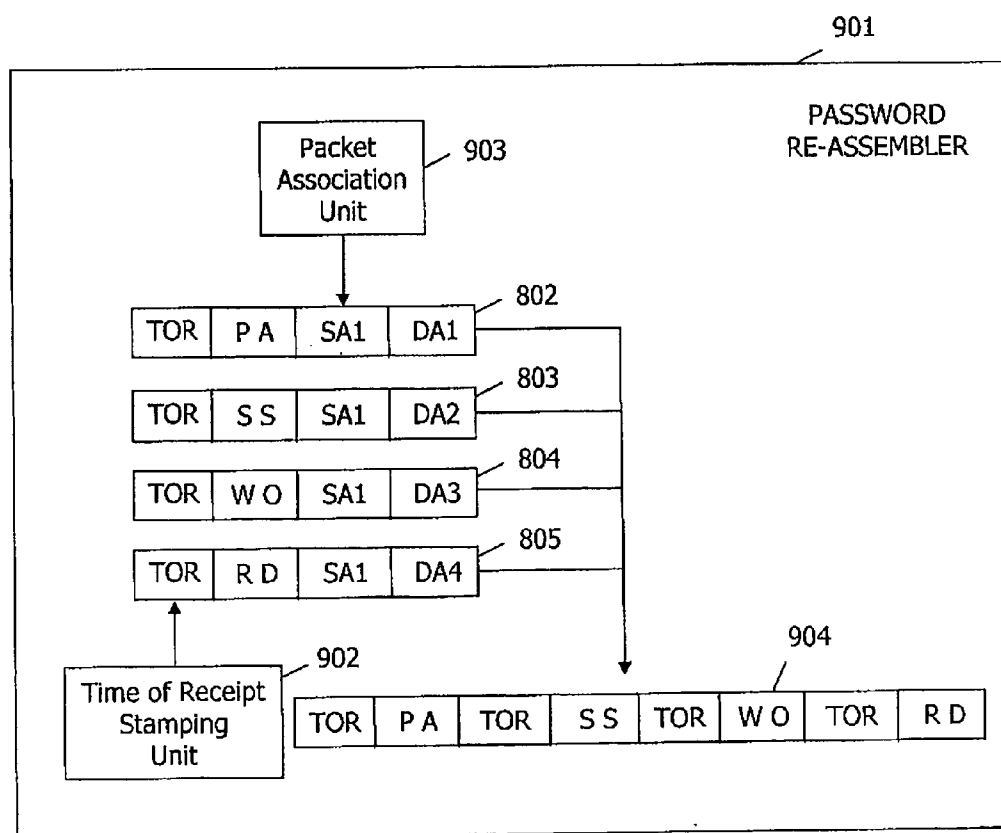


FIGURE 9

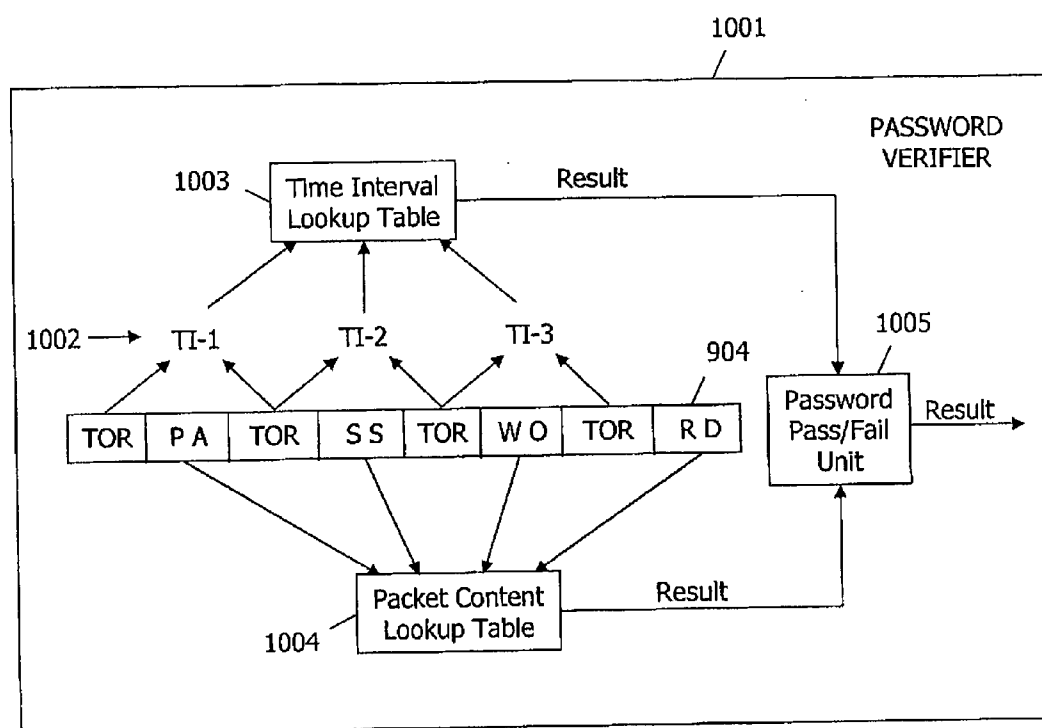


FIGURE 10

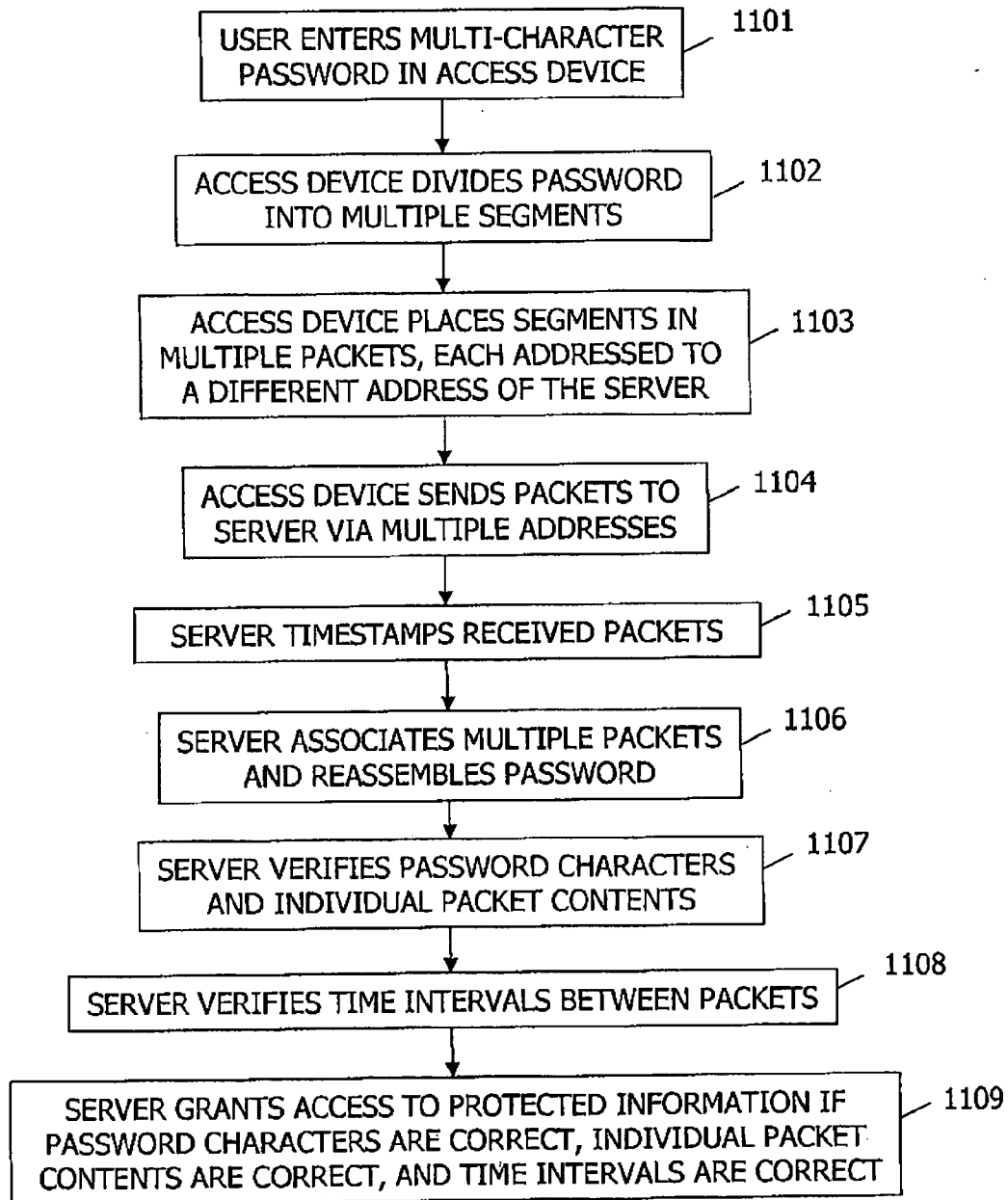
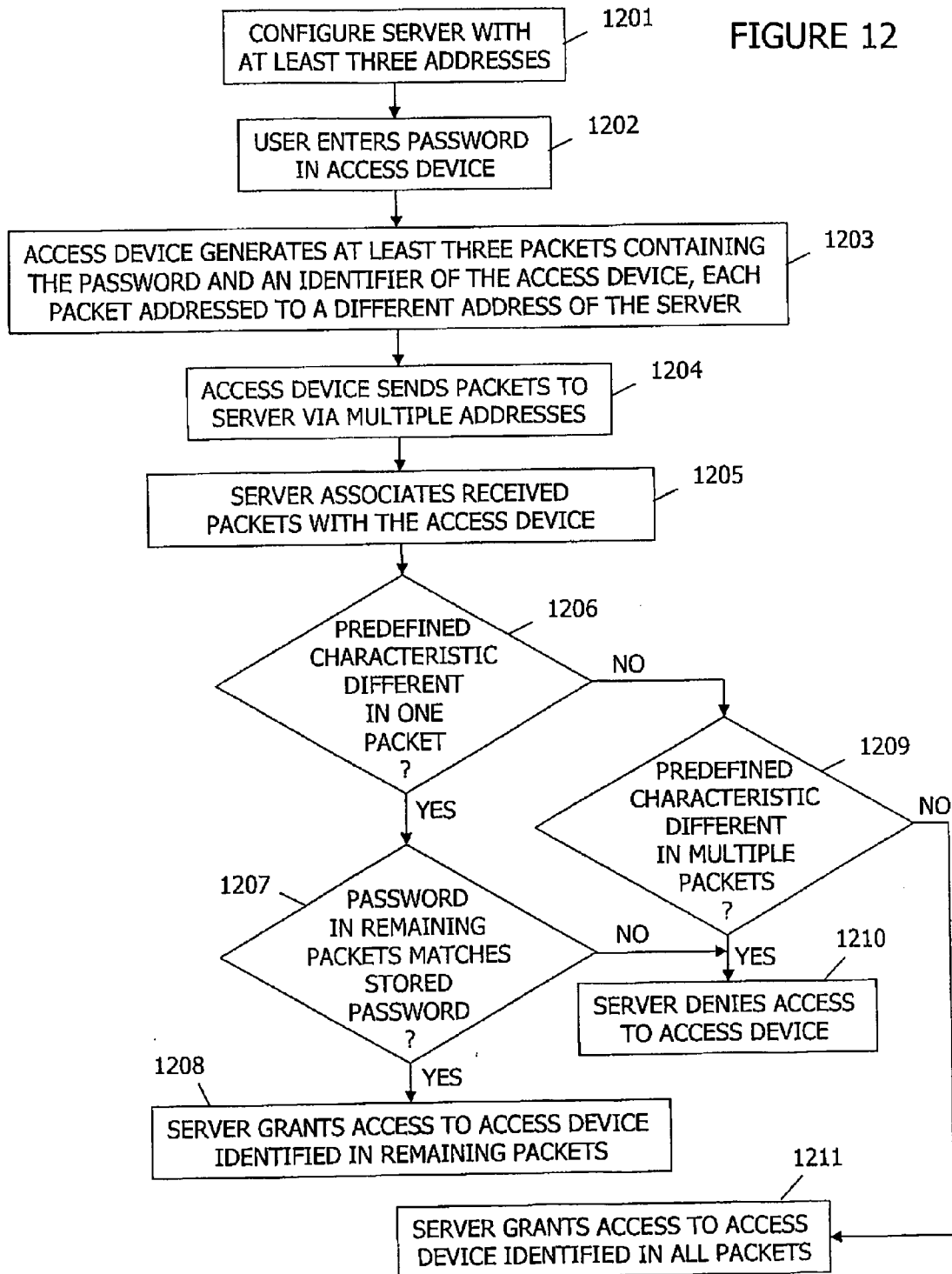


FIGURE 11

FIGURE 12



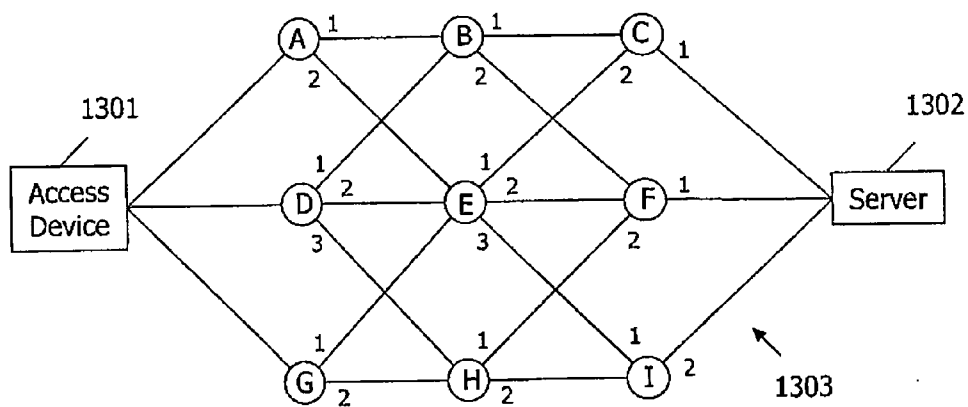


FIGURE 13

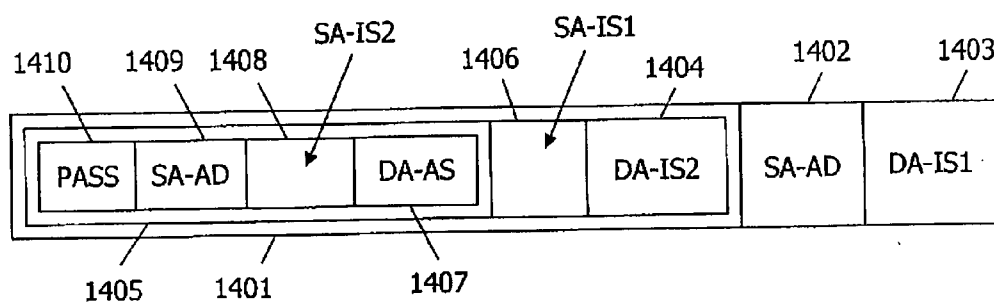


FIGURE 14

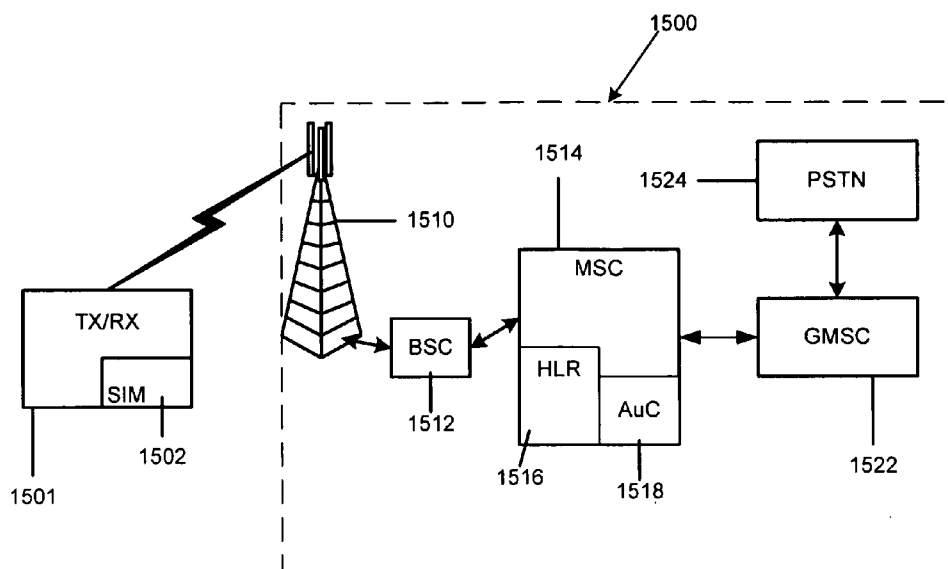


FIGURE 15
(Prior Art)

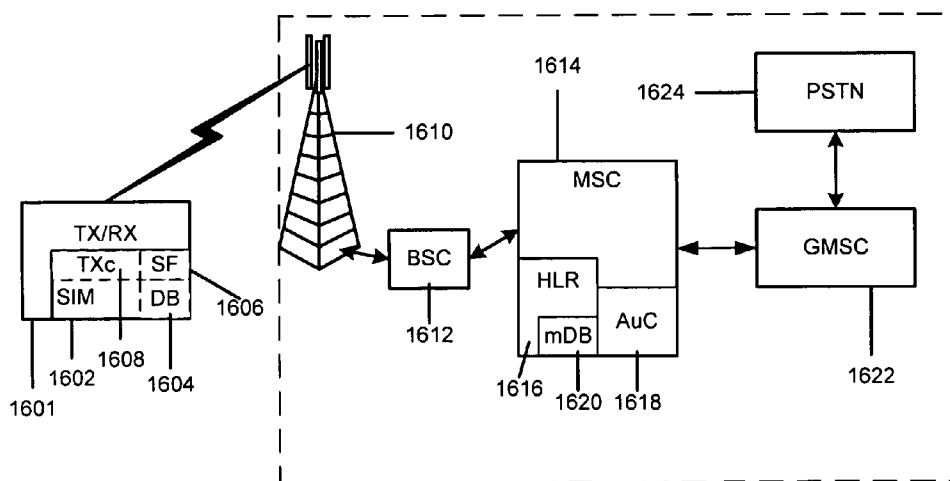
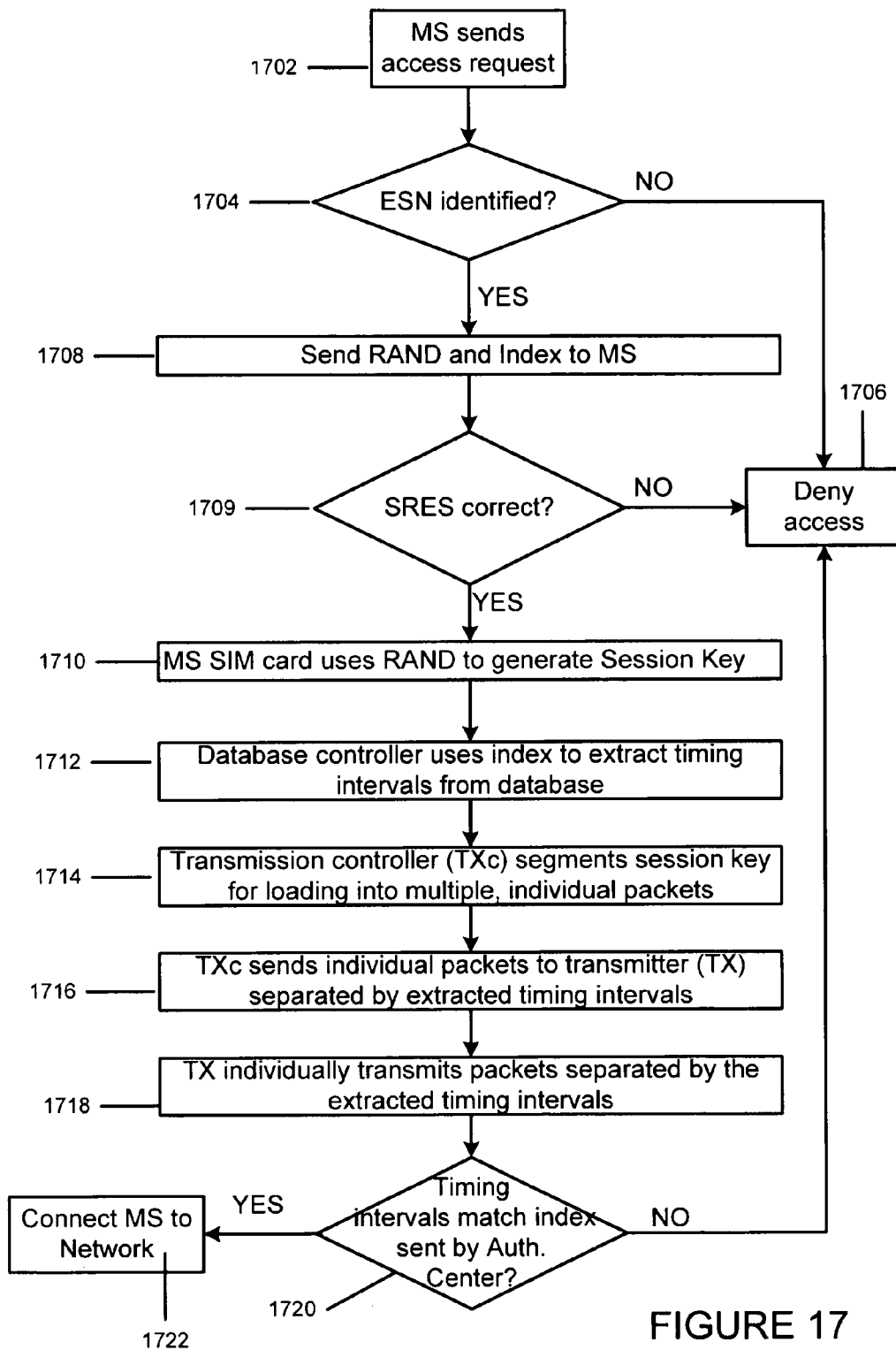


FIGURE 16



SYSTEM METHOD FOR PROVIDING SECURE ACCESS TO A COMMUNICATIONS NETWORK

RELATED APPLICATIONS

[0001] This application is a continuation-in-part of co-pending U.S. patent application Ser. No. 11/607,764 filed Dec. 1, 2006, which is a continuation-in-part of U.S. patent application Ser. No. 09/783,049 filed Feb. 14, 2001, now U.S. Pat. No. 7,043,640, the entire disclosures of which are incorporated by reference herein.

BACKGROUND OF THE INVENTION

[0002] The present invention is directed, in general, to communication security systems. More particularly, and not by way of limitation, the present invention is directed to a system and method for providing secure access to a communications network.

[0003] Computers and networks are often protected by passwords. In order to gain access to the computer or network, a user must enter a password. The computer or network controller (server) authenticates the password by comparing the password entered by the user with a stored password. If the entered password matches the stored password, the user is given access. If not, the user is denied access.

[0004] A major problem with password-protected computer systems is the already large and growing threat from "hackers." The popular definition of a hacker refers to individuals who gain unauthorized access to computer systems for the purpose of stealing and/or corrupting data. Hackers are known for breaking into supposedly secure computer systems and damaging web sites, credit card accounts, internal databases, and the like.

[0005] Hacker software tools include programs that try many combinations of numbers and letters over a set period of time in an attempt to compromise a password-protected system. On some computer operating systems, as each letter or number is presented by the hacker, the letter or number is confirmed by the system as being correct or incorrect. This serial confirmation sequence actually makes it easier for a hacker to gain entry because fewer combinations of letters and numbers have to be tried. On other operating systems, the password must be completely entered correctly before confirmation is supplied by the system. This may slow down the password discovery process, but with time, the hacker can eventually present a correct password to the target computer system.

[0006] A passive hacker may monitor communications between a client device and an authentication server to learn the user's password. The passive hacker may then use the learned password to gain access to the server at a later time. For this reason, many organizations have their users periodically change their passwords. This is a great inconvenience for the users. To defeat the passive hacker, solutions have been tried which change the password for each access. Each time the user logs on, the user types his personal password plus a six-digit number which changes for every logon attempt. Once again, this is a great inconvenience for the user.

[0007] An active hacker may actually intercept and alter data packets sent from the client device to the authentication server, preventing the original packets from arriving at the server. The active hacker may then alter the data contents of the packets or may alter address information, thereby posing

as the authorized user. The above solution of adding a changing six-digit number to the user's personal password does not defeat this type of active hacker if the hacker can access the server while the changing number is still valid.

[0008] In another type of active hacking, the hacker intercepts and alters the destination address of the client's data packets to a fake website which simulates the website the user was trying to reach. For example, the hacker may reroute a user to a fake website which is set up to appear as the user's bank. In an alternative form of this technique, known as phishing, the hacker sends an e-mail to the user posing as his bank's security department and asks the user to click on a link to verify his account information. The link takes the user to a fake site where the user is asked to enter his password and his account number. The hacker then uses this information to access the user's account at his bank.

[0009] In yet another type of hacking, the hacker may install a program known as a Trojan on the user's computer. The Trojan monitors the user's keyboard and captures the keystrokes as the user enters his password. The Trojan then reports the password to the hacker who uses it to gain access to the user's protected information.

[0010] Currently, there is no known solution for countering all of the above hacker threats. Therefore, a need exists in the art for an improved system and method for providing secure access to a computer system, which overcomes the shortcomings of the prior art and protects computer systems from unauthorized access by both passive and active hackers. The present invention provides such a system and method.

[0011] In a cellular network, similar hacker problems exist for wireless subscribers and the network operators. For instance, in a GSM network, security information can be copied from a subscriber's cellphone wirelessly, allowing "fraudsters" to clone the subscriber's cellphone identity and security information in another cellphone. The cloned cellphone then appears to an operator's network as the subscriber. Also, in cellular networks, Short Message Service (SMS) is a service provided through GSM that enables users to send text messages to other mobile users. Text messaging is very popular, and most users either ignore or are unaware that SMS messages are sent in clear text format. A fraudster could send a text message with instructions for a legitimate user to include sensitive information in a return text message. If the legitimate user sends the sensitive information, the fraudster could use that sensitive information in a harmful manner.

SUMMARY OF THE INVENTION

[0012] In one aspect the invention is directed to a method for authenticating a cellular device for connection to a cellular network. The method includes sending a request for connecting the cellular device (computer, cell phone, Global Positioning Service, etc.) to the cellular network and the request includes the network's required identification codes. The cellular network responds to the request and the response includes an index that corresponds to a database entry that is accessible by the authentication entity in the network. The database entry may comprise a randomly generated set of timing intervals.

[0013] The cellular device uses the index to retrieve the timing intervals indicated by the received index, from a database stored on or associated with the cellular device. A secret number known only to the authenticating entity (MSC, Authentication Center, Base Station controller, etc.) in the cellular network is utilized to generate a communication ses-

sion key, which is used to encrypt the communications between the cellular device and the network.

[0014] The session key is broken up and each portion of the key is loaded into a packet in a group of packets that contain the complete session key. The group of packets is then transmitted to the authenticating entity, with the packets being separated by the retrieved timing intervals. Upon receipt of the group of packets, the authenticating entity measures the timing intervals and determines whether the intervals correspond to the timing intervals corresponding to the index provided to the cellular device. If the index contains timing intervals that match the measured intervals, the cellular device is connected to the network; access is denied if the index and the measured intervals do not match.

[0015] In another aspect, the present invention is directed to a system for authenticating a cellular device for connection to a cellular network. The system includes means for sending a request to connect the cellular device to the cellular network, wherein the request includes secure identification of the cellular device. Additionally, the system includes the following: means at the cellular device for receiving a response from the network, which includes an index corresponding to an entry in a database stored in the cellular device and a network authenticating entity, where the entry comprises a randomly generated set of timing intervals; means in the cellular device for retrieving the timing intervals corresponding to the index, whereupon a secret number known only to the cellular device and the authenticating entity in the cellular network is utilized to generate in the cellular device a communication session key; means for inserting a portion of the generated session key in each packet of a group of packets, wherein the complete session key is contained in the group of data packets; means for transmitting the group of packets, where the packets are separated by the retrieved timing intervals in a predetermined order, to the authenticating entity whereupon the authenticating entity determines whether the timing intervals correspond to the index provided to the cellular device; and means for connecting the cellular device to the network if the timing intervals correspond to the index sent to the cellular device or denying access if otherwise.

[0016] In another aspect, the present invention is directed to securely sending a session key from a cellular access device to a cellular network authentication device. The method includes sending a request for connecting the access device to the authentication device, the request including identification of the cellular device; receiving at the access device a response from the authentication device, the response including an index corresponding to an entry in a database stored in the access device and the authentication device, the entry comprising a random set of timing intervals; retrieving the timing intervals corresponding to the index, whereupon a secret key known only to the access device and the authentication device is utilized to generate in the access device a session key for starting and maintaining communication between the access device and a network supported by the authentication device; inserting a portion of the session key in each packet of a group of packets, wherein the session key is completely contained in the group of data packets; inserting the timing intervals between each packet in the group of data packets in a predetermined order; transmitting the group of packets to the authentication device, whereupon the authentication device determines whether the timing intervals correspond to the index provided to the access device; and con-

necting the access device to the network if the timing intervals correspond to the index sent to the access device and denying access if otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, wherein like numbers designate like objects, and in which:

[0018] FIG. 1 is a high-level block diagram of an exemplary computer network system;

[0019] FIG. 1A is a high-level block diagram of an exemplary computer system in which an advantageous embodiment of the present invention is implemented;

[0020] FIGS. 2A-E illustrate exemplary embodiments of the present invention in accordance with the principles of the present invention;

[0021] FIG. 3 is a high-level flow diagram illustrating the operation of an exemplary computer password protection system according to one embodiment of the present invention;

[0022] FIG. 4 is a simplified functional block diagram of an exemplary financial authorization network modified in accordance with the teachings of the present invention;

[0023] FIG. 5 is a high-level flow diagram illustrating the steps of an exemplary embodiment of a method of generating and authenticating a password according to the teachings of the present invention;

[0024] FIG. 6 is a simplified functional block diagram of an exemplary authentication server in another embodiment of the present invention;

[0025] FIG. 7 is a high-level flow diagram illustrating the steps of an exemplary embodiment of a method of authenticating a password performed by the server of FIG. 6;

[0026] FIG. 8 illustrates an exemplary embodiment of a multi-character password divided into segments and placed into different data packets in accordance with another embodiment of the present invention;

[0027] FIG. 9 is a simplified functional block diagram of an exemplary password re-assembler in an authentication server suitable for reassembling the password of FIG. 8;

[0028] FIG. 10 is a simplified functional block diagram of an exemplary password verifier in an authentication server suitable for verifying the reassembled password shown in FIG. 9;

[0029] FIG. 11 is a high-level flow diagram illustrating the steps of an exemplary embodiment of a method of sending, reassembling, and verifying the password of FIGS. 8-10;

[0030] FIG. 12 is a high-level flow diagram illustrating the steps of another exemplary embodiment of a method of generating and authenticating a password according to the teachings of the present invention;

[0031] FIG. 13 illustrates a data network topology in which forced packet routing is implemented;

[0032] FIG. 14 illustrates a packet encapsulation method of implementing forced packet routing;

[0033] FIG. 15 depicts a high-level block diagram of an existing GSM cellular network;

[0034] FIG. 16 illustrates a high-level block diagram of a GSM network in which a preferred embodiment of the present invention is implemented; and

[0035] FIG. 17 depicts a process for protecting a session key in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0036] The present invention is an improved system and method for generating and authenticating a password to protect a computer system from unauthorized access. In the description herein, the computer system is described as a financial authorization network for exemplary purposes only. It should be understood that the invention is applicable to all types of password-protected computer systems.

[0037] FIG. 1 depicts a high-level block diagram of an exemplary computer network system. Computer 100 contains a password protection system of the present invention. The present invention comprises executable computer program instructions in a computer program that may be installed in computer 100 to monitor incoming signals and data from computer network 104. A detection portion of the executable program instructions monitors and compares incoming signals with a stored series of predetermined signals. The detection portion of the executable program instructions may comprise a "terminate and stay resident" (TSR) program. The predetermined signals may represent letters, numbers, sounds, or any signals that are readable by a computer. A password builder portion of the executable computer program generates one or more "entry events." Each entry event is made up of one or more "entry signals." Two entry events may be separated by a predetermined time interval. A series of entry events separated by predetermined time intervals comprise a password of the present invention. The password is stored in a memory accessible by computer 100.

[0038] Communication between computer 100 and network 104 is accomplished utilizing network interface device (NID) 102. NID 102 can be a LAN connection, a WAN connection, cable modem, digital subscriber line (DSL) modem, wireline modem or any other means of connecting computer 100 with a network. Network 104 can be a LAN, a WAN, the Internet or any other network that is capable of sending/transmitting data between computers, telephones or any other electronic devices (smart houses, appliances, etc.) capable of transmitting and receiving data.

[0039] Computer 106 is connected to network 104 and may communicate with computer 100. Computer 106 may attempt to access data, files or programs that are resident on computer 100. Because computer 100 is protected by a password of the present invention, computer 106 must present a password attempt that is recognized by the TSR portion of the computer program that monitors NID 102 in order to gain access to computer 100. If a password attempt is presented by computer 106 and the TSR portion of the computer program residing in computer 100 rejects the password attempt, computer 106 is unable to communicate with or access computer 100. Only when computer 106 presents a password attempt that matches the stored password is access to computer 100 granted.

[0040] FIG. 1A illustrates a high-level block diagram of computer 100. Computer 100 generally comprises central processing unit (CPU) 121, memory 130, storage device 128, external interface 102, and user input device 122. These elements of computer 100 are connected by and communicate through computer bus 126.

[0041] Computer 100 comprises memory 130 that contains password software 132 of the present invention. Controller

120 is depicted in this particular embodiment as contained within CPU 121. Controller 120 and password software 132 together comprise a password controller that is capable of carrying out the present invention. An operating system program (not shown) coordinates the operation of password software 132 with the operating system of controller 120.

[0042] Password software 132, under control of controller 120, identifies password attempts and individual password segments as they are received via interface 102. Interface 102 may comprise a network device, a modem, or any external connection device. A password attempt may also be received via user input device 122. User input device 122 may comprise a keyboard, a mouse, a floppy disk, etc. Password software 132 can detect a password attempt received by computer 100 from devices that provide local input and from network or modem type devices that provide remote input. A password attempt may be detected by receiving an entry event that signals a password attempt is to follow.

[0043] Controller 120 is capable of receiving user instructions from user input device 122. In response to user instructions, controller 120 is capable of instructing password software 132 to create elements of a new password and to modify elements of a previously stored password, where the password elements may comprise characters, symbols, numbers and time intervals. Controller 120 operates a portion of password software 132 to detect a password attempt from an external source. An external source includes, without limitation, a network connection, a modem connection, and any input device connected to computer 100 such as a keyboard, a mouse, a hard disk drive, etc. Controller 120 also operates password software 132 for comparing password attempts with a stored password (not shown in FIG. 1A).

[0044] Password software 132 is stored in memory 130 which may comprise random access memory (RAM) or a combination of random access memory (RAM) and read only memory (ROM). Memory 130 may comprise a non-volatile random access memory (RAM), such as flash memory. In an alternate advantageous embodiment of the present invention, password software 132 may be stored on a mass storage device, such as hard disk 128. In another alternate advantageous embodiment of the present invention, password software 132 may be stored on an attached peripheral drive or a removable disk drive (whether embedded or attached) of the type that reads a Read/Write DVD or a re-writable CD-ROM. These types of disk drives are illustrated schematically in FIG. 1A by Read/Write DVD 134 and re-writable CD-ROM 136.

[0045] FIGS. 2A-2E illustrate exemplary embodiments of the password of the present invention. FIG. 2A depicts a high-level time-line for password 200 containing password segment 202 that comprises time interval 206 and entry event C2. A password comparison sequence is initiated when the TSR portion of the computer program recognizes an initial entry event/signal C1. The TSR portion of the computer program begins comparison of the incoming signals with the signals of the stored password. Entry event C1 acts as a start/sync character for the password detection algorithm. An entry event and an entry signal may be the same. However, there may be a plurality of entry signals that are required to produce a character (or characters) or a symbol (or symbols), etc., that make up a single entry event.

[0046] Initial entry event C1 serves to trigger an interval timer (not shown), controlled by password software 132, by causing the interval timer to set (or reset) to zero at time A1.

In this embodiment, the timer is set upon detection of the trailing edge of entry event C1. After being set to zero, the interval timer starts calculating time intervals (in increments that may range from nanoseconds to days) for the incoming password attempt for comparison with the time intervals that are predetermined and incorporated into the stored password.

[0047] After initial entry event C1 is recognized by password software 132, a predetermined time interval 206 must occur. Time interval 206 is a period during which there are no entry events or entry signals. Should a character or entry signal be detected during time interval 206, password software 132 recognizes the “out of place” entry event as an invalid password attempt. In response to an invalid password attempt, time delay 210 is added to the actual time required to read the presented password and then returned as “access denied.” Time delay 210 is an arbitrary period of time that is generated and added by password software 132 to prevent revealing any timing parameters of the stored password.

[0048] Predetermined time interval 206 follows initial entry event C1. Time T1 (segment time) is measured from the trailing edge of initial entry event C1 and represents the total amount of time of time interval 206 and entry event C2. Predetermined time interval 206 can be a user specified amount of time or a random time interval generated by the password generating portion (not shown) of password software 132. The time required for entry event C2 (and all subsequent entry events) is calculated by using the serial bit transfer rate (baud rate) of the actual incoming signal. The length of predetermined time interval 206 is calculated by subtracting the time of entry event C2 from the segment time T1. The second entry event C2, is compared to an incoming entry event (one or more computer readable signals) received by computer 100. Alternatively, time T1 may be calculated by starting the interval timer at a signal within a first group of signals that form an entry event and the ending within a second group of signals that form a subsequent entry event.

[0049] In all computer systems, there exists an inherent delay in the computer's processing time, which must also be taken into account when measuring time intervals. In the apparatus and method of the present invention, a plus or minus percentage deviation in baud rate and processing time is addressed by providing deviation window W1. Deviation window W1 is a deviation period that accommodates the additional times required for computer 100 to recognize and read a character or group of characters. The period of deviation window W1 is based on the baud rate of the incoming signals. Generally, a deviation window is plus or minus a percentage of the preceding time interval (see Table 1). Computer 100 recognizes entry event C2 during deviation window W1 and establishes time T1. Time T1 includes a password segment's predetermined time interval 206 and the character recognition time associated with entry event C2. Time T1 must end within deviation window W1. Time interval 206, entry event C1, and entry event C2 must match the password stored in computer 100 in order to be a valid password attempt.

[0050] If time T1 does not end within deviation window W1, then password software 132 detects the error and rejects the password attempt as invalid. Arbitrary time delay Td is added before sending the rejection of the password attempt to computer 106 that is requesting access. If time T1 ends within deviation window W1, the interval timer (not shown) that provides timing for the algorithm of the stored password is stopped, reset to zero, and then re-started for arbitrary time

delay Td. A plurality of interval timers may be used to monitor time T1, time interval 206 and arbitrary time delay Td. At the conclusion of arbitrary time delay Td, if a correct password attempt has been presented, a successful password entry is acknowledged and access is granted.

[0051] Each entry event comprises of one or more predetermined entry signals that represent one or more numbers, letters, sounds, symbols, characters, etc., in any combination in the password structure. Those skilled in the art will appreciate that an entry event can, and usually does, comprise a plurality of groups of signals that represent a password.

[0052] FIG. 2B illustrates a time-line of a password 220 according to another embodiment of the present invention. Password 220 comprises time envelope 222 (total time of the entire password 220) following an initial entry event C1, entry event 224 (comprising entry event C2, entry event C3, entry event C4, zero time interval and deviation window W1), time interval 228 and entry event 226 (comprising entry event C5, entry event C6, time interval 228, terminating entry signal C7 and deviation window W2). Each segment (at least one entry event) of the password must occur within password envelope 222. An arbitrary time delay, Td, that is equal to time segment 229 is then applied to the end of the password envelope 222 before sending an acceptance or a rejection of the presented password attempt to computer 106.

[0053] FIG. 2C illustrates a time-line of another password 230 according to another embodiment of the present invention. Password 230 comprises time envelope 232 following an initial entry event C1, entry event 234, time interval 238, entry event 236 and deviation windows, W1 and W2. Entry event 234 comprises entry signals C2, C3, and C4. Entry event 236 comprises entry signals C5, C6, and C7. In this embodiment, entry signal C1 is the initiating entry signal that triggers password software 132 to began comparing the incoming signals of a password attempt to the stored password. The total password 230, in this instance, comprises entry signals C2, C3, and C4, time interval 238, and entry signals C5, C6, and C7.

[0054] However, as predetermined by the user, interval timing begins at A1 in deviation window W1 after detecting the second entry signal at A1, continues through time interval 238, and ends in deviation window W2 upon detecting entry signal C6 at time A2. Then entry signal C7 is received. The password attempt is invalid if entry signal C7 is not detected. Password acceptance is delayed by an arbitrary amount of time Td. Time Td is the sum of the time of entry signal C7 and arbitrary time segment 239. Computer 100 then sends an “access denied” signal or an “access allowed” signal to computer 106 that is presenting the password attempt. The time Td is not a part of the presented password attempt and is not a part of the stored password. It is an element that is generated by password software 132 to mask the length of time envelope 232 so that computer 106 can not determine the length of the stored password.

[0055] FIG. 2D illustrates a time-line of a password 250 that utilizes a plurality of password segments. Password 250 comprises time envelope 252 and entry signals C2, C3, . . . , and Cn, time intervals 254, 256, . . . , and 258, and deviation windows W1, W2, . . . , and Wn. Time envelope 252 is calculated from the trailing edge of initializing entry signal C1 to the trailing edge of entry signal Cn. Initializing entry signal C1 is detected by password software 132. The interval timer is then reset and begins timing time interval T1 at time A1. Time interval 254 is determined by subtracting the time of

entry signal C2 time from time T1. Time T1 is the sum of time interval 254 and the time of entry signal C2 with a deviation factor of plus or minus a predetermined percentage of the total time. Deviation window W1 is typically a ten percent (10%) deviation.

[0056] Time interval 256 is determined by subtracting the time of entry signal C3 from time T2 which ends within deviation window W2. Time T2 is measured from the trailing edge of entry signal C2 to the trailing edge of entry signal C3. All the time intervals in this embodiment are determined in the same manner as time interval 254 and time interval 256. Times T1, T2, . . . , Tn may be utilized in an embodiment of the password, along with time intervals and deviation windows, as validation factors for a presented password attempt. Time Td is an arbitrary time delay 262 added when password software 132 sends an “access denied” signal or an “access allowed” signal to computer 106.

[0057] FIG. 2E depicts a time-line of a “time lockout” password 270 of the present invention. Initializing entry signal C1 signals password software 132 that a password attempt is being presented. The interval timer is reset and started at time A1. Time T1 272 is measured from the trailing edge of entry signal C1. Time T1 272 acts as a “time lockout” so that no other character entries will be considered by password software 132 before the interval timer, which began timing at time A1 completes time interval 272. Any entry signal attempts from computer 106 will be answered with an arbitrary time delay Td (not shown) and an “access denied” signal sent to computer 106. Furthermore, time T1 must be complete (i.e., timed lockout ends within deviation window W1) before another entry event will be considered by password software 132. For example, a user may want to secure his computer overnight. In the process of activating the overnight password, the computer prompts the user for the password character(s) and the length of the desired lockout time T1. After the lockout time T1 has elapsed, password software 132 will then consider password entry attempts. Even so, the correct password, in this example entry event C2, must be entered to permit access to computer 100.

[0058] Each of the time intervals in a password can be any user-determined period of time. Further, the identity of the additional characters can (and should) be different from one another. A user can select time intervals and entry signals for inclusion in a password. Table 1 provides more detailed information concerning time intervals and entry signals for the time-line of password 250 shown in FIG. 2D.

TABLE 1

Time Interval	Entry Event	Entry Event Time	Time T	Deviation
999 ms (254)	C1 C2	1 ms	1000 ms	900 ms < W1 < 1100 ms
498 ms (256)	C3	2 ms	500 ms	450 < W2 < 550 ms
...	...	...	...	...
n ms (258)	Cn	3 ms	(n + 3) ms	n ± 0.1 (N + 3) ms

[0059] Table 1 indicates that password software 132 would read the first two segments in a maximum time of 1650 milliseconds (ms). Any additional time intervals and entry events add to the time of the time envelope. However, this does not include the variable and arbitrary time delay Td to disguise the actual length of time of the password.

[0060] The following password format is a literal representation of one embodiment of the password algorithm:

$$C1@A1+C2@A2+C3@A3+...+Cn@An+Td \quad (1)$$

where “C1” is a password initiating entry signal (or entry event); “A1” is the point that the interval timer is reset and begins timing; “A2, A3 . . . and An” are the timing points for subsequent entry events and time intervals; “C2, C3, etc.” are individual entry events that can comprise one or more computer readable signals which include characters, numbers, symbols, etc.; “Cn” is the “nth” entry event; and “Td” is a variable time delay that password software 132 waits after determining whether a password attempt is acceptable to disguise the true time of the stored password when allowing or denying entry.

[0061] As discussed previously, one of the most common schemes used by hackers is a so-called “dictionary” attack. A dictionary attack provides multiple combinations of entry events, but requires continual confirmation from the computer system under attack to confirm any correct entries. A powerful feature of the present invention requires that the hacker wait until the entire password attempt is entered before determining whether the password attempt is correct. By restricting the confirmation of a successful password attempt until the password attempt is complete in real time, the present invention prevents a hacker from determining whether progress is being made. Effectively, the hacker has to wait for the entry of a complete password attempt which may require a time of several microseconds, or eight hours, or many days.

[0062] For example, if an authorized user selected a password that included multiple time entries and entry events that totaled ten (10) seconds, each password attempt would have to be exactly ten (10) seconds long. A hacker using computer 106 would only be permitted a password attempt once every ten (10) seconds. Even if the hacker was aware that a time based password was protecting computer 100 and presented time markers for verification, the password confirmation of the present invention includes a variable time delay, Td, that password software 132 adds before sending the message “access denied.” This variable, and arbitrary, time delay is added to the password attempt and masks the true length of the stored password. The combinations could be virtually endless. A stored password could have a total time interval of eight hours or more. A stored password that might have a length of eight hours or more would discourage most hackers. Additionally, the arbitrary and variable time delay that password software 132 waits before responding to computer 106 provides a mask for the true time envelope of the stored password.

[0063] FIG. 3 depicts a high-level flow diagram illustrating the operation of an exemplary computer password protection system according to one advantageous embodiment of the present invention. The process steps are generally referred to with reference numeral 300. The process begins with a password being established and stored in computer 100, where computer 100 is subject to online entry, either authorized or unauthorized (process step 301). After the stored password is in place, an online entity (for purposes of this example, attacking computer 106) attempts to gain access to computer 100 via a modem or other communication interface device (process step 302). Protected computer 100 signals to the attacking computer 106 that a password is required (process step 304).

[0064] The attacking computer 106 transmits a password attempt in order to gain entry to the protected computer 100. Since the stored password of the present invention requires a complete password attempt before notifying attacking computer 106 of success or failure, a determination is made whether the time envelope (time measured from the first keystroke to the last keystroke) of a completely entered password attempt matches the stored password. After detecting an initial entry event (signal), the presented password attempt must be completely entered and submitted before any entry confirmation or denial is sent to attacking computer 106 (process step 306).

[0065] If the time envelope of the presented password attempt does not match the time envelope of the stored password for protected computer 100, the method of the present invention waits for an arbitrary time, time Td (process step 308) and access is denied to attacking computer 106 (process step 309). If the time envelope of the password attempt entered by attacking computer 106 matches the time envelope of the stored password, then protected computer 100 gets a first password segment (process step 310). Next, the method calculates the first time interval of the first segment (process step 311). If the first time interval (i.e., the time T1 minus the time of the entry event in the time segment) does not match the stored time interval of the first segment (process step 312), then the method of the present invention waits for an arbitrary time, time delay Td (process step 308) before notifying attacking computer 106 that access is denied (process step 309).

[0066] If the determination is made that the time interval of the first password segment of attacking computer 106 matches the time interval of the first segment of the stored password in computer 100, then the method of the present invention makes a determination of whether the entry event associated with the time interval matches the corresponding entry event of the stored password (process step 314). If there is no match, the method of the present invention waits for an arbitrary time, time delay Td (process step 308), and denies access to attacking computer 106 (process step 309). If there is a match, then the method of the present invention determines whether there are more password segments to be checked (process step 316). If there are more password segments, the method of the present invention then gets the next password segment (process step 311) and repeats the cycle of determining whether entry events and time intervals match (process steps 311-314).

[0067] If a determination is made in process step 316 that there are no more password segments (time interval and associated entry events) detected in the incoming password attempt, the incoming password attempt is deemed to present a valid password. The computer then waits an arbitrary period of time, Td, to mask the true length of the time envelope of the stored password (process step 318). The method of the present invention then grants access to protected computer 100 (process step 320).

[0068] The exemplary embodiments described above may be constructed from entries received from a computer keyboard. In other words, a user may design a stored password and password software 132 constructs the designed stored password. However, a stored password may be constructed automatically by utilizing a password software 132 that comprises a random character generator. Password software 132 can construct a stored password by inserting characters or signals for each entry event and by designating time intervals

between the entry events. Thus, it is possible to generate a stored password that may be unknown to the password holder but is stored on a floppy disk (or other similar memory device). The password holder can use the password on a floppy disk to obtain access to computer 100. For remote access to computer 100, the holder of the stored password inserts the floppy disk into a remote computer 106. The floppy disk provides the stored password for remote entry access to protected computer 100. Even though storage of the stored password on a floppy disk may make computer 100 less secure, the stored password is useful if authorized access from a remote computer is required.

[0069] FIG. 4 is a simplified functional block diagram of an exemplary financial authorization network 400 modified in accordance with the teachings of the present invention. A plurality of merchant terminals such as Merchant-A 401 communicate through a data network 402 with a financial authorization server 403. Each merchant terminal 404 includes a magnetic card reader or equivalent device for inputting customer identification and/or credit information. The merchant terminals may be further connected on the merchant side with a point-of-sale (POS) system or intranet (not shown). The data network may be, for example, an Internet Protocol (IP)-based local area network (LAN), wide area network (WAN), or the Internet. The financial authorization server may include an authentication unit 405, a merchant/password database 406, and a communication controller 407.

[0070] In conventional operation, each merchant, for example Merchant-A 401, activates his terminal each morning when the merchant prepares to open for business. The terminal includes a serial number, and the merchant enters an ID number or password assigned to him by the operator of the financial authorization network. Together, the serial number and the ID number/password comprise a prior art terminal password that is transmitted through the data network 402 to the financial authorization server 403. The terminal password is received in the authentication unit 405, which accesses the merchant/password database 406 and compares the received terminal password with a stored password. If the passwords match, the authentication unit approves Merchant-A's terminal for financial transactions and sends an approval indication to the terminal. Thereafter, when a customer's credit card is read at the merchant terminal 404, the card number together with the terminal serial number are sent to the financial authorization server. The authentication unit 405 recognizes the serial number as being approved and sends the credit card information to the communication controller 407. The communication controller then accesses secure financial information 408 to determine whether the credit card number is approved for the transaction. The controller then returns either a positive or negative indication 409 to the Merchant-A terminal.

[0071] In some networks, the merchant terminal may send its terminal password along with each credit card transaction. When the authentication unit 405 positively authenticates the password, the credit card information is passed to the communication controller 407 for access to the secure financial information 408.

[0072] In the present invention, the merchant terminal environment is modified to include a network password generator 410. The network password generator may be implemented internally in the merchant terminal or in a separate unit that interfaces with the merchant terminal. The terminal sends its standard terminal password (e.g., serial number and merchant

ID) to the network password generator. A time interval number sequence 411 is also input to the network password generator, which generates a time-multiplexed network password 412 by inserting the appropriate time intervals between the packets of the terminal password, as specified by the time interval number sequence. The time interval number sequence may be input via a standard network connection from the financial authorization server, via a secure encrypted connection, or via a physical medium such as a CD delivered to the merchant.

[0073] The network password generator 410 then sends the time-multiplexed network password 412 through the data network 402 to the server 406. The authentication unit 407 receives the network password and compares the characters received with a stored password in a merchant/password database 408. The authentication unit also compares the time intervals between the received characters with the current number set from the time interval number sequence 411, which is shared between the terminal and the server. The authentication unit positively authenticates the network password only if the received characters match the stored characters, and the time intervals between the received character-carrying packets matches the number specified by the time interval number sequence.

[0074] If the network password 412 is accompanied by a credit card number from a credit card transaction, and the authentication unit network positively authenticates the password, the credit card information is passed to the communication controller 407 for access to secure financial information 408.

[0075] In an alternative embodiment, the time interval number sequence 411 is stored only in the authorization server 403. Following a successful verification, the server sends a response message back to the merchant terminal. The response may include a next interval or set of intervals to be used by the terminal to create the time multiplexed network password. The intervals may be encoded in the response message to prevent interception by hackers or snoopers. Alternatively, the response message may include a value or values that do not directly indicate the time interval(s) to be inserted by the terminal. Instead, the terminal may be programmed with a formula that calculates the time intervals based on the value(s) received from the server. Alternatively, the terminal may include a lookup table that associates each value received from the server with a corresponding time interval to be inserted in the password.

[0076] For example, if the same time interval is to be placed between each of the characters in the password, the server may send a single value such as 24. The terminal may calculate a time interval from the value 24, or may associate a time interval with the value 24 in a lookup table, to determine that an interval such as 150 ms is to be placed between each character in the password. If a different time interval is to be placed between each of the characters in a password having, for example, 5 characters, the server may send a string of values such as 24, 10, 18 and 5. The terminal may calculate a time interval from each of the received values, or may associate a time interval with each of the received values in a lookup table, to determine four time intervals to place between the five characters. For example, time intervals such as 150 ms, 75 ms, 250 ms, and 1 second may be determined and placed between the characters in the password. Alternatively, the lookup table may associate a single value with a sequence of time intervals. Thus, the server may send a single

value such as 24, and the terminal may determine that the intervals 150 ms, 75 ms, 250 ms, and 1 second are to be placed between the characters in the password.

[0077] FIG. 5 is a high-level flow diagram illustrating the steps of an exemplary embodiment of a method of generating and authenticating a password according to the teachings of the present invention. Starting at step 501, a user enters the characters of a password into a client terminal. At step 502, a network password generator associated with the client terminal obtains the entered password characters from the client terminal and obtains a time interval number sequence that is shared with an authentication server. At step 503, the network password generator places the characters in packets and transmits the character packets with the appropriate time intervals between the packets in accordance with the time interval number sequence. At step 504, the network password generator sends the network password to the server.

[0078] At step 505, an authentication unit associated with the server determines whether or not the characters received in the network password match the characters of a stored password associated with the client terminal. If not, the process moves to step 506 where the server rejects the network password. However, if the characters match at step 505, the process moves to step 507 where the authentication unit determines whether or not the time intervals between each pair of character-carrying packets matches the time intervals specified by the time interval number sequence. If the time intervals match at step 507, the process moves to step 508 where the server positively authenticates the network password. However, if the time intervals do not match, the process moves to step 506 where the server rejects the network password.

[0079] The process then moves to step 509 where the server determines whether this client terminal has experienced a predefined number of password rejections. If not, the process moves to step 510 where the server sends a rejection indication to the client terminal. At step 511, the client terminal increments the time interval number set and generates and sends a new network password to the server. The process then returns to step 505 and repeats the authentication process for the new password.

[0080] If it is determined at step 509 that the client terminal has experienced the predefined number of password rejections, the process moves to step 512. Since multiple password rejections may be caused by the client terminal and server being out of synch regarding the correct position in the time interval number sequence, the process determines at step 512 whether or not synchronization has already been attempted. If so, the process moves to step 513 where the server locks out the client terminal. However, if synchronization has not yet been attempted, the process moves to step 514 where the server sends a synchronization signal to the client terminal specifying a synchronization position in the time interval number sequence, or alternatively, instructing the client terminal to go to a predefined synchronization position. At step 515, both the client terminal and the server move to the synchronization position in the time interval number sequence. The process then returns to step 503 where the network password generator generates a new password using the characters entered by the user and inserting time intervals between the character-carrying packets in accordance with the synchronization position in the time interval number sequence. The process then continues with the authentication procedure. If the client terminal is an authorized terminal that

was temporarily out of synch with the server, the synchronization process should correct the problem, and the password should be positively authenticated. If the client terminal is a hacker, who does not know to insert time intervals or does not have access to the time interval number sequence, the synchronization process will not correct the problem, and the hacker will be denied access.

[0081] A benefit of the present invention is that it is transparent to the user. That is, the user always uses the same terminal (with the same serial number) and the same password or ID for every transaction. The terminal and server change the network password as often as the network operator desires by changing the time intervals between packets in the manner and at the frequency defined by the network operator. The user does not have to remember multiple passwords or change his password on a periodic basis. Even if a hacker knows the user's password, the hacker cannot gain access. Since any time interval can be inserted between any two characters in the password, the combination of characters and time intervals is practically limitless. Also, the system may change the time intervals between each pair of password characters as often as each transaction. Therefore, even if a hacker intercepts a transmission and determines the time intervals between each pair of character-carrying packets, the intervals may change in the next transmission, denying the hacker access to the network.

[0082] FIG. 6 is a simplified functional block diagram of an exemplary authentication server 601 in another embodiment of the present invention. In this embodiment, designed to defeat a hacker who has obtained a user's password, the server authenticates the password and then redirects the access device to another IP address 607 known only to authorized access devices. A password is received from the access device at a first server address 602. An authentication unit 603 authenticates the password by comparing the received password with a password stored in a password database 604. Upon successful authentication, a server address/index lookup table 605 is accessed to obtain an index for the second server address 607.

[0083] An acknowledgment message generator 606 creates an acknowledgment message and includes the index of the second server address. The index may be randomly generated to preclude patterns in the use of server addresses. The server sends the acknowledgement message to the access device. The access device also includes a server address/index lookup table (which may be in a protected area), where the access device determines the second server address. The access device then sends an access request to the second server address 607. Upon receipt of the access request at the second server address, the server 601 provides the access request to a communication controller 608 and access is granted to protected information 609.

[0084] It should be noted that this embodiment is also effective against phishing sites where the user has been directed to a fake website which simulates a real website such as the website for the user's bank. The hacker may request the user to enter his password and his account number at the fake website. The hacker then attempts to access the user's account at his bank utilizing this information. With this embodiment, however, the access device expects to receive a proper index value pointing to another address in the client's lookup table. If no such index is received, or if an improper index is received, the client device may alert the user that he may be at a fake website. Note that if the hacker returns a proper index,

he will lose the user because the access device will switch to a different address to send the access request to the server.

[0085] FIG. 7 is a high-level flow diagram illustrating the steps of an exemplary embodiment of a method of authenticating a password performed by the server of FIG. 6. At step 701, the user enters his password in an access device. At step 702, the access device sends the password to the first server address 602. At step 703, the server verifies the password and returns an acknowledgment message to the access device with an index value for the second server address 607. At step 704, an index extractor in the access device extracts the index value. At step 705, the access device identifies the second server address in a lookup table using the extracted index value. At step 706, the access device requests access through the second server address 607. At step 707, the server grants access to the protected information 609 through the second server address.

[0086] FIG. 8 illustrates an exemplary embodiment of a multi-character password divided into segments and placed into different data packets in accordance with another embodiment of the present invention. In this embodiment, multiple IP addresses are assigned to the server, and are known only to authorized access devices. The access device divides the password 801 into multiple segments and places each segment in a different packet 802-805. The header of each packet includes an identifier such as a source address (SA1) that identifies the access device. Each packet header also includes a different one of the multiple IP addresses of the server as a destination address. The access device then sends the packets individually to the server. In one embodiment, the access device delays transmission of successive packets by predefined time periods known only to the access device and the server. Any hacker who has learned one of the server's IP addresses, and is monitoring that address to intercept passwords, will see only one portion of the user's password.

[0087] FIG. 9 is a simplified functional block diagram of an exemplary password re-assembler 901 in an authentication server suitable for reassembling the password of FIG. 8. Upon receiving each packet at the server, a time-of-receipt stamping unit 902 places a time-of-receipt stamp on each incoming packet 802-805. A packet association unit 903 may use the identifier of the access device or other identifier to associate the different packets which comprise the password. The data portions of the associated packets are then combined into a reassembled password 904 and sent to a password verifier 1001 (FIG. 10). If time delays are also being utilized as a second or third factor of the password, the time-of-receipt stamps are also sent to the password verifier.

[0088] FIG. 10 is a simplified functional block diagram of an exemplary password verifier 1001 in an authentication server suitable for verifying the reassembled password 904 of FIG. 9. If time delays are being utilized as a second or third factor of the password, the verifier calculates the difference between each succeeding time-of-receipt stamp to determine time intervals 1002, labeled as TI-1 through TI-3 in FIG. 10. A time interval lookup table 1003 determines whether the calculated time intervals match stored time intervals associated with the access device. A tolerance factor may be applied to account for small variances in the time intervals due to timing delays in the data network between the access device and the server. The result is sent to a password pass/fail unit 1005. Likewise, a packet content lookup table 1004 determines whether the data portions of the reassembled password

match stored packet content information associated with the access device. The result is sent to the password pass/fail unit. The password pass/fail unit verifies the password only if the password characters are correct, the packet content of each packet is correct, and the time intervals between packets are correct, within any predefined tolerance values.

[0089] FIG. 11 is a high-level flow diagram illustrating the steps of an exemplary embodiment of a method of sending, reassembling, and verifying the password of FIGS. 8-10. At step 1101, the user enters a multi-character password in the access device. At step 1102, the access device divides the password into multiple segments. At step 1103, the access device places the segments in multiple packets, each addressed to a different address of the server. At step 1104, the access device sends the packets to the server via the multiple server addresses.

[0090] At step 1105, the server receives the packets and places a time-of-receipt stamp on each received packet. At step 1106, the server utilizes the identifier of the access device to associate the multiple packets and reassemble the password. At step 1107, the server verifies that the password characters of the reassembled password are correct, and the packet contents of each individual packet match stored packet contents associated with the access device. At step 1108, the server calculates time intervals between the packets and verifies that the calculated time intervals match stored time intervals associated with the access device. At step 1109, the server grants access to protected information if the password characters are correct, the packet content of each packet is correct, and the time intervals between packets are correct, within any predefined tolerance values.

[0091] FIG. 12 is a high-level flow diagram illustrating the steps of another exemplary embodiment of a method of generating and authenticating a password according to the teachings of the present invention. In this embodiment, multiple addresses are assigned to the server, and are known only to authorized access devices. The access device sends its password in different packets to several of the server's addresses. If a hacker intercepts one of the password packets and attempts to gain access, a predefined characteristic of the packet will be changed. For example, the access device may transmit the packets with time delays known to the server. The hacker's interception and modification of a packet will cause an excessive delay, which is recognized by the server. Thereafter, the server may deny access or may grant access to the access device identified in the packets that were timely received.

[0092] At step 1201, the server is configured with at least three addresses. At step 1202, the user enters his password in the access device. At step 1203, the access device generates at least three packets containing the password and an identifier of the access device. Each packet is addressed to a different address of the server. At step 1204, the access device sends the packets to the server via the multiple addresses. The packets may be transmitted with one or more predefined time delays between the subsequent packets.

[0093] At step 1205, the server receives the packets and utilizes the identifier to associate the received packets with the access device. At step 1206, the server determines whether a predefined characteristic is different in one of the received packets. This characteristic may be, for example, the identifier of the access device, a source address, or the expected time of receipt of the packet. If a predefined characteristic is different in one of the received packets, the

method moves to step 1207, where the server determines whether the password in the remaining packets matches a stored password for the identified access device. If so, the method moves to step 1208, where the server grants access to the access device identified in the remaining packets. If the password in the remaining packets does not match the stored password for the identified access device, the method moves instead to step 1210, where the server denies access to the access device.

[0094] If it is determined at step 1206 that the predefined characteristic is not different in one of the received packets, the method moves to step 1209 where it is determined whether the predefined characteristic is different in multiple packets. If so, the method moves to step 1210 where the server denies access to the access device. If the predefined characteristic is not different in multiple packets at step 1209, then it is the same in all received packets. Therefore the method moves to step 1211 where the server grants access to the access device identified in all received packets.

[0095] FIG. 13 illustrates a data network topology in which forced packet routing is implemented. In one embodiment, routers in the network are modified with a dynamic routing table. When a packet is received with a predefined destination address associated with, for example a financial institution, the router is programmed to send the packet out on a designated port. For example, an access device 1301 may send password packets over a network 1303 to a server 1302 located at a bank. Router-A may be programmed to send packets with the bank's destination address on port 1 to Router-B. Likewise, Router-B may be programmed to send packets with the bank's destination address on port 1 to Router-C. At some later time, the routing table may be modified so that Router-A sends packets with the same destination address on port 2 to Router-E, which is programmed to send the packets through either port 1, 2, or 3 to Router-C, Router-F, or Router-I, respectively. Thus, rather than letting the routers choose the shortest path or lightest loaded path, which may almost always be the same, the routers are forced to vary the path according to their dynamic routing tables.

[0096] In one embodiment of the present invention, the access device 1301 divides the password into multiple segments and sends each segment in a different packet to a different router. The first packet may be sent to Router-A, the second packet to Router-D, and the third packet to Router-G, for example. Each packet includes the bank's address as its destination address. Each router uses its dynamic routing table to further route the packet it receives. If a hacker is monitoring a router such as Router-D because it is on the shortest path to the server 1302, the hacker will only see the second packet and will not learn all of the characters of the password.

[0097] In another embodiment of the present invention, the server 1302 has multiple IP addresses which are known to the access device 1301. The access device divides the password into multiple segments and sends each segment in a different packet. Each packet is addressed to a different IP address of the server. The routers in this embodiment may be configured with static routing tables. When a packet is received with a predefined destination address, the router is programmed to send the packet out on a designated port. The password packets follow different routes to the server because the routing tables route packets addressed to the different IP addresses through different ports of each router. Thus, packet routing is changed by changing the destination address. Once again, if a

hacker is monitoring a router such as Router-D because it is on the shortest path to the server, the hacker will not learn all of the characters of the password.

[0098] It should also be understood that the forced packet routing of the present invention may be performed through nodes other than routers. For example, if a large corporation or financial institution has many offices and many servers distributed around the country, the routing tables may be implemented in the company's servers and the password packets may be routed through intermediate company servers before arriving at the authentication server. The intermediate servers may perform the functions described above for routers. In this manner, forced packet routing may be achieved even though the company has no control over routers, for example, in the Internet.

[0099] As an example, a user in Dallas may desire to log onto his bank's website, the server for which is located in Chicago. The access device divides the password into multiple segments and sends each segment to the authentication server in a different packet. Each packet is sent via a different one of the bank's servers. For example, a first packet may be sent to an intermediate server in Denver, while a second packet is sent to an intermediate server in Atlanta. A third packet may be sent to an intermediate server in St. Louis. Each of the intermediate servers may forward its received packet to another intermediate server or may send the packet directly to the authentication server in Chicago. Once again, a hacker attempting to capture the password from a router located between Dallas and Chicago will not be able to capture all of the password characters.

[0100] It should also be noted that when the inventive time delays of the present invention are used as a second or third password factor in embodiments in which the packets are forced to follow different paths, it is not possible for the hacker to determine the inter-packet timing, even if the hacker distributes his monitoring efforts and intercepts all of the password packets.

[0101] FIG. 14 illustrates a packet encapsulation method of implementing forced packet routing. In this embodiment, the access device again divides the password into multiple segments and sends each segment to the authentication server in a different packet. The packets are sent through intermediate servers or routers. In the example shown, a packet is sent through two intermediate servers, IS1 and IS2. The access device sends the password packet and a header for the second intermediate server within an outer encapsulation frame **1401**. The outer encapsulation frame includes its own header comprising the source address for the access device (SA-AD) **1402** and the destination address for the first intermediate server (SA-IS1) **1403**.

[0102] When the first intermediate server receives the outer encapsulation frame, the server strips off the header, revealing the destination address for the second intermediate server (DA-IS2) **1404** in a header for an inner encapsulation frame **1405**. The first intermediate server adds its own source address (SA-IS1) **1406** to the header for the inner encapsulation frame and sends the frame to the second intermediate server. When the second intermediate server receives the inner encapsulation frame, the server strips off the header, revealing the destination address for the authentication server (DA-AS) **1407** in a header for the password packet. The second intermediate server adds its own source address (SA-IS2) **1408** to the header for the password packet and sends the packet to the authentication server. When the authentication

server receives the packet, the server strips off the header, revealing the source address (or other identifier) of the access device **1409** and the password characters (PASS) **1410**.

[0103] By encapsulating each of the password packets with the addresses of different intermediate servers or routers, the access device can control the path which each packet follows to the authentication server. Once again, if the packets follow different paths, a hacker monitoring a single router or path will not obtain all of the password characters. Also, when the inventive time delays of the present invention are used as a second or third password factor, it is not possible for the hacker to determine the inter-packet timing.

Securing Cellular Systems

[0104] The Global System for Mobile Communications (GSM) represents the largest number of cellular communications networks in the world. Wireless, cellular networks connect cell phones, computers and virtually any wireless device to each other and to the Public Switched Telephone network. Since the beginning of GSM, cellular operators have had a serious problem with criminals using cloned cell phones to gain fraudulent access to the operators' networks. The present invention is also applicable to wireless networks such as cellular communication networks.

[0105] FIG. 15 depicts a high-level diagram of a GSM cellular network. In a GSM network, Mobile Station **1501** attempts to access Network **1500** through BTS **1510** by sending a request for connection (other examples of devices connecting to a cellular network include computers, GPS devices, etc.). The request is passed by Base Station Controller (BSC) **1504** to Mobile Services Switching Center (MSC) **1506**. MSC **1514** determines the identity of MS **1501** by checking for the profile of MS **1501** in Home Location Register (HLR) **1516**. If MS **1501** is roaming, a Visiting Location Register (VLR) would retrieve the profile from the subscriber's HLR and supply the profile. Authentication Center (AuC) **1518** provides authentication parameters for MSC **1514**. Gateway MSC (GMSC) **1522** provides access to and from Public Switched Telephone Network (PSTN) **1524**.

[0106] GSM cellular network **1500** is a relatively secure communications network. MS **1501** is provided with a Subscriber Authentication key in Subscriber's Identification Module (SIM) **1502**. The Subscriber Authentication key, Ki, is a 128 bit key and is known only to the SIM and HLR **1516**.

[0107] When MS **1501** attempts to access network **1500**, a 128-bit Random Number (RAND) challenge to MS **1501** is sent by MSC **1514** to MS **1501** via BTS **1510**. MS **1501** receives the random challenge from BTS **1510** and with the Individual Subscriber Authentication Key (Ki) the Mobile Station utilizes, currently, the A8 algorithm, to combine with RAND and send a Signed Response (SRES) to MSC **1514** to verify.

[0108] SIM **1502** then generates a Session Key (Kc) for encrypting transmission data to network **1500**. MS **1501** sends the Session Key (Kc) to the BSC **1512** and MSC **1506** sends a Session Key (Kc) generated from the RAND, the Subscriber Authentication Key to BSC **1512**. BSC **1512** compares and verifies the Session Keys from MS **1501** and MSC **1506** and if they match, connection is completed.

[0109] It has been shown that even though Ki is known only to the MSC and the SIM on the subscriber's cell phone, Ki can be derived by hackers by intercepting Kc. A "fraudster" can then use the derived Ki to clone a legitimate user's phone by

programming a SIM card and installing it in another cell phone to duplicate those signals.

[0110] FIG. 16 illustrates a high-level block diagram of the invention according to a preferred embodiment of the present invention. In a GSM network, Mobile Station (MS) 1601 accesses Network BTS 1510 with a request for connection. MS 1601 includes a transceiver (Tx/Rx) and Subscriber Identity Module (SIM) card 1602. SIM card 1602 includes timing interval database (DB) 1604 for storing indexed timing intervals, Segmenting Function (SF) 1606 for segmenting text or numerical entries and Transmission Controller (TXc) 1608 for presenting segments to the transceiver of MS 1601.

[0111] MS 1601 sends a request for access to the network via Base Transceiver Station (BTS) 1610. Base Station Controller (BSC) 1612, which typically controls many BTSs (not shown to more clearly describe the invention), passes the message to Mobile Service Switching Center (MSC) 1614. MSC 1614 comprises Home Location Register (HLR) 1616, Authentication Center (AuC) 1618 and Interval Timing master Database (mDB) 1620. Gateway MSC (GMSC) 1622 provides access for the Public Switched Telephone Network (PSTN) 1624 to the mobile network and to MS 1601 via MSC 1614 and BSC 1612.

[0112] mDB 1620 is a database containing indexed timing intervals. When mDB 1620 receives acknowledgement that MS 1601 has presented satisfactory identification a function, associated with MSC 1614 such as Authentication Center 1618, randomly selects an index corresponding to a set of timing intervals from mDB 1620 and sends the index to MSC 1614. MSC 1614 sends the index to BSC 1612, which forwards the index to MS 1601 via BTS 1610. A security function on board SIM 1602 (not shown) receives the index and attempts to match it with one of the indexes corresponding to timing intervals in DB 1604. If the index matches, the associated timing intervals in DB 1604 are provided to TXc 1608 while at the same time Segmenting Function (SF) 1606 segments the Session key (Kc) that is generated from the Subscriber Authentication number and the RAND and loads each segment into a packet. SF 1606 provides the group of packets containing Kc to TXc 1608 which then transmits the packets, separated by the timing intervals, to BTS 1610.

[0113] The packets are received at BTS 1610 and BSC 1612 passes the packets to MSC 1614. The packets are assembled in the proper order and the timing intervals, measured between the packets, are checked, in mDB 1620, against timing intervals that are associated with the index initially sent to MS 1601. If the timing intervals match and the Kc is correct, an acknowledge message is sent to the BSC and MS 1601 is connected to the network. If the timing intervals do not match, MS 1601 is not allowed to connect to the network.

[0114] Shown below in Table 2 is a portion of the database assigned to MS 1601, which is associated with the authenticating entity in the network. As noted above an identical database is stored in the cellular device/cell phone.

TABLE 2

INDEX	1	2	3	4
A	2, 5, 3, 7	1, 14, 9, 6	12, 13, 14, 1	2, 19
B	6, 4, 8, 22	1, 35, 5	5, 12, 4, 13, 9	12, 1, 3
C	6, 8, 5, 4, 1	7, 8, 2, 4, 5	3, 3, 3, 12	7, 5, 7, 7, 7

[0115] For instance, INDEX A4 dictates to the programming in the cellular device that a session key, Kc, is to be segmented into thirds and the Kc segments are each loaded into a packet. The packets are transmitted to the authenticating entity in the network separated by 2 and 19 milliseconds. Even though the timing intervals are set in milliseconds a person skilled in the art can mix the times in the cells, e.g. milliseconds, seconds, tens of seconds, etc. The database illustrated is mDB 1620 as shown in FIG. 16. DB 1604 on board MS 1601 is indexed the same as mDB 1620 so that indexes in both databases are associated with identical timing intervals.

[0116] FIG. 16 depicts a process for protecting a session key in accordance with a preferred embodiment of the present invention. The process begins at step 1602 when a Mobile Station (MS) initiates a request for access to a cellular network. The MS transmits data identifying the subscriber and cellphone to a nearby BTS to request connection of the MS to the network. The network then sends the data to the MS's Home Location Register to verify the identity and begin an identification process to determine whether to provide a secure connection.

[0117] The process moves to step 1604 where the MSC determines from the received access request (e.g., ESN, IMEI, IMSI) whether the cellphone matches previously stored identifiers of the cellphone. If they don't match, the process moves to step 1606 and the network denies access to the MS. If they do match, the process then proceeds to step 1608 and the MSC sends a Random number (RAND) and an index to the MS. The RAND is used with the Subscriber Authentication number, Ki, to generate a predictable response, a Signed Response (SRES), and the index is an indicator associated with a set of timing intervals stored in a database in the network. The network database may be a specific database assigned to the particular cellphone or a large database assigned to multiple cell phones. The timing intervals are re-indexed and changed either randomly or periodically. Any changes to the database can be downloaded to the cell phone, e.g., during an authorized call to the network.

[0118] Typically, the corresponding database in the cell phone would be stored in the SIM, but a person skilled in the art would understand that with today's cell phones, a removable memory card or even cell phone permanent memory could hold the database and the programming necessary for utilizing information in the SIM database to process the session key. Additionally, a person skilled in the art would understand that the contents of the database can be altered (periodically or randomly) by downloading the data and programming from the network or by replacing the removable memory card with new, indexed database entries and/or additional programming information.

[0119] The process continues to step 1609, where the MS calculates a SRES with the algorithm on board the SIM using the RAND and the Ki residing in the SIM. The MS then sends the SRES to the MSC, which can confirm the SRES by comparing the SRES from the MS and the SRES generated from the information provided by the HLR. If the MSC does not confirm the SRES, access to the network is denied. If the SRES is confirmed, then the process continues to step 1610 where the SIM card uses the RAND to generate a session key, Kc, to encrypt data for transmission to the network.

[0120] Next, the process proceeds to step 1612 where a database controller on the SIM uses the received index to retrieve the associated timing intervals and passes the timing

intervals to a transmission controller. In step 1614, the transmission controller segments the session key, Kc, into random portions that are each loaded into a corresponding number of packets. After the session key is loaded into the group of packets, the process then proceeds to step 1616, where the transmission controller sends the individual packets to the cellphone transmitter, each packet being separated by one of the retrieved timing intervals. Continuing to step 1618, the cellphone transmitter transmits each packet individually according to the extracted timing intervals.

[0121] Upon receipt of the packets the MSC, in step 1620, compares the timing intervals, measured by the network MSC to determine whether the measured timing intervals are the same as the timing intervals corresponding to the index sent to the SIM. Regardless of whether the Kc is correct, if the timing intervals do not correspond to the timing intervals represented by the index as sent to the SIM card, the process moves to step 1606 where access to the network is denied. If the timing intervals are correct and the Kc is correct, the process then proceeds to step 1622, where the MS is connected to the network.

[0122] If the session key is provided to the network by a cloned phone, the cloned phone will not have the database and cannot provide the indexed timing intervals required by the network and thus will not be able to properly respond. The MSC randomly selects and sends an index each time the MS attempts to connect. The indexes in the SIM on board the MS correspond to identical indexes in the MS profile stored in the HLR or VLR in the MSC. If a cloned phone (where the Kc has been derived) responds with a recorded response from the fraudster, the attempted connection will fail since the index changes each time the phone registers with the network. The MSC can then deregister the cloned phone from the network.

[0123] The described method can be applied to any wireless or wireline transmission requiring serious security in virtually any network and though the GSM network is a relatively secure network, there are weaknesses that are exploited by fraudsters and hackers. For instance, cipher keys and authentication values (IMSI, RAND, SRES, Kc) are transmitted in the clear within and between networks providing easy targets. Though the successor to GSM, 3GPP, has dramatically improved on security, GSM is still the dominant system. Systems with 3GPP accept GSM phones, but since the security system is for 3GPP phones, the access requests and calls are accepted and actually passed through the 3GPP network for verification by the GSM system.

[0124] Another security problem with wireless GSM networks is Short Message Service (SMS). SMS is a service provided through GSM that allows users to send text messages to other mobile users. Text messaging is very popular and most users either ignore or are unaware that SMS messages are sent in clear text format. Text messages could be sent with instructions to include sensitive information in the return text message and the receiver of the text message could then use that sensitive information in a manner that could be harmful to the sender. The indexed database in the SIM can be used to secure the text transmissions in a similar manner as the secure transmission of the session key Kc.

[0125] Every text transmission may be separated into segments and each of the segments can be transmitted to the network. The segments may be transmitted, each segment being separated by a timing interval provided by the SIM indexed database. The network authentication entity processes the packet transmissions from the user to convert the

segmented text message to plain text for transfer to a recipient, e.g., a bank in the instance of a message containing private account information.

[0126] If the text message is between users, the process can be continued where the authentication entity acts as a middleman to confirm the identification of each user and send an index from a database corresponding to each user. The text messages are received by the network in, e.g., a short messaging system server, and the timing interval comparisons are made for each group of packets that include a text message. There is no need to provide encryption as each group of packets is broken apart according to the sending user's index, reassembled in the server and broken apart and packaged with timing intervals corresponding to the index associated with the receiving user for transmission to the recipient. Thus, there is an intermediary that provides a different index to both parties and facilitates secure SMS packet transfers between the users without the need for encryption.

[0127] The present invention may also use information from the database to alter transmissions in the basic registration procedure, but this approach is more problematic because the basic procedure is subject to industry standardization. The preferred approach leaves the basic registration procedure as it is, and provides the cellular network operator with the ability to perform post-registration interrogation as a means of identifying and deregistering fraudulent users.

[0128] This process is completely hidden from the legitimate user, who only has to turn on his phone as usual. In addition, his telephone service is not affected by the fact that the network deregistered the cloned phone. As long the legitimate user's phone is able to properly respond to the post-registration interrogation, he can continue to register with the network and make calls.

[0129] It is important to note that while the present invention has been described in the context of a fully functional computer system, and an exemplary financial authorization network, those skilled in the art will appreciate that the instructions for practicing the method of the present invention are capable of being recorded on any type of a computer readable medium. The steps of the method of the present invention are executed, regardless of the particular type of signal-bearing media actually utilized. Examples of computer readable media include: nonvolatile, hard-coded type media such as read only memories (ROMs) or erasable, electrically programmable read only memories (EEPROMs), recordable type media such as floppy disks, hard disk drives, solid state drives, flash memory and CD-ROMs, and transmission type media such as digital and analog communication links.

[0130] It is thus believed that the operation and construction of the present invention will be apparent from the foregoing description. While the system and system shown and described has been characterized as being preferred, it will be readily apparent that various changes and modifications could be made therein without departing from the scope of the invention as defined in the following claims.

What is claimed is:

1. A method of authenticating a cellular device for connection to a cellular network, the method comprising:
 - sending a request for connection of the cellular device to the cellular network via a Base Transceiver Station (BTS), wherein the request includes an identification of the cellular device;

receiving at the cellular device a response from the network via the BTS, the response including an index corresponding to an entry in a database stored in the cellular device and a network authenticating entity, the entry comprising a random set of timing intervals;

retrieving the timing intervals corresponding to the index, whereupon a secret number known only to the cellular device and an authenticating entity in the cellular network is utilized to generate in the cellular device a communication session key;

inserting a portion of the session key in each packet of a group of packets, wherein the complete session key is contained in the group of data packets;

transmitting the group of packets each of the packet being separated by one of the retrieved timing intervals to the authenticating entity, whereupon the authenticating entity determines whether the timing intervals correspond to the index provided to the cellular device; and

connecting the cellular device to the network if the timing intervals correspond to the index sent to the cellular device or denying access if otherwise.

2. The method of claim 1, wherein the database in the cellular device is stored on one of a removable data card, the cellular device's permanent memory, and a Subscriber Identity Module (SIM) card.

3. The method of claim 1, wherein the cellular device comprises one of a Personal Digital Assistant, a computer, and a cell phone.

4. The method of claim 1 further comprising the steps of:

- downloading programming to update or replace the current programming for separating data in the cellular device; and
- downloading different timing intervals and corresponding indexes to the database in the cellular devices, wherein the downloading steps are either periodic or random.

5. The method of claim 1, wherein the authenticating entity is connected to the cellular network and comprises one of an authentication center (AuC), a mobile switching center (MSC), and the BTS.

6. A system for authenticating a cellular device for connection to a cellular network, the system comprising:

- means for sending a request for connection of the cellular device to the cellular network via a Base Transceiver Station (BTS), wherein the request comprises secure identification of the cellular device;
- means for receiving at the cellular device a response from the network via the BTS, the response including an index corresponding to an entry in a database stored in the cellular device and a network authenticating entity, the entry comprising a random set of timing intervals;
- means for retrieving the timing intervals corresponding to the index, whereupon a secret number known only to the cellular device and an authenticating entity in the cellular network is utilized to generate in the cellular device a communication session key;
- means for inserting a portion of the session key in each packet of a group of packets, wherein the complete session key is contained in the group of data packets;
- means for transmitting the group of packets, the packets separated by the timing intervals in a predetermined order, to the authenticating entity whereupon the authenticating entity determines whether the timing intervals correspond to the index provided to the cellular device; and

means for connecting the cellular device to the network if the timing intervals correspond to the index sent to the cellular device or denying access if otherwise.

7. The system of claim 6, wherein the database in the cellular device is stored on one of a removable data card, the cellular device's permanent memory, and a Subscriber Identity Module (SIM) card.

8. The system of claim 6, wherein the cellular device comprises one of a Personal Digital Assistant, a computer, and a cell phone.

9. The system of claim 6, further comprising:

- means for downloading programming to update or replace the current programming for separating data in the cellular device; and

- means for downloading different timing interval data with corresponding indexes to the database in the cellular devices, wherein the schedule for effecting the downloading is either periodic or random.

10. The system of claim 6, wherein the authenticating entity is connected to the cellular network and comprises one of an authentication center (AuC), a mobile switching center (MSC), and the BTS.

11. A method of securely sending a session key from a cellular network access device to a network authentication device, said method comprising the steps of:

- sending a request for connection of the access device to the authentication device, wherein the request comprises identification of the cellular device;

- receiving at the access device a response from the authentication device, the response including an index corresponding to an entry in a database stored in the access device and the authentication device, the entry comprising a random set of timing intervals;

- retrieving the timing intervals corresponding to the index, whereupon a secret key known only to the access device and the authentication device is utilized to generate in the access device a session key for starting and maintaining communication between the access device and a network supported by the authentication device;

- inserting a portion of the session key in each packet of a group of packets, wherein the session key is completely contained in the group of data packets; and

- transmitting the group of data packets to the authentication device, wherein each packet is individually transmitted to the authentication device separated in time from a preceding data packet by one of the timing intervals corresponding to the index provided to the access device.

12. The method of claim 11, wherein the database in the access device is stored on one of a removable data card, the access device's permanent memory, or an additional memory card.

13. The method of claim 11, wherein the access device comprises one of a Personal Digital Assistant, a computer, and a cell phone.

14. The method of claim 11, further comprising the steps of:

- downloading programming to update or replace the current programming for separating data in the access device; and

- downloading different timing intervals and corresponding indexes to the database in the access device, wherein the downloading steps are either periodic or random.

15. The method of claim **11**, wherein the authentication device is connected to a cellular network and comprises one of an authentication center (AuC), a mobile switching center (MSC), and a base transceiver station (BTS).

16. In a user device, a computer-implemented method of constructing and transmitting a secret key to an authentication device that authenticates the secret key and grants the user device access to a radio telecommunication network, said method comprising the steps of:

- receiving an index value from the authentication device;
- utilizing the index value to retrieve from a database, a set of predefined time intervals;
- dividing the secret key into a plurality of segments; and
- individually transmitting the segments to the authentication device, wherein each of the segments is separated in time from a previously transmitted segment by one of the predefined time intervals, wherein the time intervals between the segments are part of the secret key.

16. In a user device, a method of constructing and transmitting a text message to another user device in a radio telecommunication network, said method comprising the steps of:

- signing on to a text messaging server in the network;
- receiving an index value from an authentication entity in the network;
- utilizing the index value to retrieve from a database, a set of predefined time intervals;
- dividing the text message into a plurality of segments;
- individually transmitting the segments to the authentication entity for transfer to the another user device, wherein each of the segments is separated in time from a previously transmitted segment by one of the predefined time intervals;
- the authentication entity, determining the address of the another user device and providing an index corresponding to a database connected to the another user for use in segmenting and separating, with time intervals, any response messages to the user; and
- the authentication entity, sending, receiving and converting text message segments, separated by the indexed timing intervals unique to each user, between the user and the another user.

* * * * *