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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 September 2002 (19.09.2002)

PCT

(10) International Publication Number
WO 02/073945 A1

(51) International Patent Classification⁷: H04M 5/00

(21) International Application Number: PCT/US01/50885

(22) International Filing Date: 9 November 2001 (09.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/709,592 10 November 2000 (10.11.2000) US

(71) Applicant: SECURELOGIX CORPORATION [US/US]; Suite 230, 13750 San Pedro, San Antonio, TX 78232 (US).

(72) Inventors: **SCHMID, Gregor**; 30 Cutter Green, San Antonio, TX 78248 (US). **PICKENS, Keith, S.**; 431 Honey Oaks Lane, San Antonio, TX 78248 (US). **HEILMANN, Craig**; 13750 San Pedro, Suite 230, San Antonio, TX 78232 (US).

(74) Agents: **THIELE, Alan, R.** et al.; Jenkens & Gilchrist, Suite 3200, 1445 Ross Avenue, Dallas, TX 75202 (US).

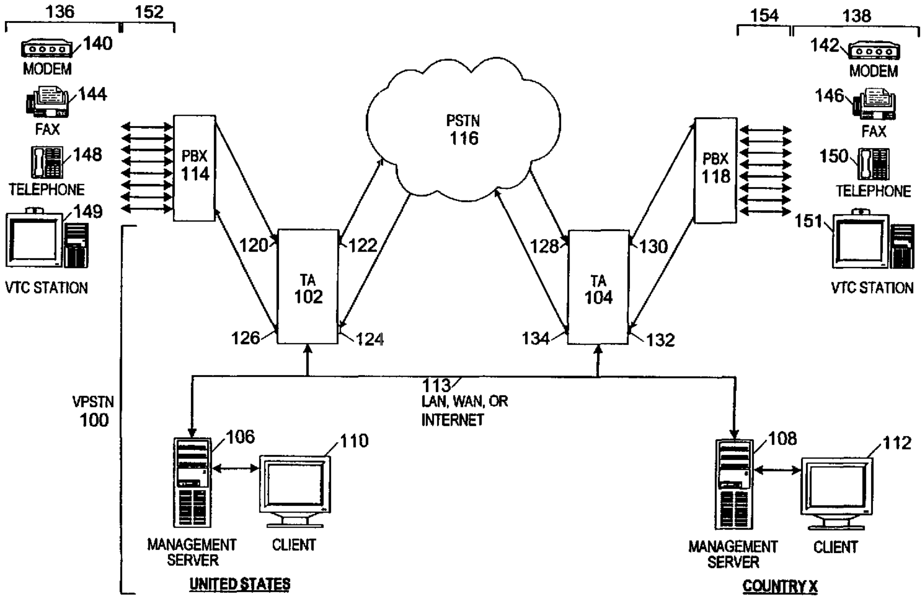
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: ENCAPSULATION, COMPRESSION, AND ENCRYPTION OF PCM DATA



(57) **Abstract:** A system and method to provide secure access across the untrusted public switched telephone network (116) is described. The system and method can be initiated by a security policy defining actions, including conducting the call in secure mode, to be taken based upon at least one detected attribute of the call.

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Title: ENCAPSULATION, COMPRESSION AND ENCRYPTION OF PCM DATA

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. Patent Application Serial No. 09/210,347 entitled TELEPHONY SECURITY SYSTEM filed December 11, 1998, now U.S. Patent No. US 6,249,575 B1; and is related to U.S. Patent Application Serial No. 09/457,494 entitled A TIGHTLY INTEGRATED COOPERATIVE TELECOMMUNICATIONS FIREWALL AND SCANNER WITH DISTRIBUTED CAPABILITIES filed December 8, 1999, now U.S. Patent No. US 6,226,372 B1; both assigned to the assignee of the present application and incorporated herein by reference.

TECHNICAL FIELD

The invention relates generally to telecommunications access control systems and more particularly, to a system and method whereby a virtual private telephone network is autonomously constructed between at least two in-line devices.

BACKGROUND OF THE INVENTION

Historically, government and business entities could be reasonably confident that their sensitive information communicated by telephone, fax, or modem was confidential, and that no one would monitor or eavesdrop on their plans and strategies. This is no longer true. In the past several years, as interception and penetration technologies have multiplied, information assets have become increasingly vulnerable to interception while in transit between the intended parties.

A wide range of communications, from those concerning military, government, and law enforcement actions, to contract negotiations, legal actions, and personnel issues, all require confidentiality; as do communications concerning new-product development, strategic planning, financial transactions, or any other competition-sensitive matter. These confidential matters often require exchanges via telephone, fax, Video TeleConference (VTC), data (modem) transmission, and other electronic communication. As businesses depend on their communications systems more and more, those systems are delivering an ever-increasing volume of information, much of which is proprietary and extremely valuable to competitors.

It's not just business competitors that companies have to be concerned about. Risks are particularly high for businesses with operations outside the United States. Many nations are defining their national security as economic security, and are putting their intelligence agencies into the business of industrial and economic espionage. As a result, some foreign intelligence agencies actively and aggressively spy on businesses to collect technology and proprietary information.

The increasing prevalence of digital communications systems has led to the widespread use of digital encryption systems by governments and businesses concerned with communications security. These systems have taken several forms, from data Virtual Private Networks (VPN), to secure voice/data terminals.

Communications and computer systems move massive amounts of information quickly and routinely. Businesses are communicating using voice, fax, data, and video across the untrusted Public Switched Telephone Network (PSTN). Unfortunately, whereas a data VPN protects information traveling over the Internet, a data VPN is not designed to protect voice, fax, modem, and video calls over the untrusted PSTN.

While Internet Protocol(IP)-based VPN technology is automated and widely available, solutions for creating safe tunnels through the PSTN are primarily manual, requiring user participation at both ends to make a call secure. This is the case with the use of secure voice/data terminals, such as Secure Telephone Units (STU-IIIs), Secure Telephone Equipment (STE), and hand-held telephony encryption devices.

When used, secure voice/data terminals effectively protect sensitive voice and data calls. However, their design and typical deployment can be self-defeating. For example, to enter a secure mode on a STU-III or STE device, both call parties must retrieve a physical encryption key from a safe storage location and insert the key into their individual device each time a call is placed or received. Also, STU-III and STE devices are expensive, so they are typically located at a special or central location within a department or work center, but not at each work station. If a STU-III or STE call is not scheduled ahead of time, the caller may have to wait while the called party is brought to the phone—with a key.

If the secure voice/data terminal is installed on an analog line, transmission speed and voice recognition quality is low. Slow speed may be tolerated for secure data transfer, but slow transmission speeds can make secure voice communication difficult and frustrating. Good speed and voice quality is attainable on Integrated Services Digital Network (ISDN) or Trunk level 1 (T1) lines (or trunks), but replacement of analog lines is expensive and many organizations prefer to keep their existing equipment.

The inconvenience, frustration, and poor voice quality of using manually activated secure voice/data terminals can motivate individuals to "talk around" the sensitive material on non-secure phones. Although the confidential information is not directly spoken, these vague conversations can be pieced together to get a fair idea of the information that was supposed to be protected. Use of secure voice/data terminals for the communication of sensitive information can be mandated by policy, but there is no way to properly enforce such a requirement.

Additionally, secure voice/data terminals secure only one end-user station per device. As point-to-point devices, secure voice/data terminals cannot protect the vast majority of calls occurring between users who do not have access to the equipment. And while there are policies that specifically prohibit it, sensitive material can be inadvertently discussed on non-secure phones and thereby distributed across the untrusted PSTN.

Secure voice/data terminals cannot implement an enterprise-wide, multi-tiered policy-based enforcement of a corporate security policy, establishing a basic security structure across an enterprise, dictated from the top of the tier downward. Neither can secure voice/data terminals implement an enterprise-wide, multi-tiered policy-based enforcement of selective event logging and consolidated reporting to be relayed up the tier.

Secure voice/data terminals cannot provide the capability of "live" viewing of all secure call actions performed by the device.

Lastly, secure voice/data terminals cannot provide call event logs detailing secure calls. Therefore, a consolidated detailed or summary report of a plurality of call event logs can not be produced for use by security personnel and management in assessing the organization's security posture.

Clearly, there is a need for a system and method to provide secure access across the untrusted PSTN through telephony resources that can be initiated by a security policy defining actions to be taken based upon at least one attribute of the call, providing multi-tiered policy-based enforcement capabilities and visibility into security events.

SUMMARY OF THE INVENTION

A system and method to provide secure access across the untrusted PSTN is described. The system and method utilizes telephony resources that can be initiated by a security policy defining actions to be taken based upon at least one attribute of the call, and provides multi-tiered policy-based enforcement capabilities and visibility into security events.

Some primary advantages of the disclosed system and method are: (1) operator-transparency, i.e., secure communications is implemented and enforced via a security policy and requires no action by the call parties in order to conduct a secure call;

(2) secured communication for multiple end-use stations (i.e., all calls on a trunk) by deployment on the trunks from the Central Office (CO) instead deployment of point devices at each end-user station; (3) implementation and enforcement of a security policy designating that all calls are conducted in secure mode, allowing or denying select calls and performing other actions, such as sending a tone or message, logging the call or sending notifications, if the call can not be conducted in secure mode; (4) implementation and enforcement of a security policy designating that select calls are conducted in secure mode based on designated attributes of the call, allowing or denying the call and performing other actions, such as sending a tone or message, logging the call or sending notifications, if the call can not be conducted in secure mode; (5) allowing or denying select calls and performing other actions based on the reason the call can not be conducted in secure mode; (6) secure transport of voice, fax, and modem calls; (7) secure transport of communications unaffected by transcoding; (8) a message channel separate from the secured call data, allowing the message and the secured call to be sent concurrently; (9) automatic enforcement of a security policy; (10) implementation and enforcement of the security policy based on call attributes such as inbound call source, outbound call source, inbound call destination, outbound call destination, call type, etc.; (11) implementation and enforcement of a basic security structure and policy across an enterprise, dictated from the top of the tier downward; and (12) implementation and enforcement an enterprise-wide policy of selective event logging and consolidated reporting to be relayed up the tier.

Some secondary advantages of the disclosed system and method are: (1) creation of a new key is for each session, eliminating the need for static secret keys; (2) automatic generation of each session key, eliminating the need for manual keys, (3) the message channel stays active throughout the duration of the call, and sends control and status messages to initiate or discontinue secure mode transmission while the call is in progress; (4) line impairments are assessed as part of secure mode call setup and secure call setup is discontinued if the line conditions will not support secure communications; (5) voice quality is equal to toll quality, i.e., the quality of an uncompressed pulse code modulated digital signal level-0 channel at 64, 000 bps.

Therefore, in accordance with the previous summary, objects, features and advantages of the present invention will become apparent to one skilled in the art from the subsequent description and the appended claims taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

A better understanding of the system and method for autonomously constructing a virtual private telephone network between at least two in-line devices may be had by reference to the drawing figures wherein:

Figure 1 is a schematic drawing of an exemplary telecommunications virtual private switched telephone network of the present invention;

Figure 2 is a schematic block diagram of a virtual private switched telephone network Digital Signal level 0 (DS-0) sample;

Figure 3 is a process flow diagram illustrating the virtual private switched telephone network where a call is conducted in secure mode;

Figures 4A and 4B are a process flow diagram illustrating a secure call setup where secure mode capabilities between the call source and the destination are established prior to exchange of the session secret key;

Figures 5A and 5B are a process flow diagram illustrating the compression and encryption process where a non-secure digital signal level 1 (DS-1) circuit is processed for secure transport;

Figures 6A and 6B are a process flow diagram illustrating the decryption and decompression process where a non-secure digital signal level 1 (DS-1) circuit is restored to its original non-secure state.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention can be described with several examples given below. It is understood, however, that the examples below are not necessarily limitations to the present invention, but are used to describe typical embodiments of operation.

Figure 1 is a schematic block diagram of an exemplary telecommunications Virtual Private Switched Telephone Network (VPSTN) 100 of the present invention, similar to the telecommunications firewall implemented as shown and described in U.S. Patent Application Serial No. 09/210,347, now U.S. Patent No. US 6,249,575 B1. The VPSTN 100 can be combined with the telecommunications firewall to act as an integrated VPSTN 100 and a firewall simultaneously, or to result in a mixture of capabilities of each device, similar to the integrated telecommunications firewall and scanner implemented as shown and described in U.S. Patent Application Serial No. 09/457,494, now U.S. Patent No. US 6,226,372 B1.

The VPSTN 100 includes a plurality of Telephony Appliances (TA) 102 and 104, management servers 106 and 108, and clients 110 and 112, all interconnected by a TCP/IP-based Local Area Network (LAN), Wide Area Network (WAN), or Internet (any of which are identified herein with numeral 113), for interaction as described below.

The VPSTN 100 provides secure communication between two geographically separate, even globally distributed locations. The TA 102 or 104 is installed in-line on a Digital Signal level 1 (DS-1) circuit. The capacity (i.e., quantity and speed of channels) on a DS-1 circuit varies relative to global location. For instance, a T1 or J1 trunk, used in North America and Japan respectively, operates at 1,544,000 bits per second (bps) and carries 24 time-division-multiplexed (TDM) Digital Signal level 0 (DS-0) channels. Additionally, in North America, an Integrated Services Digital Network Primary Rate Interface (ISDN PRI) trunk may carry either 23 TDM DS-0 channels with one signaling channel, or 24 TDM DS-0 channels. In Europe, an E1 trunk operates at 2,048,000 bps and carries 30 TDM DS-0 channels in addition to 2 signaling channels. A DS-0 channel operates at 64,000 bps. An additional variation relative to global location is the difference in the form of PCM encoding. Typically, mu-law is the standard used in North American and Japanese telephone networks, and A-law is used in European and most other national public switched telephone networks. Transcoding, or modifying the data stream from mu-law to A-law, so that it can be carried via a different network, may cause the PCM value to change. Regardless of whether the T1, J1, ISDN PRI, E1, etc., trunk carrying the DS-1 circuit between the VPSTN 100 and the PSTN is the same on both sides of the PSTN, (i.e., T1 trunk to PSTN to T1 trunk, as may occur with calls conducted within North America), or is some combination of trunk types, (i.e., T1 trunk to PSTN to E1 trunk, as would occur with an international call), all operations are transparent to the individuals placing and receiving the call (i.e., neither call party is required to take any specific actions in order to initiate or conduct a secure call).

The TA 102 is installed in-series on a DS-1 circuit between a Public Branch eXchange (PBX) 114 and a Public Switched Telephone Network (PSTN) 116. The TA 104 is installed in-series on the DS-1 circuit, between the PSTN 116 and a PBX 118. The TA 102 has two input and two output ports; specifically, a PBX-in port 120, a PSTN-out port 122, a PSTN-in port 124, and a PBX-out port 126. Similarly, the TA 104 has two input and two output ports; specifically, a PSTN-in port 128, a PBX-out port 130, a PBX-in port 132, and a PSTN-out port 134.

The client 110 and 112 is a point of user-interface for the system administrator configuring a security policy and other operational features of the TA 102 and 104 respectively; for displaying and viewing real-time alerts, viewing real-time event logs, and printing event logs and consolidated reports, and other operational features of the VPSTN 100.

A security policy is a sequential listing of rules that define whether certain calls to or from an end-user station will be allowed, denied (hung-up), conducted in secure mode, monitored for content, logged. The security policy also defines whether other additional actions such as sending a tone or message to call parties to indicate the ability or inability to conduct the call in secure mode, and sending notifications such as electronic mail notification, pager alerting, console messaging, or a Simple Network Management Protocol (SNMP) trap notification are required.

The management server 106 and 108 receive the security policy from the client 110 and 112, and push a copy of the security policy to the TA 102 and 104 respectively. The management server 106 and 108 are connected to the TA 102 and 104 respectively for consolidation and management of reports and call logs. Historical logging and_archiving of calls, pursuant to a predetermined security policy, may be accomplished on the local management server, or stored via a network-accessible log server (not shown).

The TA 102 and 104 receive the security policy, and as appropriate, monitor inbound and outbound, allow, deny, or otherwise manipulate calls, including conducting calls in secure mode, all pursuant to the security policy, and based on a plurality of call attributes, including call type (voice, fax, modem, VTC, etc.).

The TA 102 and 104 may combine call-progress monitoring, caller-id (CND) and/or Automatic Number Identification (ANI) decoding, digital line protocol reception, decoding, demodulation, pulse dial detection, Dual-Tone MultiFrequency

(DTMF) and MultiFrequency (MF) tone detection, with microprocessor control, access-control logic, and call-interrupt circuitry for implementing the desired VPSTN functions.

Also in Figure 1, numerals 136 and 138 designate end-user stations, representing as examples, one or more modems 140 and 142, fax machines 144 and 146, telephones 148 and 150, and VTC stations 149 and 151, which may send or receive calls over the VPSTN 100. The modems 140 and 142 may support a desktop or portable personal computer, for example. Individual station extensions 152 and 154 connect the end-user stations 136 and 138 to the PBX 114 and 118 respectively.

For clarity and simplicity of explanation, Figure 1 and subsequent figures show a complete DS-1 circuit (specifically, all 32 DS-0 channels on an E1 trunk), connected between the TA 102, the PSTN 116, and the TA 104; although typically, the DS-0 channels that make up the DS-1 circuit may be individually switched by the PSTN 116 to different locations relevant to call destination. All of the DS-0 channels on the DS-1 circuit are shown herein to be processed using the VPSTN 100, although a security policy can be configured such that the VPSTN 100 is selectively applied to calls, based on call attributes such as the call direction (inbound, outbound); the call source number; the call destination number; call type; the date; the time; the call duration, etc. Additionally, in the examples provided, voice is the media transported, although the present invention also provides secure transport for a plurality of media in addition to voice, including fax, modem and VTC. The inventive functions described herein as being performed by the TA 102 are similarly performed by the TA 104.

Additionally, the system and method supports a multi-tiered security policy. For example, a corporate-dictated security policy will contain basic rules for the Security Rule database. These rules are classified as either "Required" or "Optional". Each level of the hierarchical environment must adhere to a required rule, but can choose to ignore optional rules. Each level of the tier is capable of making their local rules and the rules for the tiers below it more stringent than the corporate-dictated rules, but can not make the rules more lax. In this way, a basic security structure is ensured across the enterprise.

The corporate-dictated security policy contains basic security rules that dictate what information will be reported upward, thereby providing visibility into only the most important local security events at the corporate level. Just as the corporate-dictated rules send security guidelines that may become more stringent as they are passed downward, the policy institutes an information filter that becomes more selective as email, logs and reports, etc., are routed upward. The tasks in the "Tracks" column of the corporate-dictated rule (such as email notification, pager notification, logging of events, etc.), that are of interest at a local level but are not of interest at higher levels, are designated to be filtered out if notification of a rule firing is to be routed up the tier. All logging is real-time, both at the location where the event occurs and at upper levels of the organization that, in accordance with the security policy, may or may not require notification of the event.

Figure 2 is a schematic block diagram of a VPSTN DS-0 channel sample 1100 of the present invention. The DS-0 channel is the atomic level (the lowest level) of a standard telephony call, regardless of whether the call is voice, fax, modem, or VTC. As previously mentioned, the DS-0 channel operates at 64,000 bps. The present invention subdivides the VPSTN DS-0 channel sample 1100 into three subrate channels. The term subrate is used because each of the three channels operate below the full DS-0 channel rate of 64,000 bps. The three subrate channels include a bearer channel 1102, a Encrypted Packet (EP) boundary channel 1104, and a message channel 1106. The bearer channel 1102 operates at a DS-0 channel subrate of

40,000 bps (5-bits per sample). The EP boundary channel 1104 and message channel 1106 each operate at a subrate of 8,000 bps (1-bit per sample). The three subrate channels add up to a rate of 56 (40 + 8 + 8) Kbps. The remaining 8 Kbps, is used for a Least Significant Bit (LSB) 1108 position. The LSB 1108 is set high during transmission and is discarded after it is received.

The three subrate channels are assigned bit positions within each VPSTN DS-0 channel sample 1100. The bearer channel 1102 is assigned bit positions 3, 4, 5, 6, and 7. The EP boundary channel 1104 is assigned bit position 2, and the message channel 1106 is assigned bit position 1.

The bearer channel 1102 carries the audio signal in a compressed format. The ITU-T G.726 Recommendation, Adaptive Differential Pulse Code Modulation (ADPCM) in 5-bit mode, is used to compress the audio signal. In 5-bit mode (which operates at 40K bps), the voice quality is equal to that of an uncompressed Pulse Code Modulated (PCM) DS-0 channel at 64 Kbps (toll quality). The 5-bit ADPCM mode was designed specifically to allow voice-band data modem calls to be transported using ADPCM at modem speeds greater than 4800 baud. The ITU has conducted extensive tests and found that 5-bit ADPCM G.726 allows voice-band data modems to operate at speeds up to 19,200 baud. Therefore, using the VPSTN 100 may cause a V.90 or V.34 modem to connect at a slower speed than would be possible on a DS-0 channel not using the VPSTN 100. Moreover, because Group 3 fax transmissions operate at speeds less than 19,200 baud, using the VPSTN 100 should not impact fax transmission speeds.

The EP boundary channel 1104 is used to create encryption packets made up of five 64-bit words (blocks). A 64-bit block size allows a 64-bit encryption/decryption engine to process the 64-bit blocks. An encryption packet of five 64-bit blocks are 8 milliseconds in length (1/125 of a second). The EP boundary is not relative to framing, such as the D3/D4 framing or Extended Super Frame (ESF) formats.

The message channel 1106, created as a result of the compression of the signal on the bearer channel 1102 from 8-bit to 5-bit, is used to send messages between the TA 102 and 104. An extensible protocol such as the IETF's Session Initiation Protocol (SIP) is used to send ASCII text-based message packets over the 8,000 bps channel in alignment with the encryption packet boundary established for the bearer channel 1102. Messages are used to setup a secure call, exchange and negotiate TA capabilities, exchange encryption keys, report errors, and control the call session. The message channel 1106 remains active throughout the duration of a call, and is used to initiate or discontinue secure mode while a call is in progress. The 64-bit message packet may be subdivided into fields. The fields may contain the packet header, TA identification, message sequence numbers, timestamps, checksums, etc.

The LSB 1108 of the VPSTN DS-0 channel sample 1100 is discarded on receive channels and set high (1) on transmit channels. The LSB 1108 data is not used because the PSTN 116 may cause some LSB 1108 values to change during transport. Changes in the value of the LSB 1108 can be caused by robbed-bit signaling, transcoding (mu-law to A-law to mu-law), or digital Packet Assembler/Disassembler (PAD) circuits.

Figure 3 is a process flow diagram illustrating the VPSTN process 1200 whereby a voice call is conducted in secure mode. Imagine the following example. The President of a bank in the United States places a call from the telephone 148, to the Comptroller of the bank's branch office in "Country *X*", who receives the call on the telephone 150. The corporate security policy held by the TA 102 includes the following rule: "Encrypt all outgoing voice, fax, modem and VTC traffic, from all extensions, at any time, on any day, to destination numbers in the Country *X* group. If the call can not be made secure, allow the call, play a warning message, generate an electronic mail notification and log the call." Adherence to this rule is required. Since the failure to secure a call is an indication of the security posture, it is of interest to the upper echelon. As notification of the failure to conduct the secure call is made at each upper level of the hierarchy, the system logs the event for report generation, but filters the task of electronic mail notification from the upper level. The system generates electronic mail notification of the failure to secure the call and sends it only to local and Country *X* security personnel (call source and call destination).

Pursuant to the security policy, the VPSTN 100 autonomously sets up and conducts a secure audio call, transparent to both the President initiating the call and the Comptroller receiving the call. The VPSTN 100 also logs the event and generates alerts or notifications pursuant to the security policy.

Now referring to Figure 3 (reference will also be made to the elements within Figure 1 for this example), in step 1202, the PSTN 116 uses the normal, non-secure telecommunications processes for connecting two terminals (phone sets 148 and 150). When the security policy rule requiring secure communication with the Country *X* phone number fires, the TA 102 contacts the TA 104 to establish whether, and under what conditions, the call between the two locations can be conducted in secure mode.

The session's secret key is exchanged between the TA 102 and the TA 104 in step 1204. A unique secret key, generated for each session by the call-originating TA, is exchanged and used by both the TA 102 and 104 for encryption and decryption of each direction's bearer channel 1102. The exchange of the session secret key is performed using Public Key Exchange (PKE) on the message channel 1106. Steps 1202 and 1204 take place in less than three seconds. During that time, the TA 102 may play a tone or some other audio message to the phone sets, which is heard by both parties involved with the call.

In step 1206, the PBX-in port 120 receives the non-secure DS-1 circuit data from the PBX 114. The TA 102 manipulates, compresses and encrypts the non-secure data bit stream, thereby generating the secure VPSTN DS-0 channel sample 1100 bit stream. The PSTN-out port 122 transmits the secure DS-1 circuit data to the PSTN 116, where it is switched to the PBX 118.

In step 1208, the PSTN-in port 128 receives the secure DS-1 circuit data from the PSTN 116. The TA 104 manipulates, decrypts and decompresses the secure data stream, thereby restoring the non-secure DS-1 circuit data that was previously compressed and encrypted in step 1206. The PBX-out port 130 transmits the non-secure DS-1 circuit data stream to the PBX 118, which transmits the signal to the telephone 150.

While not shown, it is understood that the VPSTN 100 is capable of operating in a continuous loop, synchronously handling the flow of both the receiving and transmitting DS-0 channel data streams. The process loop continues until the call is "hung up". The PSTN 116 tearsdown the call using the normal telecommunications processes for disconnecting the two phone sets 148 and 150, as shown in steps 1210 and 1212.

In step 1214, the call event is logged, and any other actions required by the security policy, such as generation of notifications are executed.

Figures 4A and 4B collectively show a process flow diagram for the secure call setup process 1202 of Figure 3, whereby secure mode capabilities between the call source and destination are established prior to exchange of the session secret key (reference will also be made to the elements in Figure 1 for this flowchart). In step 1302, an audio connection is established between the telephone 148, PBX 114, PSTN 116, PBX 118, and the telephone 150 in the normal, non-secure method used for connecting two phone sets across the

PSTN 116. Once the audio connection is established, two non-secure DS-0 channel data streams flow in a full duplex manner between the two phone sets.

In step 1304, if the fired security rule does not require the call to be conducted in secure mode, the call continues to be conducted in the normal, non-secure method used by the PSTN 116, in step 1306. If in step 1304, at least one call attribute (such as source number, destination number, call type, time of call, etc.) fires a security rule that requires the call to be conducted in secure mode, the TA 102 responds accordingly to setup a secure call with the TA 104, as described below.

In step 1308, shortly after audio establishment between the two telephones 148 and 150, the TA 102 sends an "invite" message packet over the message channel 1106 to the TA 104, and waits for a response. The invite message indicates that the TA 102 is attempting to initiate a secure call with the TA 104. The invite message also indicates the capabilities of the TA 102, such as compression and encryption options.

In step 1310, if the TA 104 is not VPSTN-capable, or if there is no TA 104 at the destination, the TA 102 times-out while waiting for an acknowledge message from the TA 104. If the TA 102 times-out in step 1310, the TA 102 discontinues the secure call setup process 1202, and responds to the failure to setup a secure call in step 1312, pursuant to the security policy.

In step 1312, the security policy may require one or more of the following responses by the TA 102 and management server 106 if the secure call setup process 1202 is discontinued: terminate the call; allow the call to continue in non-secure mode; provide a warning tone or message indicating to the call parties that the call is not secure; log the event; or send notifications to designated personnel.

If the TA 104 is VPSTN-capable, it receives the invite message and sends a "acknowledge" message over the transmit message channel 1106, which is received by the TA 102 in step 1310.

In step 1314, additional message packets are exchanged to coordinate capabilities such as the encryption algorithm and compression algorithm that should be used for this session.

In step 1316, the TA 102 disables the PSTN echo suppressor. The echo suppressor must be disabled because it hinders full duplex transmission of data. Full duplex transmission is necessary for encrypted data blocks to be synchronously transmitted and received by both the TA 102 and 104. The TA 102 sends a message packet to the TA 104 to indicate that a echo suppressor disabler tone (typically equal to 2025 Hz), will be generated over the DS-0 channel for the next *x* seconds. When the TA 102 receives an acknowledge message from the TA 104, the TA 102 generates the disabler tone.

After the disabler tone playback period, the TA 102 and TA 104 exchange messages to determine the existence of line impairments of the two DS-0 channels flowing between the TA 102 and 104 in step 1318. The TA 102 sends a "known" frame over the bearer channel 1102, the content of which is known by both the TA 102 and 104. For example, the known frame may consist of a sequential count of 0 through 63. The TA 104 compares the received "known" with an unmodified known frame and determines if line impairments changed some of the bearer channel "known" frame bit values during transmission of the frame from the TA 102 to the TA 104.

If in step 1320, the TA 104 determines that bits have changed value during transmission, the bearer channel 1102 cannot support the VPSTN process 1200. If this is the case, the TA 104 sends a message packet telling the TA 102 to discontinue the secure call setup process 1202, in step 1322. Upon receipt of the discontinue message, the TA 102 and management server 106 respond to the failure to conduct the call in secure mode (terminate call, allow call, provide warning tone or message, log the event, send notifications, etc.), pursuant to the security policy, in step 1312.

If in step 1320, the TA 104 determines that bit values have not changed during transmission, the line impairments test is repeated on the return DS-0 channel. In step 1324, the TA 104 sends a "known" frame over the bearer channel 1102 to the TA 102. The TA 102 compares the received "known" frame with the unmodified known frame and determines if bit values changed.

If in step 1326, the TA 102 determines that bit values have changed during the transmission, the TA 102 discontinues the secure call setup process 1202. The TA 102 and management server 106 respond to the failure to conduct the call in secure mode pursuant to the security policy (terminate call, allow call, provide warning tone or message, log the event, send notifications, etc.), in step 1312. If the TA 102 determines that bit values have not changed, the TA 102 and 104 exchange the call session secret key in step 1204.

Figures 5A and 5B collectively illustrate a process flow diagram of the compression and encryption process 1206, whereby non-secure DS-1 circuit data is processed for secure transport into the PSTN 116. In step 1500, the TA 102 receives the non-secure DS-1 circuit data from the PBX 114.

In step 1502, a data signal, a frame signal, and a bit-clock signal are extracted from the serial data stream and placed on a TDM highway. The TDM highway has 32 timeslot channels clocked at 2.048 Mbps, and consists of the data signal, the frame signal, and the bit-clock signal. The data signal carries the DS-0 channel data bit stream. The frame signal indicates the beginning of the first 8-bit timeslot, sets the 8-bit timeslot boundaries and operates at 8 KHz. The bit-clock signal synchronizes the DS-0 channel data bit stream and operates at 2.048 MHz. If the PBX-in link is a T1 or J1 trunk, 24 DS-0 channel data bit streams are placed in timeslots 0 through 23, while the remaining 8 timeslots remain empty (set to some value). If the PBX-in link is an E1 trunk, the 30 DS-0 channel data bit streams are placed in their respective timeslots, while timeslot 0 and 16 are reserved for signaling.

In step 1504, the data signal serial bit stream is converted to an 8-bit word stream. An 8-bit sample is output 256,000 times per second (one every 3.9 microseconds). In step 1506, the 8-bit word stream is compressed into a 5-bit ADPCM word stream. In step 1508, the 5-bit ADPCM word stream is demultiplexed into individual non-TDM 5-bit ADPCM word streams for each DS-0 channel (0 through 31).

In step 1510, for each DS-0 channel, 64 5-bit ADPCM words are formatted into five 64-bit plaintext blocks, as required by the encryption algorithm. In step 1512, the five 64-bit plaintext blocks are encrypted and output as five 64-bit cyphertext (encrypted) blocks.

It is understood that 625 (5 x 125) 64-bit plaintext blocks are encrypted/ decrypted per second for each DS-0 channel data bit stream that requires encryption. If all the DS-0 channel data bit streams in a T1 or J1 trunk require secure communication, 15,000 (24 x 625) 64-bit plaintext blocks are encrypted/ decrypted per second. This rate means the single 64-bit plaintext block is encrypted/decrypted in less than 66.7 microseconds. If all the DS-0 channel data bit streams in an E1 trunk require secure communication, 18,750 (30 x 5 x 125) 64-bit plaintext blocks are encrypted/decrypted per second. This rate means the single 64-bit plaintext block is encrypted/decrypted in less than 53.3 microseconds. Additionally, if the TA 102 is handling four E1 trunks, and every DS-0 channel data bit stream must be secured, 75,000 (4 x 18,750) 64-bit plaintext blocks are encrypted/decrypted per second, equal to a block every 13.3 microseconds.

In step 1514, for each DS-0 channel, the five 64-bit cyphertext (encrypted) blocks are formatted into a 5-bit encrypted word stream (destined to be carried on the bearer channel 1102); a 64-bit Encryption Packet (EP) boundary pattern is generated (destined to be carried on the EP boundary channel 1104); a 64-bit message packet is generated (destined to be carried on the message channel 1106), and an LSB serial bit stream is uploaded. The EP boundary pattern is a constant 64-bit pattern that performs the encryption packet boundary function. As previously discussed, messages on the message channel 1106 are exchanged between the TA 102 and the TA 104 to setup a secure call, exchange and negotiate TA capabilities, exchange session secret keys, report errors, etc. The LSB 1108 is always set high in order to increase one's density on the DS-1 circuit.

In step 1516, for each DS-0 channel, the 5-bit encrypted word stream, the 64-bit EP boundary pattern, the 64-bit message packet, and the LSB bit stream are formatted for output as a serial stream of the VPSTN DS-0 channel sample 1100 (i.e., a secure DS-0 channel data bit stream).

In step 1518, each separate secure DS-0 channel data bit stream (channel 0-31) is multiplexed onto a single 2.048 Mbps TDM highway timeslot, as a secure data signal. The timeslot of each encrypted DS-0 channel data bit stream on the outgoing TDM highway is the same timeslot used by that non-secure DS-0 channel data bit stream on the inbound TDM highway previously discussed with reference to step 1502. In addition to the secure data signal, the frame signal and the bit-clock signal are also placed on the TDM highway.

In step 1520, the secure data signal is framed, and the PSTN-out port 122 transmits the secure DS-1 circuit data to the PSTN 116, where each DS-0 channel data bit stream is switched to one or more destinations. Steps 1500-1520 are performed at a rate of 64,000 bps.

In most cases the 24 or 30 encrypted DS-0 channel data bit streams in a T1, J1 or E1 trunk will be routed to multiple locations. However, for the following discussion related with the decryption and decompression process of Figures 6A and 6B, assume that the entire T1, J1 or E1 trunk (i.e., the entire DS-1 circuit), is switched between the TA 102 and the TA 104.

Figures 6A and 6B collectively illustrate a process flow diagram of the decryption and decompression process 1208, whereby secure DS-0 channel data bit streams are restored to their original, non-secure state.

In step 2700, the TA 104 receives the secure DS-1 circuit data from the PSTN 116 on the PSTN-in port 128. In step 2702, the secure data signal, the frame signal, and bit-clock signal are extracted from the serial data stream and placed on a TDM highway. The TDM highway has 32 timeslot channels clocked at 2.048 Mbps.

In step 2704, the secure data signal is converted to an 8-bit encrypted word stream. The 8-bit encrypted word stream is made up of the 8-bit VPSTN DS-0 channel sample 1100 which is output 256,000 times per second (one every 3.9 microseconds). In step 2706, the 8-bit encrypted word stream is demultiplexed (i.e., the 32-TDM 8-bit encrypted word stream is separated into individual non-TDM 8-bit encrypted word streams for each DS-0 channel 0 through 31).

In step 2708, for each channel *n*, the LSB 1108 of the 8-bit encrypted word stream is discarded. Of the resulting 7-bit encrypted word stream, the 5 bits which make up the contents of the bearer channel 1102 are each formatted into one of five 64-bit encrypted blocks for decryption processing; the single bit which makes up the contents of the EP boundary channel 1104 is formatted into one 64-bit block for verifying (step 2710) that all five of the 64-bit encrypted blocks are fully formatted and loaded for decryption processing (step 2712); and the last remaining bit which makes up the contents of the message channel 1106 is also formatted into one 64-bit block.

In step 2710, a determination is made whether the 64-bit block containing contents from the EP boundary channel 1104 is formatted and loaded, thereby verifying that all five of the 64-bit encrypted blocks are fully loaded for decryption processing. If the determination in step 2710 is negative, the process returns to step 2708 as formatting and loading of the 7-bit word stream continues. If the determination in step 2710 is positive, the five 64-bit blocks are decrypted in step 2712, thereby restoring the five 64-bit plaintext (ADPCM) blocks.

In step 2714, the 64-bit data stream making up the message block loads into a first-in first-out (FIFO) memory buffer and is asynchronously accessed by the TA 104 host Computer Processing Unit (CPU). In step 2716, the five 64-bit ADPCM blocks output from the decryption process are formatted into a 5-bit ADPCM word stream. In step 2718, the 5-bit ADPCM word stream from each DS-0 channel (0-31) is time-division-multiplexed into a TDM 5-bit ADPCM word stream, and then converted into a TDM 8-bit mu-law PCM word stream.

In step 2720, the TDM 8-bit mu-law PCM word stream is converted into a TDM serial bit stream (data signal), and placed with the frame signal, and the bit-clock signal on a TDM highway. In step 2722, the data signal is framed and the PBX-out port 130 transmits the TDM non-secure DS-1 circuit data to the PBX 118.

It is understood that the present invention can take many forms and embodiments. The embodiments shown herein are intended to illustrate rather than to limit the invention, it being appreciated that variations may be made without departing from the spirit of the scope of the invention. For example, any number of different rule criteria for the security policy may be defined. Different attribute descriptions and rule descriptions are contemplated. The algorithms and process functions performed by the system may be organized into any number of different modules or computer programs for operation on one or more processors or workstations within the system. Different configurations of computers and processors for the system are contemplated, including those in which the functions of the management server may be inserted into the system at the TA. The programs used to implement the methods and processes of the system may be implemented in any appropriate programming language and run in cooperation with any hardware device. The system may be used for enterprises as small as a private home or business with just a few lines as well as for large enterprises with multiple PBX locations around the world, interconnected in one or more private networks or virtual private networks. In the case where multiple extensions are involved, it is understood that the extensions may be PBX extensions or direct line extensions.

Although illustrative embodiments of the invention have been shown and described, it is understood that a wide range of modifications, changes and substitutions are intended in the foregoing disclosure, including various encryption engines, encryption algorithms, compression algorithms, the various resulting word block sizes, and various arrangements in the placement of the bearer channel 1102, encrypted packet boundary channel 1104, and message subrate channel 1106 within the DS-0 channel sample 1100 (i.e., following the bearer channel, leading the bearer channel, and sandwiching the bearer channel). In some instances, some features of the invention will be employed without a corresponding use of other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.

CLAIMS

1. A virtual private switched telephone network system for providing secure transport of a call between one or more end-user stations within a first enterprise location, across a public switched telephone network, to one or more end-user stations within a second enterprise location, said system being located between said one or more end-user stations and their respective circuits into said public switched telephone network, and the system including:

a database containing at least one security rule, said at least one security rule specifying at least one action to be taken based upon at least one attribute of an incoming or an outgoing call on the line, wherein said at least one action includes conducting said incoming or outgoing call in secure mode, and wherein said at least one attribute is determined within the enterprise location; and

at least one telephony appliance within said first enterprise location and within said second enterprise location, said at least one telephony appliance for determining a call-type of the incoming or outgoing call, wherein the at least one telephony appliance includes means for determining the at least one attribute and for performing the at least one action on selected calls based upon the at least one attribute of the call, in accordance with the at least one security rule.

2. The system of Claim 1 wherein other attributes of the incoming or outgoing call determined by the system include at least one from the group consisting of: inbound source number, outbound source number, inbound destination number, outbound destination number, line identification, call date, call time, call duration.

3. The system of Claim 1 wherein said determined call-type of the incoming or outgoing call includes at least one of the following: voice, fax, data transmission (modem), and video teleconference.

4. The system of Claim 1 wherein the at least one security rule specifies additional actions that include one or more of the following: allow or deny the call, send a tone or message, log the call, generate a report, and provide an alert, whereby options for said alert may include one or more of the following: electronic mail notification, pager dialing, console messaging, or via a Simple Network Management Protocol (SNMP) trap.

5. The system of Claim 1 wherein said telephony appliance is programmed at the telephony appliance or programmed from a management server.

6. The system as defined in Claim 4 wherein said generated report includes post event analysis or batch analysis.

7. A method for providing secure transport of a call between one or more end-user stations within a first enterprise location, across a public switched telephone network, to one or more end-user stations within a second enterprise location, said system being located between said one or more end-user stations and their respective circuits into said public switched telephone network, said method including the steps of:

defining at least one security rule within both said first enterprise location and said second enterprise location for each of the end-user stations within the enterprise location, said at least one security rule specifying at least one action such as conducting an incoming or outgoing call in secure mode, said at least one action to be taken on selected incoming or outgoing calls based upon at least one attribute of the call on the line and contained in the at least one security rule;

detecting and analyzing calls on said line to determine said at least one attribute of the call, wherein the at least one attribute of the call includes at least one from the group consisting of: inbound source number, outbound source number, inbound destination number, outbound destination number, line identification, call type, call date, call time, and call duration, and wherein said detecting and analyzing occurs within the enterprise location; and

performing the at least one action on selected incoming or outgoing calls based upon the at least one attribute of the call, pursuant to the at least one security rule.

8. The method of Claim 7 wherein the at least one security rule specifies additional actions that include one or more of the following: allow or deny the call, send a tone or message, log the call, generate a report, and provide an alert, whereby options for said alert may include one or more of the following: electronic mail notification, pager dialing, console messaging, or via a Simple Network Management Protocol (SNMP) trap.

9. The method of Claim 7 wherein said determined call type of the incoming or outgoing call includes at least one of the following: voice, fax, modem, and video teleconference.

10. The method of Claim 7 wherein conducting a call in secure mode includes continuously exchanging control and status messages between the present invention at each enterprise location concurrent with an exchange of secure call data.

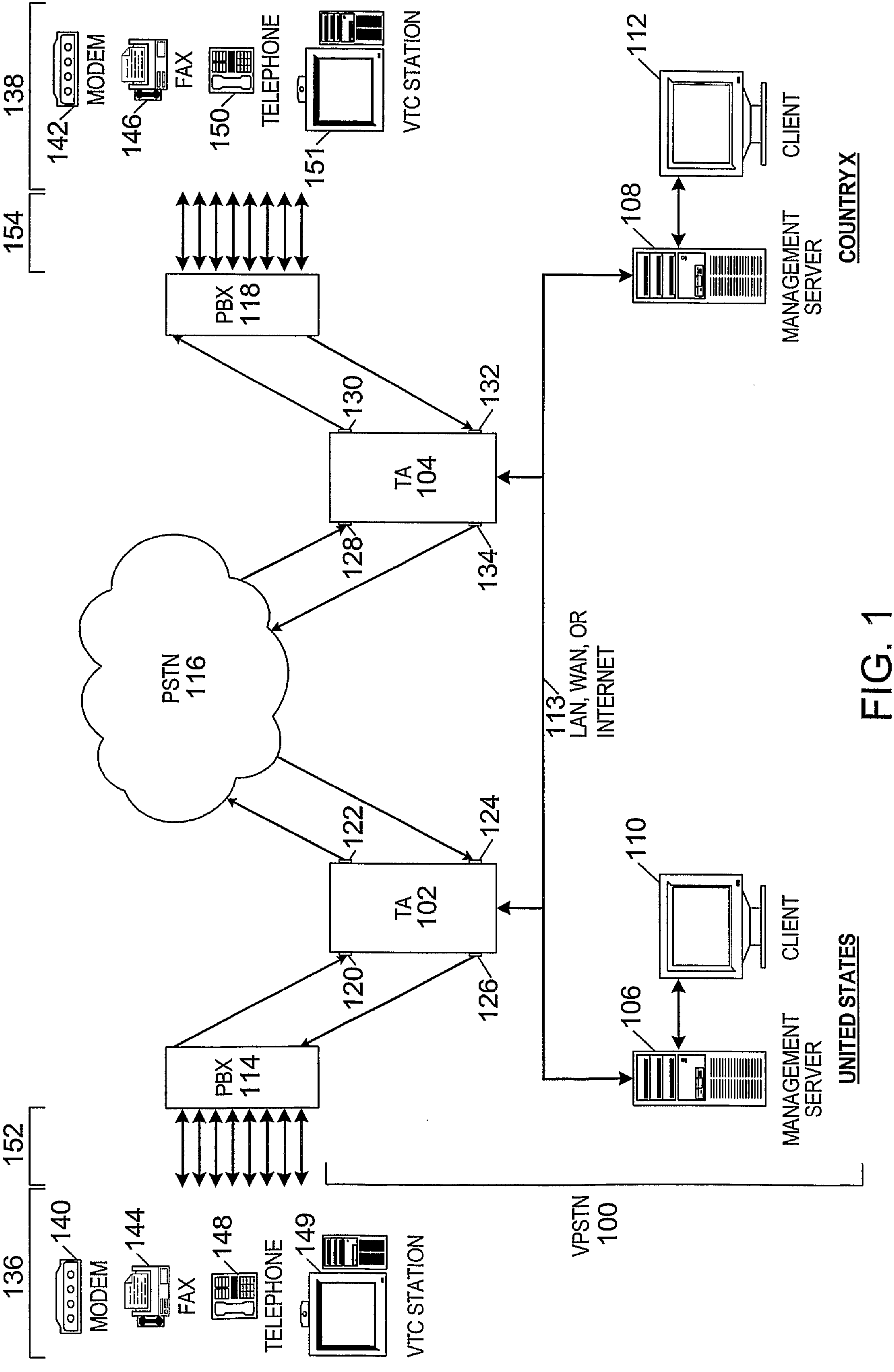

138
142
MODEM
146
FAX
150
TELEPHONE
151
VTC STATION
154
PBX 118
130
132
TA 104
128
134
PSTN 116
122
124
TA 102
120
126
PBX 114
152
136
140
MODEM
144
FAX
148
TELEPHONE
149
VTC STATION
113
LAN, WAN, OR INTERNET
108
MANAGEMENT SERVER
112
CLIENT
COUNTRY X
106
MANAGEMENT SERVER
110
CLIENT
UNITED STATES
VPSTN 100

FIG. 1

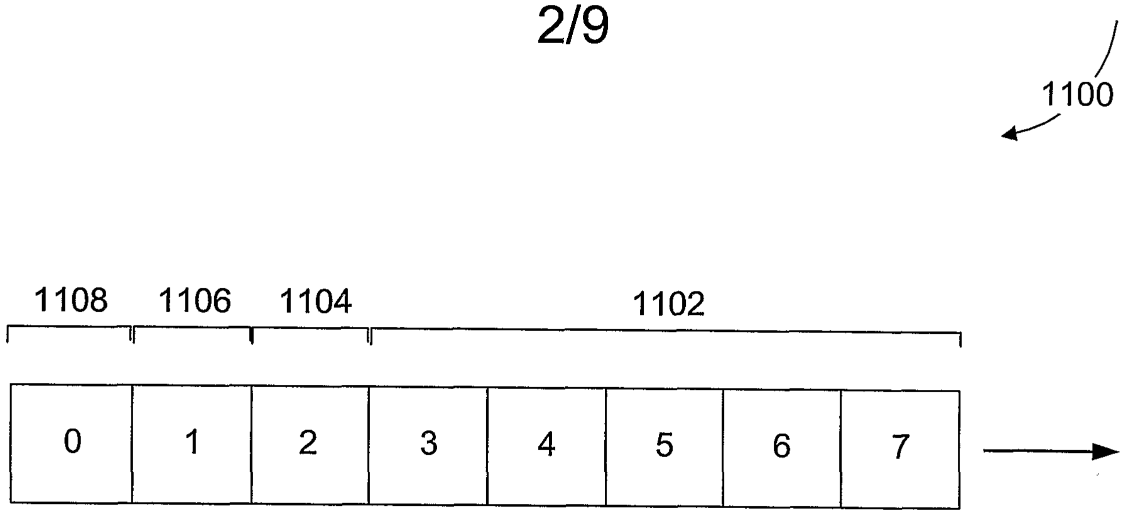


FIG. 2

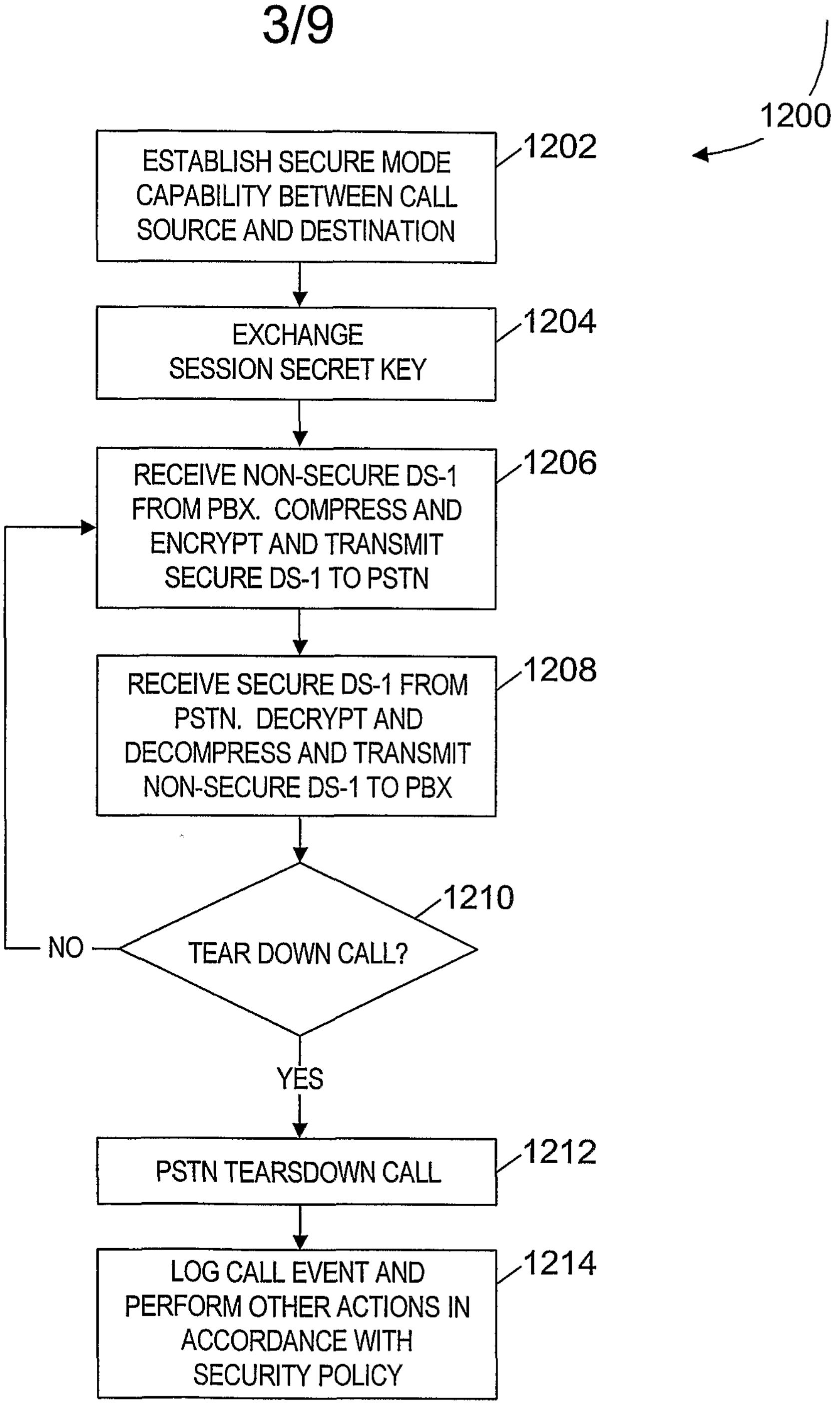

1200
1202
ESTABLISH SECURE MODE CAPABILITY BETWEEN CALL SOURCE AND DESTINATION
1204
EXCHANGE SESSION SECRET KEY
1206
RECEIVE NON-SECURE DS-1 FROM PBX. COMPRESS AND ENCRYPT AND TRANSMIT SECURE DS-1 TO PSTN
1208
RECEIVE SECURE DS-1 FROM PSTN. DECRYPT AND DECOMPRESS AND TRANSMIT NON-SECURE DS-1 TO PBX
1210
TEAR DOWN CALL?
NO
YES
1212
PSTN TEARSDOWN CALL
1214
LOG CALL EVENT AND PERFORM OTHER ACTIONS IN ACCORDANCE WITH SECURITY POLICY

FIG. 3

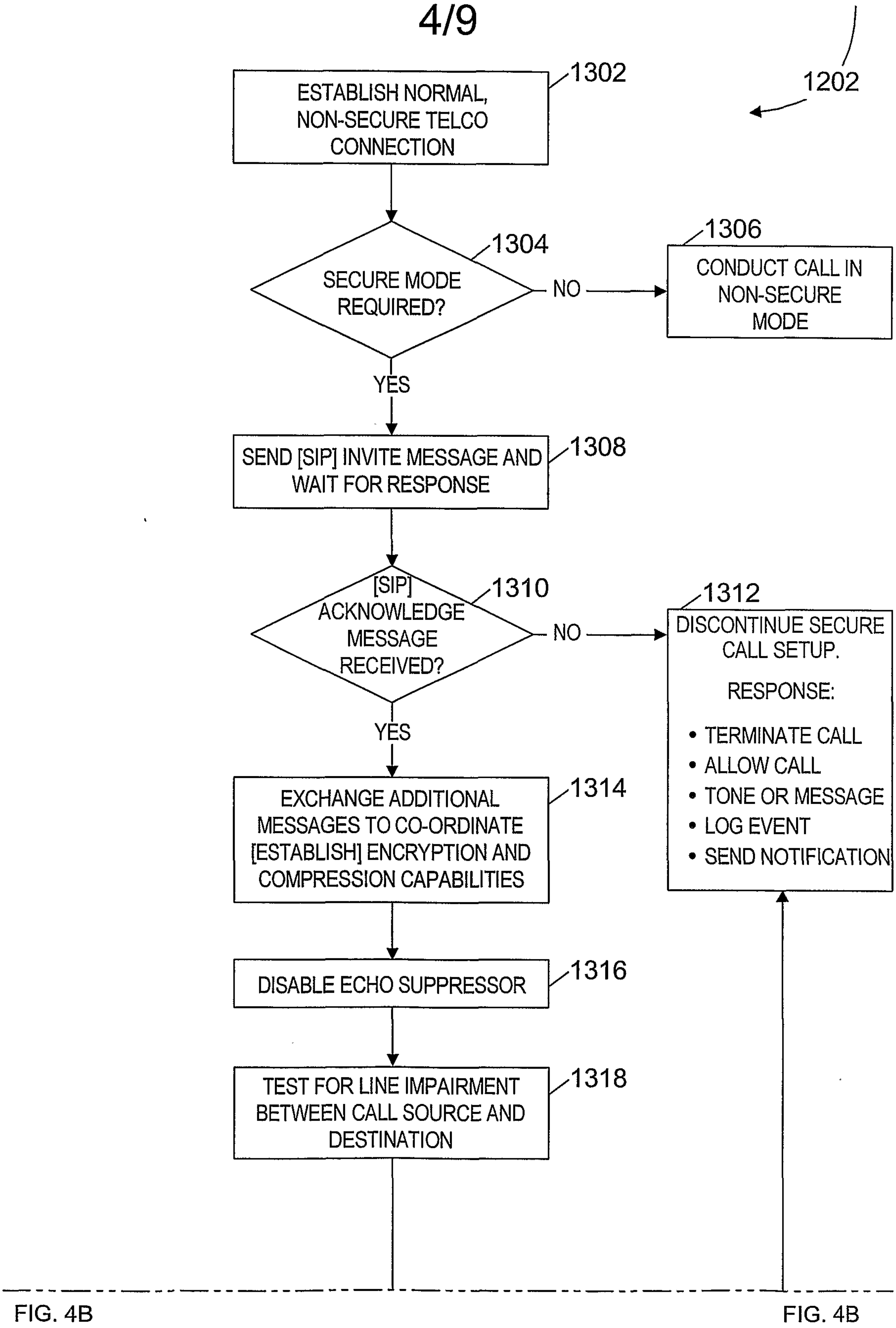

1202
1302
ESTABLISH NORMAL, NON-SECURE TELCO CONNECTION
1304
SECURE MODE REQUIRED?
NO
1306
CONDUCT CALL IN NON-SECURE MODE
YES
1308
SEND [SIP] INVITE MESSAGE AND WAIT FOR RESPONSE
1310
[SIP] ACKNOWLEDGE MESSAGE RECEIVED?
NO
1312
DISCONTINUE SECURE CALL SETUP.
RESPONSE:
• TERMINATE CALL
• ALLOW CALL
• TONE OR MESSAGE
• LOG EVENT
• SEND NOTIFICATION
YES
1314
EXCHANGE ADDITIONAL MESSAGES TO CO-ORDINATE [ESTABLISH] ENCRYPTION AND COMPRESSION CAPABILITIES
1316
DISABLE ECHO SUPPRESSOR
1318
TEST FOR LINE IMPAIRMENT BETWEEN CALL SOURCE AND DESTINATION
FIG. 4B
FIG. 4B

FIG. 4A

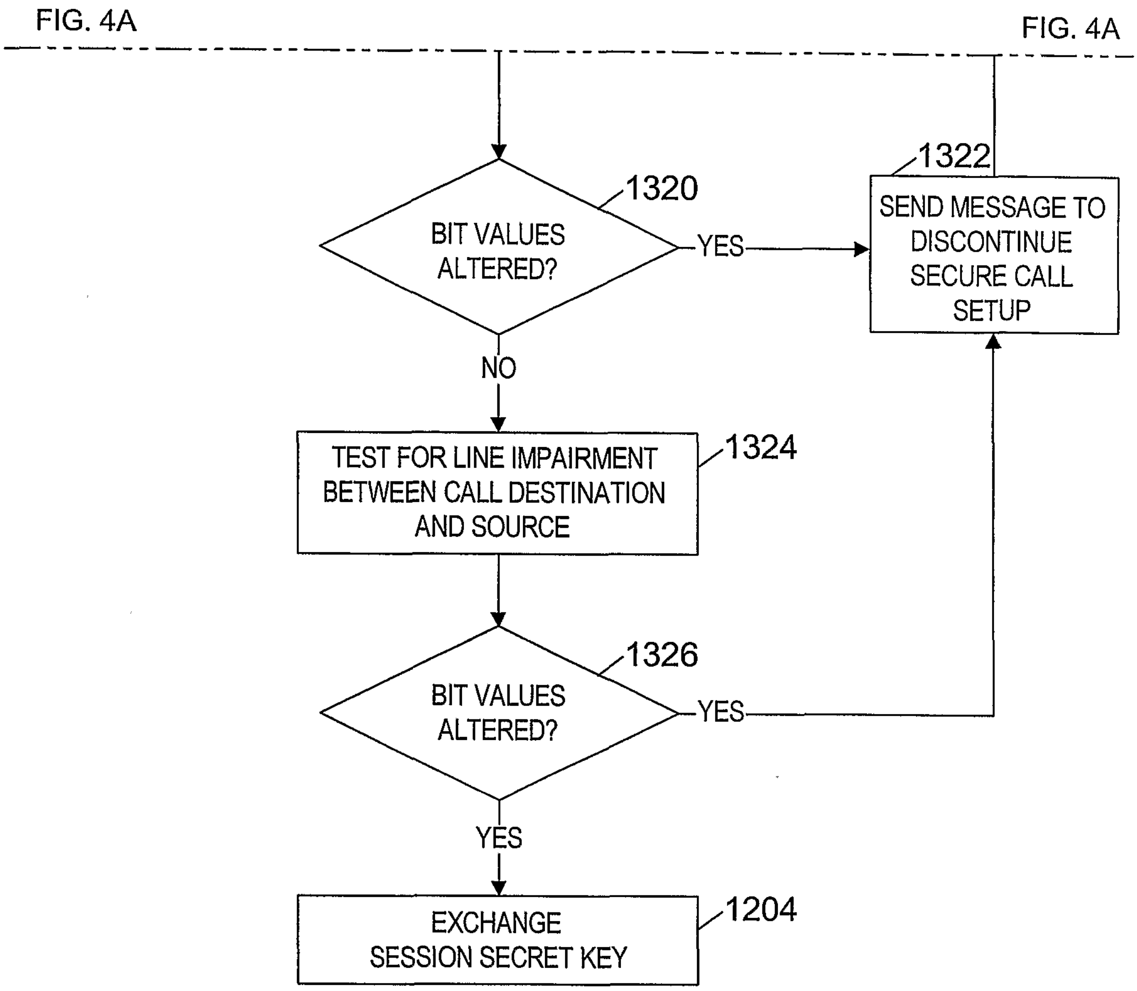


FIG. 4A
FIG. 4A
1320
BIT VALUES ALTERED?
YES
NO
1322
SEND MESSAGE TO DISCONTINUE SECURE CALL SETUP
1324
TEST FOR LINE IMPAIRMENT BETWEEN CALL DESTINATION AND SOURCE
1326
BIT VALUES ALTERED?
YES
YES
1204
EXCHANGE SESSION SECRET KEY

FIG. 4B

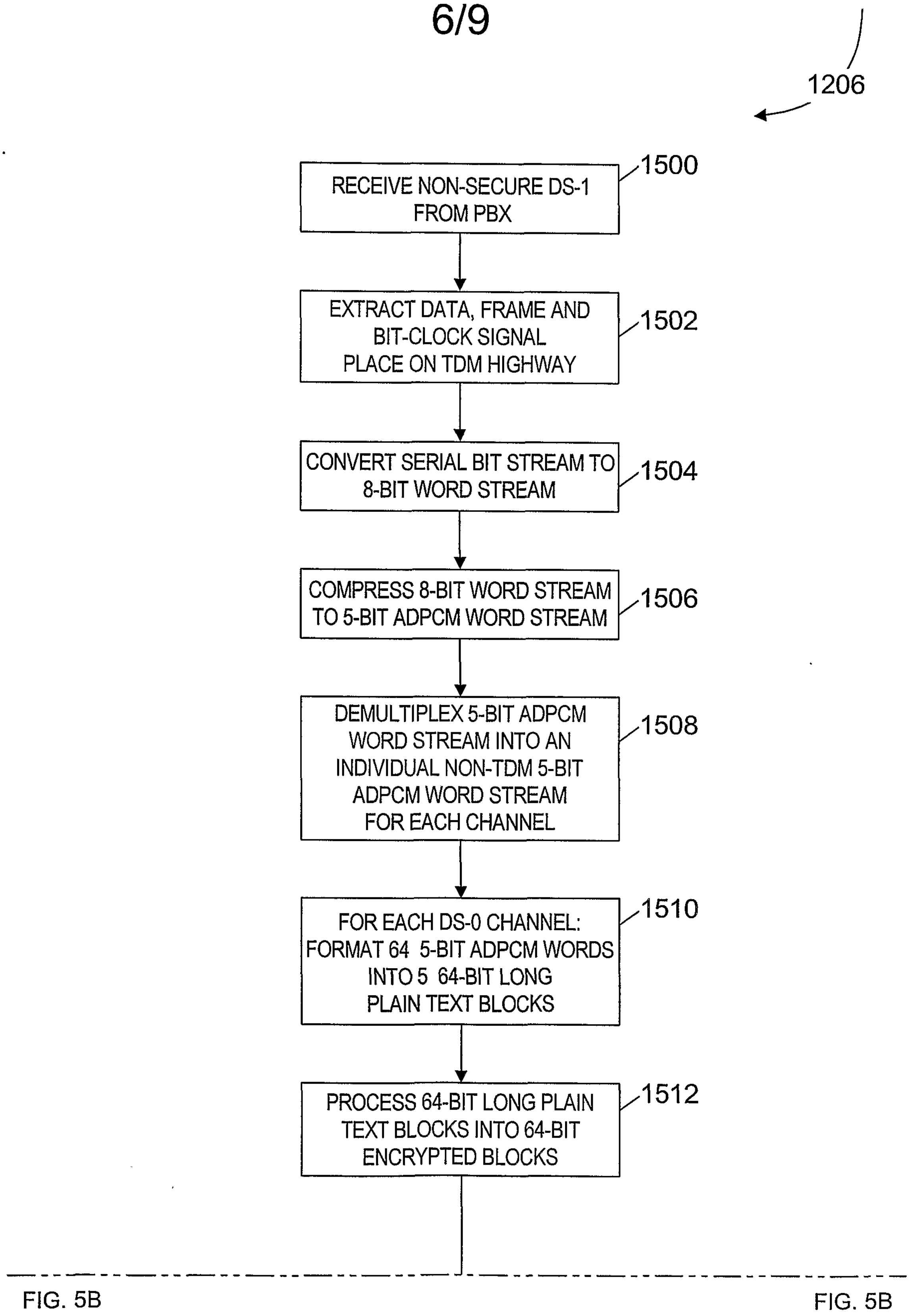

1206
RECEIVE NON-SECURE DS-1 FROM PBX
1500
EXTRACT DATA, FRAME AND BIT-CLOCK SIGNAL PLACE ON TDM HIGHWAY
1502
CONVERT SERIAL BIT STREAM TO 8-BIT WORD STREAM
1504
COMPRESS 8-BIT WORD STREAM TO 5-BIT ADPCM WORD STREAM
1506
DEMULTIPLEX 5-BIT ADPCM WORD STREAM INTO AN INDIVIDUAL NON-TDM 5-BIT ADPCM WORD STREAM FOR EACH CHANNEL
1508
FOR EACH DS-0 CHANNEL: FORMAT 64 5-BIT ADPCM WORDS INTO 5 64-BIT LONG PLAIN TEXT BLOCKS
1510
PROCESS 64-BIT LONG PLAIN TEXT BLOCKS INTO 64-BIT ENCRYPTED BLOCKS
1512
FIG. 5B
FIG. 5B

FIG. 5A

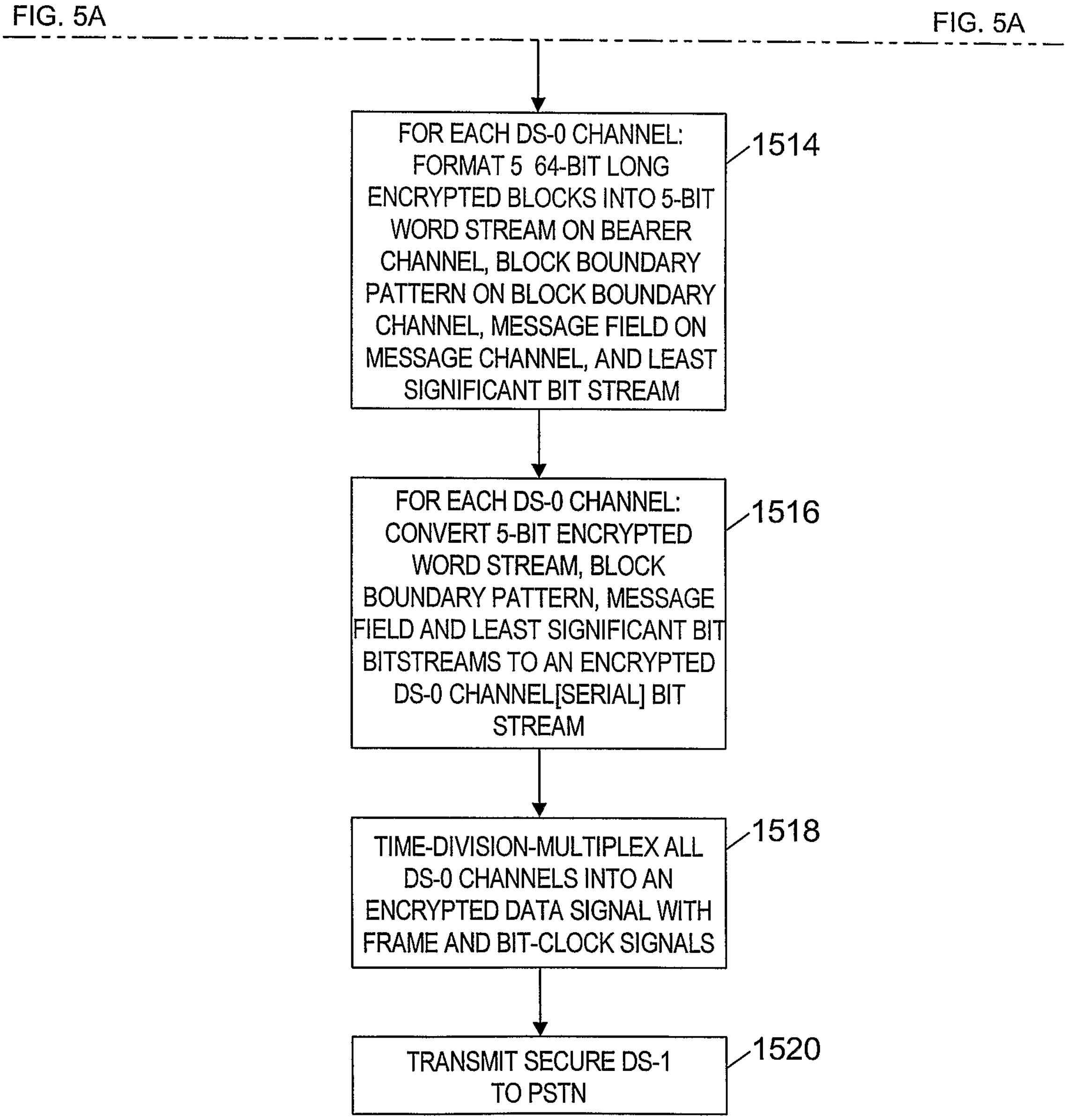


FIG. 5A
FIG. 5A
FOR EACH DS-0 CHANNEL: FORMAT 5 64-BIT LONG ENCRYPTED BLOCKS INTO 5-BIT WORD STREAM ON BEARER CHANNEL, BLOCK BOUNDARY PATTERN ON BLOCK BOUNDARY CHANNEL, MESSAGE FIELD ON MESSAGE CHANNEL, AND LEAST SIGNIFICANT BIT STREAM
1514
FOR EACH DS-0 CHANNEL: CONVERT 5-BIT ENCRYPTED WORD STREAM, BLOCK BOUNDARY PATTERN, MESSAGE FIELD AND LEAST SIGNIFICANT BIT BITSTREAMS TO AN ENCRYPTED DS-0 CHANNEL[SERIAL] BIT STREAM
1516
TIME-DIVISION-MULTIPLEX ALL DS-0 CHANNELS INTO AN ENCRYPTED DATA SIGNAL WITH FRAME AND BIT-CLOCK SIGNALS
1518
TRANSMIT SECURE DS-1 TO PSTN
1520

FIG. 5B

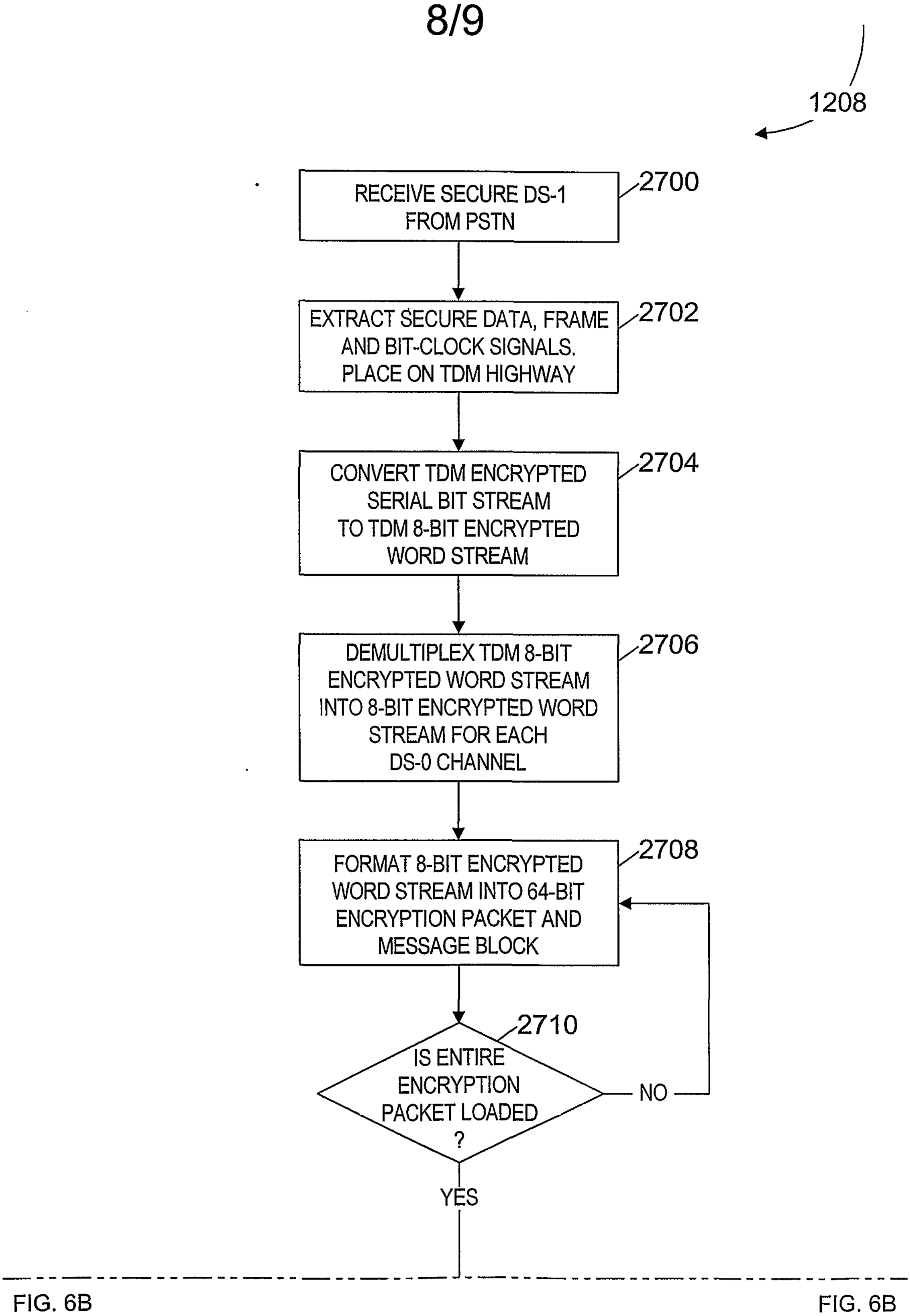

1208
RECEIVE SECURE DS-1 FROM PSTN
2700
EXTRACT SECURE DATA, FRAME AND BIT-CLOCK SIGNALS. PLACE ON TDM HIGHWAY
2702
CONVERT TDM ENCRYPTED SERIAL BIT STREAM TO TDM 8-BIT ENCRYPTED WORD STREAM
2704
DEMULTIPLEX TDM 8-BIT ENCRYPTED WORD STREAM INTO 8-BIT ENCRYPTED WORD STREAM FOR EACH DS-0 CHANNEL
2706
FORMAT 8-BIT ENCRYPTED WORD STREAM INTO 64-BIT ENCRYPTION PACKET AND MESSAGE BLOCK
2708
IS ENTIRE ENCRYPTION PACKET LOADED ?
2710
NO
YES
FIG. 6B
FIG. 6B

FIG. 6A

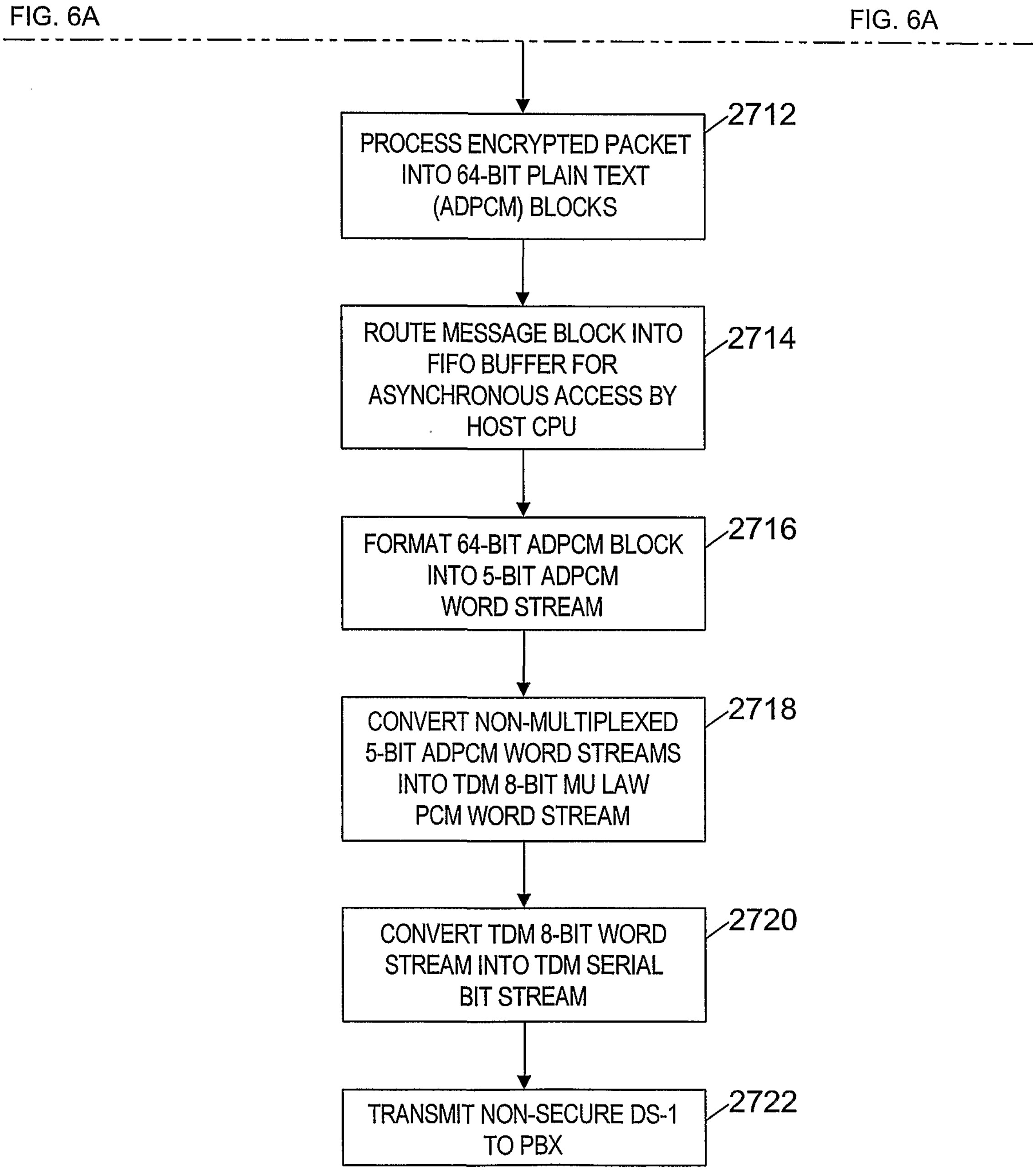


FIG. 6A
FIG. 6A
PROCESS ENCRYPTED PACKET INTO 64-BIT PLAIN TEXT (ADPCM) BLOCKS
2712
ROUTE MESSAGE BLOCK INTO FIFO BUFFER FOR ASYNCHRONOUS ACCESS BY HOST CPU
2714
FORMAT 64-BIT ADPCM BLOCK INTO 5-BIT ADPCM WORD STREAM
2716
CONVERT NON-MULTIPLEXED 5-BIT ADPCM WORD STREAMS INTO TDM 8-BIT MU LAW PCM WORD STREAM
2718
CONVERT TDM 8-BIT WORD STREAM INTO TDM SERIAL BIT STREAM
2720
TRANSMIT NON-SECURE DS-1 TO PBX
2722

FIG. 6B

INTERNATIONAL SEARCH REPORT

Inte onal application No.
PCT/US01/50885

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :HO4M 3/00
US CL :379/189
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 379/189, 93.09, 93.11, 93.24, 156, 157, 188, 196, 198

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

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

EAST
SEARCH TERMS: PRIVATE NETWORK, SECURITY RULE OR POLICY, ATTRIBUTE OR CHARACTERISTIC, CALL TYPE, DETECT OR SENSE.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,098,172 A (COSS et al) 01 August 2000, Abstract, col. 1, line 59-col. 2, line 62, col. 3, line 21-col. 11, line 10.	1-10
Y	US 5,946,386 A (ROGERS et al) 31 August 1999, Abstract, col. 9, lines 2-11, col. 19, line 20-col. 20, line 13, col. 36, lines 12-65.	1-10
Y	US 5,907,602 A (PEEL et al) 25 May 1999, Abstract, col. 26, line 35-col. 34, line 25.	1-10
Y	US 5,892,903 A (KLAUS) 06 April 1999, Abstract, col. 6, line 22-col. 7, line 60.	1-10
Y	US 5,706,338 A (RELYEA et al) 06 January 1998, Abstract, col. 2, line 36-col. 6, line 31.	1-10

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

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

Date of the actual completion of the international search 26 JUNE 2002	Date of mailing of the international search report 02 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer AHMAD MATAR Eugenia Logan Telephone No. (703) 305-4731

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,627,886 A (BOWMAN) 06 May 1997, Abstract, col. 3, line 63-col. 18, ln 46.	1-10
Y	US 5,606,604 A (ROSENBLATT et al) 25 February 1997, Abstract, col. 3, line 66-col. 9, line 42.	1-10
Y	US 5,495,521 A (RANGACHAR) 27 February 1996, Abstract, col. 2, line 45-col. 12, line 24.	1-10
Y, P	US 6,226,751 B1 (ARROW et al) 01 May 2001, Abstract, col.4, line 41-col. 11, line 67.	1-10