Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2644015 C 2016/10/18

(11)(21) **2 644 015**

(12) BREVET CANADIEN / CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2007/04/13
(87) **Date publication PCT/PCT Publication Date:** 2007/10/25
(45) **Date de délivrance/Issue Date:** 2016/10/18
(85) **Entrée phase nationale/National Entry:** 2008/09/26
(86) **N° demande PCT/PCT Application No.:** CA 2007/000608
(87) **N° publication PCT/PCT Publication No.:** 2007/118307
(30) **Priorité/Priority:** 2006/04/13 (US60/791,434)

(51) **Cl.Int./Int.Cl.** ***H04L 29/06*** (2006.01), ***H04L 1/00*** (2006.01), ***H04L 12/22*** (2006.01), ***H04L 9/14*** (2006.01), ***H04L 9/18*** (2006.01), ***H04L 9/32*** (2006.01)

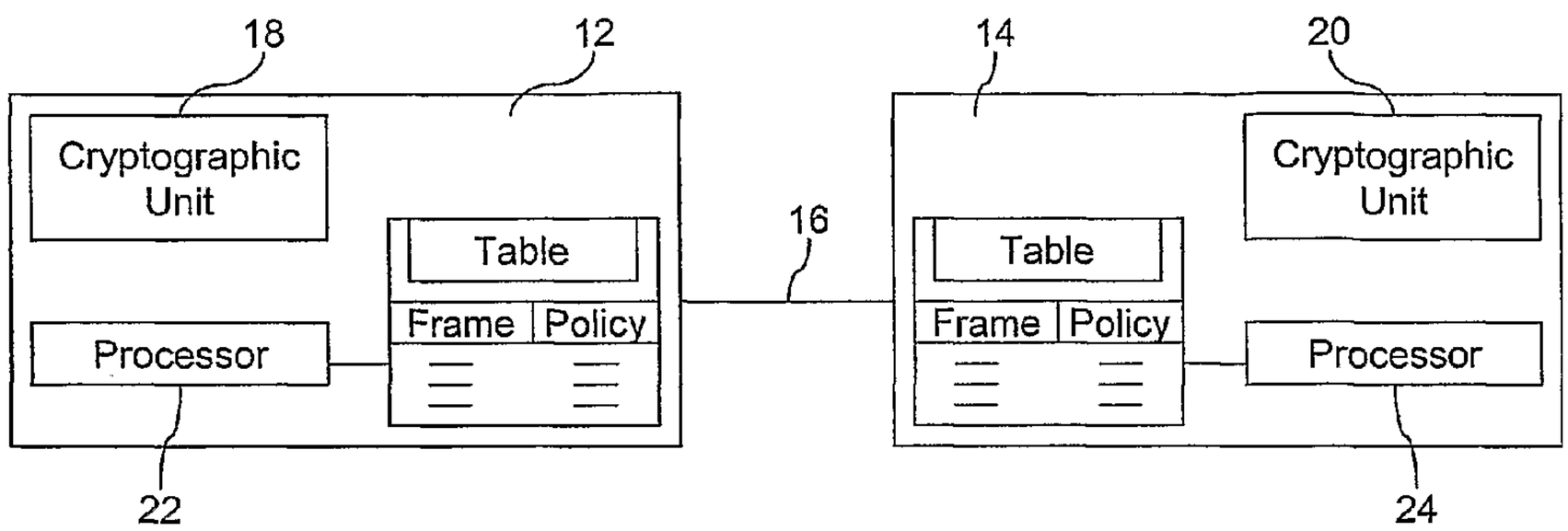
(72) **Inventeur/Inventor:**
STRUIK, MARINUS, CA

(73) **Propriétaire/Owner:**
CERTICOM CORP., CA

(74) **Agent:** INTEGRAL IP

(54) **Titre : PROCEDES ET APPAREIL POUR PROCURER UN NIVEAU DE SECURITE ADAPTABLE DANS UNE COMMUNICATION ELECTRONIQUE**

(54) **Title: METHOD AND APPARATUS FOR PROVIDING AN ADAPTABLE SECURITY LEVEL IN AN ELECTRONIC COMMUNICATION**



(57) **Abrégé/Abstract:**
A method of communicating in a secure communication system, comprises the steps of assembling a message at a sender, then determining a frame type, and including an indication of the frame type in a header of the message. The message is then sent to a recipient and the frame type used to perform a policy check.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2007 (25.10.2007)

PCT

(10) International Publication Number
WO 2007/118307 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/30* (2006.01)
H04L 12/54 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/CA2007/000608

(22) International Filing Date: 13 April 2007 (13.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/791,434 13 April 2006 (13.04.2006) US

(71) Applicant *(for all designated States except US)*: **CERTICOM CORP.** [CA/CA]; 5520 Explorer Drive, 4th Floor, Mississauga, Ontario L4W 5L1 (CA).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **STRUIK, Marinus** [NL/CA]; 723 Carlaw Avenue, Toronto, Ontario M4K 3K8 (CA).

(74) Agents: **SLANEY, Brett J.** et al.; Blake, Cassels & Graydon LLP, 199 Bay Street, Suite 2800, Commerce Court West, Toronto, Ontario M5L 1A9 (CA).

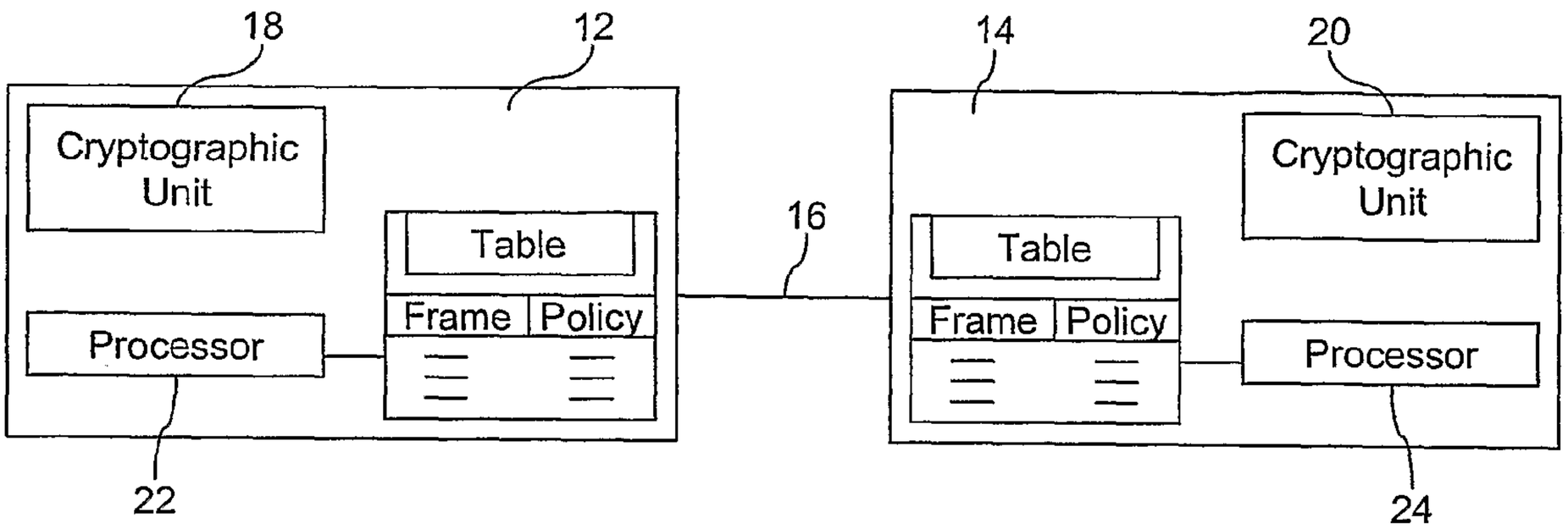
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

(54) Title: METHOD AND APPARATUS FOR PROVIDING AN ADAPTABLE SECURITY LEVEL IN AN ELECTRONIC COMMUNICATION



(57) Abstract: A method of communicating in a secure communication system, comprises the steps of assembling a message at a sender, then determining a frame type, and including an indication of the frame type in a header of the message. The message is then sent to a recipient and the frame type used to perform a policy check.

WO 2007/118307 A1

METHOD AND APPARATUS FOR PROVIDING AN ADAPTABLE SECURITY LEVEL IN AN ELECTRONIC COMMUNICATION

FIELD OF THE INVENTION

[0001] The present invention relates to a method and apparatus for providing an adaptable security level in an electronic communication.

DESCRIPTION OF THE PRIOR ART

[0002] In electronic communications, it is often necessary to prevent an eavesdropper from intercepting a message. It is also desirable to have an indication of the authenticity of a message, that is a verifiable identification of the sender. These goals are usually achieved through the use of cryptography. Private key cryptography requires sharing a secret key prior to initiating communications. Public key cryptography is generally preferred as it does not require such a shared secret key. Instead, each correspondent has a key pair including a private key and a public key. The public key may be provided by any convenient means, and does not need to be kept secret.

[0003] There are many variations in cryptographic algorithms, and various parameters that determine the precise implementation. In standards for wireless communications, it has been customary to set these parameters in advance for each frame type. However, this approach limits the flexibility of the parameters.

[0004] When one device is communicating with several other devices, it will often need to establish separate parameters for each communication.

[0005] It is an object of the present invention to obviate or mitigate the above disadvantages.

SUMMARY OF THE INVENTION

[0006] In one aspect, there is provided a method of communicating between a first correspondent and a second correspondent in a data communication system comprising assembling a data stream at said first correspondent, said data stream having at least one frame, said frame having a header and data; incorporating in said header, an indication of a frame type; and forwarding said frame to said second correspondent to enable said second correspondent to determine the acceptability of said frame according to said frame type.

[0007] In another aspect, there is provided a method of verifying a communication between a first correspondent and a second correspondent in a data communication system comprising said second correspondent: receiving from said first correspondent, a frame having a header and data, said header including an indication of a frame type; determining said frame type from said header; and correlating said frame type to a policy to determine if said frame type is acceptable for at least one attribute of said frame.

[0008] In yet another aspect, there is provided a method of communicating between a pair of correspondents in a data communication system comprising exempting one of said pair of correspondents from security rules associated with said communication system to enable said one correspondent to initialize communication with the other of said correspondents.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] An embodiment of the invention will now be described by way of example only with reference to the accompanying drawings in which:

[0010] Figure 1 is a schematic representation of a communication system;

[0011] Figure 2 is a schematic representation of an information frame exchanged in the communication system of Figure 1;

[0012] Figure 3 is a schematic representation of a frame control portion of the frame of Figure 2;

[0013] Figure 4 is a schematic representation of a method performed by a sender in Figure 1;

[0014] Figure 5 is a schematic representation of a method performed by a recipient in Figure 1;

[0015] Figure 6 is a schematic representation of a network protocol used in one embodiment of the communication system;

[0016] Figure 7 is a schematic representation of an embodiment of the communication system;

[0017] Figure 8 is a schematic representation of another embodiment of the communication system.

[0018] Figure 9 is a schematic representation of another frame;

[0019] Figure 10 is a schematic representation of a method performed by a sender using the frame of Figure 9;

[0020] Figure 11 is a schematic representation of a method performed by a recipient using the frame of Figure 9;

[0021] Figure 12 is a schematic representation of another communication system; and

[0022] Figure 13 is a schematic representation of a method performed by a correspondent in Figure 12.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0023] Referring to Figure 1, a communication system 10 includes a pair of correspondents 12, 14 connected by a communication link 16. Each correspondent 12, 14 includes a respective cryptographic unit 18, 20.

[0024] Each correspondent 12, 14 can include a processor 22, 24. Each processor may be coupled to a display and to user input devices, such as a keyboard, mouse, or other suitable devices. If the display is touch sensitive, then the display itself can be employed as the user input device. A computer readable storage medium (not shown) is coupled to each processor 22, 24 for providing instructions to the processor 22, 24 to instruct and/or configure processor 22, 24 to perform steps or algorithms related to the operation of each correspondent 12, 14, as further explained below. The computer readable medium can include hardware and/or software such as, by way of example only, magnetic disks, magnetic tape, optically readable medium such as CD ROM's, and semi-conductor memory such as PCMCIA cards. In each case, the medium may take the form of a portable item such as a small disk, floppy diskette, cassette, or it may take the form of a relatively large or immobile item such as hard disk drive, solid state memory card, or RAM provided in a support system. It should be noted that the above listed example mediums can be used either alone or in combination.

[0025] In order to transfer data between the correspondents 12, 14, a packet stream 30 is assembled at one of the correspondents in accordance with a defined protocol. The packet stream 30 is shown schematically in Figure 2 and is composed of one or more frames each of which has a header 32 and data 34. In some protocols, the packet may itself be organised as a frame with a header 32a and the data 34a consisting of a collection of individual frames. The header 32 is made up of a string of bits and contains control information at specified locations within the bit string.

[0026] Included in each of the headers 32 are security control bits 33, that include a security mode bit 35 and integrity level bits 36,37.

[0027] In this embodiment, security mode bit 35 is used to indicate whether encryption is on or off. Integrity level bits 36 and 37 together are used to indicate which of four integrity levels, such as 0, 32, 64, or 128 bit key size is utilised. The security mode bit 35 may be used to indicate alternative modes of operation, such as, authentication and the number of bits may be increased (or decreased) to accommodate different combinations. It will be recognized that providing security bits in each frame 31 of the stream 30 allows the security level to be on a frame-by-frame basis rather than on the basis of a pair of correspondents, therefore providing greater flexibility in organizing communications.

[0028] In order to provide security, certain minimum security levels may be used. These levels should be decided upon among all of the correspondents through an agreed-upon rule. This rule may be either static or dynamic.

[0029] In operation, the correspondent 12 performs the steps shown in Figure 4 by the numeral 100 to send information to the correspondent 14. First, the correspondent 12 prepares data and a header at step 102. Then it selects the security level at step 104. The security level is determined by considering the minimum security level required by the recipient, the nature of the recipient, and the kind of data being transmitted. If the security level includes encryption, then the correspondent 12 encrypts the data at step 106. If the security level includes authentication, then the correspondent 12 signs the data at step 108. Then the correspondent 12 includes bits indicating the security mode and security level in the frame control at step 110. The correspondent 12 then sends the frame to the correspondent 14 at step 112.

[0030] Upon receiving the frame, the correspondent 14 performs the steps shown in Figure 5 by the numeral 120. The correspondent 14 first receives the frame at step 122. It then extracts the security bits at step 124. If the security mode bit 35 indicates encryption, then the correspondent 14 decrypts the data at step 126. If the security bits indicate authentication, then the correspondent 14 verifies the signature at step 126. Finally, the correspondent 14 checks the security level to ensure it meets predetermined minimum requirements at step 128. If either the encryption or authentication fails, or if the security level does not meet the minimum requirements, then the correspondent 14 rejects the message and, if the encryption and authentication do not fail, and the security level meets the minimum requirements then the message is accepted, at step 130.

[0031] It will be recognized that providing security bits and an adjustable security level provides flexibility in protecting each frame of the communication. It is therefore possible for the sender to decide which frames should be encrypted but not authenticated. Since authentication typically increases the length of a message, this provides a savings in constrained environments when bandwidth is at a premium.

[0032] In a further embodiment, the correspondent 12 wishes to send the same message to multiple recipients 14 with varying minimum security requirements. In this case, the correspondent 12 chooses a security level high enough to meet all of the requirements. The correspondent 12 then proceeds as in Figure 4 to assemble and send a message with the security level. The message will be accepted by each recipient since it meets each of their minimum requirements. It will be recognized that this embodiment provides greater efficiency than separately dealing with each recipient's requirements.

[0033] In another embodiment, a different number of security bits are used. The actual number of bits is not limited to any one value, but rather may be predetermined for any given application. The security bits should indicate the algorithm parameters. They may be used to determine the length of a key as 40 bits or 128 bits, the version of a key to be used, or any other parameters of the encryption system.

[0034] It will be recognized that in the above embodiments, a network stack may be used to organize communications between the correspondents. Referring therefore to Figure 6, the a network stack of correspondent A is shown by the numeral 130. A network stack of correspondent B is shown by the numeral 140. The network stacks are organized into layers and have similar structures. The network stack 130 includes an application layer (APL) 132, a network layer (NWK) 134, a message authentication layer (MAC) 136, and a physical layer (PHY) 138. The network stack 140 includes similar components with similar numbering.

[0035] The sender determines how he wants to protect payload (and where to protect it, i.e., which layer). For the APL layer, security should be transparent; its role is limited to indicating at which level it wants to protect data (i.e., security services: none, confidentiality, data authenticity, or both). The actual cryptographic processing then is delegated to lower layers.

[0036] The recipient determines whether or not to accept protected payload, based on the received frame and locally maintained status information. The outcome of the cryptographic processing (done at the same layer as that of the sender), including info on the apparently

offered protection level, is passed to the application layer, who determines whether the offered protection level was adequate. The recipient may acknowledge proper receipt of the frame to the original sender, based on this `adequacy test`.

[0037] The acknowledgement (ACK), if present, is then passed back to the sender and passed up to the appropriate level (if protected message sent at APL layer, then ACK should also arrive back at that level; similar for lower layers of course).

[0038] The sender A determines that it wants to protect payload m using the protection level indicated by SEC (taking into account its own security needs and, possibly, those of its intended recipient(s). The payload m and desired protection level SEC is then passed to a lower layer (e.g., the MAC layer, as in the diagram) which takes care of the actual cryptographic processing. (This message passing could include additional status information that aids in the processing of the frame, such as the intended recipient(s), fragmentation info, etc. Note that the delegation of the cryptographic processing to a lower layer is only a conceptual step if cryptographic processing takes place at the same layer at which the payload m originates.)

[0039] Cryptographic processing involves protecting the payload m and, possibly, associated information such as frame headers, using the cryptographic process indicated by the desired protection level SEC. The key used to protect this information is derived from shared keying material maintained between the sender and the intended recipient(s). After cryptographic processing, the protected frame, indicated by [m]K, SEC in Figure 6, is communicated to the intended recipient(s) B.

[0040] The intended recipient (s) retrieves the payload m' from the received protected frame, using the cryptographic process indicated by the observed protection level SEC', using a key that is derived from shared keying material maintained between the sender and the recipient(s) in question. The retrieved payload m' and the observed protection level SEC' is passed to the same level at which the payload was originated by the sender, where the adequacy of the observed protection level is determined. The observed protection level SEC' is deemed sufficient, if it meets or exceeds the expected protection level SEC_0, where the parameter SEC_0 might be a fixed pre-negotiated protection level that does or does not depend on the retrieved payload m' in question. (Defining SEC_0 in a message-dependent way would allow fine-grained access control policies, but generally involves increased storage and processing requirements.)

[0041] The above approach works in contexts where expected and observed protection levels can be compared, e.g., where the set of protection levels is a partial ordering or where a membership test is performed (one of a set of protection levels). One example is the context where protection involves a combination of encryption and/or authentication, with as ordering the Cartesian product of the natural ordering for encryption (encryption OFF<Encryption ON) and the natural ordering of authentication (ordered according to increasing length of data authenticity field). Moreover, if the set of protection levels has a maximum element, then the sender can use this maximum protection level to ensure that (unaltered) messages always pass the adequacy test. In another example, the observed protection level is compared to SEC_0, where SEC_0 is a set of protection levels rather than only a minimum security level. In this way, if SEC0 = {None, Auth-32, Auth-64, Auth-128} and SEC=Auth-32, then the adequacy test would pass, whereas if SEC0 is the same as above and SEC=Auth-32 + Confidentiality (e.g. encryption), then the adequacy test would fail.

[0042] In the above embodiments, each sender pre-negotiates the minimum expected protection level SEC_0 with each intended recipient. Thus, the approach might not be as adaptive as desirable for some applications and may involve additional protocol overhead at every change of the SEC_0 parameter. These disadvantages can be overcome by using the acknowledgement (ACK) mechanism from recipient(s) to sender as a feedback channel for passing the SEC_0 info. This is performed by incorporating in each acknowledgement message an indication as to the expected protection level. This information can then be collated by the original sender to update the minimum protection level expected by its recipient(s), whether or not this is message-dependent or not.

[0043] In a further embodiment, a method of synchronizing security levels is shown. Referring to Figure 7, another embodiment of the communication system is shown.

The system includes a sender A 162 and recipients 168 in a group labelled G. The sender A includes parameters SEC_A 164 and SEC_G 166.

[0044] Sender A wants to securely communicate a message m to a group G of devices. The sender A has access to the two parameters, e.g., (1) The minimum level SEC_A at which it would like to protect this message (in general, SEC_A might depend on the group it sends information to and the message itself, so proper notation would be SEC_A (m,G)); (2) The minimum protection level SEC_G that the group G of recipients expects (again, the proper notation would be SEC_G(m,A) if this level would depend on the sender and the message itself

as well). Here, the minimum expectation level of a group is the maximum over all group members of the minimum expectation level for each group member.

[0045] Initialization:

[0046] Sender A assumes that each parameter SEC_G is set to the maximum protection level (for each group G it securely communicates with).

[0047] Operational Usage:

[0048] Sender A determines the minimum protection level SEC_A at which it wants to protect the message m. The actual protection level SEC applied to the message m meets both its own adequacy test (i.e., $SEC \geq SEC_A$) and the minimum expected level by the group G (i.e., $SEC \geq SEC_G$).

[0049] Each recipient B that is in the group G of recipients (i.e., $B \in G$) indicates in its secure acknowledgement message the minimum expected protection level (for sender A and message m) at that particular moment of time.

[0050] A updates the parameter SEC_G such that it is consistent with all the minimum protection levels indicated in each of the acknowledgement messages it received back (i.e., $SEC_G \geq SEC_B$ for all responding devices B).

[0051] Note that the procedure described above sends messages with a protection level that satisfies both the needs of the sender and expectations of recipient(s) and is adaptable to changes herein over time. Alternatively, the sender might only take its own protection needs into account, at the cost of potentially sending messages that will be rejected by one or more recipients due to insufficient--since less than expected--protection level.

[0052] The procedure described above can be generalized towards a general self-synchronization procedure for status information among devices in any network topology, where the feedback info on status information may be partially processed along the feedback path from recipient(s) towards sender already, rather than at the sender itself only (in the example above, this graph is a tree with root A and leaves the recipient(s) and the synchronization involves a specific security parameter).

[0053] As seen in Figure 8, A sends a payload secured at protection level SEC to a group of devices consisting of B1-B4. The recipients B1-B4 provide feedback to the sender A on the expected protection level (indicated in the diagram as the integers 1, 3, 2, 5, where these integers are numbered in order of increasing protection level). The feedback is communicated back to A via intermediate nodes C1 and C2, who collect the respective feedbacks of devices

in their respective groups G1 and G2 and process this, before returning a condensed acknowledge message representing both groups to sender A. The condensed feedbacks provided by these intermediate devices provides A with the same information on the minimum protection level that satisfies the expectations of all recipients as would have been the case if this information would have been forwarded to A without intermediate processing. (Here, we assume that the intermediate devices do not cheat in their calculations)

[0054] In another embodiment, each frame in the communication is structured as shown in Figure 9 and is generally denoted by numeral 170. The frame 170 generally comprises a header 172, a payload 174 and a footer 176. The footer 176 typically comprises one or more bits that represent an error code. The payload 174 includes the data which is to be sent in that particular frame 170, e.g. a message.

[0055] An exemplary header 172a is also shown in greater detail in Figure 9. The header 172a includes a key identifier 178, a representation of a key 180, a frame type 182, a security level 184 (as before) and an indication of the originator 186 of the message, e.g. the sender 12.

[0056] Each portion of header 172a contains one or more bits that represents a certain attribute of the transmission or includes a piece of information. The key identifier 178 and the representation of the key 180 are typically used to determine not only what key is to be used but also how the key is to be used, e.g. for broadcast or unicast communications.

[0057] The frame type 182 provides an indication as to what type of transmission is being sent in that particular frame 172a. Typical frame types 182 include data, command, acknowledgement and beacon frames. Data-type frames transmit data, command-type frames transmit commands, acknowledgement-type frames transmit information back to a sender, e.g., an acknowledgement from the recipient that a frame has been properly received, and beacon frames are typically used to divide a transmission into time intervals.

[0058] In order to provide security, in addition to providing a minimum security level for the recipient 14, the sender 12 includes the frame type 182 in the header 172a. The frame type 182 is used by the recipient 14 to perform a policy check to determine if the security level, key, key usage, etc. are appropriate for the type of frame being transmitted. For example, inadequate security for a frame type that should normally include high security would be rejected.

[0059] In operation, the sender 12 performs the steps shown in Figure 10 by the numeral 200 to send information to the recipient 14. First, the sender 12 prepares the frame at step 202 according to steps 102-110 discussed above. It will be appreciated that these steps would also include preparation of the header 172a to include the representation of the bits shown in Figure 9. At step 204, the sender 12 determines the frame type 182 and includes one or more bits into the header 172a to indicate the frame type 182. The sender 12 then sends the frame 170 to the recipient 14 at step 206.

[0060] Upon receiving the frame 170, the recipient 14 performs the steps shown in Figure 11 by the numeral 208. The recipient 14 first receives the frame at step 210 and then performs the steps 124-126 discussed above at step 212. The recipient 14 then extracts the frame type 182 from the header 172a at step 214. The frame type 182 is then correlated to a policy in order to perform a policy check at step 216. In particular, a look-up-table is accessed by the recipient that indicates one or more policy for each frame type. The recipient 14 then determines if the policy is met at step 218 and either rejects or accepts the frame 170 at step 220 based on whether or not the policy is met.

[0061] The policy check includes a correlation of the frame type 182 to some other data, preferably something included in the frame. For example, the policy may include certain correlations between key types and frame types such that based on the representation of the key 160 the frame is accepted or rejected depending on whether or not the key is acceptable for use with the particular frame type 182. In the result, a certain type of key (or key usage) is required in order for the policy to be met. If the key is not of the correct type, then the frame 170 is not accepted by the recipient 14. If a single header 32a is used for multiple frames 34a as shown in Figure 2 then the policy will also apply to the remaining frames in the message.

[0062] In another example, the policy is set based on the security level 184 that is included in the frame 170, e.g. minimum security level SEC_0 discussed above. The frame 170 includes a certain minimum security level that has been included at the time when the header 172 is prepared by the sender 12, and this minimum security level is correlated to the particular frame type 162. If the security level 184 is suitable for the frame type 162 then the frame 170 is passed by the recipient at step 220 and if not it is rejected. It will be appreciated that the policy can be adapted to correlate any suitable information included in the frame with the frame type 182.

[0063] The above principles enable security checks to be adapted to various messages, frame types etc. in order to protect against combinations of security features that are more prone to an attack. For example, a policy can cause a recipient to reject a frame for using no encryption and only authentication, when that frame type is particularly vulnerable to an attack when encryption is not used.

[0064] In general there are three security level checks that possess different levels of granularity. The first is where SEC_0 is message independent. In this case, the minimum level of security is set once, and only one value needs to be stored locally for performing a policy check. However, where SEC_0 is message independent, a minimum granularity is provided since there is only one minimum security level for all messages and message types.

[0065] The second is where SEC_0 is completely message-dependent. In this case, a high level of granularity is provided since each message has its own minimum security level. However, this requires an enumeration of all messages and corresponding minimum security levels to be stored locally in a table.

[0066] The third is where SEC_0 is partially message dependent, namely, as discussed making reference to Figures 9-11, messages are divided into different types (e.g. by frame type) and, a minimum security level is allocated to each message type. This case balances the competing space requirements and granularity of performing a policy check based on the minimum security level. Typically, the number of frame types is significantly less than the number of messages and thus more feasible to implement in a table.

[0067] In another embodiment shown in Figure 12 a network N comprises one or more correspondents (e.g. A, B) communicating through a central correspondent C. Correspondent A communicates over the network N by transmitting frames to the central correspondent C using, e.g., any of the principles described above. When correspondent A first wishes to engage the network N, they do not have a key and thus cannot be authenticated to communicate in the network N. The general steps for an initialization procedure are shown in Figure 13. The correspondent C first obtains an indication that A wishes to join the network N at step 224. This indication can be provided through a suitable registration procedure. Correspondent C then includes A in a table that indicates its status, and sets the status for correspondent A to "Exempt" at step 226. The exempt status takes into account that an initialization procedure is required so that correspondent A can communicate unsecurely until it has been initialized in the network N.

[0068] At step 228, correspondent A sends a frame to central correspondent C. Correspondent C checks the table at step 230. In this first communication, the status of correspondent A is exempt and a key exchange or other initialization procedure is carried out at step 232 and the status of correspondent A is then changed to "not exempt" (or an exempt indicator is removed, set to zero etc.) at step 234. Correspondent A then sends frames to correspondent C subject to normal security rules. At step 230 the status for correspondent A would thereafter be determined as not exempt and the regular security rules are applied at step 236, e.g. by checking the security level, frame type etc. It can be appreciated that A could also exempt C such that the roles are reversed and A is allowing C to communicate therewith (e.g. where A is part of another network).

[0069] In an example implementation of the network N shown in Figure 12, the above minimum security level test takes into account the frame and also the originator 186. In this case, the sender is correspondent A and the recipient is correspondent B. A check for the minimum security level would thus be $SEC \geq SEC_B(m,A)$. If the minimum security level is independent of originator A, this comes down to check $SEC \geq SEC_B(m)$, as discussed before. The same storage considerations as with original security level test would then be used (case 1).

[0070] If the minimum security level is completely dependent on the originator A, a minimum security level table is enumerated (dependent on frame *m*, frame type of *m*, or message dependent – as discussed before), but now for each originator (case 2). If the minimum security level is independent of originator A, except when originator is in an explicitly enumerated set of exempt devices, e.g. denoted by ExemptSet in the table, a single minimum security level table is implemented for devices outside the ExemptSet (potentially depending on frame type, etc.) and, additionally, a minimum security level table for each individual member of ExemptSet is implemented (case 3). Thus, if a correspondent (and device associated therewith) is part of the ExemptSet table, case 2 is utilized and, if no device is in the ExemptSet table, case 1 is utilized.

[0071] Case 3 can be made more implementation-friendly if correspondents in the ExemptSet table, a minimum security level table that is independent of the particular device in the ExemptSet is used. This requires that one security level table is implemented for devices that are not in the ExemptSet table and one table is implemented for devices that are in the ExemptSet table (case 4).

[0072] A further optimization of case 4 is where, for all devices in the ExemptSet table, the minimum security level – which is potentially message or message type dependent (as discussed before) – is either set to the minimum security level that holds for all devices that are outside ExemptSet or is set to a prespecified value that may hold for all devices inside ExemptSet. Since this would lead to only two choices (e.g. per frame, frame type, overall), this can be indicated using a Boolean parameter.

[0073] In summary:

[0074] $SEC \geq SEC_B(m,A))$, where

- $SEC_B(m,A) = SEC_B(m)$ if A is not a member of ExemptSet.
- $SEC_B(m,A) = SEC_B(m)$ if A is a member of ExemptSet and Override parameter *OverrideSEC(m)* for message *m* is set to FALSE.
- $SEC_B(m,A) = ExemptSEC_B(m)$ if A is a member of ExemptSet and Override parameter *OverrideSEC(m)* for message *m* is set to TRUE.

[0075] In general, the most practical scenario is where $ExemptSEC_B(m)$ is set to 'no security'.

[0076] It is noted that one scenario allows devices that do not have a key yet (e.g., because these just joined the network and still have to set up a key, e.g., via key agreement or key transport protocol or PIN or any other mechanism) to "by-pass" the minimum security level check (i.e., the security check always succeeds), if these have been labeled by recipient B as belonging to ExemptSet (and $ExemptSEC_B(m)$ is set to 'no security').

[0077] The by-passing of minimum security level checks may depend on the message *m* received, the frame type of message *m* (which is visible to the recipient if the frame type of *m* is included in the transmitted frame – normally frame types and other frame control information is not encrypted), or a parameter that can be set via the Override parameter *OverrideSEC(m)*.

[0078] It is also noted that operations on the set ExemptSet by the recipient effectively govern the operation of the minimum security level check (inclusion of a device in that set may allow by-passing or lowered security requirements, while exclusion of a device from that set restores the ordinary minimum security level check and make it applicable (possibly again) to the originating device in question).

[0079] Thus, the above allows a flexible mechanism to take into account transitionary behaviour of a correspondent (and their device) during the system's lifetime, and facilitates the transgression of a device from some initial stage where it does not yet have a key, to the

stage where it has established a key and can be enforced to adhere to normal strict minimum security level policies.

[0080] The override parameter *OverrideSEC(m)* allows fine-tuning of "by-passing" the minimum security level check and make this dependent on the message *m* received (or message type – obviously one can make granularity as fine-grained as possible, at expense of table implementation cost). As an example, in the scenario where a device joins a network and still has to set up a key, one could set the Override parameter to TRUE only for those messages or message types minimally required for the originating device A to set up a key with the recipient device B (or with some other device T in the network that could notify B once the key has been established), thus restricting the permissible behavior of device A, but not ruling out all behaviors. This can also be used for any other initialization procedure or set-up procedure and should not be limited to key set up.

[0081] Again, operations on the Override parameter *Override(m)* by the recipient B allow for a very flexible and low-cost fine-tuning of security control policies. As an example, by setting all Override parameters to FALSE, one effectively closes down all network operations to devices that do not have a key (since all cryptographically unsecured messages to recipient B will ultimately be rejected) – the so-called stealth mode – while setting all Override parameters to TRUE allows unlimited flows of unsecured information to device B, since this may result in the minimum security level test to be effectively by-passed.

[0082] It will be recognized that the security rules can be adapted to provide flexibility not only on a frame-by-frame basis but also based on the frame type such that a policy check can determine if certain security rules or key types can be used with a particular frame type.

[0083] Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the scope of the invention as outlined in the claims appended hereto.

What is claimed is:

1. A method comprising:

a communication device preparing a plurality of frames, each frame having a header, data, and a plurality of security features;

on a frame-by-frame basis, said communication device processing each frame by:

determining a frame type of that frame based on a type of transmission being sent in that frame, wherein a policy indicates appropriate security features for said frame type; and

including frame type data in said header of that frame, the frame type data indicating, based on said frame type, the type of transmission;

wherein said frame type is one of a plurality of predetermined frame types, the plurality of predetermined frame types includes two or more of data-type, command-type, acknowledgement-type, and beacon-type, said header includes a representation of a key and an indication of a security level, and said policy indicates an acceptable frame type for said key, and said policy indicates an acceptable frame type for said security level; and

providing each said frame with said appropriate security features; and

said communication device providing the plurality of frames for transmission.

2. The method according to claim 1, wherein the communication device provides the plurality of frames for transmission to at least one recipient device, the policy comprises a policy of said at least one recipient device, and the method further comprises said at least one recipient device:

receiving the plurality of frames;

for each frame, determining said frame type from said header of that frame; and

for each frame, comparing said frame type to said policy to determine if said frame type is acceptable for said plurality of security features.

3. The method according to claim 2 further comprising accepting said frame if said policy is met, and rejecting said frame otherwise.

4. The method according to claim 2 or claim 3 wherein said policy indicates frame types vulnerable to an attack where one or more combinations of security features of said frame are present, said method comprising rejecting said frame if one of said combinations is found.

5. The method according to any one of claims 2 to 4 further comprising said at least one recipient device using said indication of said security level to determine said security level for each frame.

6. The method according to any one of claims 1 to 5 wherein said indication of said security level for that frame comprises one or more security bits.

7. The method according to claim 6 further comprising encrypting said data of that frame according to said security level.

8. The method according to claim 7, further comprising said at least one recipient device decrypting said data for that frame.

9. The method according to any one of claims 6 to 8, further comprising signing said data of that frame according to said security level.

10. The method according to claim 9, further comprising said at least one recipient device authenticating said data for that frame.

11. The method according to any one of claims 1 to 10 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is independent of said data of that frame.

12. The method according to any one of claims 1 to 10 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is dependent on said data of that frame.

13. The method according to any one of claims 1 to 10 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is partially data dependent such that said minimum acceptable security level can differ according to said frame type for that frame.

14. The method according to any one of claims 2 to 13 wherein said policy comprises a look up table correlating frame types to attributes of said plurality of frames.

15. The method according to any one of claims 1 to 14 wherein each frame comprises a footer having one or more bits representing an error code.

16. The method according to any one of claims 1 to 15 wherein said header for that frame comprises a key identifier, the representation of a key corresponding to said key identifier, the security level, and an originator, for determining acceptability of said frame type.

17. A system comprising a communication device that is operable to perform operations comprising:

preparing a plurality of frames, each frame having a header, data, and a plurality of security features;

on a frame-by-frame basis, said communication device processing each frame by:

determining a frame type of that frame based on a type of transmission being sent in that frame, wherein a policy indicates appropriate security features for said frame type; and

including frame type data in said header of that frame, the frame type data indicating, based on said frame type, the type of transmission;

wherein said frame type is one of a plurality of predetermined frame types, the plurality of predetermined frame types includes two or more of data-type, command-type,

acknowledgement-type, and beacon-type, said header includes a representation of a key and an indication of a security level, and said policy indicates an acceptable frame type for said key, and said policy indicates an acceptable frame type for said security level; and

providing each said frame with said appropriate security features; and

providing the plurality of frames for transmission.

18. The system according to claim 17, further comprising at least one recipient device, wherein the communication device provides the plurality of frames for transmission to said at least one recipient device, the policy comprises a policy of said at least one recipient device, and said at least one recipient device is operable to perform operations comprising:

receiving the plurality of frames;

for each frame, determining said frame type from said header of that frame; and

for each frame, comparing said frame type to said policy to determine if said frame type is appropriate for said plurality of security features.

19. The system according to claim 18, said at least one recipient device operable to perform operations further comprising accepting said frame if said policy is met, and rejecting said frame otherwise.

20. The system according to claim 18 or claim 19 wherein said policy indicates frame types vulnerable to an attack where one or more combinations of security features of said frame are present, said at least one recipient device operable to perform operations further comprising rejecting that frame if one of said combinations is found.

21. The system according to any one of claims 18 to 20, wherein said at least one recipient device is operable to perform operations further comprising using said indication of said security level to determine said security level.

22. The system according to any one of claims 18 to 21, wherein said indication of said security level for that frame comprises one or more security bits.

23. The system according to claim 22, wherein said at least one recipient device is operable to encrypt said data of that frame, according to said security level.

24. The system according to claim 23 wherein said at least one recipient device is operable to decrypt said data for that frame.

25. The system according to any one of claims 22 to 24, wherein said at least one recipient device is operable to sign said data of that frame, according to said security level.

26. The system according to any one of claims 25, wherein said at least one recipient device is operable to authenticate said data for that frame.

27. The system according to any one of claim 17 to 26 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is independent of said data of that frame.

28. The system according to any one of claim 17 to 26 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is dependent on said data of that frame.

29. The system according to any one of claim 17 to 26 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is partially data dependent such that said minimum acceptable security level can differ according to said frame type for that frame.

30. The system according to any one of claims 18 to 29 wherein said policy comprises a look up table correlating frame types to attributes of said plurality of frames.

31. The system according to any one of claims 17 to 30 wherein each frame further comprises a footer comprising one or more bits representing an error code.

32. The system according to any one of claims 17 to 31 wherein said header for that frame comprises a key identifier, the representation of a key corresponding to said key identifier, the security level, and an originator, for determining acceptability of said frame type of that frame.

33. A computer readable medium comprising computer executable instructions that are operable to cause a communication device to perform operations comprising:

preparing a plurality of frames, each frame having a header, data, and a plurality of security features;

on a frame-by-frame basis, said communication device processing each frame by:

determining a frame type of that frame based on a type of transmission being sent in that frame, wherein a policy indicates appropriate security features for said frame type; and

including frame type data in said header of that frame, the frame type data indicating, based on said frame type, the type of transmission;

wherein said frame type is one of a plurality of predetermined frame types, the plurality of predetermined frame types includes two or more of data-type, command-type, acknowledgement-type, and beacon-type, said header includes a representation of a key and an indication of a security level, and said policy indicates an acceptable frame type for said key, and said policy indicates an acceptable frame type for said security level; and

providing each said frame with said appropriate security features; and

providing the plurality of frames for transmission.

34. The computer readable medium according to claim 33, wherein the communication device provides the plurality of frames for transmission to at least one recipient device, the policy comprises a policy of said at least one recipient device, and the computer readable medium further comprising instructions executed by said at least one recipient device to cause said at least one recipient device to perform operations comprising:

receiving the plurality of frames;

for each frame, determining said frame type from said header of that frame; and

for each frame, comparing said frame type to said policy to determine if said frame type is appropriate for said plurality of security features.

35. The computer readable medium according to claim 34, the operations performed by the at least one recipient device further comprising accepting said frame if said policy is met, and rejecting said frame otherwise.

36. The computer readable medium according to claim 34 or claim 35 wherein said policy indicates frame types vulnerable to an attack where one or more combinations of security features of said frame are present, said operations performed by the at least one recipient device further comprising rejecting said frame if one of said combinations is found.

37. The computer readable medium according to any one of claims 34 to 36, said operations performed by the at least one recipient device further comprising using said indication of said security level to determine said security level for each frame.

38. The computer readable medium according to any one of claims 33 to 37 wherein said indication of said security level for that frame comprises one or more security bits.

39. The computer readable medium according to claim 38 further comprising encrypting said data of that frame, according to said security level.

40. The computer readable medium according to claim 39, said operations performed by the at least one recipient device further comprising decrypting said data for that frame.

41. The computer readable medium according to any one of claims 38 to 40, further comprising signing said data of that frame, according to said security level.

42. The computer readable medium according to claim 41, said operations performed by the at least one recipient device further comprising authenticating said data for that frame.

43. The computer readable medium according to any one of claims 33 to 42 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is independent of said data of that frame.

44. The computer readable medium according to any one of claims 33 to 42 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is dependent on said data of that frame.

45. The computer readable medium according to any one of claims 33 to 42 wherein said security level provides an indication of a minimum acceptable security level, wherein said minimum acceptable security level is partially data dependent such that said minimum acceptable security level can differ according to said frame type for that frame.

46. The computer readable medium according to any one of claims 34 to 45 wherein said policy comprises a look up table correlating frame types to attributes of said plurality of frames.

47. The computer readable medium according to any one of claims 33 to 46 wherein each frame comprises a footer having one or more bits representing an error code.

48. The computer readable medium according to any one of claims 33 to 47 wherein said header for that frame comprises a key identifier, the representation of a key corresponding to said key identifier, the security level, and an originator, for determining acceptability of said frame type.

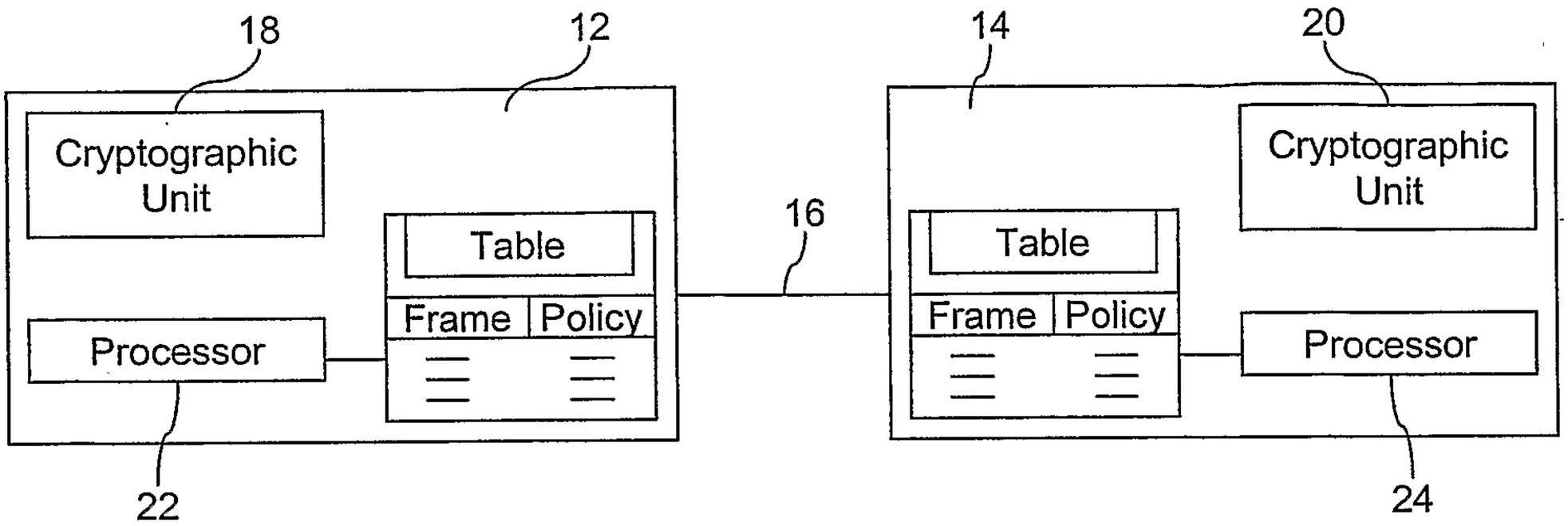


Figure 1

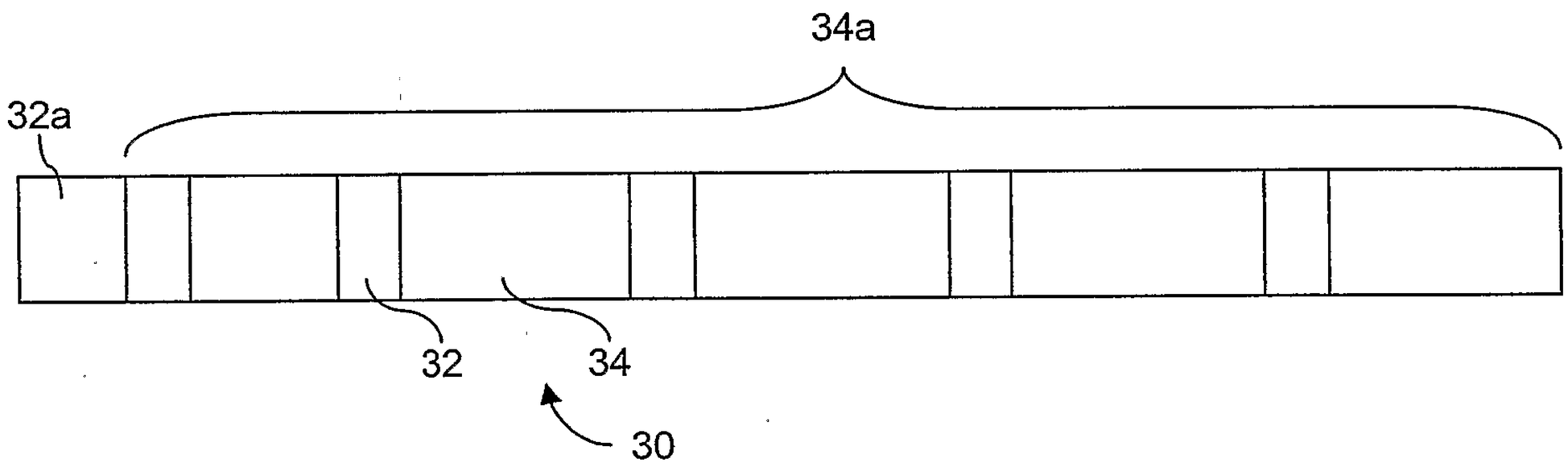


Figure 2

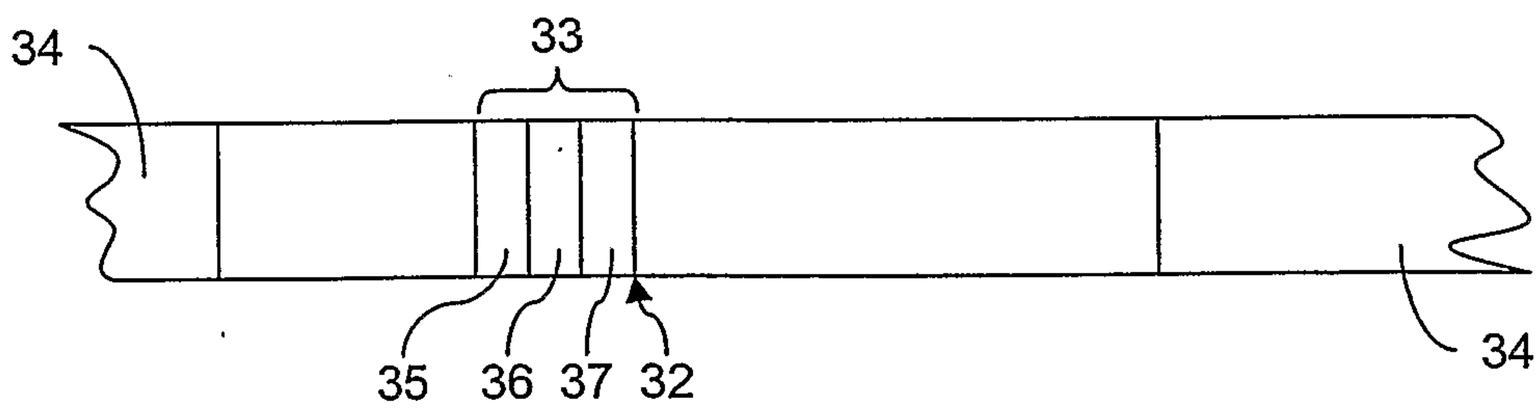


Figure 3

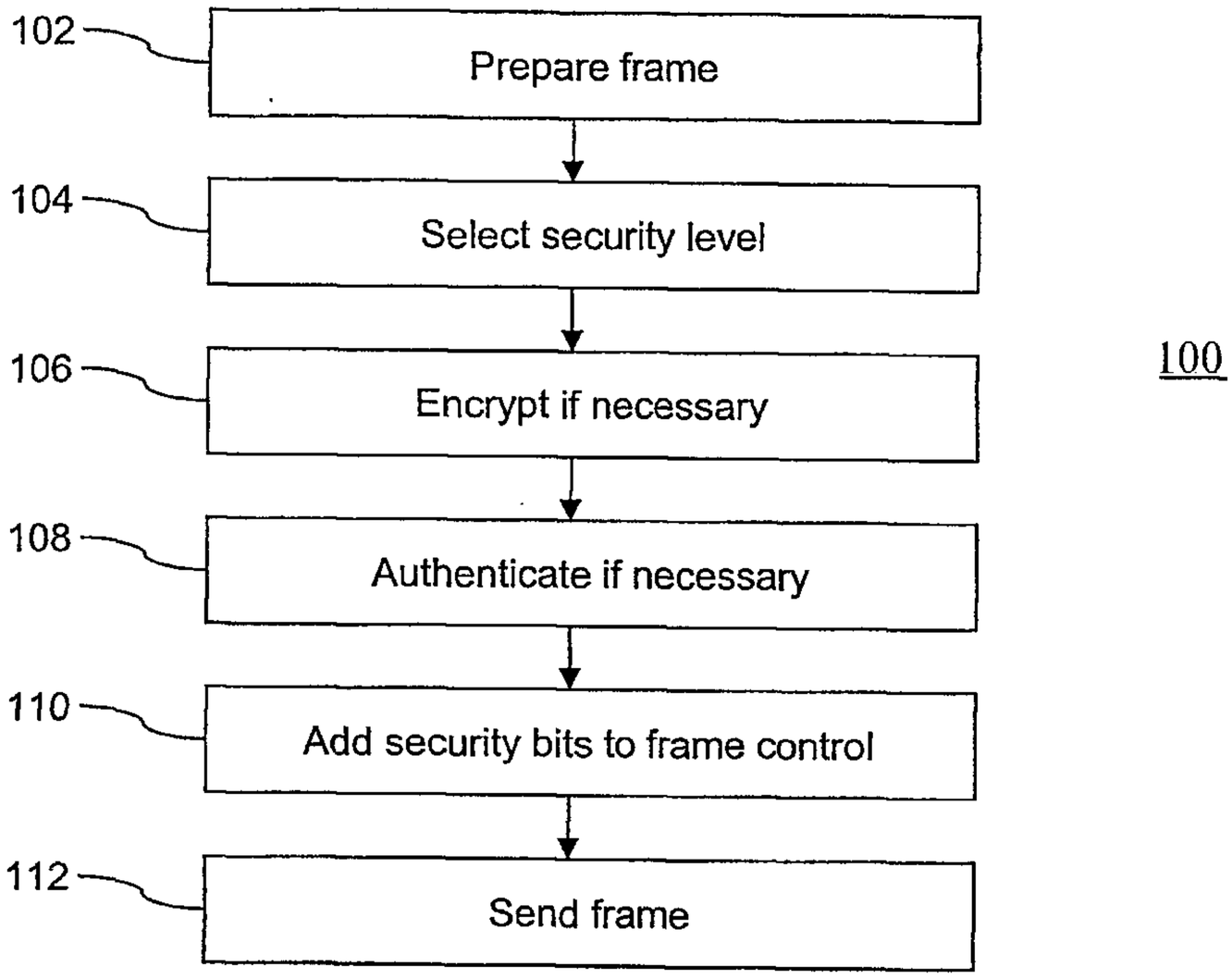

102
Prepare frame
104
Select security level
106
Encrypt if necessary
108
Authenticate if necessary
110
Add security bits to frame control
112
Send frame
100

Figure 4

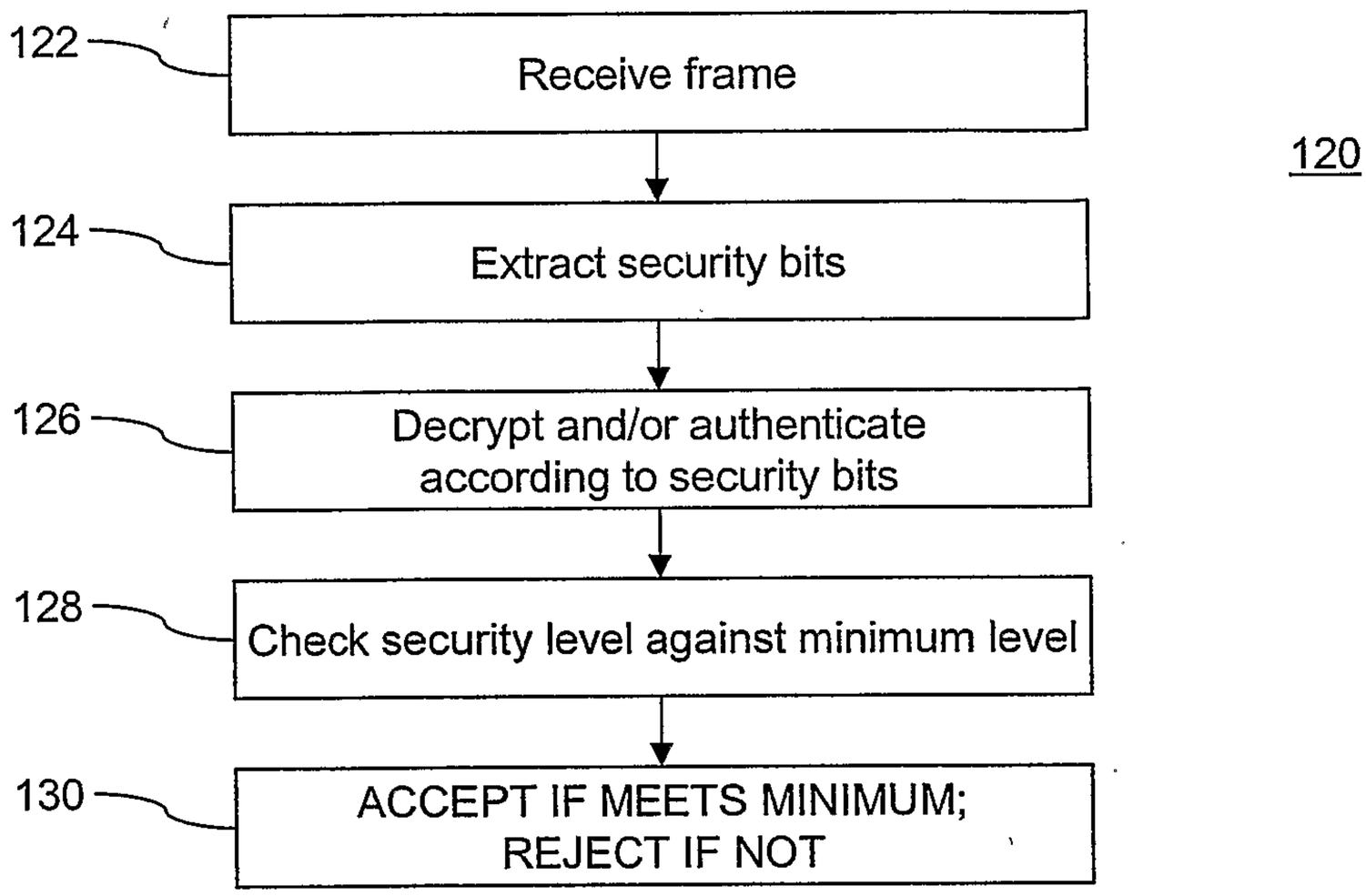

122
Receive frame
120
124
Extract security bits
126
Decrypt and/or authenticate according to security bits
128
Check security level against minimum level
130
ACCEPT IF MEETS MINIMUM; REJECT IF NOT

Figure 5

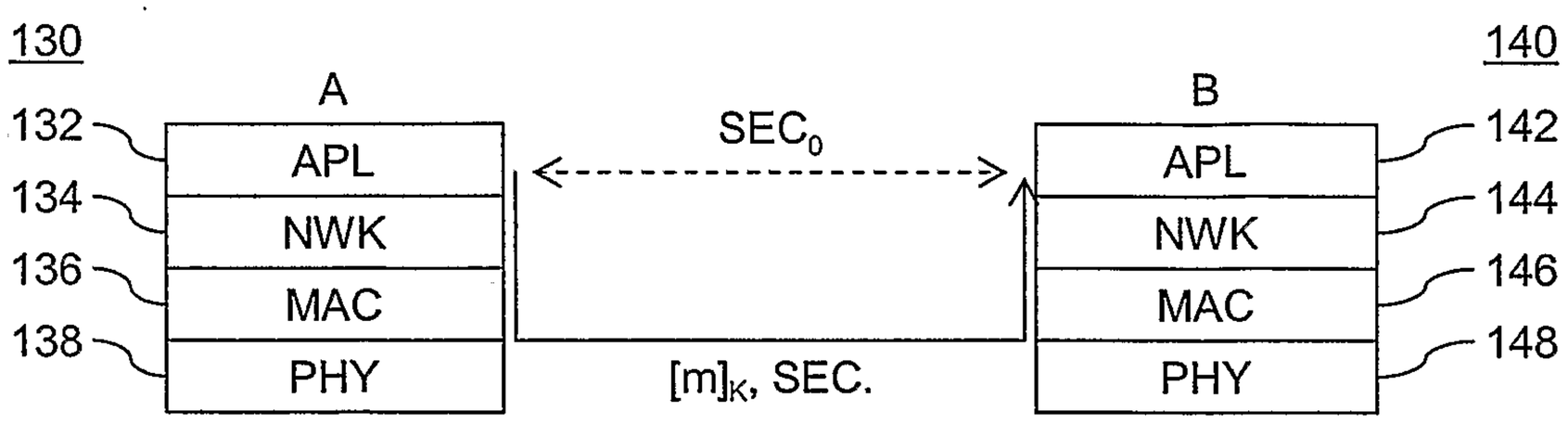


Figure 6

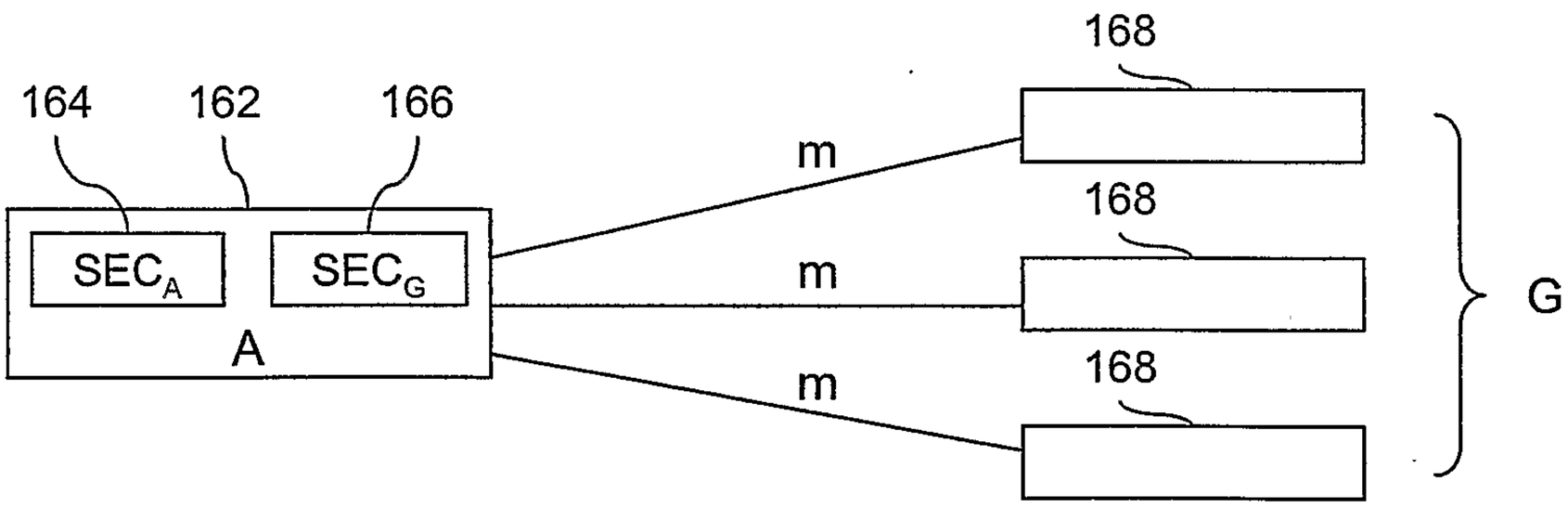


Figure 7

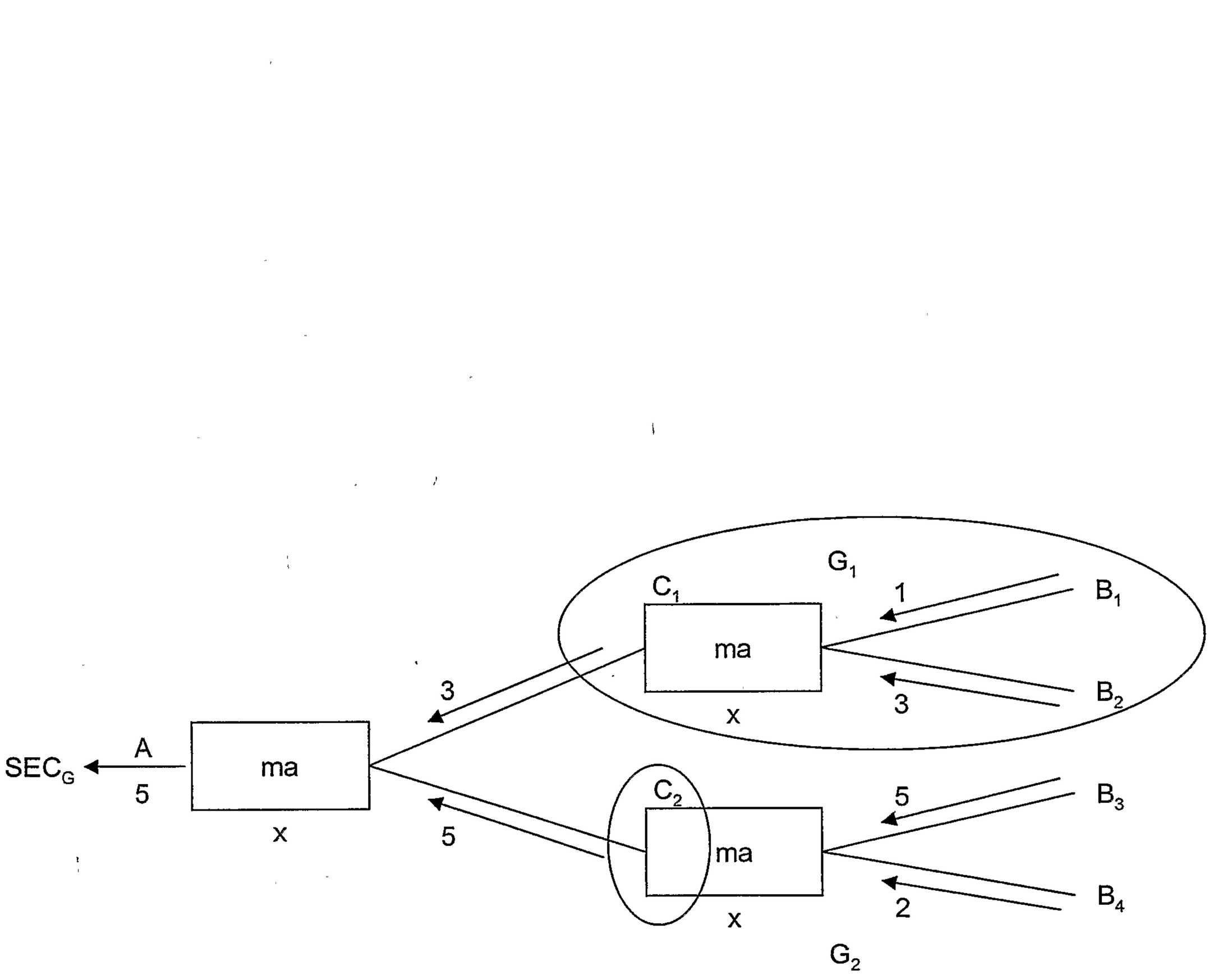


Figure 8

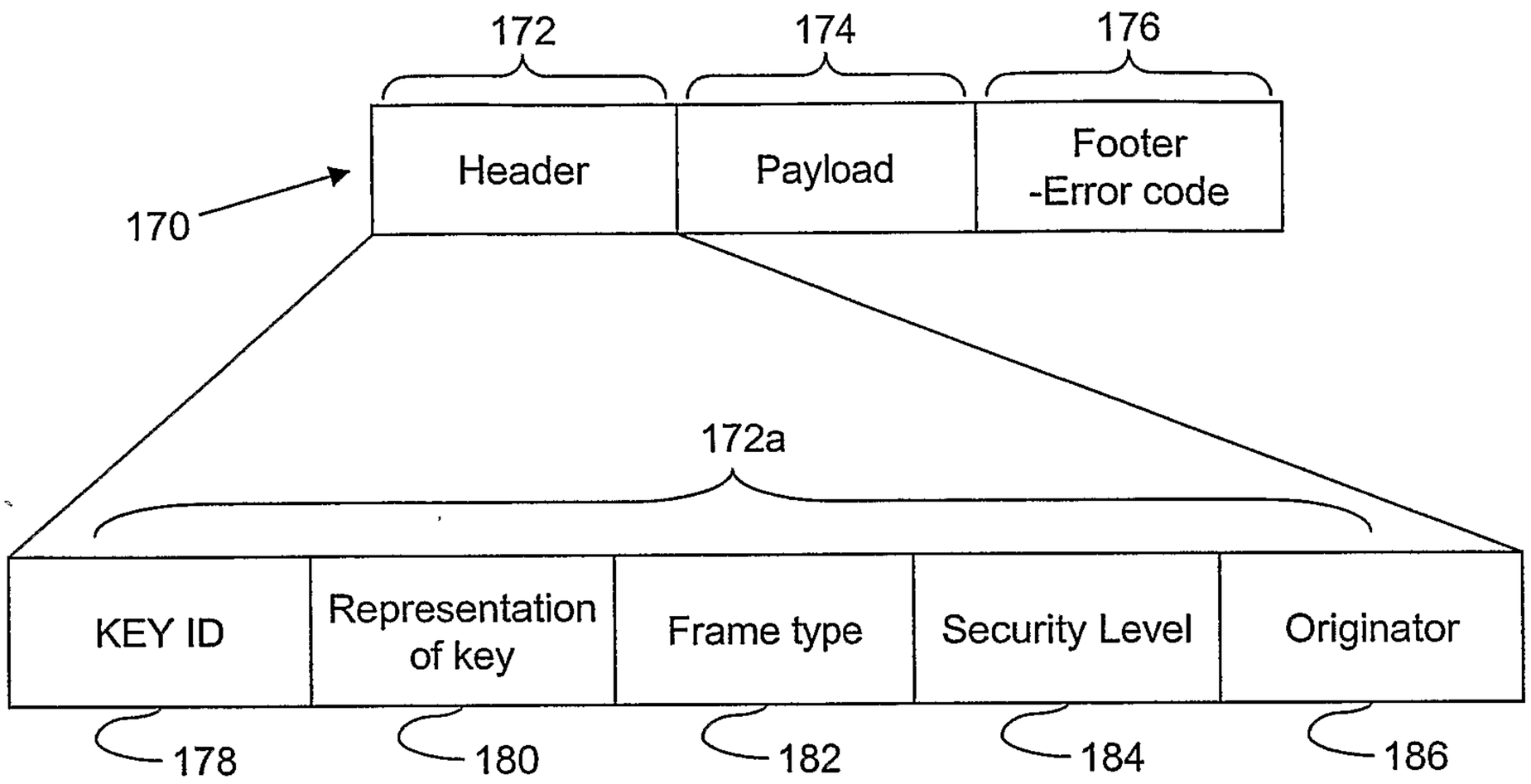


Figure 9

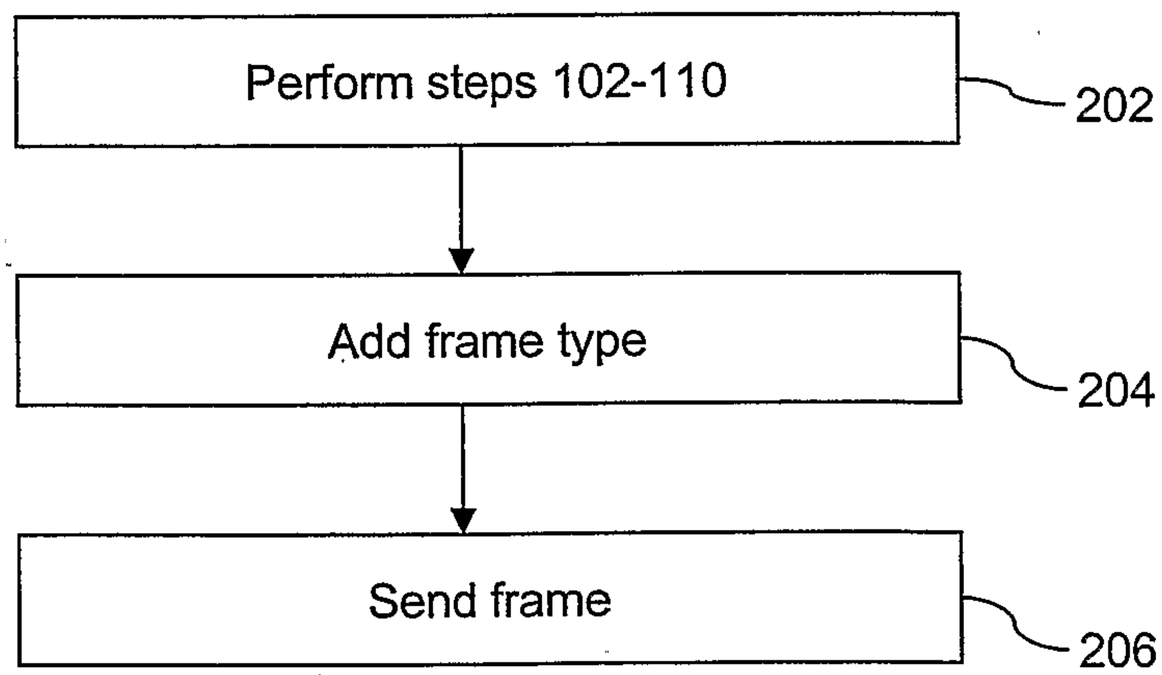


Figure 10

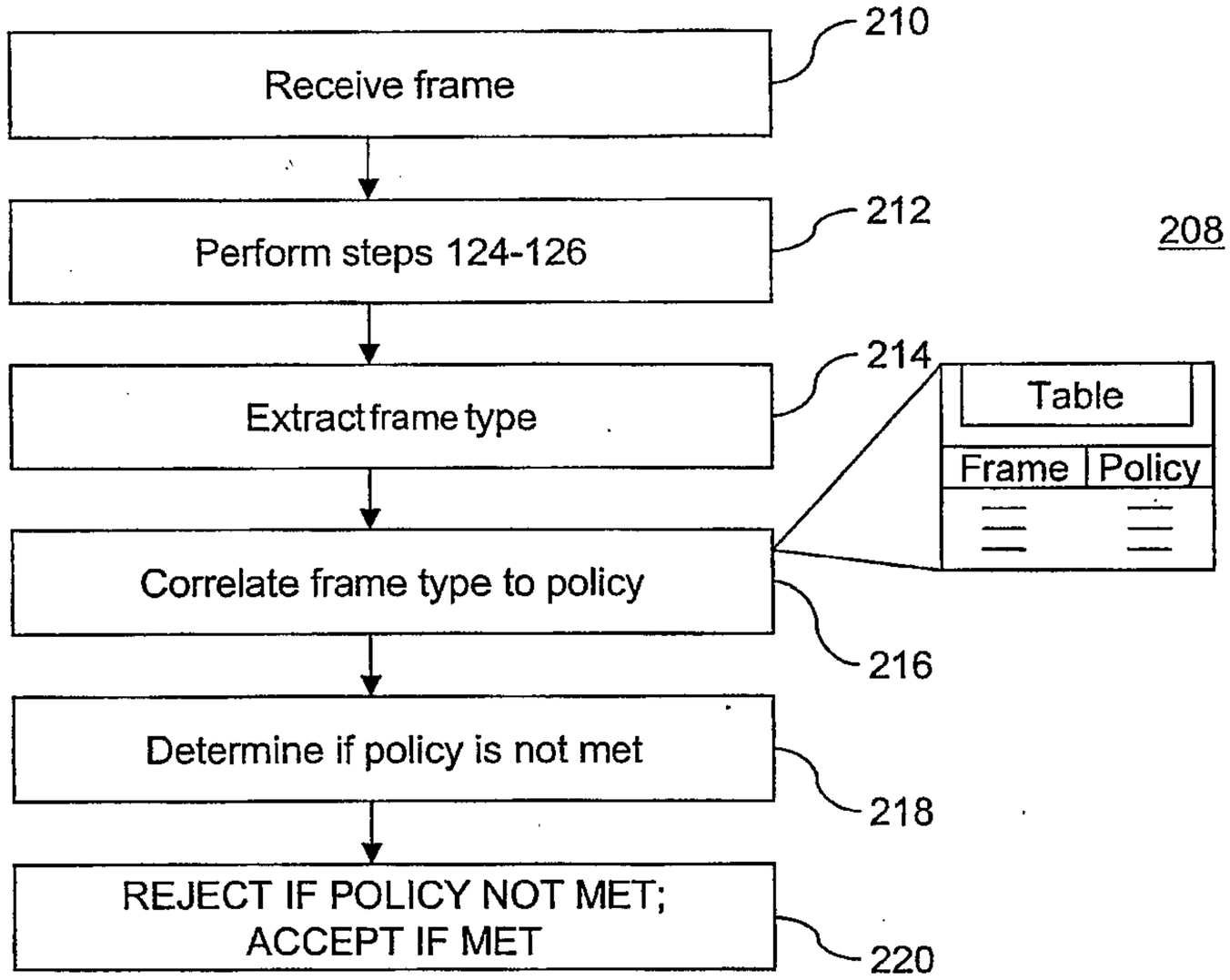

Receive frame
210
Perform steps 124-126
212
208
Extract frame type
214
Table
Frame
Policy
Correlate frame type to policy
216
Determine if policy is not met
218
REJECT IF POLICY NOT MET;
ACCEPT IF MET
220

Figure 11

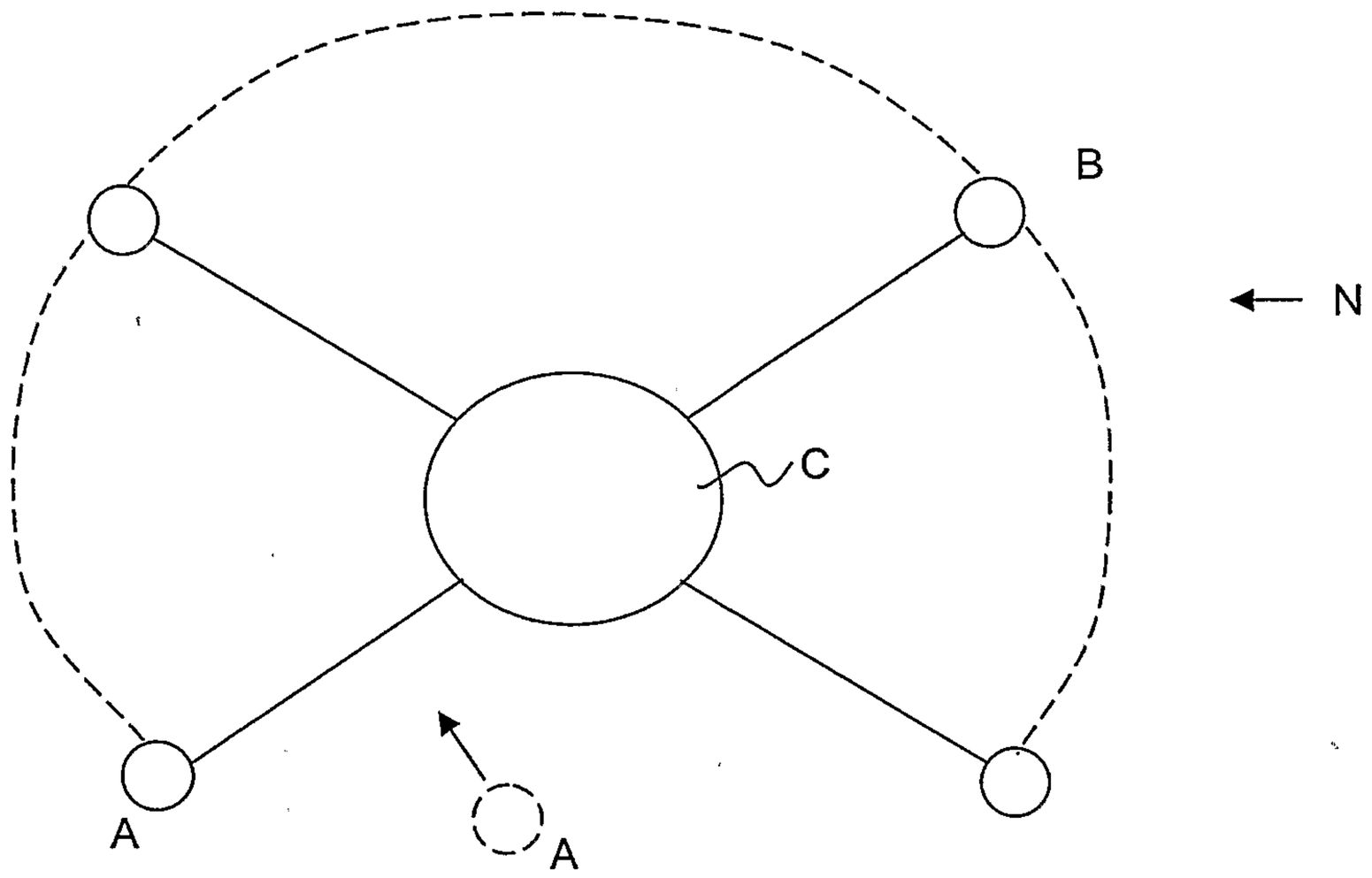


Figure 12

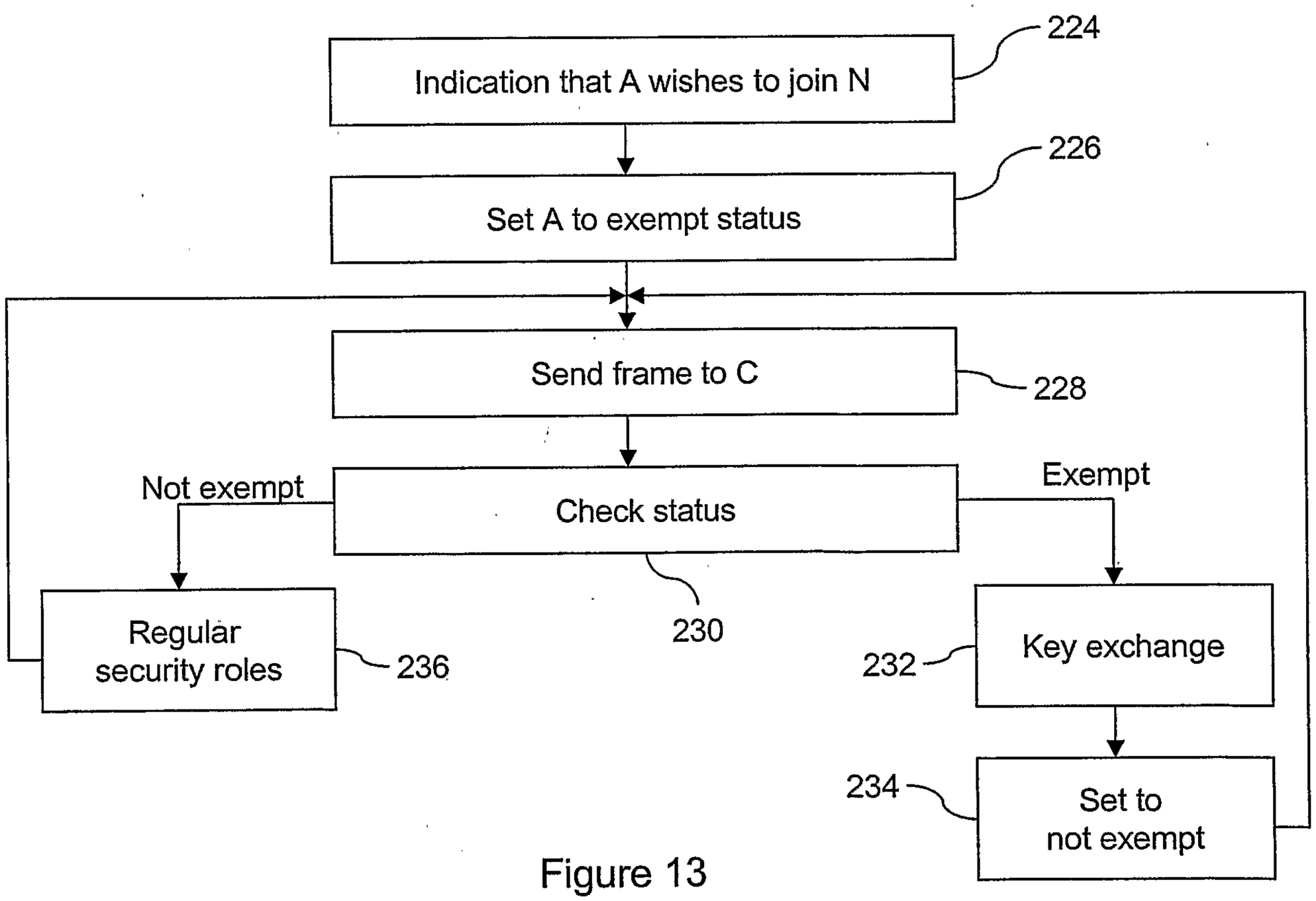
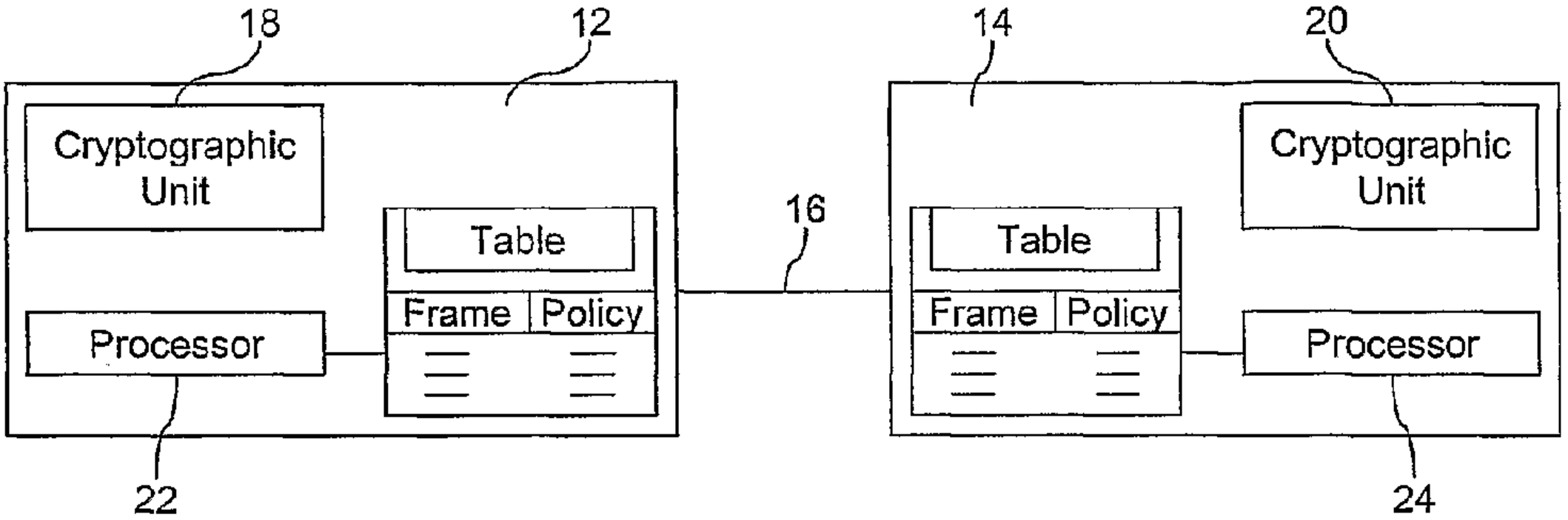


Figure 13


18
12
14
20
Cryptographic Unit
Table
16
Table
Cryptographic Unit
Frame
Policy
Frame
Policy
Processor
Processor
22
24