

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
2 December 2004 (02.12.2004)

PCT

(10) International Publication Number
WO 2004/105285 A2

(51) International Patent Classification⁷: **H04L**
(21) International Application Number:
PCT/US2004/012121
(22) International Filing Date: 20 April 2004 (20.04.2004)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
10/442,027 20 May 2003 (20.05.2003) US

(71) Applicant (for all designated States except US): **MOTOROLA, INC., A CORPORATION OF THE STATE OF DELAWARE** [US/US]; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **BIGGS, Robert A.**, [GB/US]; 2201 Pioneer Road, Evanston, Illinois 60201 (US). **NEWBERG, Donald G.**, [US/US]; 4240 Haman Avenue, Hoffman Estates, Illinois 60195 (US).

(74) Agents: **SALADI, Indira**, et al.; 1303 East Algonquin Road, Schaumburg, Illinois 60196 (US).

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

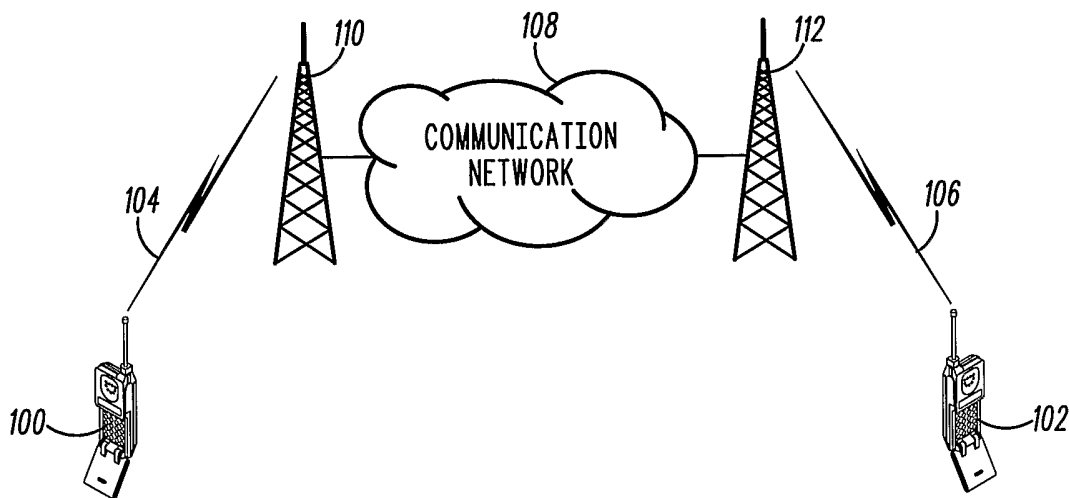
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL,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

Published:

— without international search report and to be republished upon receipt of that report

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

(54) Title: METHOD FOR UTILIZING MULTIPLE LEVEL ENCRYPTION



(57) Abstract: In a wireless communication system with an air interface comprised of a plurality of bursts, a communication device (102) receives a burst (200). The burst (200) comprises payload (206, 208), a first indicator (202) and a second indicator (204). Upon receipt of the burst (200), the communication device (102) determines a value of the first indicator (202) to determine whether end-to-end encryption is applied to at least a portion of the payload, and determines a value of the second indicator (204) to determine whether air interface encryption is applied to at least a portion of the payload.

METHOD FOR UTILIZING MULTIPLE LEVEL ENCRYPTION

Field of the Invention

5 The present invention relates generally to a method for utilizing multiple level encryption.

Background of the Invention

10 In wireless communication systems, both air interface encryption and end-to-end encryption play a part in providing confidentiality services. Air interface encryption is applied to information carried on the wireless link between a base radio and a communication device, whereas end-to-end encryption is applied to information exchanged between the source communication device and the final destination communication device of the information where the information may traverse multiple wireless and/or wire-line links.

15 Encryption requires synchronization of any encryption parameters between the transmitting device and the receiving device in order for information to be successfully decrypted. Typically, the base radio and communication device establish a relationship well before the start of communication, allowing the air interface encryption synchronization parameters to be known *a priori* by the receiving communication device. However, communication devices may exchange information with a large number of other communication devices, many of which are not known before the start of communication. Because of this, the receiving communication device does not know *a priori* the encryption synchronization parameters for end-to-end encryption.

25 Flexible communication systems demand that end-to-end encryption (i.e., the confidentiality service) is applied dynamically, establishing synchronization parameters whenever communication is initiated. These synchronization parameters are typically signaled in their entirety at the beginning of a transmission. These synchronization parameters are also signaled in part throughout the duration of the transmission at a very slow rate (due to limited bandwidth) to accommodate communication devices that enter the communication session after the initial signaling, a condition that is called "late-entry". Because the encryption

synchronization information is re-transmitted throughout the transmission at a rate that is typically much slower than the information it protects, this late entry condition can cause ambiguity in the receiving communication device. Thus, if the receiving communication device misses the initial transmission of encryption synchronization
5 information, the receiving communication device is forced to either assume an encryption state, which will likely result in processing errors, or acquire the encryption synchronization information when re-transmitted throughout the transmission at the very slow rate which will result in additional delays. For example, if a receiving communication device mistakenly believes that an end-to-end encrypted
10 call is sent unencrypted or visa-versa, objectionable noises may be generated.

Thus, there exists a need for a method for indicating and processing multiple levels of encryption.

Brief Description of the Figures

15 A preferred embodiment of the invention is now described, by way of example only, with reference to the accompanying figures in which:

FIG. 1 (prior art) illustrates a system topology of a wireless communication system;

20 FIG. 2 illustrates an example structure of a burst in which no encryption is applied to the information in accordance with the preferred embodiment of the present invention;

FIG. 3 illustrates an example structure of a burst in which only air interface encryption is applied to the information in accordance with the preferred embodiment of the present invention;

25 FIG. 4 illustrates an example structure of a burst in which only end-to-end encryption is applied to the information in accordance with the preferred embodiment of the present invention;

FIG. 5 illustrates an example structure of a burst in which both end-to-end encryption and air interface encryption is applied to the information in accordance
30 with the preferred embodiment of the present invention; and

FIG. 6 illustrates a flowchart of the operation of the receiving device to determine the earliest possible time at which the receiving device may process the received information

5 **Detailed Description of the Preferred Embodiment**

It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements are exaggerated relative to each other. Further, where considered appropriate, reference numerals have been repeated among the
10 figures to indicate identical elements.

The present invention provides a first indicator to indicate whether end-to-end encryption is applied to at least a portion of the payload and a second indicator to indicate whether air interface encryption is applied to at least a portion of the payload in each over-the air burst (i.e., over-the-air fragment); thus, the first indicator and the
15 second indicator are present at the same layer of the protocol stack (e.g., the link layer). The receiving device uses the indicators to efficiently determine any decryption mechanism, if any, required to recover/process the received information/payload. It should be noted that the present invention uses the term “fragment” and/or “burst” to describe the smallest standalone entity of the air
20 interface. In a time division multiple access (“TDMA”) system, this may also be called a slot.

Turning now to the figures, as illustrated in FIG. 1, a first communication device 100 is communicating with a second communication device 102 via wireless links 104, 106 and a communication network 108. For ease of explanation, the first
25 communication device 100 is the transmitting communication device, and the second communication device 102 is the receiving communication device, however, each communication device 100, 102 is capable of both transmitting and receiving.

Air interface encryption, if utilized, may be applied to information exchanged between the first communication device 100 and a first base radio 110, information
30 exchanged between the second communication device 102 and a second base radio 112, or both. End-to-end encryption, if utilized, may be applied to information exchanged between the first communication device 100 and the second

communication device 102. Typically, the information to which end-to-end encryption is applied is to real-time media, such as voice, video and/or the like, but is not limited to such. Both air interface encryption and end-to-end encryption are optional and thus four combinations of encryption are possible. These are addressed in FIGS. 2-6.

FIGS. 2-5 illustrates examples of the structure of a burst 200 comprising the first indicator 202, the second indicator 204 and two fields of payload 206, 208 in accordance with the preferred embodiment of the present invention; FIG. 6 illustrates a flowchart of the operation of the receiving communication device 102 to determine the earliest point in time at which the receiving communication device 102 may process the received payload 206, 208. Some of the payload fields are capable of being protected with end-to-end encryption, while all of the fields are capable of being protected with air interface encryption. It should be noted that while FIGS. 2-5 illustrate two fields of payload 206, 208 in the burst 200, the burst 200 may containing any number of fields, including one, and still remain within the spirit and scope of the present invention.

The first of the four possible combinations of encryption is illustrated in FIG. 2 and in steps 600-608 of FIG. 6. In the first combination, when the receiving communication device 102 receives a burst 200, the values of the indicators 202, 204 indicate that neither end-to-end encryption nor air interface encryption is applied to the payload 206, 208. Since no encryption synchronization parameters are needed to process the payload 206, 208, providing the first indicator 202 and the second indicator 204 in each burst 200 allows the receiving communication device 102 to detect this state as the current burst 200 is being received and begin processing the payload 206, 208 from the current and subsequently received bursts at the earliest point in time (i.e., immediately).

The second of the four possible combinations of encryption is illustrated in FIG. 3 and in steps 600, 602, and 610-616 of FIG. 6. In the second combination, when the receiving communication device 102 receives a burst 200, the values of the indicators 202, 204 indicate that only air interface encryption 300 is applied to at least a portion of the payload 206, 208. The present invention assumes that the receiving communication device 102 knows *a priori* the encryption synchronization parameters

for the air interface encryption 300. Since no further encryption synchronization is needed, providing the first indicator 202 and the second indicator 204 in each burst 200 allows the receiving communication device 102 to detect this state as the burst 200 is being received, and begin decrypting the air interface encryption 300 and
5 processing the payload 206, 208 from the current burst and subsequently received bursts at the earliest point in time (i.e., immediately).

The third of the four possible combinations of encryption is illustrated in FIG. 4 and in steps 600-604 and 618-624 of FIG. 6. In the third combination, when the receiving communication device 102 receives a burst 200, the values of the indicators
10 202, 204 indicate that only end-to-end encryption 400 is applied to at least a portion of the payload 206. If the receiving communication device 102 has not yet acquired the encryption synchronization parameters for the end-to-end encryption 400 (e.g., due to late entry), the receiving communication device 102 cannot yet process the portion of the payload 206 that is end-to-end encrypted. Thus, the first indicator 202
15 indicates to the receiving communication device 102 that end-to-end encryption 400 is applied to at least a portion of the payload 206, thus triggering the receiving communication device 102 to start acquiring the encryption synchronization parameters immediately, starting with the current burst 200. It should be noted that acquiring the encryption synchronization parameters for end-to-end encryption 400
20 might span several additional bursts due to the slow speed nature of the signaling. In other words, the receiving communication device 102 may need to receive a plurality of bursts 200 before it is able to acquire the encryption synchronization parameters for the end-to-end encryption 400; thus, upon receiving the plurality of bursts 200, the receiving communication device 102 extracts information from each burst 200 and
25 optionally discards the payload associated therewith until the encryption synchronization parameters for the end-to-end encryption 400 are acquired. Once the encryption synchronization parameters for the end-to-end encryption 400 are acquired, the receiving communication device 102 can then decrypt the end-to-end encryption 400 from the payload 206 and process the payload 206 from subsequently
30 received bursts 200.

The fourth of the four possible combinations of encryption is illustrated in FIG. 5 and in steps 600, 602, 610, and 626-636 of FIG. 6. In the fourth combination,

when the receiving communication device 102 receives a burst 200, the values of the indicators 202, 204 indicate that both air interface encryption 300 and end-to-end encryption 400 are applied to at least a portion of the payload 206, 208. As noted above, the present invention assumes that the receiving communication device 102 knows *a priori* the encryption synchronization parameters for the air interface encryption 300, and thus, is able to decrypt the air interface encryption 300 at the earliest point in time (i.e., immediately). However, if the receiving communication device 102 has not yet acquired the encryption synchronization parameters for the end-to-end encryption 400 (e.g., due to late entry), the receiving communication device 102 cannot yet decrypt the end-to-end encryption 400 and process at least a portion of the payload 206; thus, the first indicator 202 indicates to the receiving communication device 102 that end-to-end encryption 400 is applied to at least a portion of the payload, thus triggering the receiving communication device 102 to start acquiring the encryption synchronization parameters for the end-to-end encryption at the earliest point in time (i.e., immediately), starting with the current burst 200. Once the encryption synchronization parameters for the end-to-end encryption 400 are acquired as described above in the third combination, the receiving communication device 102 can continue decrypting the air interface encryption 300, start decrypting the end-to-end encryption 400 and processing the payload 206 from subsequently received bursts 200.

Thus, the present invention uses the indicators 202, 204 to indicate the status of each encryption within each burst 200. The indicators 202, 204 allows the receiving communication device 102 to detect the status of encryption (i.e., the state of the payload 206, 208) and process the payload 206, 208 correctly (i.e., the indicators 202, 204 prevent mismatches in the possible combinations of encryption that result in noise in an audio stream) at the earliest point in time; for example, the receiving communication device 102 can play audio as soon as possible. The present invention is preferably implemented in software, but could also be implemented in firmware, hardware or any combination of software, hardware and/or firmware. It should be noted that the present invention can be embodied in a storage medium having stored thereon a set of instructions which, when loaded into a hardware device,

causes the hardware device to perform the following functions of the present invention.

While the invention has been described in conjunction with specific embodiments thereof, additional advantages and modifications will readily occur to those skilled in the art. The invention, in its broader aspects, is therefore not limited to the specific details, representative apparatus, and illustrative examples shown and described. Various alterations, modifications and variations will be apparent to those skilled in the art in light of the foregoing description. Thus, it should be understood that the invention is not limited by the foregoing description, but embraces all such alterations, modifications and variations in accordance with the spirit and scope of the appended claims.

Claims

We claim:

1. In a wireless communication system with an air interface comprised of a
5 plurality of bursts, a method comprising the steps of:
receiving a burst, wherein the burst comprises payload, a first indicator and a
second indicator;
determining a value of the first indicator to determine whether end-to-end
encryption is applied to at least a portion of the payload; and
10 determining a value of the second indicator to determine whether air interface
encryption is applied to at least a portion of the payload.
2. The method of claim 1 wherein the value of the first indicator indicates that
end-to-end encryption is not applied to at least a portion of the payload, and wherein
15 the second indicator indicates that air interface encryption is not applied to at least a
portion of the payload, and further comprising the step of immediately processing the
payload.
3. The method of claim 1 wherein the value of the first indicator indicates that
20 end-to-end encryption is not applied to at least a portion of the payload, and wherein
the second indicator indicates that air interface encryption is applied to at least a
portion of the payload, and further comprising the steps of decrypting the air interface
encryption with encryption synchronization parameters known *a priori*, and
processing the payload immediately.
25
4. The method of claim 1 wherein the value of the first indicator indicates that
end-to-end encryption is applied to at least a portion of the payload, and wherein the
30

second indicator indicates that air interface encryption is not applied to at least a portion of the payload, and further comprising the steps of:

- acquiring encryption synchronization for end-to-end encryption; and
 - decrypting the end-to-end encryption using the acquired encryption
- 5 synchronization for end-to-end encryption.

5. The method of claim 4 wherein the step of acquiring comprises extracting information from at least one additional burst, and discarding payload associated with the burst and the at least one additional burst.

10

6. The method of claim 1 wherein the value of the first indicator indicates that end-to-end encryption is applied to at least a portion of the payload, and wherein the second indicator indicates that air interface encryption is applied to at least a portion of the payload, and further comprising the steps of:

- 15 decrypting the air interface encryption with encryption synchronization parameters for air interface encryption known *a priori*;
 - acquiring encryption synchronization parameters for end-to-end encryption;
 - and
 - decrypting the end-to-end encryption using the acquired encryption
- 20 synchronization parameters for end-to-end encryption.

7. The method of claim 6 wherein the step of acquiring comprises extracting information from at least one additional burst, and discarding payload associated with the burst and the at least one additional burst.

25

8. The method of claim 1 wherein at least the portion of the payload in which end-to-end encryption is applied is real-time media.

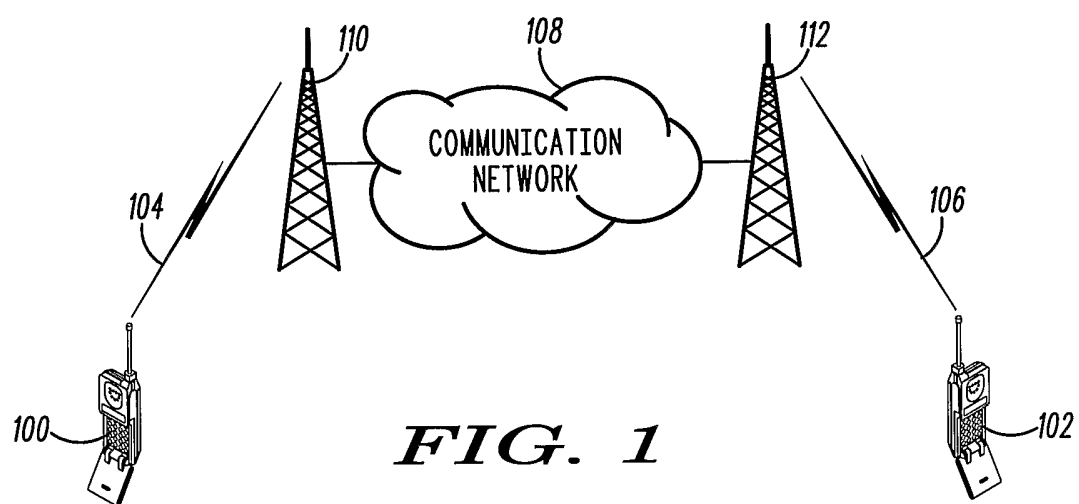
9. The method of claim 1 further comprising the step of receiving at least a second burst, wherein each burst comprises payload, the first indicator and the second

30 indicator.

10. A storage medium having stored thereon a set of instructions which, when loaded into a hardware device, causes the hardware device to perform the following functions:

- 5 receive a burst, wherein the burst comprises payload, a first indicator and a second indicator;
- determine a value of the first indicator to determine whether end-to-end encryption is applied to at least a portion of the payload; and
- determine a value of the second indicator to determine whether air interface encryption is applied to at least a portion of the payload.

1/3



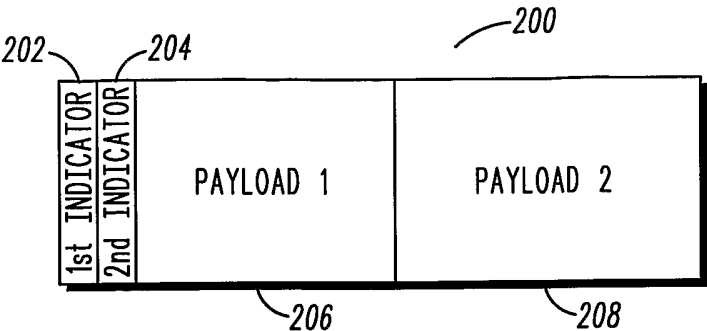


FIG. 2

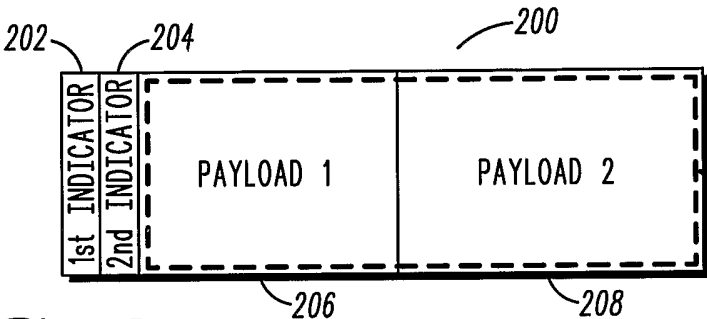


FIG. 3

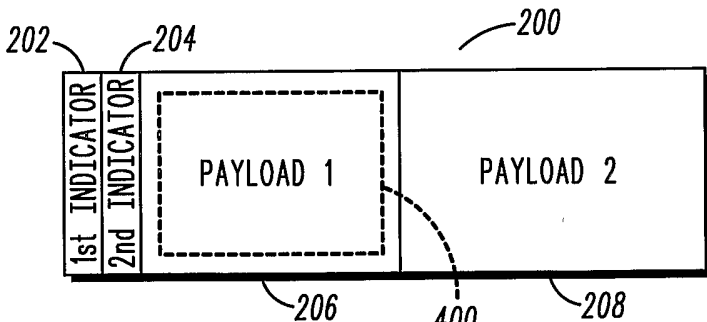


FIG. 4

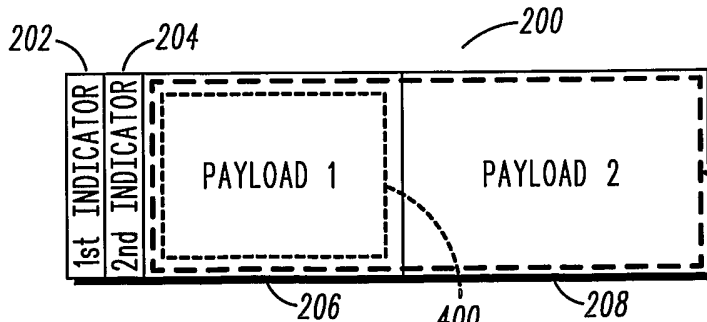


FIG. 5

3/3

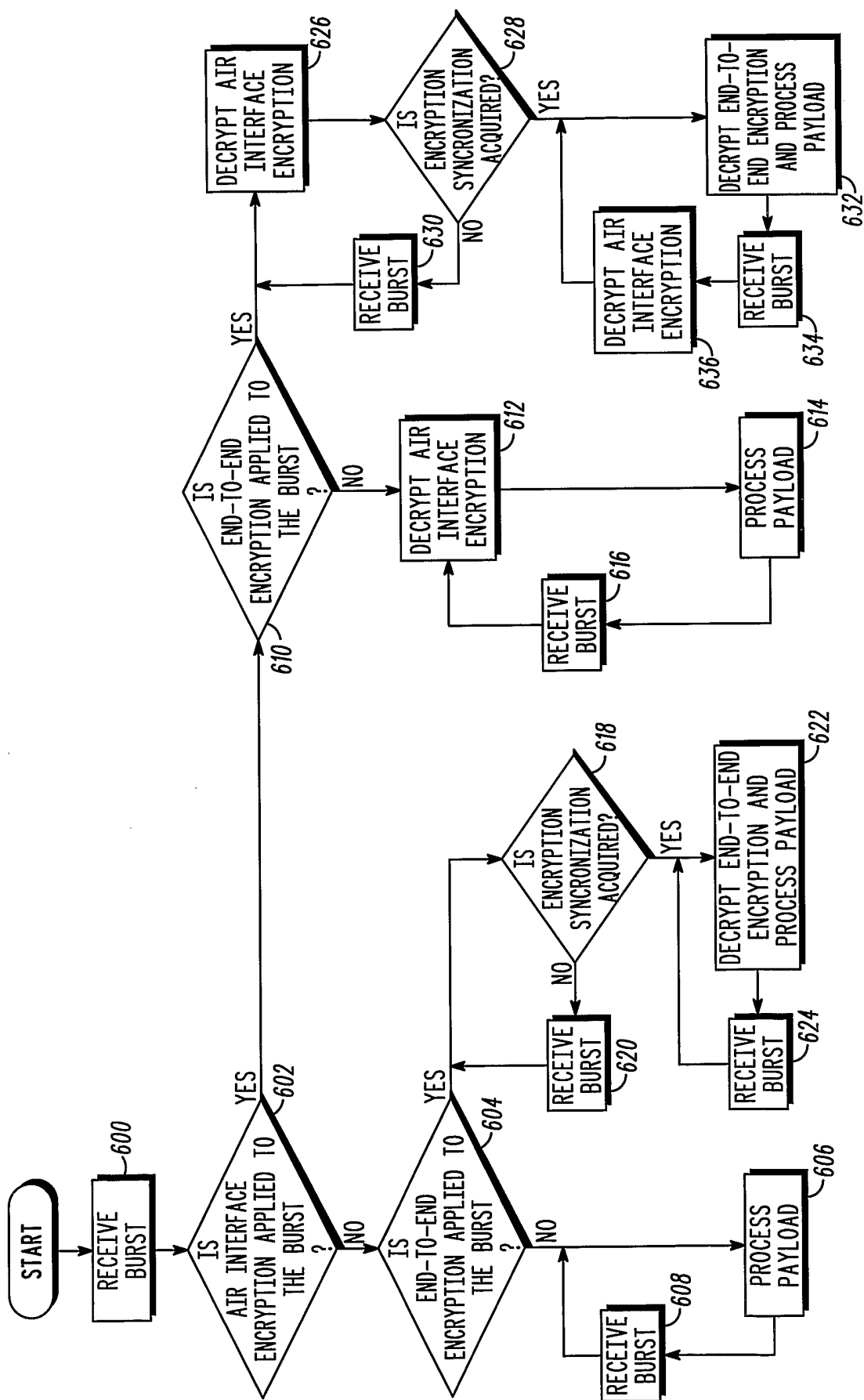


FIG. 6