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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 February 2004 (19.02.2004)

PCT

(10) International Publication Number
WO 2004/015900 A1

(51) International Patent Classification[7]: H04J 3/24

(21) International Application Number:
PCT/US2003/025103

(22) International Filing Date: 11 August 2003 (11.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/217,097 12 August 2002 (12.08.2002) US

(71) Applicant: **HARRIS CORPORATION** [US/US]; 1025 W.NASA Blvd., Melbozrne, FL 32919 (US).

(72) Inventor: **BILLHARTZ, Thomas, Jay**; 2355 Polonius Lane, Melbourne, FL 32934 (US).

(74) Agents: **YATSKO, Michael, S.** et al.; Harris Corporation, 1025 W. Nasa Blvd., Melbourne, FL 32919 (AU).

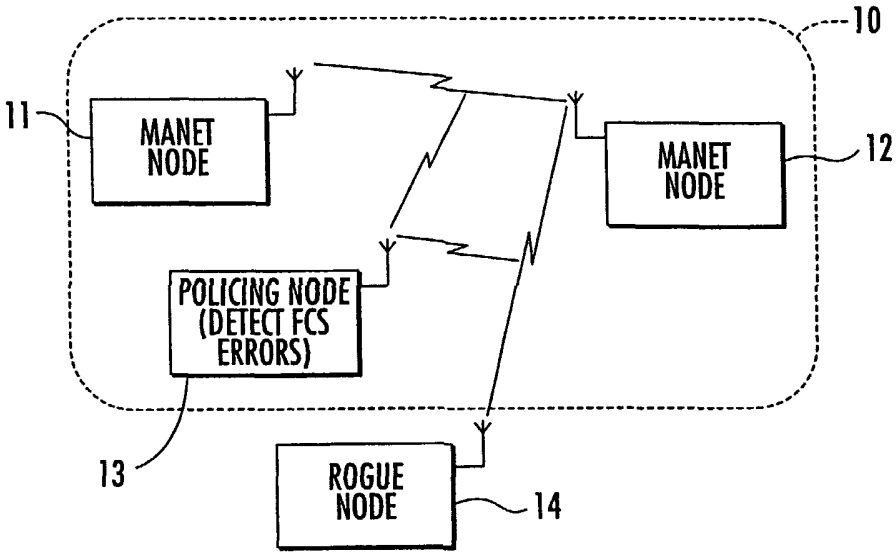
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT,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

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (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: MOBILE AD-HOC NETWORK WITH INTRUSION DETECTION FEATURES AND RELATED METHODS



(57) Abstract: A mobile ad-hoc network (MANET 10, 20, 30, 40, 50, 60) may include a plurality for nodes for transmitting data therebetween using a media access layer (MAC), where each of the nodes has a respective MAC address associated therewith. The MANET may also include a policing node (13, 23, 33, 43, 53, 63) for detecting intrusions (14, 24, 34, 44, 54, 64) into the MANET by monitoring transmissions among the plurality of nodes to detect frame check sequence (FCS) errors from a MAC address, and generating an intrusion alert based upon detecting a number of FCS errors for the MAC address exceeding a threshold. The policing node may also detect intrusions based upon one or more of failed MAC address authentications, illegal network allocation vector (NAV) values, and unexpected contention or contention-free operation.

WO 2004/015900 A1

MOBILE AD-HOC NETWORK WITH INTRUSION DETECTION FEATURES AND RELATED METHODS

Background of the Invention

Wireless networks have experienced increased development in the past decade. One of the most rapidly developing areas is mobile ad-hoc networks, or MANETs for short. Physically, a mobile ad-hoc network includes a number of geographically-distributed, potentially mobile nodes sharing a common radio channel. Compared with other types of networks, such as cellular networks or satellite networks, the most distinctive feature of mobile ad-hoc networks is the lack of any fixed infrastructure. The network may be formed of mobile nodes only, and a network is created "on the fly" as the nodes come close enough to transmit with each other. The network does not depend on a particular node and dynamically adjusts as some nodes join or others leave the network.

Because of these unique characteristics, routing protocols for governing data flow within ad-hoc networks are required which can adapt to frequent topology changes. Two basic categories of ad-hoc routing protocols have emerged in recent years, namely reactive or "on-demand" protocols, and proactive or table-driven protocols. Reactive protocols collect routing information when a particular route is required to a destination in response to a route request. Examples of reactive protocols include ad-hoc on demand distance vector (AODV) routing, dynamic source routing (DSR), and the temporally ordered routing algorithm (TORA).

On the other hand, proactive routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. Such protocols typically require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout

the network to maintain a consistent view of the network. Examples of such proactive routing protocols include destination-sequenced distance-vector (DSDV) routing, which is disclosed in U.S. Patent No. 5,412,654 to Perkins; the wireless routing protocol (WRP); and clusterhead gateway switch routing (CGSR). A hybrid protocol which uses both proactive and reactive approaches is the zone routing protocol (ZRP), which is disclosed in U.S. Patent No. 6,304,556 to Haas.

One challenge to the advancement of ad-hoc network development is that of security. More particularly, since nodes in a mobile ad-hoc network all communicate wirelessly, there is a much greater risk of intrusion by unauthorized users. Because of the early stage of development of ad-hoc networks and the numerous other challenges these networks present, the above routing protocols have heretofore primarily focused solely on the mechanics of data routing and not on intrusion detection.

Some approaches are now being developed for providing intrusion detection in mobile ad-hoc networks. One such approach is outlined in an article by Zhang et al. entitled "Intrusion Detection in Wireless Ad-Hoc Networks," ACM MOBICOM, 2000. In this article, an intrusion detection architecture is proposed in which every node in the MANET participates in intrusion detection and response. That is, each node is responsible for detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively investigate in a broader range. Moreover, intrusion detection is based upon anomaly detections, such as the detection of abnormal updates to routing tables or anomalies in certain network layers, such as with media access control (MAC) layer protocols. Another similar MANET intrusion detection architecture is disclosed in "Security in Ad Hoc Networks: a General Intrusion Detection Architecture

Enhancing Trust Based Approaches," by Albers et al., in Proceedings of the International First Workshop on Wireless Information Systems (Wis-2002), April 2002.

While the architectures discussed in the above articles may provide a convenient starting point for implementing intrusion detection, much of the details regarding the implementation of intrusion detection in MANETs have yet to be determined. That is, the particular types of node characteristics which can reliably indicate whether a node is a rouge node attempting to intrude upon the network still remain largely undefined.

Summary of the Invention

In view of the foregoing background, it is therefore an object of the present invention to provide a mobile ad-hoc network (MANET) with intrusion detection features and related methods.

This and other objects, features, and advantages in accordance with the present invention are provided by a MANET which may include a plurality of nodes for transmitting data therebetween using a media access (MAC) layer, where each of the nodes has a respective MAC address associated therewith. The MANET may also include a policing node for detecting intrusions into the network. This may be done by monitoring transmissions among the plurality of nodes to detect frame check sequence (FCS) errors from a MAC address, and generating an intrusion alert based upon detecting a number of FCS errors for the MAC address exceeding a threshold.

Furthermore, the policing node may detect intrusions into the wireless network by monitoring transmissions among the plurality of nodes to detect failed attempts to authenticate MAC addresses, and generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address. More specifically, the policing

node may generate an intrusion alert based upon detecting the number of failed attempts to authenticate a MAC address within a predetermined period.

In addition, the plurality of nodes may transmit request to send (RTS) and clear to send (CTS) packets therebetween prior to transmitting data. The RTS and CTS packets may include a network allocation vector (NAV) indicating a time duration reserved for transmitting the data. As such, the policing node may further detect intrusions into the MANET by monitoring the RTS and CTS packets sent between the plurality of nodes to detect an illegal NAV value therein and generate an intrusion alert based thereon.

The plurality of nodes may also intermittently operate in a contention-free mode during a contention-free period (CFP). Thus, the policing node may also advantageously detect intrusions into the wireless network by monitoring transmissions among the plurality of nodes to detect contention-free mode operation outside of a CFP (or vice versa) and generate an intrusion alert based thereon.

Additionally, the MANET may have at least one service set ID associated therewith. Accordingly, the policing node may further detect intrusions into the MANET by monitoring transmissions among the plurality of nodes to detect service set IDs associated therewith. The policing node may further generate an intrusion alert based upon one of the detected service set IDs being different than the at least one service set ID of the MANET. Also, the plurality of nodes may transmit data over at least one channel, and the policing node may detect transmissions over the at least one channel not originating from one of the plurality of nodes and generate an intrusion alert based thereon.

The policing node may advantageously transmit an intrusion alert to at least one of the plurality of nodes in

some embodiments. As such, the appropriate countermeasures may be taken to respond to the intrusion.

An intrusion detection method aspect of the invention is for a MANET including a plurality of nodes. The method may include transmitting data between the plurality of nodes using a MAC layer, where each of the nodes has a respective MAC address associated therewith. Moreover, transmissions among the plurality of nodes may be monitored to detect FCS errors from a MAC address, and an intrusion alert generated based upon detecting a number of FCS errors for the MAC address exceeding a threshold.

Additionally, the method may also include monitoring transmissions among the plurality of nodes to detect failed attempts to authenticate MAC addresses, and generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address. In particular, an intrusion alert may be generated based upon detecting a number of failed attempts to authenticate a MAC address within a predetermined period.

Furthermore, the method may include transmitting RTS and CTS packets between the plurality of nodes prior to transmitting data. As noted above, the RTS and CTS packets typically include NAV values indicating a time duration reserved for transmitting the data. Moreover, the RTS and CTS packets transmitted between the plurality of nodes may be monitored to detect an illegal NAV value therein, and an intrusion alert generated based upon the detected illegal NAV value.

The plurality of nodes may intermittently operate in a contention-free mode during a CFP. As such, the method may also include monitoring transmissions among the plurality of nodes to detect contention-free mode operation outside of a CFP (or vice versa), and generating an intrusion alert based thereon.

In addition, the MANET may have at least one service set ID associated therewith. Thus, the method may further include monitoring transmissions among the plurality of nodes to detect service set IDs associated therewith, and generating an intrusion alert based upon one of the detected service set IDs being different than the at least one service set ID of the wireless network. Also, the plurality of nodes may transmit data over at least one channel. Transmissions over the at least one channel not originating from one of the plurality of nodes may therefore be detected, and an intrusion alert generated based thereon. The method may also include transmitting the intrusion alert to at least one of the plurality of nodes.

Brief Description of the Drawings

FIG. 1 is a schematic block diagram of a MANET in accordance with the present invention for providing intrusion detection based upon frame check sequence (FCS) errors.

FIG. 2 is a schematic block diagram of an alternate embodiment of the MANET of FIG. 1 for providing intrusion detection based upon failed authentications of media access control (MAC) addresses.

FIG. 3 is a schematic block diagram of another alternate embodiment of the MANET of FIG. 1 for providing intrusion detection based upon illegal network allocation vectors (NAVs).

FIGS. 4 and 5 are schematic block diagrams of further alternate embodiments of the MANET of FIG. 1 for providing intrusion detection based upon contention-free mode operation outside of a contention-free period (CFP) and based upon contention mode operation during a CFP, respectively.

FIG. 6 is a schematic block diagram of another alternate embodiment of the MANET of FIG. 1 for providing

intrusion detection based upon transmissions occurring during an unauthorized period.

FIG. 7 is a schematic block diagram of still another alternate embodiment of the MANET of FIG. 1 for providing intrusion detection based upon detecting integrity check values which do not correspond with their respective data packets.

FIG. 8 is a schematic block diagram of yet another alternate embodiment of the MANET of FIG. 1 for providing intrusion detection based upon detecting usage of non-consecutive MAC sequence numbers by a node.

FIG. 9 is a schematic block diagram of another alternate embodiment of the MANET of FIG. 1 for providing intrusion detection based upon detecting collisions of packets having a predetermined packet type.

FIG. 10 is a schematic block diagram of yet another alternate embodiment of the MANET of FIG. 1 for providing intrusion detection based upon detecting collisions of a same MAC address.

FIG. 11 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting FCS errors.

FIG. 12 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting failed authentications of MAC addresses.

FIG. 13 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting illegal network allocation vector (NAV) values.

FIGS. 14 and 15 are flow diagrams illustrating intrusion detection methods in accordance with the present invention based upon detecting contention-free mode operation outside of a CFP and detecting contention mode operation during a CFP, respectively.

FIG. 16 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting transmissions occurring during an unauthorized period.

FIG. 17 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting integrity check values which do not correspond with their respective data packets.

FIG. 18 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting usage of non-consecutive MAC sequence numbers by a node.

FIG. 19 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting collisions of packets having a predetermined packet type.

FIG. 20 is a flow diagram illustrating an intrusion detection method in accordance with the present invention based upon detecting collisions of a same MAC address.

FIG. 21 is a flow chart illustrating additional method aspects of the invention for intrusion detection.

Detailed Description of the Preferred Embodiments

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. Rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

For purposes of the foregoing discussion, like numbers refer to like elements throughout. Moreover,

referring particularly to FIGS. 1-10, reference numerals differing by decades are used to indicate similar elements in alternate embodiments. For example, the mobile ad-hoc network (MANET) nodes **11**, **21**, **31**, **41**, **51**, **61**, **71**, **81**, **91**, and **101** illustrated in FIGS. 1-10 are all similar elements, and so on. As such, these elements may only be described in detail upon their first occurrence to avoid undue repetition, but later occurring elements are understood to be similar to those first described.

Referring now to FIG. 1, a MANET **10** in accordance with the present invention illustratively includes nodes **11**, **12**. While only the two nodes **11**, **12** are shown for clarity of illustration, those of skill in the art will appreciate that any number of nodes may be included within the MANET **10**. Such nodes may be laptop computers, personal data assistants (PDAs), cellular telephones, or other suitable devices, as will be appreciated by those of skill in the art. Further, in some embodiments one or more nodes in the MANET **10** may be fixed to provide a bridge to a wired (or satellite) communications infrastructure, such as a telephone network, for example.

Before describing the MANET **10** in further detail, a brief discussion regarding MANET protocols in general is warranted. While MANETs are still in their infancy and there is as yet no one common standard governing communications in such networks, one likely characteristic of MANETs is that MANET nodes will operate in accordance with the open system architecture (OSI) model for data transfer, which includes seven layers at which certain types of data are sent using various protocols. These layers include the application layer, presentation layer, session layer, transport layer, network layer, data link layer, and physical layer.

The data link layer further includes media access control (MAC) and logical link control sub-layers. In

accordance with the invention, the nodes **11, 12** preferably use the MAC layer for transmitting data therebetween, and each has a respective MAC addresses associated therewith, as will be appreciated by those of skill in the art. Of course, the remaining layers of the OSI model may also be used for data transmission as well, and other suitable network data transfer models may also be used. Moreover, such data is typically sent in packets, and various packets types are used for different types of message data, as will be described further below.

In accordance with the invention, the MANET **10** illustratively includes one or more policing nodes **13** for detecting intrusions into the network by a rogue node **14**. By way of example, the rogue node **14** may be used by a would-be hacker attempting to hack into the MANET **10**, or it may simply be a node from a different MANET that is operating too closely to the MANET **10**. In the present example, the policing node **13** monitors transmissions among the nodes **11, 12** to detect frame check sequence (FCS) errors from a given MAC address. If a number of FCS errors detected for a given MAC address exceeds a threshold, the policing node **13** generates an intrusion alert based thereon.

It should be noted that, as used herein, the phrase "transmissions among the nodes" is intended to mean any transmission directly to or from one of the nodes **11, 12**, as well as any transmission within an operating range of the MANET **10**. In other words, the policing node **13** may monitor transmissions directed to or originating from the nodes **11, 12** as well as any other transmissions it may receive whether or not they are specifically directed to or originate from a node in the MANET **10**.

In the above-described embodiment (and those described below), the policing node **13** may advantageously transmit the alert to one or more of the nodes **11, 12** in the

MANET **10**. By way of example, the policing node **13** may transmit the intrusion alert directly to the node **12**, which may then notify all of the remaining nodes in the wireless network. Alternately, the policing node **13** may broadcast the intrusion alert to all network nodes. In either case, the appropriate countermeasures may then be taken to respond to the unauthorized intrusion, as will be appreciated by those skilled in the art. Such countermeasures are beyond the scope of the present invention and will therefore not be discussed herein.

Turning now to FIG. 2, a first alternate embodiment of the MANET **20** is now described. In this embodiment, the policing node **23** detects intrusions into the wireless network **20** by monitoring transmissions among the nodes **21, 22** to detect failed attempts to authenticate MAC addresses. Upon detecting a certain predetermined number of failed attempts to authenticate a particular MAC address, the policing node **23** will generate an intrusion alert.

Any number of failed attempts may be used as the threshold for generating the intrusion alert, but it may generally be desirable to allow a node at least one attempt to authenticate its MAC address without generating the intrusion alert. Moreover, in some embodiments the policing node **23** may advantageously only generate the intrusion alert if the detected number of failures occur within a predetermined period (e.g., an hour, day, etc.).

Turning now additionally to FIG. 3, in accordance with another aspect of the invention the two nodes **31, 32** of the MANET **30** transmit request to send (RTS) and clear to send (CTS) packets therebetween prior to transmitting data. The reason for this is to avoid collisions with other transmissions. That is, since many or all of the remaining nodes in the MANET **30** may be communicating on the same channel, these nodes may need to ensure that they are not

transmitting at the same time, as this could result in interference and network disruption.

Also, the RTS and CTS packets preferably include a network allocation vector (NAV) indicating a time duration reserved for transmitting the data. This information is transmitted to adjacent nodes in the MANET **30**, which will then stop transmission during the specified period, for example.

Accordingly, the policing node **33** may therefore detect intrusions into the wireless network **30** by monitoring RTS and CTS packets sent between the nodes **31, 32** to detect an illegal NAV value therein. For example, the MANET **30** may be implemented in such a way that data transmission may not exceed a certain amount of time, which will be known to all of the authorized nodes participating therein. Thus, if the policing node **33** detects a NAV value outside of the allotted amount of time, it will then generate an intrusion alert based thereon.

In accordance with a another embodiment of the MANET **40** illustrated in FIG. 4, the nodes **41, 42** may operate in contention or contention-free modes. That is, in a contention mode all network nodes are required to contend for access to the particular channel being used for each packet of data that is transmitted. During a contention-free period (CFP), channel usage is controlled by a designated control node, which thus eliminates the need for nodes to contend for channel access. In the case of MANETs having nodes arranged in groups or clusters, a cluster leader node may designate when a CFP is to be implemented, for example, as will be appreciated by those of skill in the art.

Thus, the policing node **43** may advantageously detect intrusions into the MANET **40** by monitoring transmissions among the nodes **41, 42** to detect contention-free mode operation outside of a CFP. As such, an intrusion alert may be generated by the policing node **43** based upon such detection.

In other words, detection of a node operating in contention-free mode outside of a CFP indicates that this node is not an authorized node, as all authorized nodes will be informed by the designated control node when a CFP has been instituted.

Of course, this would also be the case when contention mode operation is detected during a CFP, and such embodiment is illustratively shown in FIG. 5. It will be appreciated by those skilled in the art that either one or both of the above CFP intrusion detection approaches may be implemented in a given application.

Referring now to FIG. 6, another embodiment of MANET **60** is now described. Here, the policing node **63** detects intrusions into the MANET **60** by monitoring transmissions among the nodes **61, 62** to detect transmissions during an unauthorized period. That is, the MANET **60** may be implemented such that no users are allowed to access the network during specified hours (e.g., between midnight and 6:00 AM). Thus, upon detecting transmissions within this unauthorized period, the policing node **63** may advantageously generate an intrusion alert.

Turning now additionally to FIG. 7, still another embodiment of the MANET **70** is now described. In this embodiment, the various nodes **71, 72** generate integrity check values for data sent therefrom. These integrity check values are then verified by the receiving node to ensure that the integrity of the originally transmitted message data has not been compromised. By way of example, the integrity check value may be generated by processing the message data with an algorithm to provide a value to be included in the message text. This value may then be verified by a receiving node using the algorithm and the data received.

Thus, the policing node **73** detects intrusions into the MANET **70** by monitoring transmissions among the nodes **71, 72** to detect integrity check values which do not correspond

with their respective data packets. That is, if an incorrect data encryption key is used to generate the message ciphertext, or if the message has been tampered with by the rouge node **84**, the integrity check value will most likely be corrupted. As such, the policing node **73** may generate an intrusion alert when such errant integrity check values are detected, as will be appreciated by those of skill in the art.

Still another MANET **80** in accordance with the invention is now described with reference to FIG. 8. Typically, when the above-noted OSI network model is used, a respective MAC sequence number is generated and sent with each data packet from the nodes **81, 82**. That is, with each successive data packet the MAC sequence number is incremented, and thus each packet has a unique MAC sequence number associated therewith. As such, the policing node **83** may detect intrusions into the MANET **80** by monitoring transmissions among the nodes **81, 82** to detect usage of non-consecutive MAC sequence numbers by a node, and generate an intrusion alert based thereon.

Turning now additionally to FIG. 9, another embodiment of the MANET **90** is illustrated in which the policing node **93** detects intrusions into the network by monitoring transmissions among the nodes **91, 92** to detect collisions of packets having a predetermined packet type. In particular, the predetermined packet type may include management frame packets (e.g., authentication, association, and beacon packets), control frame packets (e.g., RTS and CTS packets), and/or data frame packets. The policing node **93** may thus generate an intrusion alert based upon detecting a threshold number of collisions of the predetermined packet type.

As used herein, "collisions" is meant to include simultaneous transmission of packets as well as transmissions within a certain time of one another. That is, if a certain

type of packet is supposed to have a time delay between transmissions, (e.g., a few seconds, etc.), if two such packet types are transmitted too close together (i.e., with less than the requisite delay time between them), this would be considered a collision. By way of example, the threshold number of collisions may be greater than about three, for example, although other thresholds may be used as well. Moreover, the threshold number may be based upon the particular packet type in question, i.e., the threshold number may be different for different packet types.

Additionally, the threshold number may be based upon a percentage of a total number of monitored packets having the predetermined packet type. For example, if a certain percentage (e.g., greater than about 10%) of packets transmitted during a period (e.g., one hour) are involved in collisions, then the intrusion alert may be generated. Alternatively, if a certain percentage of packets out of a total number of packets monitored (e.g., 3 out of 10) are involved in collisions, then the intrusion alert may be generated. Of course, other suitable threshold numbers and methods for establishing the same may also be used.

Referring now to FIG. 10, another embodiment of the MANET **100** is described in which the policing node **103** detects intrusions into the network by monitoring transmissions among the nodes **101**, **102** to detect collisions of a same MAC address. That is, if multiple terminals lay claim to the same MAC address simultaneously or relatively closely to one another, then either an error has occurred or one of the nodes is a rouge node **104**. As such, the policing node **103** generates an intrusion alert based upon detecting a threshold number of such collisions, e.g., greater than about three. Here again, other threshold numbers may also be used, and the threshold number may also be based upon a percentage, as previously discussed above.

An intrusion detection method aspect of the invention for the MANET **10** will now be described with reference to FIG. 11. Beginning at Block **110**, the method includes transmitting data between the plurality of nodes **11**, **12** using the MAC layer, as previously noted above, at Block **111**. The transmissions among the nodes **11**, **12** are monitored to detect FCS errors from one of the MAC addresses, at Block **112**. If a number of FCS errors for the MAC address exceeds a threshold, at Block **113**, an intrusion alert is generated based thereon, at Block **114**, thus ending the method (Block **115**). Otherwise, the transmissions will continue to be monitored, as illustratively shown.

In accordance with a first alternate method aspect of the invention now described with reference to FIG. 12, the method begins (Block **120**) with transmitting data between the nodes **21**, **22**, at Block **121**, and monitoring transmissions to detect failed attempts to authenticate MAC addresses, at Block **122**, as previously noted above. If a number of failed attempts to authenticate a MAC address is detected, at Block **123**, then an intrusion is generated, at Block **124**, thus concluding the method (Block **125**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

A second alternate method aspect of the invention will now be described with reference to FIG. 13. The method begins (Block **130**) with transmitting RTS and CTS packets between the nodes **31**, **32** and then transmitting data, at Block **131**. The RTS and CTS packets transmitted between the nodes **31**, **32** are monitored to detect an illegal NAV value therein, at Block **132**, as previously described above. If an illegal NAV value is detected, at Block **133**, an intrusion alert is generated based thereon, at Block **134**, thus concluding the method (Block **135**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

Turning now to FIG. 14, a third alternate method aspect of the invention is now described. The method begins (Block **140**) with transmitting data between the nodes **41**, **42**, at Block **141**, and monitoring transmissions to detect contention-free mode operation outside of a CFP, at Block **142**, as previously described above. If such operation is detected outside a CFP, at Block **143**, an intrusion alert is generated based thereon, at Block **144**, thus concluding the method (Block **145**). Otherwise, the intrusion monitoring may continue, as illustratively shown. The opposite case in which transmissions are monitored for contention mode operation during CFPs is illustratively shown in FIG. 15 at Blocks **150**-**155**. Here again, both of these methods could be used in a single embodiment, though this need not always be the case.

A fourth method aspect of the invention will now be described with reference to FIG. 16. The method begins (Block **160**) with transmitting data between the nodes **61**, **62**, at Block **161**, and monitoring to detect transmissions during an unauthorized period, at Block **162**, as previously described above. If transmissions are detected during an unauthorized period, at Block **163**, an intrusion alert is generated based thereon, at Block **164** thus concluding the method (Block **165**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

Yet another intrusion detection method aspect of the invention will now be described with reference to FIG. 17. The method begins (Block **170**) with transmitting data between the nodes **71**, **72**, at Block **171**, and monitoring transmissions **172** to detect integrity check values which do not correspond with their respective data packets, as previously described above. If this is the case, an intrusion alert is generated, at Block **173**, thus ending the method (Block **175**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

Turning now to FIG. 18, still another method aspect of the invention is described. The method begins (Block **180**) with transmitting data between the nodes **81**, **82**, at Block **181**. Thus, the method may also include monitoring transmissions to detect usage of non-consecutive MAC sequence numbers by a node, at Block **182**, as previously described above. If such usage is detected, at Block **183**, an intrusion alert is generated, at Block **184**, thus ending the method (Block **185**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

Referring additionally to FIG. 19, another method aspect of the invention begins (Block **190**) with transmitting data packets between the nodes **91**, **92**, at Block **201**, and monitoring transmissions to detect collisions of packets having a predetermined packet type, as noted above, at Block **192**. If a threshold number of collisions of packets having the predetermined packet type are detected, at Block **193**, then an intrusion alert is generated, at Block **194**, ending the method (Block **195**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

Another intrusion detection method aspect of the invention will now be described with respect to FIG. 20. The method begins (Block **200**) with transmitting data between the nodes **101**, **102**, and monitoring transmissions to detect collisions of a same MAC address, at Block **202**, as previously described above. If a threshold number of collisions of a same MAC address are detected, at Block **203**, an intrusion alert is generated, at Block **204**, thus ending the method (Block **205**). Otherwise, the intrusion monitoring may continue, as illustratively shown.

Further intrusion detection aspects of the invention will now be described with reference to FIG. 21. In accordance with the invention, a network or service set identification may be associated with the MANET **10**, or smaller

subsets (e.g., groups/clusters) thereof. As illustratively shown, beginning at Block **210**, data may be transmitted between the nodes **11**, **12**, at Block **211**, and the service set IDs transmitted therewith to identify authorized nodes of the MANET **10**. As such, transmissions among the plurality of nodes **11**, **12** may be monitored to detect service set IDs associated therewith and/or transmissions over a designated network channel not originating from an authorized node, at Block **212**.

As such, if a service set ID that is different from an authorized service set ID of the MANET **10** and/or transmission from an unauthorized node on a network channel is detected, at Block **213**, an intrusion alert may be generated based thereon, at Block **214**. Moreover, the intrusion alert may advantageously be transmitted to one or more nodes in the network, as previously described above, or to another source, at Block **215**. Otherwise, the intrusion monitoring may continue, as illustratively shown.

It will be understood by those skilled in the art that the above described method aspects may all be implemented in one or more of the MANETs described above. Also, additional method aspects of the invention will be apparent to those of skill in the art based upon the above description and will therefore not be discussed further herein.

It will also be appreciated that the above-described invention may be implemented in several ways. For example, the policing node **13** could be implemented in one or more separate, dedicated devices that are not already part of the MANET **10**. Alternately, the invention may be implemented in software to be installed on one or more existing nodes in a MANET where intrusion detection is desired.

Further, many of the above-described aspects of the present invention may advantageously be used for detecting network intrusion even when a rogue node has an authorized network or MAC ID (e.g., contention-free operation outside a

CFP, transmission during an unauthorized period, etc.) Moreover, one or more of the above aspects may advantageously be used in a given application to provide a desired level of intrusion detection. A further advantage of the invention is that it may be used to supplement existing intrusion detection systems, particularly those that focus on intrusion in the upper OSI network layers.

CLAIMS

1. A mobile ad-hoc network (MANET) comprising:

a plurality of nodes for transmitting data therebetween using a media access layer (MAC), each of said nodes having a respective MAC address associated therewith; and

a policing node for detecting intrusions into the MANET by monitoring transmissions among said plurality of nodes to detect at least one of:

(a) frame check sequence (FCS) errors from a MAC address;

(b) failed attempts to authenticate MAC addresses;

(c) service set IDs associated with the MANET;

(d) an illegal network allocation vector (NAV) value, the NAV value indicating a time duration reserved for transmitting the data generated from request to send (RTS) and clear to send (CTS) packets transmitted among said plurality of nodes prior to transmitting data forming;

(e) contention-free mode operation by said plurality of nodes outside of contention-free periods (CFPs); and

(f) contention mode operation during a CFP; and then

generating an intrusion alert based upon at least one of:

(a) detecting a number of FCS errors for the MAC address exceeding a threshhold;

(b) detecting a number exceeding a threshhold of failed attempts to authenticate a MAC address;

(c) one of the detected service set IDs being different than the service set ID of the MANET;

(d) the detected illegal NAV value;

(e) detecting contention mode operation during a CFP; and

(f) detecting contention-free mode operation outside a CFP.

2. The MANET of Claim 1 wherein said plurality of nodes transmit data over at least one channel; and wherein said policing node further detects transmissions over the at least one channel not originating from one of the plurality of nodes and generates an intrusion alert based thereon.

3. The MANET of Claim 1 wherein said policing node further transmits an intrusion alert to at least one of said plurality of nodes.

4. An intrusion detection method for a mobile ad-hoc network (MANET) comprising a plurality of nodes, the method comprising:

transmitting data between the plurality of nodes using a media access layer (MAC), each of the nodes having a respective MAC address associated therewith;

monitoring transmissions among the plurality of nodes to detect at least one of:

(a) frame check sequence (FCS) errors from a MAC address;

(b) failed attempts to authenticate MAC addresses;

(c) service set Ids associated with the MANET;

(d) an illegal network allocation vector (NAV) value, the NAV value indicating a time duration reserved for transmitting the data generated from request to send (RTS) and clear to send (CTS) packets transmitted among said plurality of nodes prior to transmitting data forming;

(e) contention-free mode operation by said plurality of nodes outside of contention-free periods (CFPs); and

(f) contention mode operation during a CFP; and then

generating an intrusion alert based upon at least one of:

(a) detecting a number of FCS errors for the MAC address exceeding a threshhold;

(b) detecting a number exceeding a threshhold of failed attempts to authenticate a MAC address;

(c) one of the detected service set IDs being different than the service set ID of the MANET;

(d) the detected illegal NAV value;

(e) detecting contention mode operation during a CFP; and

(f) detecting contention-free mode operation outside a CFP.

5. The method of Claim 4 including transmitting data over at least one channel by said plurality of nodes; and wherein said policing node further comprises detecting transmissions over the at least one channel not originating from one of the plurality of nodes and generating an intrusion alert based thereon.

6. The method of Claim 4 wherein said policing node further comprises transmitting an intrusion alert to at least one of said plurality of nodes.

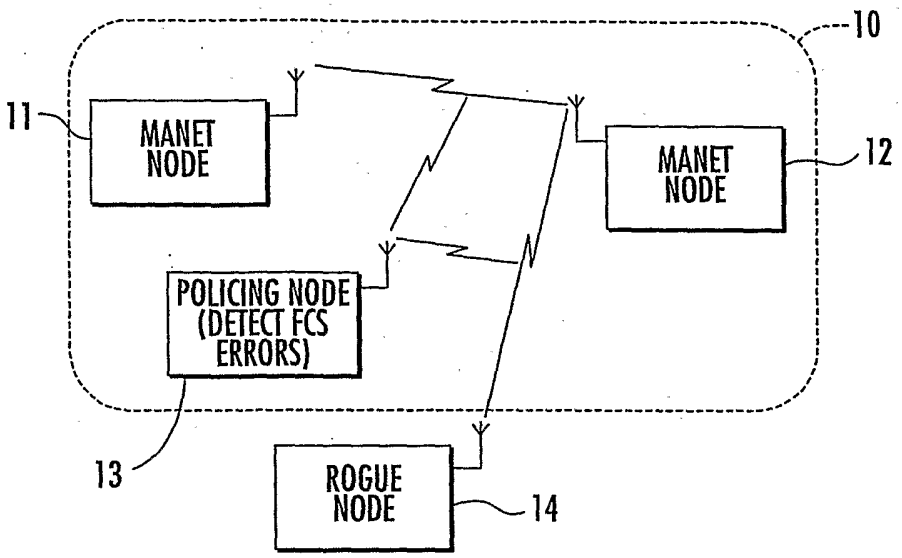

10
11
MANET NODE
MANET NODE
12
POLICING NODE (DETECT FCS ERRORS)
13
ROGUE NODE
14

FIG. 1.

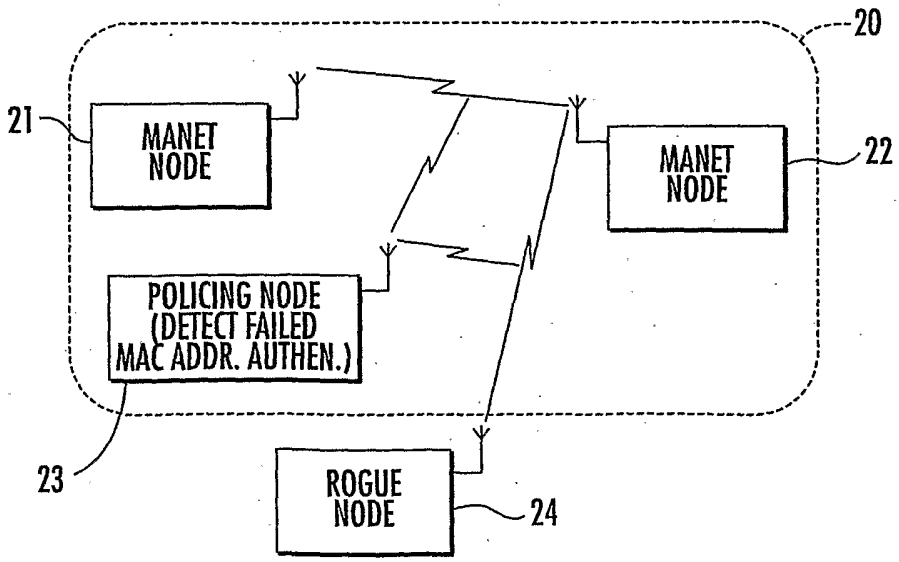

20
21
MANET NODE
MANET NODE
22
POLICING NODE (DETECT FAILED MAC ADDR. AUTHEN.)
23
ROGUE NODE
24

FIG. 2.

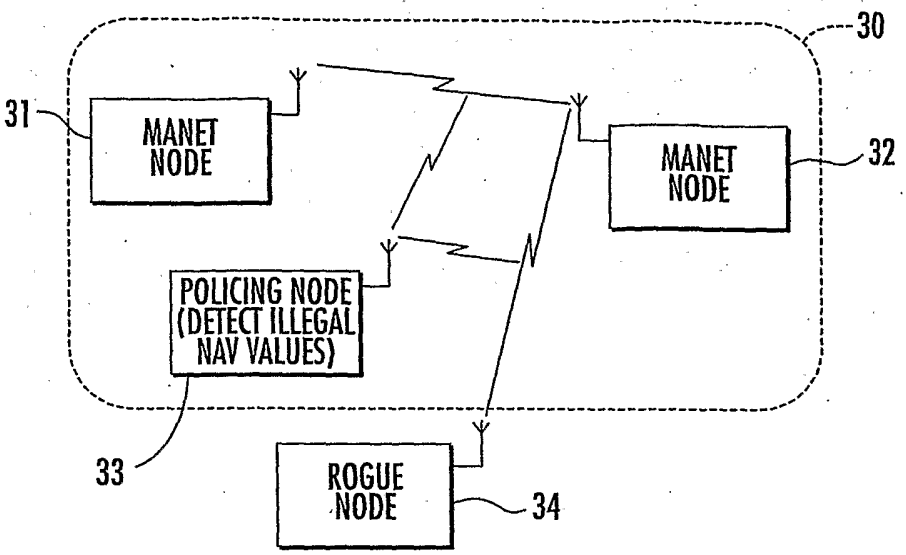

30
31
MANET NODE
MANET NODE
32
POLICING NODE (DETECT ILLEGAL NAV VALUES)
33
ROGUE NODE
34

FIG. 3.

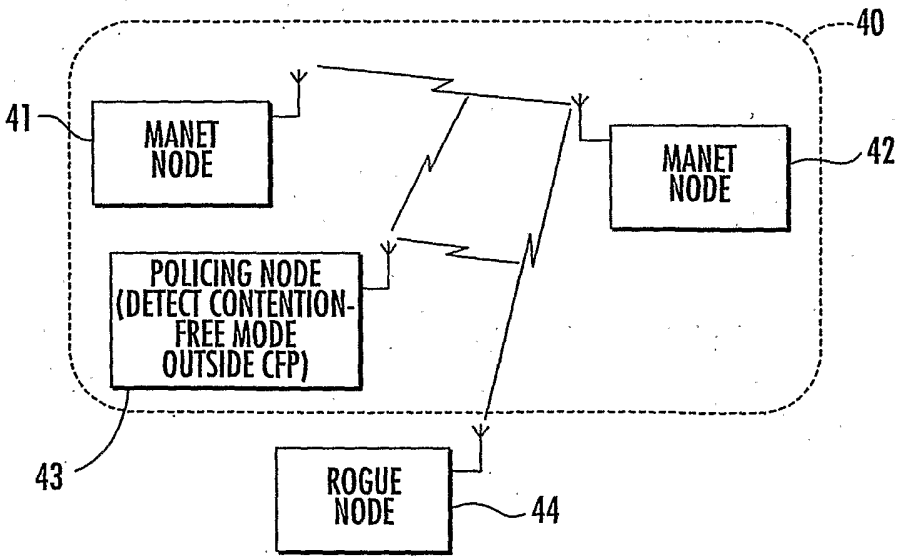

40
41
MANET NODE
MANET NODE
42
POLICING NODE (DETECT CONTENTION-FREE MODE OUTSIDE CFP)
43
ROGUE NODE
44

FIG. 4.

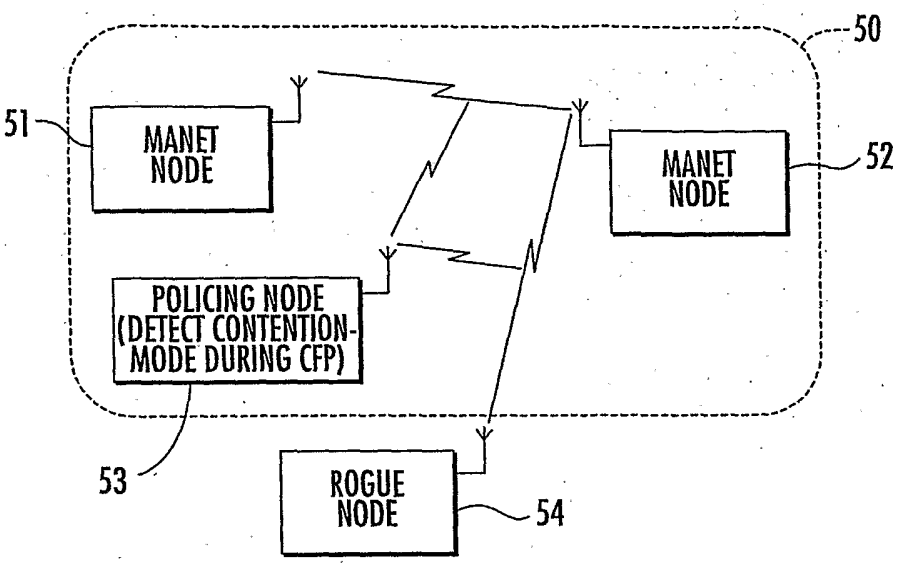

50
51
MANET NODE
MANET NODE
52
POLICING NODE (DETECT CONTENTION-MODE DURING CFP)
53
ROGUE NODE
54

FIG. 5.

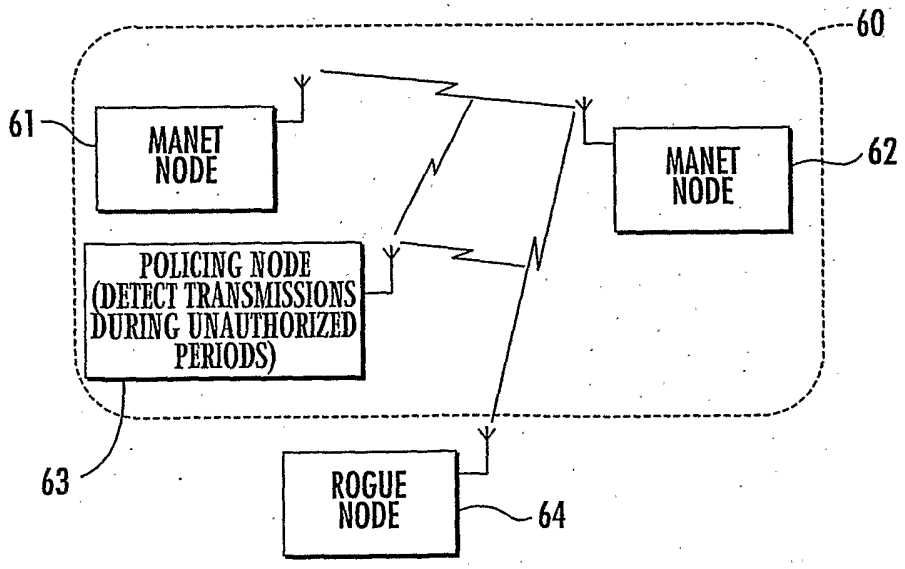

60
61
MANET NODE
MANET NODE
62
POLICING NODE (DETECT TRANSMISSIONS DURING UNAUTHORIZED PERIODS)
63
ROGUE NODE
64

FIG. 6.

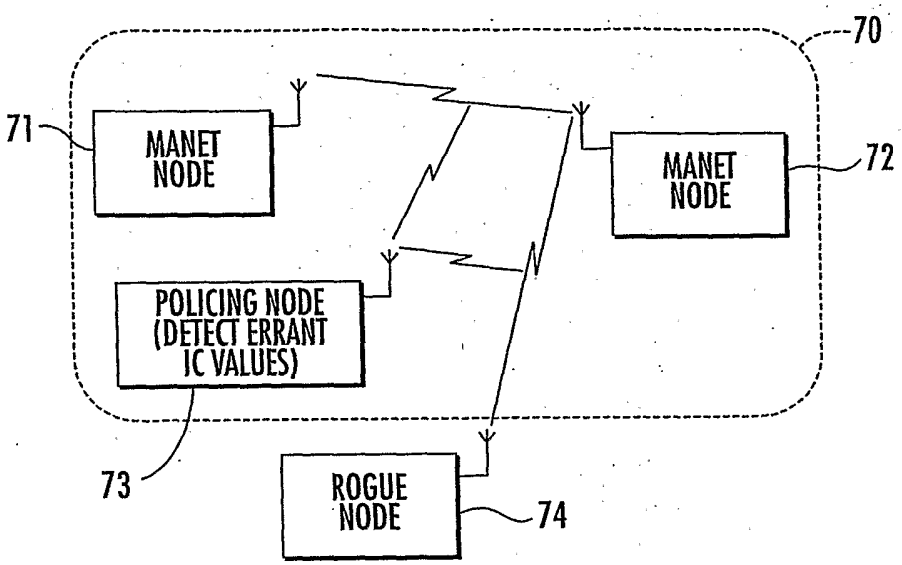

70
71
MANET NODE
MANET NODE
72
POLICING NODE (DETECT ERRANT IC VALUES)
73
ROGUE NODE
74

FIG. 7.

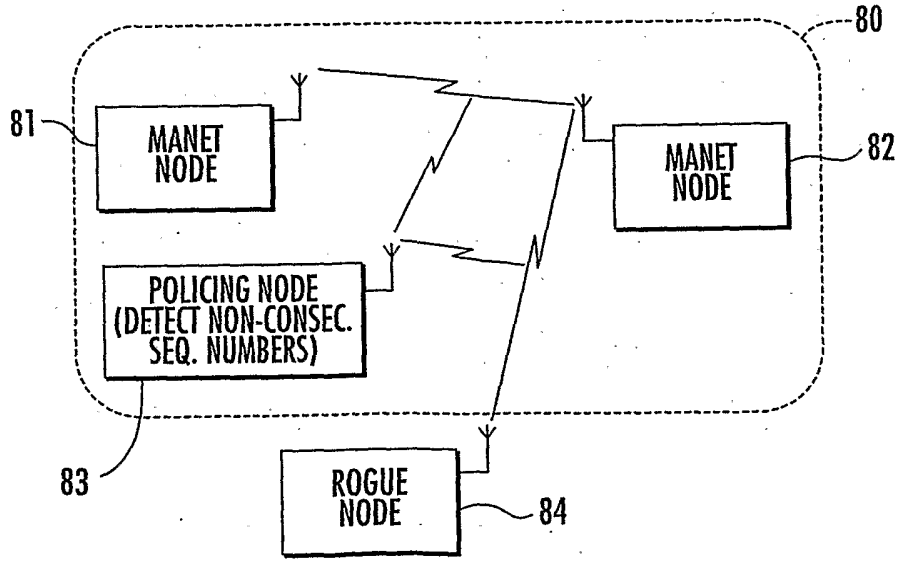

80
81
MANET NODE
MANET NODE
82
POLICING NODE (DETECT NON-CONSEC. SEQ. NUMBERS)
83
ROGUE NODE
84

FIG. 8.

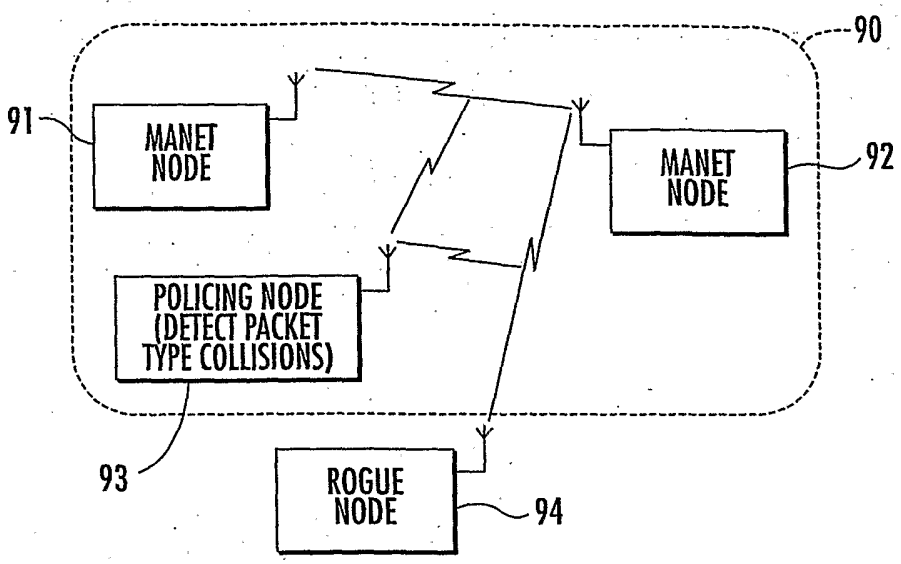

90
91
MANET NODE
MANET NODE
92
POLICING NODE (DETECT PACKET TYPE COLLISIONS)
93
ROGUE NODE
94

FIG. 9.

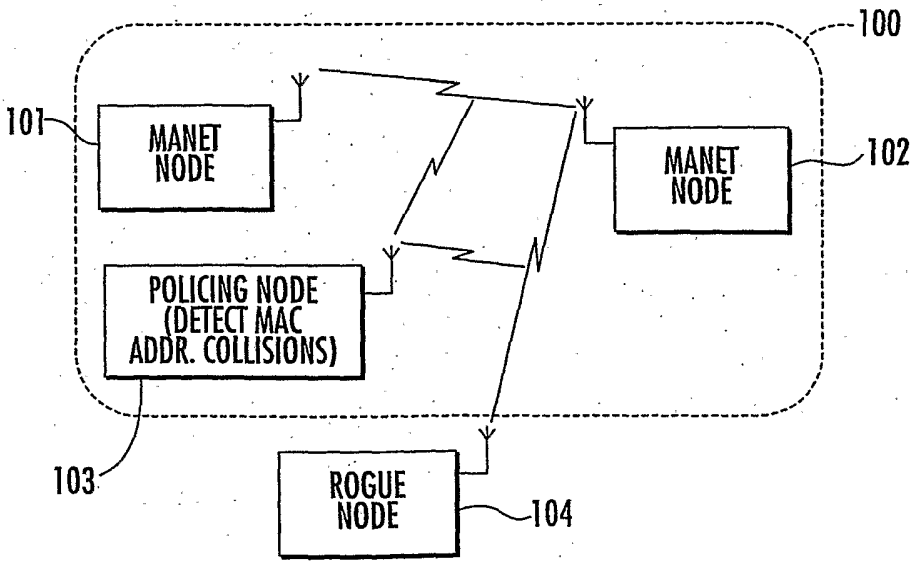

100
101
MANET NODE
MANET NODE
102
POLICING NODE (DETECT MAC ADDR. COLLISIONS)
103
ROGUE NODE
104

FIG. 10.

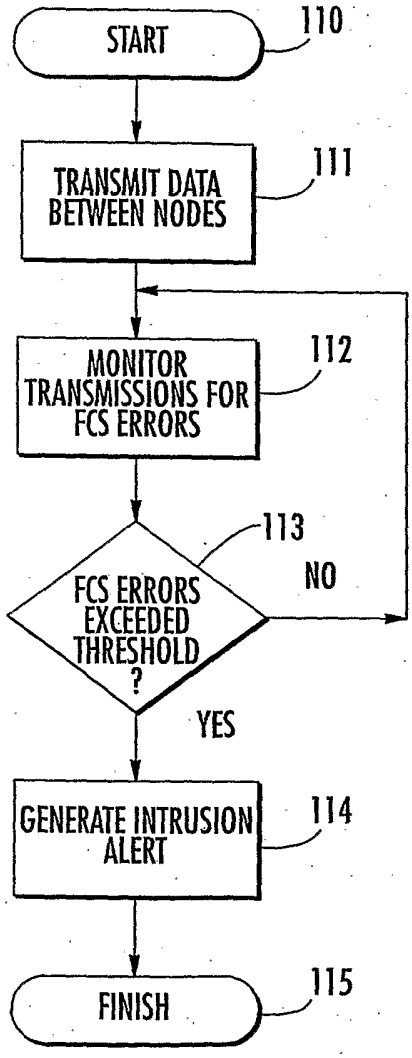

START
110
TRANSMIT DATA BETWEEN NODES
111
MONITOR TRANSMISSIONS FOR FCS ERRORS
112
FCS ERRORS EXCEEDED THRESHOLD ?
113
NO
YES
GENERATE INTRUSION ALERT
114
FINISH
115

FIG. 11.

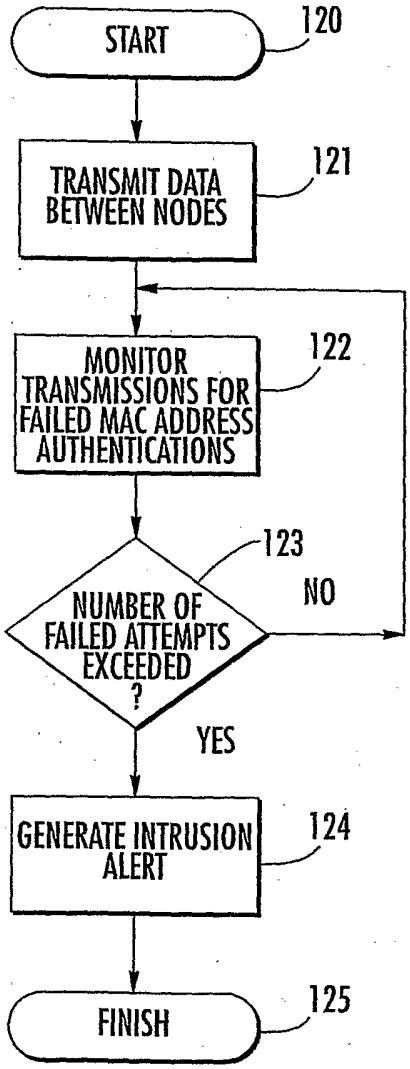

START
120
TRANSMIT DATA BETWEEN NODES
121
MONITOR TRANSMISSIONS FOR FAILED MAC ADDRESS AUTHENTICATIONS
122
NUMBER OF FAILED ATTEMPTS EXCEEDED ?
123
NO
YES
GENERATE INTRUSION ALERT
124
FINISH
125

FIG. 12.

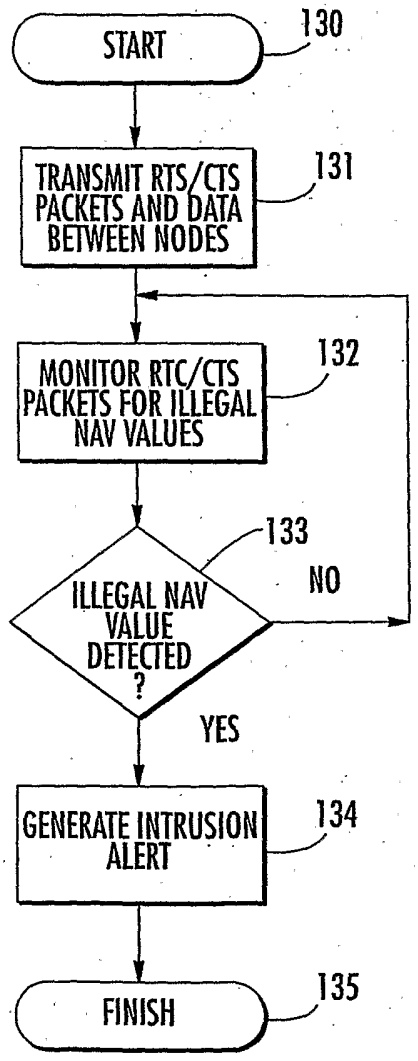

START
130
TRANSMIT RTS/CTS PACKETS AND DATA BETWEEN NODES
131
MONITOR RTC/CTS PACKETS FOR ILLEGAL NAV VALUES
132
ILLEGAL NAV VALUE DETECTED ?
133
NO
YES
GENERATE INTRUSION ALERT
134
FINISH
135

FIG. 13.

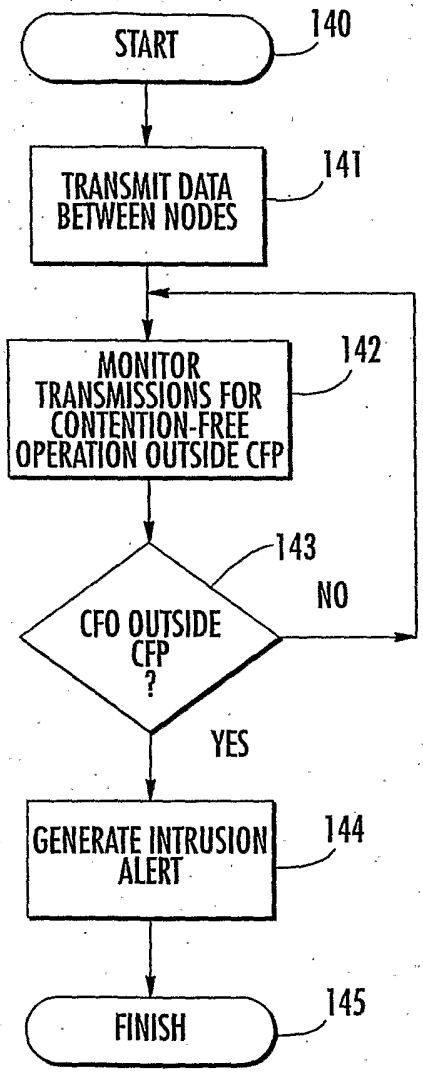

START
140
TRANSMIT DATA BETWEEN NODES
141
MONITOR TRANSMISSIONS FOR CONTENTION-FREE OPERATION OUTSIDE CFP
142
CFO OUTSIDE CFP ?
143
NO
YES
GENERATE INTRUSION ALERT
144
FINISH
145

FIG. 14.

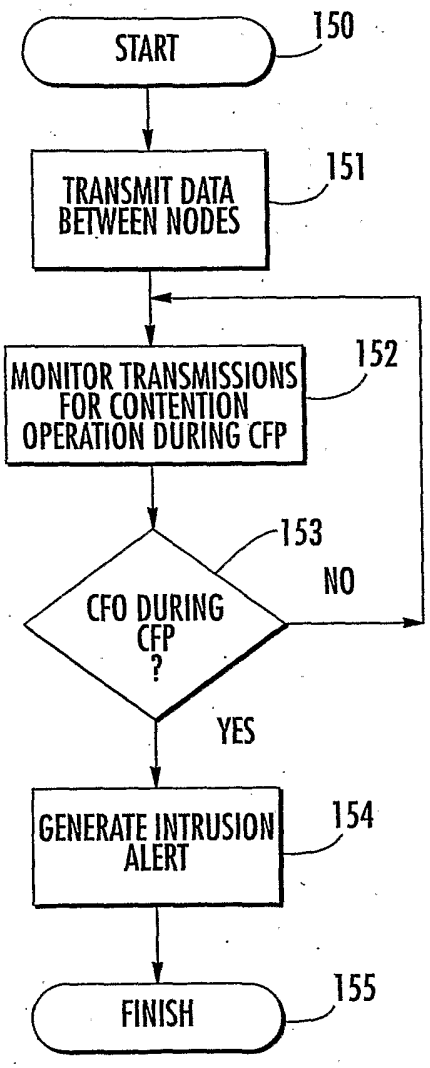

START
150
TRANSMIT DATA BETWEEN NODES
151
MONITOR TRANSMISSIONS FOR CONTENTION OPERATION DURING CFP
152
CFO DURING CFP ?
153
NO
YES
GENERATE INTRUSION ALERT
154
FINISH
155

FIG. 15.

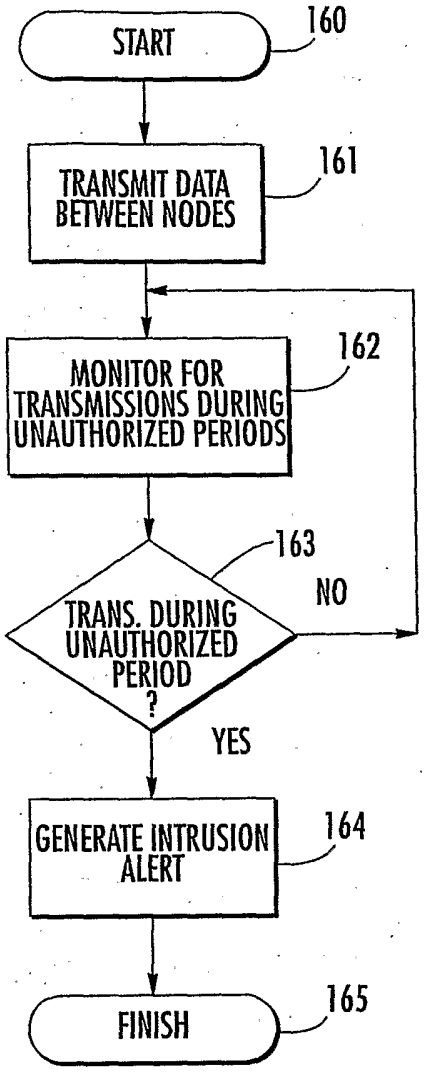

START
160
TRANSMIT DATA BETWEEN NODES
161
MONITOR FOR TRANSMISSIONS DURING UNAUTHORIZED PERIODS
162
TRANS. DURING UNAUTHORIZED PERIOD ?
163
NO
YES
GENERATE INTRUSION ALERT
164
FINISH
165

FIG. 16.

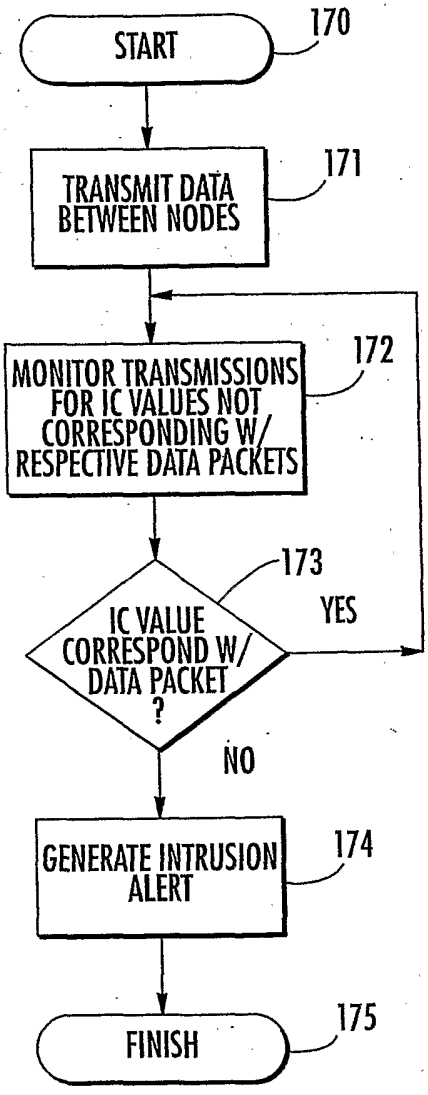

START
170
TRANSMIT DATA BETWEEN NODES
171
MONITOR TRANSMISSIONS FOR IC VALUES NOT CORRESPONDING W/ RESPECTIVE DATA PACKETS
172
IC VALUE CORRESPOND W/ DATA PACKET ?
173
YES
NO
GENERATE INTRUSION ALERT
174
FINISH
175

FIG. 17.

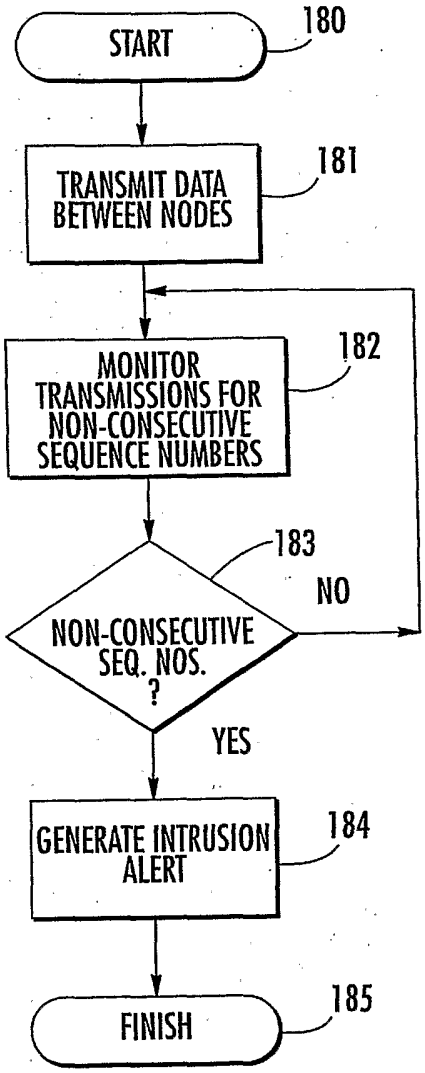

START
180
TRANSMIT DATA BETWEEN NODES
181
MONITOR TRANSMISSIONS FOR NON-CONSECUTIVE SEQUENCE NUMBERS
182
NON-CONSECUTIVE SEQ. NOS. ?
183
NO
YES
GENERATE INTRUSION ALERT
184
FINISH
185

FIG. 18.

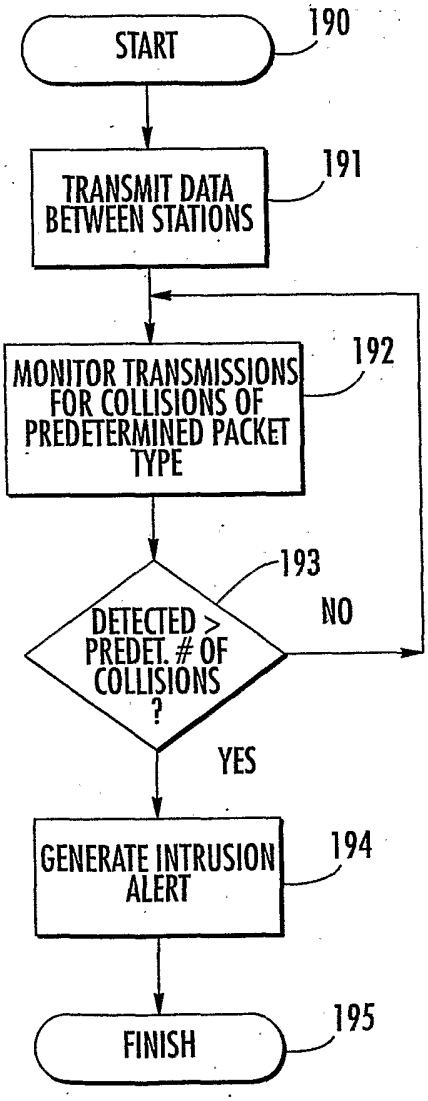

START
190
TRANSMIT DATA BETWEEN STATIONS
191
MONITOR TRANSMISSIONS FOR COLLISIONS OF PREDETERMINED PACKET TYPE
192
DETECTED > PREDET. # OF COLLISIONS ?
193
NO
YES
GENERATE INTRUSION ALERT
194
FINISH
195

FIG. 19.

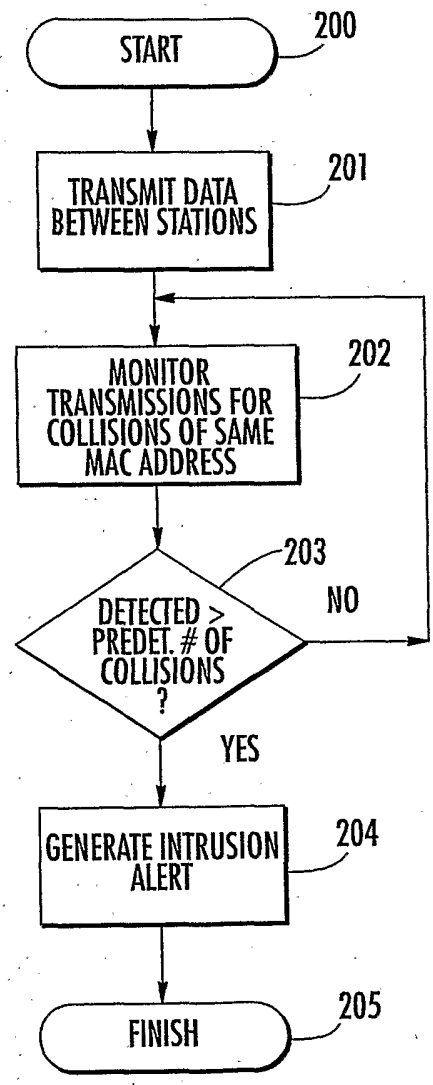

START
200
TRANSMIT DATA BETWEEN STATIONS
201
MONITOR TRANSMISSIONS FOR COLLISIONS OF SAME MAC ADDRESS
202
DETECTED > PREDET. # OF COLLISIONS ?
203
NO
YES
GENERATE INTRUSION ALERT
204
FINISH
205

FIG. 20.

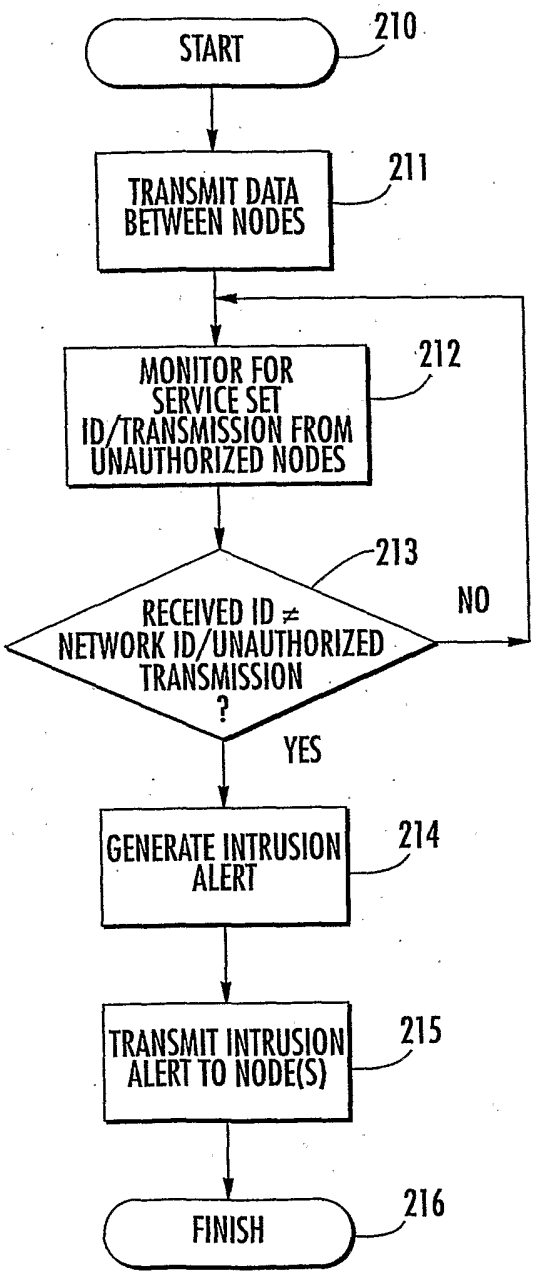

START
210
TRANSMIT DATA BETWEEN NODES
211
MONITOR FOR SERVICE SET ID/TRANSMISSION FROM UNAUTHORIZED NODES
212
RECEIVED ID ≠ NETWORK ID/UNAUTHORIZED TRANSMISSION ?
213
NO
YES
GENERATE INTRUSION ALERT
214
TRANSMIT INTRUSION ALERT TO NODE(S)
215
FINISH
216

FIG. 21.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/25103

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04J 3/24
US CL : 370/349

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. : 370/349,312-313,408-409,474-475.

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,160,804 A (AHMED et al.) 12 December 2000 (12.12.2002), see abstract	1-6
A	US 6,047,330 A (STRACKE, JR.) 04 April 2000 (04.04.2002), See Abstract.	1-6

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2003 (28.11.2003)	11 DEC 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer DANG TON Telephone No. (703) 872-9314

Form PCT/ISA/210 (second sheet) (July 1998)