

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/014891 A2

(51) International Patent Classification⁷: **G06F 1/00**

(21) International Application Number: PCT/US02/23226

(22) International Filing Date: 19 July 2002 (19.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/309,862 3 August 2001 (03.08.2001) US
09/992,310 19 November 2001 (19.11.2001) US

(71) Applicant: **THE BOEING COMPANY** [US/US]; P.O.
Box 3707, M/S 13-08, Seattle, WA 98124-2207 (US).

(72) Inventor: **ROCKWELL, Lawrence, I.**; 8018-146th Av-
enue NE, Redmond, WA 98052 (US).

(74) Agent: **GALBRAITH, Ann, K.**; The Boeing Company,
P.O. Box 3707, M/S 13-08, Seattle, WA 98124-2207 (US).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, 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, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (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: AN AIRBORNE SECURITY MANAGER

(57) **Abstract:** An airborne security management system is provided for monitoring security activities in a mobile network platform. The airborne security management system includes a mobile network that is interconnected via an unreliable communication link to a terrestrial-based network security management system; an intrusion detection system connected to the mobile network and operable to detect a security intrusion event whose origination is associated with the mobile network; and a mobile security manager adapted to receive the security intrusion events from the intrusion detection system. The mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system. The mobile security manager is further operable to command security response activities on the mobile network platform, when the mobile network platform is not connected with network security management system.



WO 03/014891 A2

AN AIRBORNE SECURITY MANAGER

[0001] This application claims priority under 35 U.S.C. §119(e) to United States Provisional Application No. 60/309,862 filed on August 3, 2001, and entitled "An Airborne Security Manager" the specification and drawings of which are hereby expressly incorporated by reference.

TECHNICAL FIELD

5 **[0002]** The present invention relates generally to an airborne security management system for monitoring security activities in a mobile network platform, and more particularly to an autonomous airborne security manager for responding to detected security intrusion events when the mobile network platform is or is not in communication with a terrestrial-based network security
10 management system.

BACKGROUND OF THE INVENTION

[0003] Broadband data and video services, on which our society and economy have grown to depend, have heretofore generally not been readily available to users onboard mobile network platforms such as aircraft, ships, trains,
15 automobiles, etc. While the technology exists to deliver such services to most forms of mobile network platforms, past solutions have been generally quite expensive, with low data rates and/or available to only very limited markets of government/military users and some high-end maritime markets (i.e., cruise ships).

[0004] Previously developed systems which have attempted to provide data and video services to mobile network platforms have done so with only limited success. One major obstacle has been the high cost of access to such broadband data and video services. Another problem is the limited capacity of
5 previously developed systems, which is insufficient for mobile network platforms carrying dozens, or even hundreds, of passengers who each may be simultaneously requesting different channels of programming or different data services. Furthermore, presently existing systems are generally not readily scalable to address the demands of the traveling public.

10 [0005] Of particular interest, presently existing systems also have not comprehensively addressed security issues relating to the mobile network platform. Therefore, it is desirable to provide a network security architecture for monitoring, reporting and responding to onboard security activities in a mobile network platform. It is envisioned that such a network security architecture should
15 be designed to (a) secure computing resources to which passengers may have access on the mobile platform; (b) communicate reliably with terrestrial-based system components over an unreliable communication link; (c) provide a policy mediated response to detected security intrusion events occurring on the mobile platform; and (d) scale the management of the system to hundreds or thousands
20 of mobile platforms.

SUMMARY OF THE INVENTION

[0006] In accordance with the present invention, an airborne security management system is provided for monitoring security activities in a mobile network platform. The security management system includes a mobile network that is interconnected via an unreliable communication link to a terrestrial-based network security management system; an intrusion detection system connected to the mobile network and operable to detect a security intrusion event whose origination is associated with the mobile network; and a mobile security manager adapted to receive the security intrusion events from the intrusion detection system. The mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the network security management system. The mobile security manager is further operable to command security response activities on the mobile network platform, when the mobile network platform is not connected with network security management system.

20

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] The various advantages of the present invention will become apparent to one skilled in the art by reading the following specification and subjoined claims and by referencing the following drawings in which:

[0008] Figure 1 is a block diagram depicting a network security

architecture for a mobile network platform in accordance with the present invention;

[0009] Figures 2A and 2B are state machine diagrams illustrating a security policy for a given user access point on the mobile network platform in accordance with the present invention;

[0010] , Figure 3 is a diagram of an exemplary data structure for implementing the security policies of the present invention;

[0011] Figure 4 is a diagram depicting the primary software components of the network security architecture of the present invention;

10 **[0012]** Figure 5 is a block diagram depicting the functional software modules which comprise the airborne security manager in accordance with the present invention;

[0013] Figure 6 is a block diagram depicting the functional components implementing the terrestrial control and data storage functions of a terrestrial-based network security system in accordance with the present invention;

[0014] Figure 7 is an exemplary aircraft browser window used to implement the monitoring and manual control functions of a terrestrial-based network security system in accordance with the present invention; and

[0015] Figure 8 is an exemplary aircraft status window used to
20 implement the monitoring and manual control functions of a terrestrial-based network security system in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Figure 1 illustrates a network security architecture 10 for

monitoring security activities in an unattended mobile network platform 12. The primary purpose of the network security architecture 10 is to monitor, record, report and respond to security-relevant events associated with the mobile network platform 12. In a preferred embodiment, the network security architecture 10 supports a mobile network platform residing in an aircraft. The mobile network platform 12 is in turn interconnected via one or more unreliable wireless communication links 14 to a terrestrial-based communication system 16, including a terrestrial-based network security management system 18. While the following description is provide with reference to an airborne application, it is readily understood that the broad aspects of the network security architecture are applicable to mobile network platforms which may reside in passenger buses, cruise ships, etc.

[0017] It is envisioned that the mobile network platform 12 provides aircraft passengers a suite of broadband two-way data and video communication services. The infrastructure allows information to be transferred to and from the aircraft at high enough data rates to support a variety of services. To do so, the mobile network platform 12 is primarily comprised of four subsystems: an antenna subsystem 22, a receive and transmit subsystem (RTS) 24, a control subsystem 26, and a cabin distribution subsystem 28. Each of these four subsystems will be further described below.

[0018] The antenna subsystem 22 provides two-way broadband data connectivity and direct broadcast television reception capability to the aircraft. Although the invention is not limited thereto, the antenna subsystem 22 is generally designed to provide this connectivity during cruise conditions (limited roll

and pitch angles) of the aircraft. Connectivity with the aircraft is most commonly achieved via a K band Fixed Satellite Service (FSS) satellite, a Broadcast Satellite Service (BSS) satellites, and/or a direct broadcast television service (DBS) satellite.

5 **[0019]** For illustration purposes, additional description is provided for the processing associated with Ku band satellite broadcast signals. The antenna subsystem 22 may receive and/or transmit Ku band satellite broadcast signals. The antenna system 22 down-converts an incoming Ku-band signal, amplifies, and outputs the L-band signals to the RTS 24. The antenna system may also
10 provide a broadband downlink capability. In this case, the antenna system 22 receives an L-band data signal from an on-aircraft modem, up-converts this signal, amplifies it and then broadcasts as a Ku band signal to selected satellite transponders.

[0020] The receive and transmit subsystem (RTS) 24 operates in
15 receive and transmit modes. In receive mode, the RTS 24 may receive rebroadcast video signals, rebroadcast audio signals and/or IP data embedded in an L-band carrier. The RTS 24 in turn demodulates, de-spreads, decodes, and routes the received signals to the cabin distribution subsystem 28. In transmit mode, the RTS 24 sends IP data modulated into an L-band signal. The RTS 24
20 encodes, spreads, and modulates the signal the IP data it receives from the cabin distribution subsystem 28.

[0021] The control subsystem 26 controls the operation of the mobile security platform 12 and each of its four subsystems. Of particular interest, the control subsystem 26 includes one or more intrusion detection subsystems 32 and

an airborne security manager 34. An intrusion detection subsystem 32 is operable to detect security intrusion activities which may occur on or in relation to the mobile network platform. To do so, an intrusion detection subsystem 32 inspects all of the data packets entering a computing device on which it is hosted and, upon detection of a security intrusion activity, transmits a security intrusion event to the airborne security manager 34. As will be apparent to one skilled in the art, the intrusion detection subsystem 32 may be implemented using one of many commercially available software products.

[0022] The airborne security manager 34 is responsible for enforcing security policy for an aircraft. Because communication with the aircraft may be sporadic, the airborne security manager 34 must provide the capability to act autonomously when responding to security intrusion events. When a security intrusion event is detected, the airborne security manager 34 responds appropriately in accordance with a customizable security policy. Thus, the airborne security manager 34 is adapted to receive security intrusion events from any of the intrusion detection subsystems and operable to implement a security response. Exemplary responses may include warnings one or more passengers on the aircraft, alerting terrestrial-based security administrators, and/or disconnecting a passenger's network access.

[0023] The cabin distribution subsystem (CDS) 28 provides network connectivity through a plurality of user access points to the passengers of the aircraft. In a preferred embodiment, the cabin distribution system may be composed of either a series of 802.3 Ethernet switches or 802.11X wireless access points. It should be noted that the current 802.11B standard only allows

for a shared secret between all users of a wireless access point and thus is not suitable for providing the desired level of communication privacy in the passenger cabin. In contrast, next generation wireless standards, such as 802.11X ("X" denotes a revision of 802.11 beyond "B") will support "channelized" or individual user level encryption. It is envisioned that such wireless standards are within the scope of the present invention.

[0024] Each user access point preferably has the properties of a managed layer 3 switch. First, each user access point must enforce the association of IP address and MAC address with a particular port. This requirement is applicable to either a wired and wireless cabin environment. A second requirement for each user access point is to accept a command to shut off its access port. In the case of a wireless access device, a communication channel consisting of a particular frequency, time division or sub-frame substitutes for the physical access port. A third requirement for each user access point is to preclude passengers from eavesdropping or receiving Ethernet packets not directly addressed to them. In a wired cabin distribution system, this can be accomplished through the use of a switched Ethernet architecture. In a wireless cabin distribution system, this can be accomplished through the use of "channel level encryption" specific to a particular user.

[0025] The design of a security policy mechanism is the most fundamental element of the network security architecture 10. In accordance with the present invention, it is envisioned that the security policy will be designed within the following design constraints. First, the security policy mechanism should map different security intrusion events to different responses. It should be

appreciated that the severity of response is based on the danger of the detected activities. Second, the automated response policy has to be enforced at all times (subject to over-ride conditions), regardless of whether airborne to terrestrial communications are available or not. If the automated responses are disabled
5 during periods of connectivity, the connectivity might fail before a security administrator has a chance to take action in which case the system reverts to the automated policy in effect prior to the override. The security administrator can retract the response if they desire. Third, the policy mechanism has to arbitrate between automated responses from the airborne security manager and manual
10 commands received from terrestrial-based security administrators. If the automated system mistakenly blocks a passenger's network address, and the terrestrial administrator overrides that action, the security policy mechanism needs to know about that action and not try to enforce the block.

[0026] State machines are a flexible, yet intuitively appealing,
15 mechanism for modeling complex behaviors. Therefore, state-machines have been chosen to represent the security policies of the present invention. Figures 2A and 2B illustrates basic UML state machines which model the security policy associated with an user access point in the mobile network platform.

[0027] In Figure 2A, each user access point can be in one of three
20 defined states. By default, all user access points begin in a normal state 42. A security intrusion event of any kind will result in a transition to either a suspected state 44 or a disconnected state 46 for the applicable user access point. Each transition is in the form of "event/response" where events are the external triggers that cause the state transition and responses are external actions that the system

initiates when making the transition. For instance, a low or medium priority event 48 occurring in a normal state will cause the system to log the event and/or attempt to provide a warning to the passenger connected at that user access point. The user access point then transitions to the suspected state as shown in

5 Figure 2A.

State machine models may be enhanced to incorporate manual controls. Specific manual control commands enable a terrestrial-based security administrator to explicitly disable or enable a user access point from the ground. By adding a state that indicates that the user access point is under manual control 10 ensures that the automated responses do not override the manual control command received from the security administrator. Therefore, it is envisioned that each state machine may provide an autoreponse disable state 50 as shown in Figure 2B. Transitions to and from the autoreponse disable state are commanded by a terrestrially-based security administrator. While in the 15 autoreponse disable state, the administrator can initiate any one of various predefined security responses. In the event connectivity is lost between the administrator and the aircraft, the state machine model reverts to the normal state or the previous state depending on configuration settings.

State machines models are also used to represent each of the host servers 20 or other types of computing devices which reside on the mobile security platform. In this way, a server that is under attack may respond differently than a user access point. It is also envisioned that each of the state machines can be tied together through synthetic event generation, such that when a server is under attack, the user access points may employ a different security policy that is less

tolerant of suspicious behavior.

[0028] Each state machine can be represented by a data structure 51 as depicted in Figure 3. The data structure includes a current state 52, a possible security event 54, a resulting state 56 and a possible response 58. In this way, 5 each state can be cross-referenced against possible events to produce a resulting state and a list of possible actions. Possible events may include (but are not limited to) a security intrusion event having high priority, a security intrusion event having medium priority, a security intrusion event having a low priority, a reset event, a timer expiration event, a communication link up event, a communication 10 link down event and one or more custom events for supporting manual control commands from the security administrator. Possible responses may include (but are not limited to) setting a timer, installing a filter, resetting a filter, alerting control panel, alerting terrestrial-based security administrator, disconnecting user access point, issuing a passenger warning, and one or more predefined customer 15 responses. One skilled in the art will readily recognize from such discussion how to implement a security policy mechanism in accordance with the present invention.

[0029] Referring to Figure 4, the overall network security architecture 10 may be logically decomposed into five major components. The five major 20 components are airborne policy enforcement 62, air-ground communication 64, terrestrial control and data storage 66, terrestrial monitoring and manual control 68, and terrestrial policy editing and assignment 70. Each of these logical components are also mapped to their physical location within the network security architecture 10 as shown in Figure 4.

[0030] The airborne policy enforcement component 62 is provided by the airborne security manager 34. The primary responsibilities of the airborne security manager include (but are not limited to) managing and monitoring intrusion detection sensors, monitoring other airborne event sources, responding to security events in accordance with the applicable security policy, monitoring the airborne intrusion detection sensors, configuring static network traffic filters at user access points, executing any manual overrides commands from the terrestrial-based network security management system, installing new security policies received from the terrestrial-based network security management system, and reporting events and status of interest to the terrestrial-based network security management system. As will be apparent to one skilled in the art, the airborne security manager 34 is comprised of one or more software applications residing on one or more server(s) on each aircraft. A configuration of redundant airborne security managers provide for fail over in the event of a hardware or software failure.

[0031] With reference to Figure 5, the airborne security manager 34 is further comprised of five functional modules: an event response module 72, an onboard status module 74, a policy manager 76, a persistent storage manager 78, and a communication manager 80. The event response module 72 is responsible for receiving events, interpreting the active security policy, and triggering the appropriate actions in response to each event. It should be appreciated that this module is adapted to handle events other than security intrusion events received from the intrusion detection subsystems.

[0032] In conjunction with the onboard status module 74, the event

response module interprets and executes the state machine representing the active security policy. For instance, upon arrival of a security intrusion event, the event response module determines whether the event is associated with an individual passenger connection, an individual host server, or the airborne security manager as a whole. This module then retrieves the current state of that passenger connection, host server, or airborne security manager from the onboard status module 74 and performs the actions associated with that state and event in accordance with the active security policy. Exemplary actions may include issuing new events, making state transitions, modifying network filters, disabling passenger connections, and/or queuing messages for transmission to the terrestrial-based network security management system.

[0033] The onboard status module 74 maintains the current state of each individual passenger connection, each host server, and of the airborne security manager as a whole for the purpose of directing the state machine event response. The onboard status module 74 also tracks the status of intrusion detection sensors (e.g., signature file, operational/inactive status, sensor configuration) as well as collects status information from the other onboard modules.

[0034] The policy manager 76 is responsible for reacting to commands from the terrestrial-based network security system regarding security policy loading and activation. The policy manager also serves as a repository for configuration information relating to the airborne security manager, including, for instance, general communications parameters that determine frequency of status reports and event reporting.

[0035] The persistent storage manager 78 manages the overall data storage requirements for the onboard network security architecture. Data residing in persistent storage generally falls into one of three categories: (1) communications queue (i.e., messages to be transmitted to the terrestrial-based security management system), (2) onboard status (i.e., per-passenger connection, per-host, and system-wide data requirements), and (3) security policies. The persistent storage manager may rely on various well known, lightweight mechanisms for data storage.

[0036] Referring to Figure 4, the terrestrial control and data storage (C&DS) component 66 is provided by the terrestrial-based network security management system 16. The control and data storage functions include (but are not limited to) storing all event data in persistent storage, tracking the desired and last known configurations for each aircraft, supporting multiple security management consoles having multiple windows, notifying open console windows of any data changes that affect the window contents, providing an interface for effecting manual overrides in security policy, offering a reporting interface for reviewing stored data, and controlling access to all stored data. This component may be implemented using Java-based applications residing on one or more terrestrial servers which constitute the network security management system 16.

[0037] A more detailed description of the terrestrial control and data storage component 66 is provided with reference to Figure 6. This terrestrial component will maintain one aircraft object 90 for each aircraft associated with the security architecture. The aircraft object 90 maintains all state information for a given aircraft as well as keeps track of the last reported and the desired state of

the airborne security manager 34 residing on the given aircraft. The aircraft object 90 is a dynamic object, such that its state is maintained in dynamic memory and can be reconstructed from event histories, if necessary. Any activity that could alter the state of the airborne security manager 34 is performed by invoking a method of the aircraft object. Each method represents an event and is logged in an appropriate event log. In addition, these methods are all synchronized, ensuring that only one thread can be effecting state changes at any given time. In order to eliminate the possibility of deadlock, none of these event operations will block on communication or issue events to other aircraft.

10 **[0038]** The aircraft object 90 uses a communication subsystem 100 to exchange information with the airborne security manager 34. The aircraft object 90 issues commands and requests for status reports as well as receives events and status reports. Until an appropriate event or status report is received, any command is considered pending. This does not mean that the command has not yet executed – it may not have been executed, or it may have been and the acknowledging status report has simply not yet been received. Due to this gap in knowledge about what is actually taking place onboard the aircraft, the aircraft object 90 must carefully differentiate between the last known status and the desired status.

20 **[0039]** The aircraft object 90 is the controller in a Model-View-Controller architecture as is well known in the art. In this paradigm, the model is the data stored in a database, and the views are the various user interfaces being used to display information about the aircraft. The aircraft object is responsible for updating all of the views any time the model changes. In order to enforce this, all

changes to the model must be performed by the aircraft object and the aircraft object must keep track of those user interfaces that could be affected by the change.

[0040] The aircraft object 90 also maintains a collection of host objects 5 92 and passenger connection objects 94. The host objects 92 are used to represent the state of each onboard host server that the airborne security manager 34 is responsible for. The passenger connection objects 94 represent the individual passenger connections to the onboard network.

[0041] The terrestrial control and data storage component 66 also 10 includes a single aircraft container object 96. It is envisioned that this object may be implemented as a collection class, such as a hash table. Under this approach, aircraft objects will be created by the aircraft container 96 for every aircraft in the system. By routing incoming communication through the aircraft container 96, we ensure that the communication subsystem 100 will be able to deliver incoming 15 messages to the appropriate aircraft object. In addition, the container concept may be used to facilitate the manner in which aircraft objects are created. For instance, aircraft objects may be created only as they are needed. When an incoming message is received, the aircraft container 96 locates the applicable aircraft object. If the aircraft object is not present in memory, the aircraft container 20 can create the object. Likewise, aircraft objects that are no longer being actively monitored could be deleted until they are needed again.

[0042] The terrestrial control and data storage component 66 will also maintain event histories for each of the aircraft in a central database 98. The database 98 will maintain a record of all the events reported by an aircraft in the

system. In addition, it will maintain a record of all of the commands performed by terrestrial-based security administrator. The former represents the last known state of each aircraft; whereas the latter represents the desired stated of each aircraft. The choice of the term "last known" reflects the time delay between
5 events occurring on board the aircraft which might not have been reflected on the ground.

[0043] Security policy files are also stored within the database 98. As a configuration option, in order to maintain a history of old policies, the policy tables may be append-only. The primary policy table will maintain a mapping of names
10 and version numbers to a series of smaller policy elements. The communication subsystem 100 interfaces with the database 98 in order to retrieve security policy files and update the policy files onboard the aircraft.

[0044] A policy manager 99 will be responsible for any changes to policy files. This object is necessary because policy is the only thing that is not
15 associated with a single aircraft. The policy manager 99 will ensure that any changes to policy files are properly versioned. It will also be responsible for delivering updated policy to one or more aircraft.

[0045] Returning to Figure 4, the terrestrial monitoring and manual control component 68 and the terrestrial policy editing and assignment component
20 70 also reside at the terrestrial-based network security management system 12. The monitoring and manual control component functions include (but are not limited to) monitoring the state and activities of a group of aircraft and selecting an individual aircraft for closing examination, monitoring the state and activities of a single aircraft and selecting an individual server or passenger connection for

closer examination, monitoring the state and activities of a single airborne server, manually controlling a single airborne server, monitoring the state and activities of a single airborne passenger connection, and manually controlling a single airborne passenger connection. This component may be implemented using a Java-based user interface running on one or more terrestrial servers.

[0046] To support the monitoring and manual control functions, the user interface includes a number of windows that may be monitored by a human network security administrator. For instance, an aircraft browser allows groups of aircraft to be navigated and aggregate/summary information displayed as shown in Figure 7. However, this window does not show the status of the communication link. In order to display such status information, the user can select a specific aircraft from the aircraft browser, thereby navigating to an aircraft status window. An exemplary aircraft status window is shown in Figure 8. The aircraft status window enables the user to view all data relevant to a specific aircraft in a single tree structure view 102. In addition, all logged events and commands are displayed in a lower log panel 104. The tabs 106 along the top of the window permit navigation to other panels which in turn focus on a different specific element associated with the aircraft. For instance, the seat panel 108 will provide status information, log detail, and manual controls for a specific seat. Other exemplary windows used to support the monitoring and manual control functions may include (but is not limited to) a passenger connection status window that focuses on displaying information for a single passenger connection, an onboard host status window that focuses on displaying information on a specific host computing device residing on the aircraft, and an events log window that displays

event information for a given group, aircraft, passenger connection or host device.

It is envisioned that the above-described windows are merely representative of some of the functionality and appearance that be used to implement the monitoring and manual control functions of the present invention.

5 **[0047]** In addition to monitoring and manual control, services for editing security policy files and distributing security policy updates also reside at the terrestrial-based network security management system 16. The policy editing and application functions include (but are not limited to) editing sensor configuration files, retrieving intrusion detection signature file updates from the applicable
10 vendor website, editing response policy state machines and parameters, editing static security configurations, combining sensor files, signature files, response policies, and static configuration into specific security policies, providing version control over security policy updates, browsing the aircraft in the system by last known policy and desired policy, and distributing a new policy to a selected group
15 of aircraft. The editing of security policy is not intended to be a routine daily activity. For this reason, policy editing and application functions are treated as a separate, distinct logical component from the other functions administered through the user interface running on the terrestrial servers.

[0048] The air-ground communication component 64 is responsible for
20 communication between the airborne security manager and the terrestrial servers. Thus, this component is distributed across these two physical locations. The air-ground communication functions include (but are not limited to) providing non-blocking communications, retrying transmissions until reliable delivery is achieved, queuing up messages during periods of non-connectivity, handling communication

session authentication, utilizing cryptographic integrity checks to protect against tampering and replay, optimizing away redundant or superseded messages where possible, utilizing available bandwidth according to message priorities, minimizing bandwidth consumption, and delivering security policy updates to aircrafts.

- 5 Logically isolating the communications component helps protect the design of the airborne security manager and the terrestrial servers from unnecessary complexity arising from sporadic connectivity.

[0049] The foregoing discussion discloses and describes preferred embodiments of the invention. One skilled in the art will readily recognize from
10 such discussion, and from the accompanying drawings and claims, that changes and modifications can be made to the invention without departing from the true spirit and fair scope of the invention as defined in the following claims.

What is claimed is:

1. A network security architecture for monitoring security activities in a mobile network platform, comprising

5 a mobile network residing on the mobile network platform, the mobile network being interconnected via an unreliable communication link to a terrestrial-based network security management system;

an intrusion detection system connected to the mobile network and residing on the mobile network platform, the intrusion detection system operable to detect a security intrusion event that is associated with the mobile network; and

10

a mobile security manager residing on the mobile network platform and adapted to receive the security intrusion events from the intrusion detection system, the mobile security manager is further operable to perform security response activities in response to the security intrusion events, when the mobile network platform is not connected with network security management system.

15

2. The network security architecture of Claim 1 wherein the mobile security manager is operable perform security response activities in accordance with a security policy resident on the mobile network platform.

20

3. The network security architecture of Claim 2 wherein the security policy is defined as a plurality of predefined security intrusion events and a

corresponding security response for each of said plurality of security intrusion events.

4. The network security architecture of Claim 2 wherein the security
5 policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element, and a security response element.

5. The network security architecture of Claim 1 wherein the mobile
10 network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one of the plurality of user access points.

6. The network security architecture of Claim 5 wherein the security
15 response is selected from the group consisting of logging the security intrusion event received from the intrusion detection system, providing a warning message to at least one of said user access points, providing an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of said user access points, and disconnecting one of said
20 user access points from the mobile network.

7. The network security architecture of Claim 5 wherein the mobile security manager maintains an indicator of the current operational state for each

of the plurality of user access points, such that the security response directed to said one of the plurality of user access points is in part based on the operational state of said one of the plurality of user access points.

5 8. The network security architecture of Claim 7 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

 9. The network security architecture of Claim 7 wherein the mobile
10 security manager is further operable to identify the current operational state for said one of the plurality of user access points and perform security response activities based in part on the identified operational state and the security intrusion event received from the intrusion detection system.

15 10. The network security architecture of Claim 9 wherein the mobile security manager is further operable to modify the current operational state for said one of the plurality of user access points in accordance with the security policy.

20 11. The network security architecture of Claim 1 wherein the mobile security manager is operable to transmit a message indicative of the security intrusion event to the network security management system and to perform security response activities in response to security commands received from the

network security management system.

12. A method for monitoring security activities associated with a network residing in a mobile network platform, the mobile network platform being
5 interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

detecting a security intrusion event whose origination is associated with the network residing on the mobile network platform;

providing a mobile security manager residing on the mobile network
10 platform, where the mobile security manager is adapted to receive the security intrusion event; and

performing a security response activity in response to the detected security intrusion event, when the mobile network platform is not connected with the network security management system.

15

13. The method of Claim 12 wherein the step of performing a security response activity further comprises applying the security response activity in accordance with a security policy, where the security policy is defined as a plurality
20 of predefined security intrusion events and a corresponding security response for each of said plurality of security intrusion events.

14. The method of Claim 12 further comprising the steps of applying the security response activity in accordance with a security policy, where the security policy is defined by a data structure having a current operational state element, a possible security intrusion event element, a resulting operational state element,
5 and a security response element.

15. The method of Claim 12 wherein the network includes a plurality of user access points, such that the security intrusion event is associated with one of the plurality of user access points and the security response is directed to said one
10 of the plurality of user access points.

16. The method of Claim 15 wherein the security response activity is selected from the group consisting of logging the security intrusion event, providing a warning message to at least one of the user access points, providing
15 an alert message to a terrestrial-based network security management system, installing a network traffic blocking filter at one of the user access points, and disconnecting one of the user access points from the network.

17. The method of Claim 15 further comprising the steps of maintaining
20 an indicator of the current operational state for each of the plurality of user access points and performing a security response activity in response to the detected security intrusion event, where the security response activity is in part based on the operational state of said one of the plurality of user access points.

18. The method of Claim 17 wherein the current operational state for any given user access point is selected from the group consisting of a normal state, a suspected state, and a disconnect state.

5

19. An airborne security system for monitoring security activities associated with a network residing on an aircraft, the aircraft being interconnected via an unreliable communication link to a terrestrial-based network security management system, comprising:

10 an intrusion detection system connected to the network and operable to detect a security intrusion event that is associated with network; and

 an airborne security manager connected to the network and adapted to receive the security intrusion event from the intrusion detection system,
15 the security manager is further operable to perform security response activities in accordance with a security policy, when the aircraft is not connected with the network security management system.

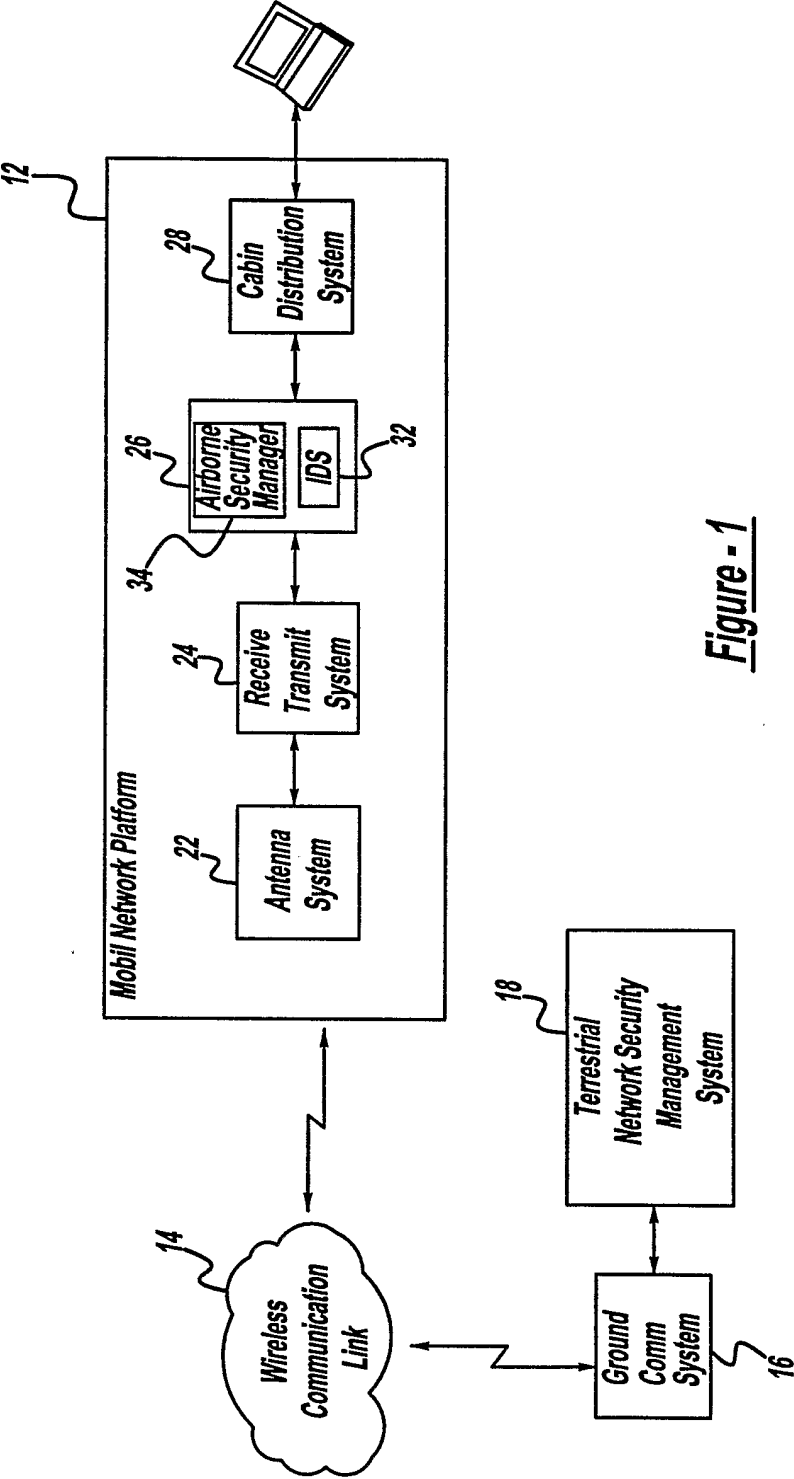


Figure - 1

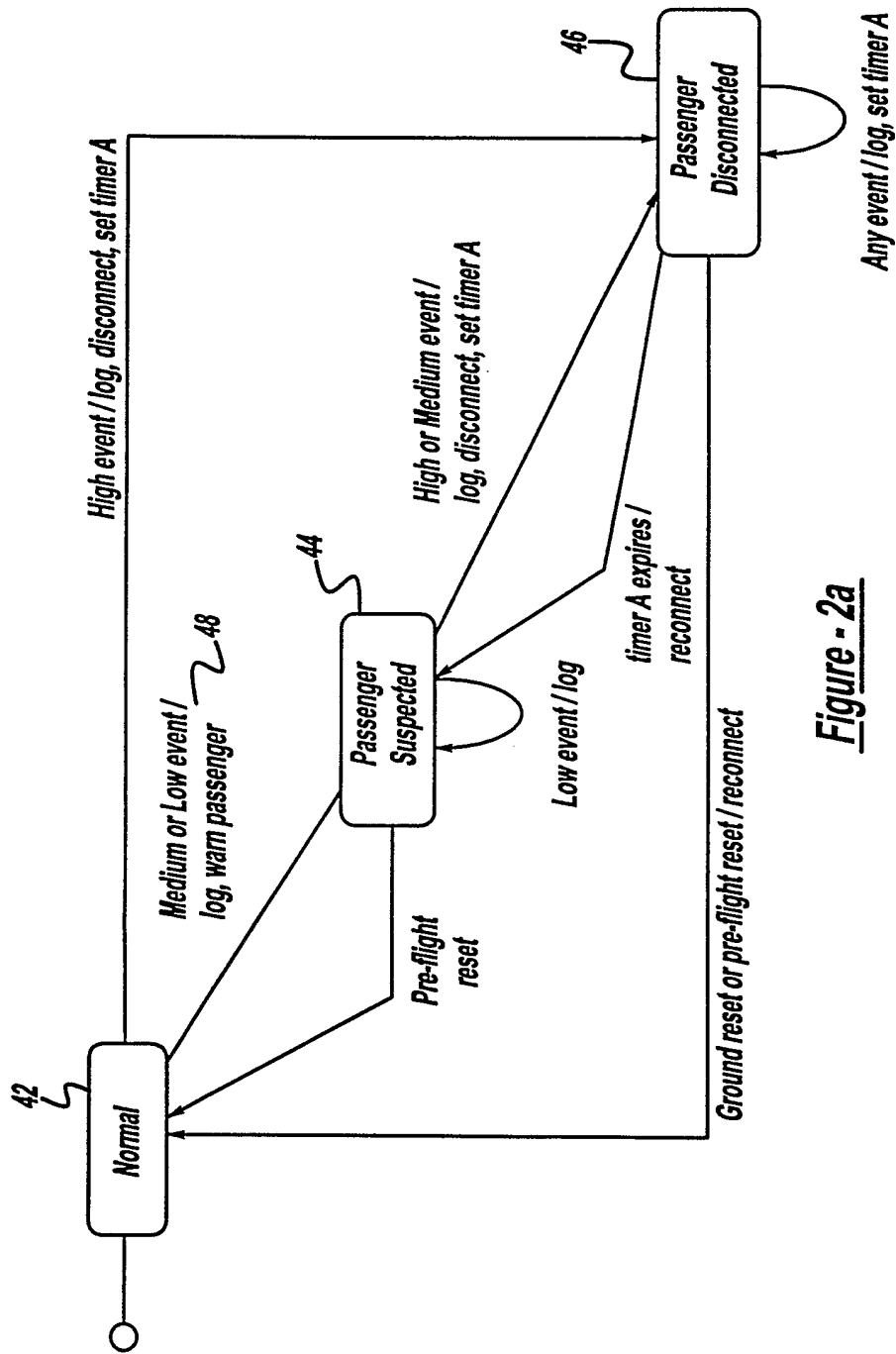


Figure - 2a

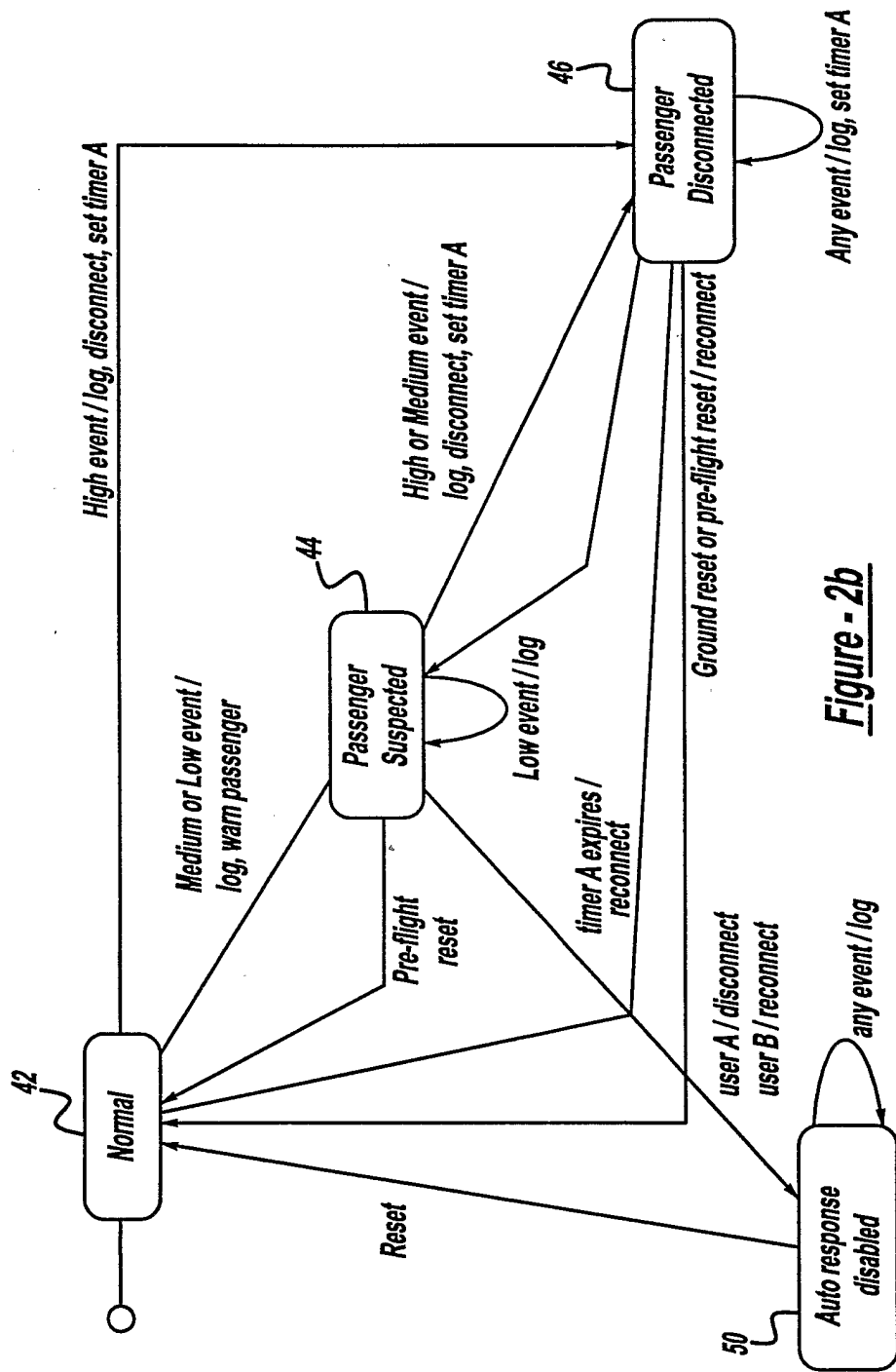


Figure - 2b

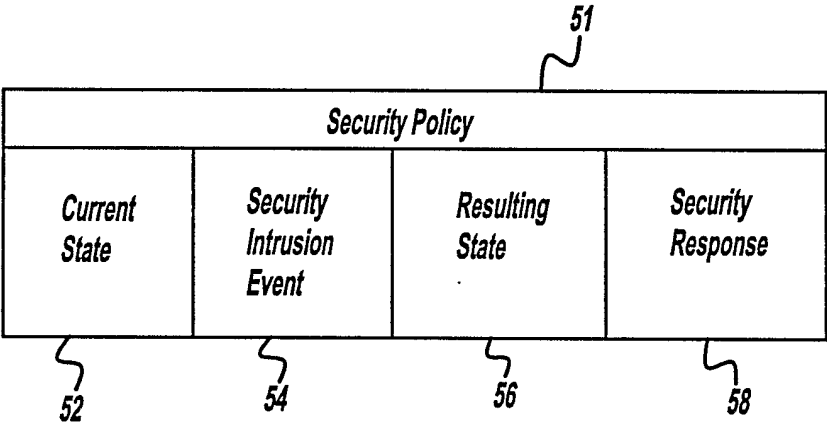


Figure - 3

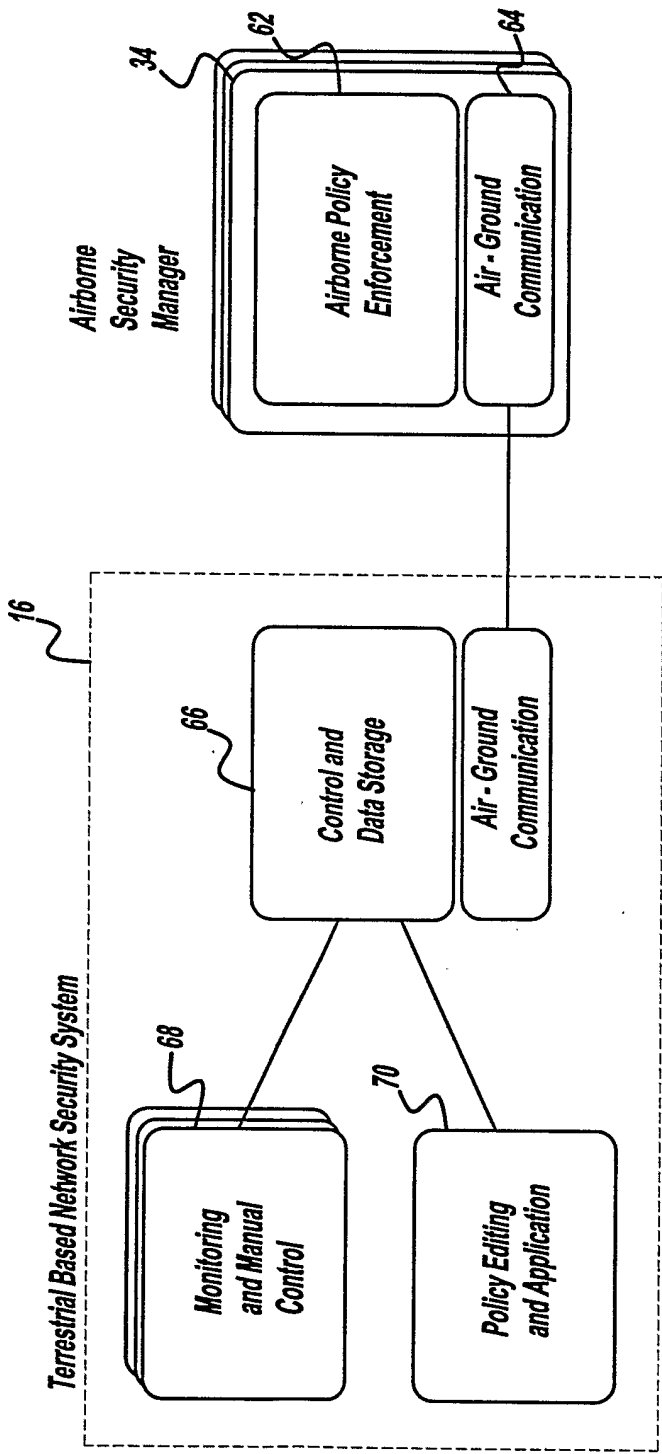


Figure - 4

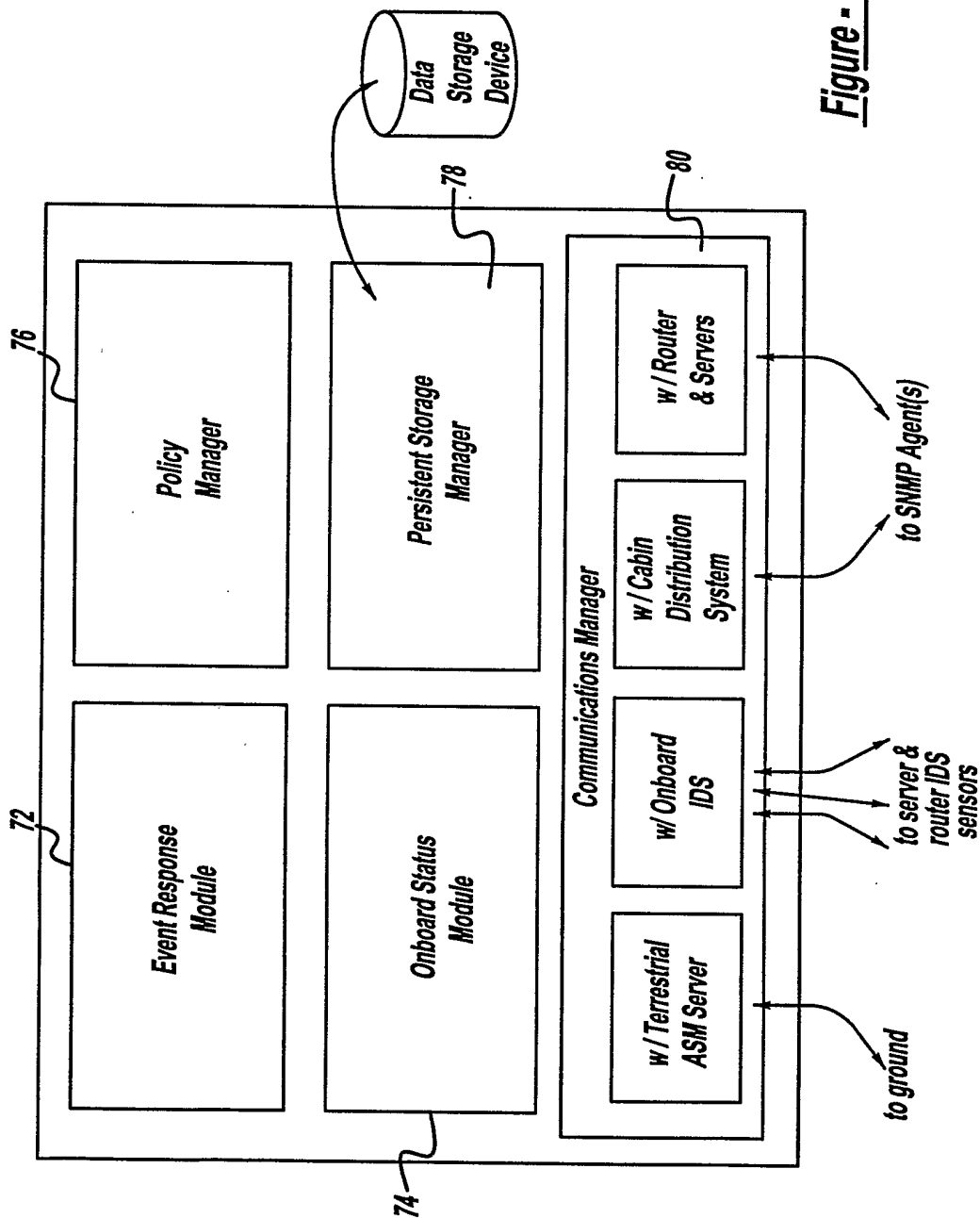


Figure - 5

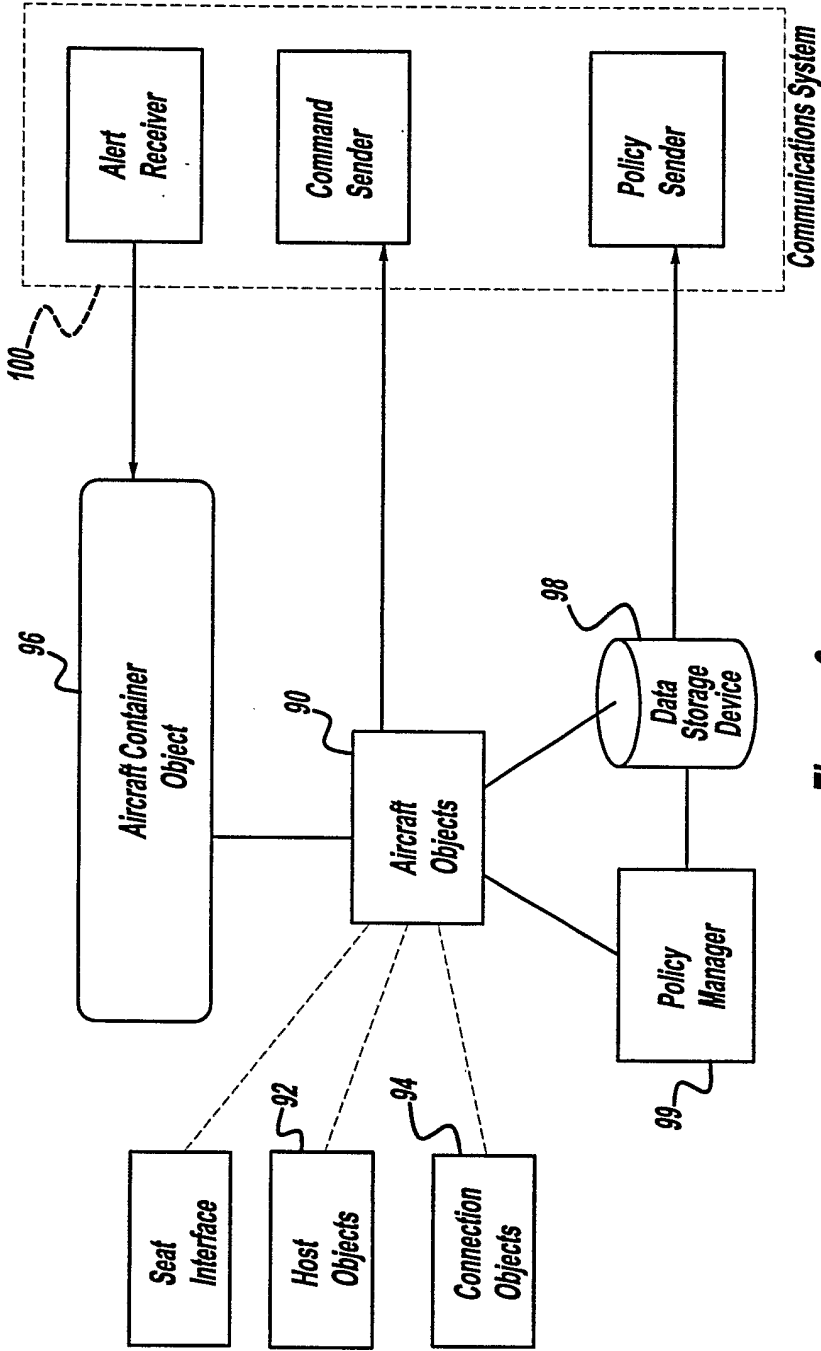


Figure - 6

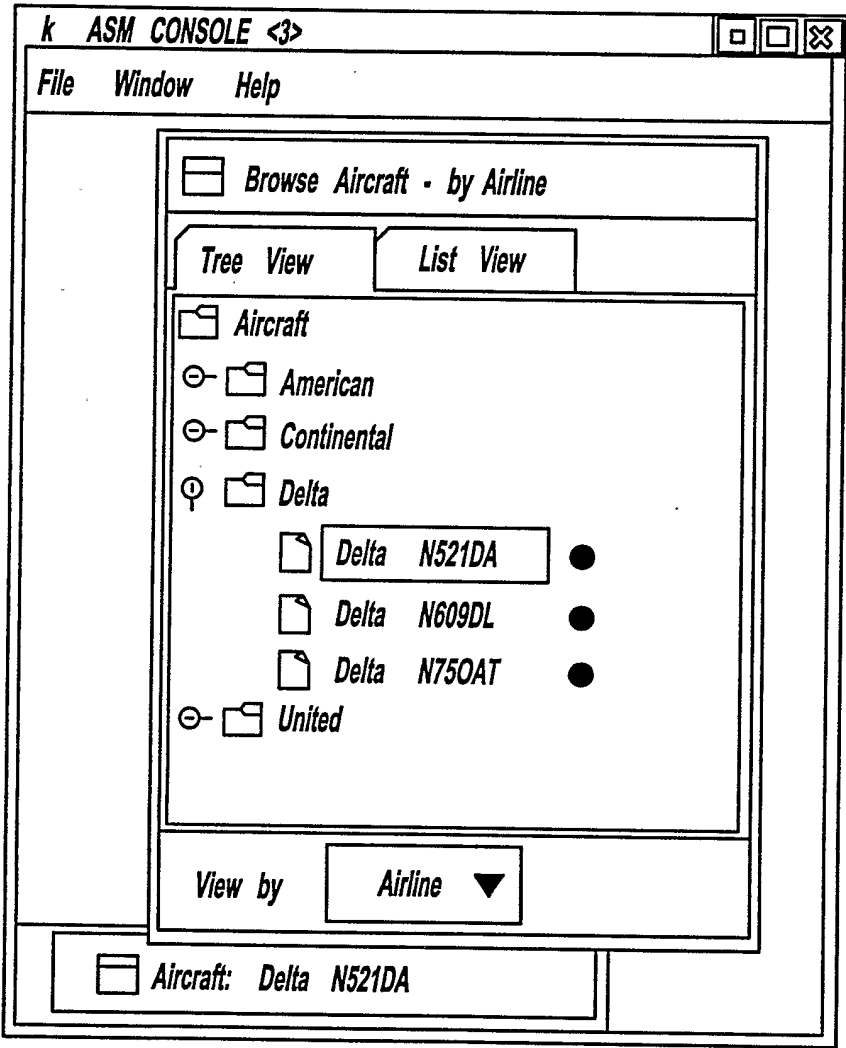


Figure - 7

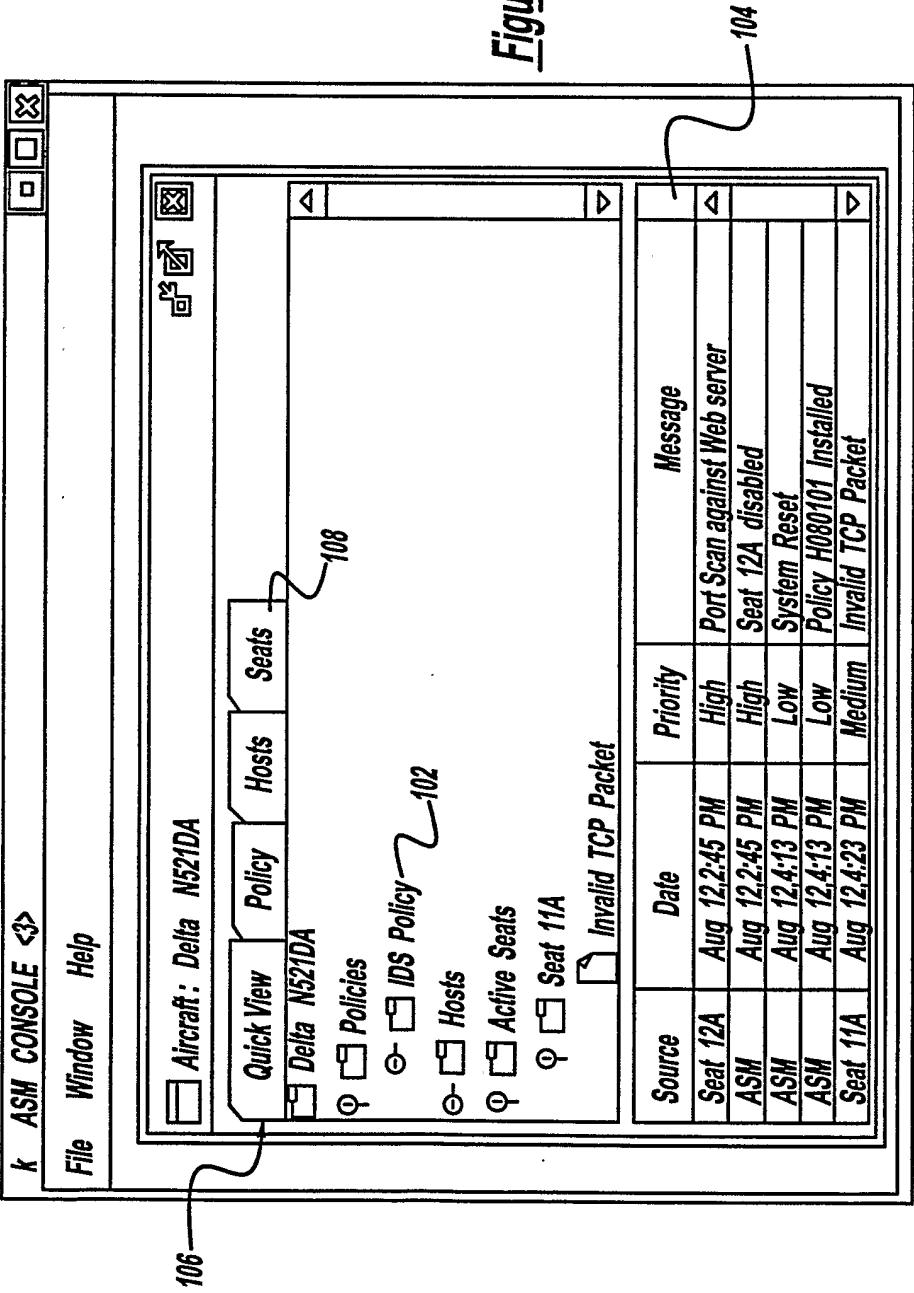


Figure - 8