(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 558 302**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **20.05.2003 E 03731262 (6)**

(97) Fecha y número de publicación de la concesión europea: **02.12.2015 EP 1522020**

(54) Título: **Sistema para manejar la actividad de una red inalámbrica**

(30) Prioridad:

20.05.2002 US 381829 P 03.06.2002 US 161137
03.06.2002 US 161142 03.06.2002 US 161440
03.06.2002 US 161443 03.06.2002 US 160904
06.02.2003 US 360587 21.04.2003 US 464464 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.02.2016

(73) Titular/es:

AIRDEFENSE, INC. (100.0%)
11475 GREAT OAK WAY, SUITE 200
ALPHARETTA, GA 30022, US

(72) Inventor/es:

HRASTAR, SCOTT, E.;
TANZELLA, FRED C.;
LYNN, MICHEAL THOMAS;
SALE, EDWIN L. y
HOLLINGSWORTH, DAWN M.

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema para manejar la actividad de una red inalámbrica

Antecedente

La presente invención está dirigida a un sistema de seguridad de una red asociada con comunicaciones electrónicas. Más específicamente sin limitación, la presente invención se relaciona con sistemas basados en ordenador para evaluar los riesgos de seguridad e identificar y responder a las amenazas en ambientes de redes inalámbricas

La Internet es una red global de redes de ordenadores conectados. Durante los últimos varios años, la Internet ha crecido de manera significativa. Un gran número de ordenadores en la Internet suministran información de varias formas. Cualquiera con un ordenador conectado a la Internet puede potencialmente acceder a esta basta fuente de información.

La información disponible por vía de la Internet comprende la información disponible por vía de una variedad de tipos de servidores de información con capas de aplicación tales como SMTP (protocolo de transferencia de correo simple), POP3 (Protocolo de Oficina Postal), GOPHER (RFC1436), WAIS, HTTP, (Protocolo de Transferencia de Hipertexto, RFC 2616) y FTP (protocolo de transferencia de archivo RFC 1123).

Uno de los métodos más ampliamente esparcidos de suministrar información sobre la Internet es por vía de la World Wide Web (la Red). La Red consiste de un subconjunto de ordenadores conectados a la Internet; los ordenadores en este subconjunto corren servidores con Protocolo de Transferencia de Hipertexto (HTTP) (servidores de la Red). Varias extensiones y modificaciones al HTTP se han propuesto incluyendo, una estructura de extensión (RFC 2774) y autenticación (RFC 2617). La información en la Internet se puede acceder a través del uso de un Identificador de Recurso Uniforme (URI, RFC 2396). Un URI solamente especifica la ubicación de una pieza particular de información en la Internet. Un URI típicamente estará compuesto de varios componentes. El primer componente típicamente designa el protocolo por medio del cual se accede a la pieza de dirección de la información (por ejemplo HTTP, GOPHER, etc.) Este primer componente es separado del resto del URI por dos puntos (":"). El resto del URI dependerá del componente del protocolo. Típicamente, el resto designa un ordenador en la Internet por el nombre o por el número IP, así como una designación más específica de la ubicación del recurso en el ordenador designado. Por ejemplo, un URI típico para un recurso HTTP podría ser:

http://www.server.com/dir1/dir2/resource.htm

donde http es el protocolo, www.server.com es el ordenador designado y/dir1/dir2/resouce.htm designa la ubicación del recurso en el ordenador designado. El término URI incluye nombres de recurso uniforme (los URN) que incluyen los URN tal como se definió de acuerdo con el RFC 2141.

La información huésped en los servidores de la red en la forma de páginas de la red; colectivamente el servidor y la información mantenida se denominan como sitio de la red. Un número significativo de páginas de la red están codificadas utilizando el Lenguaje Marcado de Hipertexto (HTML) aunque otras codificaciones que utilizan SGML, Lenguaje Marcado Extensible (XML), DHMTL o XHTML son posibles. Las especificaciones publicadas para estos lenguajes se incorporan mediante referencia aquí; Tales especificaciones están disponibles para el consorcio de la "World Wide Web" y su sitio de la red (http://www.w3c.org). Las páginas de la red en estos lenguajes de formato pueden incluir enlaces a otras páginas de la red en el mismo de la red o en otro. Como será conocido por aquellos expertos en la técnica, las páginas de la red se pueden generar dinámicamente mediante un servidor al integrar una variedad de elementos en una página de formato antes de la transmisión a un cliente de la red. Los servidores de la red, y los servidores de información de otros tipos, esperan las solicitudes para la información proveniente de los clientes de la Internet.

El software del cliente ha evolucionado lo que le permite a los usuarios de los ordenadores conectados a la Internet acceder a esta información. Los clientes avanzados tales como el Navegador de Netscape y el Internet Explorer de Microsoft le permite a los usuarios acceder al software suministrado por vía de una variedad de servidores de información en un ambiente de cliente unificado. Típicamente, tal software de cliente se denomina como un software de navegador.

El correo electrónico ("e-mail") es otra aplicación ampliamente difundida que utiliza la Internet. Una variedad de protocolos se utilizan a menudo para la transmisión, entrega y procesamiento de los "e-mail", incluyendo el SMTP y el POP3 tal como se discutió anteriormente. Estos protocolos se refieren, respectivamente, a estándares para comunicar mensajes de "e-mail" entre servidores y para comunicación de servidor-cliente relacionado con los mensajes de "e-mail". Estos protocolos se definen respectivamente en los RFC particulares (solicitud para comentario) promulgada por el IETF (Fuerza de Tarea de Ingeniería de la Internet). El protocolo SMTP se define en el RFC 821, y el protocolo POP3 se define en el RFC 1993.

Desde el principio de estos estándares, varias necesidades han evolucionado en el campo de los “e-mail” que conduce al desarrollo de estándares adicionales que incluyen el mejoramiento o protocolos adicionales. Por ejemplo, varias mejoras han evolucionado a los estándares SMTP que conducen a la evolución del SMTP extendido. Ejemplos de las extensiones se pueden ver en (1) RFC 1869 que define una red para extender el servicio SMTP al definir unos medios por medio de los cuales un servidor SMTP puede informar a un cliente SMTP en relación con las extensiones de servicio que este soporta y en (2) RFC 1891 que define una extensión para el servicio SMTP, que le permite a un cliente SMTP especificar (a) que las notificaciones de estados de entrega (DSN) se deben generar bajo ciertas condiciones, (b) si tales notificaciones deben regresar los contenidos del mensaje, y (c) información adicional, a ser regresada con un DSN, que le permite a quien lo envía identificar tanto el o los receptores para los cuales se emitió el DSN, y la transacción en la cual fue enviado el mensaje original.

Además, el protocolo IMAP ha evolucionado como una alternativa al POP3 que soporta más interacciones avanzadas entre los servidores de “e-mail” y los clientes. Este protocolo se describe en el RFC 2060.

Los varios estándares discutidos aquí mediante referencia a los RFC particulares se incorporan aquí mediante referencia para todos los propósitos. Estos RFC están disponibles al público a través de la Fuerza de Tarea de Ingeniería de la Internet (IETF) y se puede recuperar de su sitio de la red (http://www.ietf. Org/rfc.html) Los protocolos especificados no están destinados a ser limitados a los RFC específicos citados aquí anteriormente sino que también están destinados a incluir extensiones y revisiones a los mismos. Tales extensiones y/o revisiones pueden o no estar comprendidas por los RFC actuales y/o futuros.

Un huésped de un servidor de “e-mail” y los productos de cliente se han desarrollado con el fin de fomentar las comunicaciones de “e-mail” sobre la Internet. El software del servidor de “e-mail” incluye tales productos como servidores basados en envío de correo, Microsoft Exchange, Lotus Notes Server, y Novell GroupWise; servidores basados en envío de correo se refieren a un número de variaciones de servidores originalmente basados en un programa de envíos de correo desarrollado por los sistemas operativos UNIX. Un gran número de clientes de “e-mail” también han sido desarrollados lo que le permite a un usuario recuperar y ver los mensajes de “e-mail” de un servidor; productos de ejemplo incluyen Microsoft Outlook, Microsoft Outlook Express, Netscape Messenger, y Eudora. Además, algunos servidores de “e-mal” o servidores de “e-mail” en conjunto con un servidor de la red, le permiten a un navegador de la red actuar como un cliente de “e-mail” utilizando un estándar HTTP.

En la medida en que la Internet se ha vuelto más ampliamente utilizada, ésta ha creado también nuevos riesgos para las corporaciones. Fallas de seguridad de los ordenadores por los piratas y los intrusos y el potencial de comprometer información corporativa sensible son una amenaza muy real y seria.

Las redes de área local inalámbricas (WLAN) ofrecen una extensión rápida y efectiva de una red alambrada o una red de área local estándar (LAN). La Fig. 1 describe un LAN 190 típico que incluye tanto los componentes alambrados como inalámbricos. El componente cableado descrito en la Fig. 1 incluye una variedad de sistemas conectados que incluyen servidores 120 locales, los clientes 130 locales y los componentes 110 de almacenamiento de datos accesibles en la red. Al simplemente instalar los puntos 180A, 180B de acceso a la red alambrada (por ejemplo, Ethernet 150 y el enrutador 140), los ordenadores personales y los ordenadores portátiles equipados con tarjetas 170A, 170B WLAN se pueden conectar a la red alambrada a velocidades de banda ancha.

Durante los últimos pocos años, la mayoría de los desarrollos de la WLAN se han conformado al estándar del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802. 11B que opera sobre un espectro de frecuencia no regulado de 2.4 GHz. El estándar 802. 11b ofrece conectividad de hasta 11 Mbps- lo suficientemente rápida para manejar grandes anexos en el “e-mail” y correr aplicaciones intensivas de banda ancha como conferencias de video. Aunque el estándar 802.11b ahora domina el mercado de WLAN, otras variaciones del estándar 802.11, tales como 802.1 la, 802.11g, y los estándares de soporte tales como 802.1X están siendo desarrollados para mejorar velocidades crecientes y una funcionalidad mejorada. Los vendedores de WLAN se han comprometido para soportar una variedad de estándares. Los varios estándares 802.11 desarrollados por la IEEE están disponibles para bajarse vía URL: htpp://standards.ieee.org/getieee802/802.11.html; estos varios estándares se incorporan aquí mediante esta referencia.

En la medida en que los negocios conectaron sus LAN al Internet 160, ellos instalaron cortafuegos 145 para proteger sus redes locales y actuar como compuertas de seguridad para repeler tráfico no autorizado que proviene de la autopista de información de la Internet tal como un pirata 135 potencial. La movilidad de las redes inalámbricas por vía aérea crea preocupaciones de seguridad donde las amenazas pueden venir de cualquier dirección y no estar limitadas a la estructura alambrada. Prácticas de seguridad establecidas de salvaguardar unos pocos puntos de entrada alambrados a la red ya no son efectivos. Un cortafuego 145 puede disuadir efectivamente un ataque de un pirata 135 cableado por vía de la Internet 160; sin embargo, los piratas 195A, 195B inalámbricos típicamente ingresan al LAN 190 a través de los puntos 180A, 180B de acceso, que ya están detrás del cortafuego 145. Las compañías deben vigilar constantemente sus ondas de radio para medir la actividad inalámbrica y guardarse contra intrusos.

En razón a que la comunicación inalámbrica es radiodifundida sobre los fisgones 195A, 195B de ondas de radio que simplemente escuchan las ondas de radio pueden fácilmente recoger mensajes no encriptados. Adicionalmente, los mensajes encriptados con el Protocolo de Seguridad de Privacidad Equivalentes a cableado (WEP) se puede desencriptar con un poco de tiempo y con herramientas de pirateo fácilmente disponibles. Estos intrusos pasivos ponen los negocios en riesgo de exponer información sensible al espionaje corporativo.

El ladrón de las identidades de usuario autorizadas es una de las grandes amenazas. Los identificadores de conjuntos de servicio (SSID) que actúan como claves crudas y las direcciones de control de acceso de medios (MAC) que actúan como números de identificación personal son a menudo utilizados para verificar que los clientes estén autorizados para conectarse con un punto de acceso. Sin embargo, los estándares de encriptación existentes no son a prueba de tontos y les permiten a los intrusos con conocimientos recoger las direcciones SSID y MAC aprobadas para conectar una WLAN como un usuario autorizado con la capacidad de robar ancho de banda, corromper o bajar archivos, y causar estragos en la red completa.

Los extraños que no pueden obtener acceso a la WLAN pueden sin embargo ser amenazas de seguridad o inundar las ondas de radio con ruido estático que origina que las señales WLAN colisionen y produzcan errores CRC. Estos ataques de negación del servicio (DoS) efectivamente hacen caer la red inalámbrica de manera similar a como los ataques DoS afectan las redes inalámbricas.

Las acciones descuidadas y fraudulentas tanto por empleados leales como empleados descontentos también representan riesgos de seguridad y temas de desempeño para las redes inalámbricas con puntos de acceso no autorizados, medidas de seguridad inadecuadas, y abusos de la red. En razón a que un simple WLAN puede ser fácilmente instalado al unir un punto de acceso a $150 a una red alámbrica y una tarjeta WLAN de $100 a un ordenador portátil, los empleados están desplegando los WLAN no autorizados o conexiones 175 inalámbricas interpares cuando los departamentos de IT son lentos en adoptar la nueva tecnología.

Los puntos de acceso incorrectamente configurados son un hueco evitable pero significativo en la seguridad WLAN. Muchos puntos de acceso son inicialmente configurados para radiodinfundir los SSID no encriptados de usuarios autorizados. Aunque los SSID pretenden ser claves para verificar los usuarios autorizados, los intrusos pueden fácilmente robar un SSID no encriptado para asumir la identidad de un usuario autorizado.

Los usuarios autorizados pueden también amenazar la integridad de la red con abusos que drenen las velocidades de conexión, consuman ancho de banda, e impidan un desempeño completo del WLAN. Atasque en la red con archivos comerciales grandes tales como audio de MP3 o archivos de video MPEG pueden afectar la productividad de cualquiera en la red inalámbrica.

BARDWELL J: Assessing Wireless Security with AirPeek, recuperado de la Internet: (permite la detección de un punto de acceso no autorizado que ha sido conectado a una LAN inalámbrica 802. 11. La aproximación de BARDWELL es utilizar un filtro para revisar el tráfico de la red. Si el desfase de los datos en el marco 802. 11 del tráfico corresponde a un ESSID o BSSID conocido, entonces se asume que el tráfico de la red se origina de un punto de acceso autorizado. De otra forma, se asume que el tráfico de la red se origina de un punto de acceso no autorizado. De esta manera, BARDWELL confía en revisar si el tráfico de la red está realmente dirigido a una porción conocida de la LAN. Otra aproximación se conoce de la US-B-63 21338. Una aproximación adicional se conoce de DEBAR H et al: Towards a taxonomy of intrusión –detection systems, COMPUTER NETWORKS, ELSEVIER SCIENCESCIENCE PUBLISHERS B.V., vol. 31, no. 8, paginas 805-822, ISSN: 1389-1286, DOI: 10. 1016/S11389-1286 (98) 00017-6.

Los sistemas y métodos de acuerdo con la presente invención suministran soluciones a estos y otros temas de seguridad y/o manejo asociados con las WLAN y/o las redes encriptadas de ordenador.

Resumen

La presente invención está dirigida a un sistema de seguridad de la red tal como se definió en la reivindicación 1.

Una realización preferida de acuerdo con la presente invención incluye un almacén de datos del sistema (SDS), un procesador del sistema y una o más interfaces con uno o más canales de comunicación que puedan incluir una o más interfaces a una red de comunicaciones inalámbricas y/o encriptada sobre la cual son transmitidas y recibidas comunicaciones electrónicas. La SDS almacena los datos necesarios para suministrar el seguimiento de seguridad deseado y/o la funcionalidad de evaluación y puede incluir, por ejemplo, comunicaciones recibidas, datos asociados con tales comunicaciones, información relacionada con riesgos de seguridad conocidos y respuestas predeterminadas a la identificación de riesgos y situaciones de seguridad particulares. El SDS puede incluir múltiples almacenamientos de datos físicos y/o lógicos para almacenar los varios tipos de información. El almacenamiento de datos y la funcionalidad de recuperación se puede suministrar bien sea por el procesador del sistema o por los procesadores de almacenamiento asociados o incluidos dentro del SDS.

El procesador del sistema está en comunicación con el SDS por vía de cualquier canal o canales de comunicación adecuados; el procesador del sistema está en comunicación con las una o más interfaces por vía de los mismos, o diferente canal o canales de comunicación. El procesador del sistema puede incluir uno o más elementos de procesamientos que suministran recepción, transmisión, interrogación análisis y/o otras funcionalidades de la comunicación electrónica. En algunas realizaciones, el procesador del sistema puede incluir elementos de procesamiento local, central y/o extremos dependiendo del equipo y de la configuración del mismo.

Cada interfaz a una red inalámbrica incluye al menos un receptor adaptado para recibir comunicaciones inalámbricas; cada interfaz también puede incluir uno o más transmisores adaptados para transmitir comunicaciones inalámbricas. Cada interfaz a una red alambrada, si existe alguna incluye un receptor, un transmisor, ambos o una pluralidad de uno y/o ambos; tales receptores y/o transmisores adaptados para recibir o transmitir comunicación sobre una red alambrada a la cual se conecta la interfaz. En una realización preferida, la interfaz de comunicación incluye al menos un receptor inalámbrico.

Los sensores de la red de acuerdo con la presente invención pueden incluir al menos un receptor inalámbrico, el SDS (o una porción del mismo) y el procesador del sistema (o una porción del mismo). El procesador del sistema, o la porción del mismo, en los sensores de la red extraen datos en una o más unidades lógicas tales como los marcos de las señales inalámbricas recibidas de acuerdo a un protocolo inalámbrico seleccionado tal como una variante del 802. 11. Estas unidades lógicas se inspeccionan para una variedad de información (por ejemplo tipo de marco, fuente, destino, etc.). La información derivada de la inspección se almacena en el SDS, o la porción del mismo en el sensor de la red.

La información de uno o más sensores adicionales de la red se puede recibir por vía de un receptor inalámbrico o una interfaz de comunicación adicional, almacenada en el SDS y procesada por el procesador del sistema junto con la información localmente derivada. Tal almacenamiento y procesamiento puede ocurrir en el sensor de la red, uno o más sensores de red extremos o uno o más servidores centrales. La información almacenada se analiza en el agregado para generar una calificación de seguridad que es entonces sacada a un usuario o un sistema de procesamiento de datos adicional.

De acuerdo con esto, un método preferido de mejoramiento de seguridad incluye una variedad de etapas que pueden, en ciertas realizaciones, ser ejecutadas por el ambiente resumido anteriormente y más completamente descrito adelante o ser almacenado como instrucciones ejecutables por ordenador y/o sobre cualquier combinación adecuada de medios leíbles por ordenador. Se recibe la configuración de datos asociada con un punto de acceso sobre una red de ordenador inalámbrica potencialmente comprometida por un intruso. La información contenida dentro y/o derivada de los datos de la configuración recibida se almacena. La comunicación con el intruso continúa al emular las características de identificación del punto de acceso potencialmente comprometido. En algunas realizaciones, la comunicación puede parecer que venga de un punto de acceso que parezca menos seguro que en punto de acceso potencialmente comprometido. Una solicitud de cambio de canal se transmite al punto de acceso potencialmente comprometido para volver a encaminar la comunicación entre el punto de acceso potencialmente comprometido y las estaciones autorizadas de tal manera que las comunicaciones puedan continuar en un diferente canal.

En algunas realizaciones, los datos de configuración asociados con el punto de acceso potencialmente comprometido se reciben de un sistema de detección de intrusión tal como se describe con mayor detalle adelante. En tales realizaciones, los datos de configuración se pueden incluir como parte de una alarma de violación de seguridad generada. En otros casos se recibe una alarma de señal que dispara la generación y transmisión de una solicitud de información con relación al punto de acceso potencialmente comprometido. Algunas realizaciones que involucran un sistema de detección de intrusión pueden incluir el sistema de detección de intrusión mientras que otros responden a la entrada de tal sistema.

Algunas realizaciones incluyen además el mapeo de la identificación de nodos del intruso y/o el mapeo de la localización del nodo del intruso dentro de la red inalámbrica. En algunos casos, una notificación del disparo del equipo trampa se puede enviar a un administrador; algunas de tales notificaciones pueden incluir una identificación y/o localización del nodo asociado con el intruso en las realizaciones que incluyen la identificación del nodo y el mapeo de localización.

En algunas realizaciones, los datos de configuración incluyen uno o más criterios de riesgo, datos por omisión de la red, política de la red, desempeño y/o datos de uso. Esta información de la configuración puede ser recibida de una o más de una variedad de fuentes que incluyen desde un archivo de configuración, una interfaz de entrada de datos interactivos o una línea de comando o de vigilar la red inalámbrica del ordenador.

Algunas realizaciones pueden además incluir actualizar varios tipos de información almacenada; diferentes realizaciones pueden actualizar toda, ninguna o cualquier combinación de varios tipos de información almacenada. Por ejemplo, algunas realizaciones pueden actualizar información de la estación asociada con las varias estaciones de la red inalámbrica de ordenadores basada en los datos recibidos. Además, algunas realizaciones pueden actualizar la información de estado con relación a la seguridad de la red de ordenador inalámbrica con base en los

datos recibidos. Además, algunas realizaciones pueden actualizar las estadísticas con base en los datos recibidos. Tales actualizaciones pueden ocurrir cada vez que se reciben los datos, en respuesta a alcanzar una cantidad fija de tales datos actualizados, en respuesta a alcanzar un tiempo fijo o el fin de una duración predeterminada, o alguna combinación de estas aproximaciones.

Ventajas adicionales de la invención se establecerán en parte en la descripción que sigue, y en parte serán obvias de la descripción, o pueden ser aprendidas por la práctica de la invención. Las ventajas de la invención se efectuarán y lograrán por medio de los elementos y combinaciones particularmente puntualizados en las reivindicaciones finales. Se debe entender que tanto la descripción general anterior como la descripción detallada que sigue son de ejemplo y explicativas solamente y no restringen la invención, tal como se reivindica.

Breve descripción de los dibujos

Los dibujos que acompañan, que están incorporados y constituyen parte de la especificación, ilustran realizaciones de la invención y junto con la descripción, sirven para explicar los principios de la invención.

La Fig. 1 gráficamente describe un LAN típico tanto con los componentes alambrados como inalámbricos.

La Fig. 2A – E describen gráficamente los LAN que incorporan varias realizaciones preferidas de acuerdo con la presente invención.

La Fig. 3 es un diagrama de flujo de un proceso de detección de intrusión inalámbrico multidimensional de acuerdo con una realización preferida de la presente invención.

La Fig. 4 es un diagrama de flujo de un ejemplo de un proceso de detección de intrusión inalámbrico de entrada múltiple que incluye múltiple correlación de entrada y una fusión de datos de largo plazo.

La Fig. 5 es un diagrama de flujo de un proceso de defensa activo de cambio de canal dinámico de ejemplo que incluye un equipo trampa.

Las Figs. 6A – B son diagramas de flujo de identificación de la estación de ejemplo y procesos de mapeo de localización.

Las Figs. 7A – C son diagramas que describen arquitecturas de ejemplo para los dispositivos sensores.

Las Figs. 8A- B son diagramas de flujo que describen un proceso de recolección de datos de seguridad de ejemplo efectuados de acuerdo con la presente invención.

La Fig. 9 es un diagrama de flujo que describe las etapas en un proceso de seguimiento de topología de red inalámbrica de ejemplo.

La Fig. 10 es un diagrama de flujo que describe un proceso de aplicación de política de red inalámbrica automatizada.

La Fig. 11 es un diagrama de flujo que describe un proceso de exploración adaptativa.

La Fig. 12 es una figura que describe una visualización de la muestra de una topología de red inalámbrica.

Las Figs. 13A – B describen pantallas de muestra que suministran interfaces para la configuración de una aplicación de política automatizada.

La Fig. 14 describe una interfaz de ejemplo para configurar un patrón de exploración por omisión o de línea base.

Descripción detallada

Las realizaciones de ejemplo de la presente invención se describen ahora en detalle. En referencia a los dibujos, los números similares indican partes similares en todas las vistas. Como se utiliza la descripción aquí y a lo largo de las reivindicaciones que siguen el significado de “un”, “una”, y “el” incluye las referencias plurales a menos que el contexto claramente dicte otra cosa. También, como se utiliza en la descripción presente y a lo largo de las reivindicaciones que siguen, el significado de “en” incluye “en” y “sobre” a menos que el contexto claramente dicte otra cosa. Finalmente, como se utiliza en la descripción aquí y a lo largo de las reivindicaciones que siguen, el significado de “y” y “o” incluye tanto la conjunción como la disyunción y se puede utilizar intercambiablemente a menos que el contexto claramente dicte otra cosa; La frase “exclusiva o” puede ser utilizada para indicar situación donde solamente puede aplicar un significado disyuntivo.

Los rangos se pueden expresar aquí desde “aproximadamente” un valor particular, asld/o a “aproximadamente” otro valor particular. Cuando se expresa tal rango, otra realización incluye desde un valor particular y/o al otro valor particular. De manera similar, cuando se expresan valores como aproximaciones, el uso del antecedente “aproximadamente”, se entenderá que el valor particular forma otra realización. Se entenderá adicionalmente que el punto final de cada rango es significativo tanto en relación con el otro punto final, e independientemente del otro punto final.

El término “Wi-Fi” es la abreviatura para fidelidad inalámbrica y es otro nombre para el IEEE 802. 11b. La anterior discusión de las realizaciones de ejemplo puede utilizar terminología o hacer referencia al estándar IEEE 802.11b, u otra variante del 802.11 sin embargo, aquellos expertos en la técnica apreciarán que los sistemas y métodos de la presente invención se pueden aplicar al WLAN que cumple estos estándares así como también el WLAN desarrollado de acuerdo a los estándares WLAN competentes. El término “marco” como se utiliza aquí significará comunicación definida amplia y discretamente trasmitida por vía de una red de ordenador y no estará limitado por aquellos tipos de marco especifico (control, manejo, datos y error) definidos de acuerdo a los estándares del 802.11X.

Arquitectura de un ambiente de acceso típico

Las Figs. 2A-E describen varios ambientes LAN que incluyen varias realizaciones preferidas de acuerdo con la presente invención. Estas figuras describen un ambiente LAN típico como se describió en la Fig. 1 que tiene componentes alambrados e inalámbricos. En contraste a la Fig. 1, las Figs. 2A-E incluyen uno o más componentes de equipo que soportan las realizaciones preferidas de acuerdo con la presente invención. Los componentes de equipo descrito incluyen un procesador de sistema, un SDS y una o más interfaces o una o más redes de comunicación inalámbrica y/o encriptadas sobre las cuales se trasmite y reciben comunicaciones electrónicas.

Los componentes de hardware descritos en estas figuras se esbozan como sigue:

• En la Fig. 2A, los componentes de hardware incluyen un dispositivo 210A único que incluye un procesador local que sirve como el procesador del sistema, o al menos una porción del mismo, y una o más interfaces de la red inalámbrica. El dispositivo 210A es preferiblemente un sistema de ordenador móvil tal como un ordenador portátil. El almacenamiento primario y/o secundario local del dispositivo 210A puede servir como un SDS; alternativamente, las porciones del SDS pueden ser suministradas por otros sistemas capaces de comunicarse con el dispositivo 210A tal como el almacenamiento 210 de datos manejable por la red, los servidores 120 locales y/o las estaciones 170A, 170B inalámbricas. En algunas realizaciones, las interfaces del dispositivo a la red inalámbrica se pueden limitar a uno o más receptores inalámbricos. En otras realizaciones, las interfaces pueden incluir uno o más transmisores inalámbricos así como también uno o más trasmisores. Si están incluidos los trasmisores inalámbricos, el dispositivo 210 puede comunicarse sobre LAN 190 utilizando un punto 180A, 180B de acceso inalámbrico. Además, los trasmisores inalámbricos incluidos se pueden utilizar para soportar una o más de las medidas de defensa activas descritas con mayor detalle adelante. En algunas realizaciones el dispositivo 210A puede además incluir una conexión (no mostrada) alambrada a la Ethernet 150 que permite la comunicación directa entre éste y los sistemas conectados a la porción alambrada del LAN 190.

• En la Fig. 2B, los componentes del hardware incluyen múltiples dispositivos 210A, 210B, 210C, 210D. Cada dispositivo 210A-D incluye un procesador local y una o más interfaces a la red inalámbrica y es preferiblemente un sistema de ordenador móvil tal como un ordenador portátil. Los procesadores locales individuales en el agregado sirven como el procesador del sistema. El SDS puede incluir una combinación de almacenamiento local a cada uno de los dispositivos y/o almacenamiento externo accesible por vía del LAN 190. Como se describió anteriormente con respecto a la Fig. 2A, cada dispositivo incluye al menos un receptor inalámbrico pero puede también incluir receptores inalámbricos y/o transmisores inalámbricos adicionales. Cada dispositivo también puede incluir una conexión alambrada (no mostrada) a la Ethernet 150. Finalmente, los dispositivos 210A-D pueden además utilizar interfaces existentes y/o incorporar interfaces adicionales para permitir comunicación interpares entre ellos.

• En la Fig. 2C, los componentes de hardware incluyen los dispositivos 210A, 210B, 210C, 210D, 220 múltiples. Cada dispositivo 210A-D puede incluir los varios componentes como se describieron anteriormente con respecto a la Fig. 2B. el dispositivo 220 incluye un procesador local y una o más interfaces de comunicación; este dispositivo se puede denominar en lo sucesivo como el sistema huésped. El dispositivo de interfaz de comunicación de 220 puede incluir solo una interfaz de comunicación alambrada y puede recibir datos relacionados con comunicaciones inalámbricas como las enviadas por los dispositivos 210A-D sobre la Ethernet 150 alambrada. Además de, o en lugar de, la interfaz de comunicación alambrada, el dispositivo 220 puede incluir una o más interfaces de comunicación inalámbrica cada una de las cuales puede incluir un receptor inalámbrico, un transmisor inalámbrico o ambos. En la realización donde los dispositivos 210A-D soportan comunicación interpares, el dispositivo 220 puede en algunas de tales realizaciones participar en la comunicación interpares y, en tales casos sus interfaces de comunicación incluirían la interfaz de comunicación adecuada para soportar esta participación. La funcionalidad del procesador del sistema en la realización descrita se puede suministra por el sistema huésped solo y/o por alguna combinación de los dispositivos 210A-D. El sistema huésped puede en algunas realizaciones suministrar el SDS para el ambiente; de manera alternativa, el SDS se puede soportar por alguna combinación de almacenamiento local

entre los dispositivos 210A-D, el almacenamiento local en el sistema huésped y el almacenamiento externo disponible a través del LAN 190.

• En la Fig. 2D, los componentes de hardware incluyen los dispositivos 210A, 210B, 210C, 210D, 220, 230A, 230B múltiples. Los dispositivos 210A-D, 220 soportan la misma funcionalidad e incluyen el mismo rango de componentes tal como se suministró anteriormente con respecto a la Fig. 2C. Además, los dispositivos 230A, 230B son dispositivos sensores que vigilan el tráfico inalámbrico sobre la red inalámbrica. Estos dispositivo sensores al menos incluyen un receptor inalámbrico para vigilar el tráfico y una interfaz de comunicación alambrada (como se describió) o inalámbrica (no mostrada) que permite la comunicación con uno o más de los dispositivos 210A-D y/o del sistema 220 huésped. En algunas realizaciones, los dispositivos 230A, 230B sensores pueden incluir un transmisor inalámbrico para soportar la comunicación con los otros componentes del hardware y/o para soportar varias medidas defensivas de la red inalámbrica activa tal como se discute adelante. En algunas realizaciones, el dispositivo 230A, 230B sensor puede además incluir capacidad de procesamiento local y/o capacidad de almacenamiento local; en algunas de tales realizaciones, el procesador del sistema y/o el SDS puede incorporar estas capacidades locales de los dispositivos 230A, 230B sensores.

• En la FIG. 2E, los componentes del hardware incluyen los dispositivos 220, 230A, 230B múltiples. En esta realización, el sistema 220 huésped y los dispositivos 230A, 230B sensores incluyen la misma funcionalidad y el rango de componentes como se discutió anteriormente con respecto a las FIGS. 2D y 2E respectivamente. En tales realizaciones, el sistema 220 huésped típicamente suministrara una porción significativa de la funcionalidad del procesador del sistema y solo tendrá una capacidad limitada para recibir directamente comunicaciones de la red inalámbrica. En algunas de estas realizaciones, el sistema 220 huésped puede no tener interfaz de comunicación inalámbrica.

los componentes del hardware descrito incluyen un procesador del sistema que potencialmente incluye múltiples elementos de procesamiento, que se pueden distribuir a través de los componentes del hardware descrito, donde cada elemento de procesamiento puede ser soportado por vía de plataformas de procesador compatibles Intel que utilizan preferiblemente al menos un procesador clase PENTIUM III o CELERON (Intel Corp., Santa Clara, CA); procesadores alternativos tales como el UltraSPARC (Sun Microsystems, Palo Alto, CA) se podrían utilizar en otras realizaciones. En algunas realizaciones, la funcionalidad de mejoramiento de seguridad, como se describe adicionalmente adelante, se puede distribuir a través de múltiples elementos de procesamiento. El término elemento de procesamiento puede referirse a (1) un proceso que corre sobre una pieza particular, o a través de piezas particulares, del equipo, (2) una pieza particular del equipo, o (1) o (2) según el contexto lo permita. Los dispositivos 230A, 230B sensores descritos en las Figs.2D-E pueden en algunas realizaciones preferidas incluir procesadores locales optimizados más limitados tales como un procesador de señal digital (DSP). Otra realización puede utilizar circuitos integrados específicos de aplicación (ASIC) o unos arreglos de compuerta de campo programable (FPGA).

Los componentes de hardware descritos incluyen un SDS que podría incluir una variedad de elementos de almacenamiento primario y secundario. En una realización preferida, el SDS incluiría el RAM como parte del almacenamiento primario; la cantidad de RAM podría variar desde 64 MB a 4GB en cada dispositivo de hardware individual aunque estas cantidades podrían variar y representan el uso traslapante tal como cuando el sistema 220 huésped soporta funcionalidad adicional tal como la integrada con el sistema 145 cortafuegos para suministrar seguridad alambrada e inalámbrica unificada. El almacenamiento primario puede en algunas realizaciones incluir otras formas de memoria tal como la memoria cache, registradores, memoria no volátil (por ejemplo, FLASH, ROM, EPROM, etc.), etc. los dispositivos 230A, 230B sensores descritos en las Figs. 2D-E pueden en algunas realizaciones preferidas incluir más cantidades limitadas de clases de almacenamiento primario. En algunas realizaciones preferidas, el almacenamiento primario en los dispositivos sensores incluye memoria FLASH.

El SDS también puede incluir almacenamiento secundario que incluye servidores únicos, múltiples y/o variados y elementos de almacenamiento. Por ejemplo, el SDS puede utilizar dispositivos de almacenamiento internos conectados al procesador del sistema. En realizaciones en donde el elemento de procesamiento único soporta toda la funcionalidad de análisis de seguridad, tal como se ve en las Figs. 2A y 2E, una unidad de disco duro local pude servir como el almacenamiento secundario del SDS, y el sistema operativo de disco que ejecuta tal elemento de procesamiento único pueda actuar como un servidor de datos que recibe y sirve a las solicitudes de datos.

Se entenderá por aquellos expertos en la técnica que la diferente información utilizada en los procesos de mejoramiento de la seguridad y los sistemas de acuerdo con la presente invención pueden ser segregados lógica o físicamente dentro de un dispositivo único que sirve como almacenamiento secundario para el SDS; múltiples almacenamientos de datos relacionados accesibles a través de un sistema de manejo unificado, que sirven juntos como el SDS; o múltiples almacenes de datos independientes individualmente accesibles a través de sistemas de manejos dispares, que pueden en algunas realizaciones ser colectivamente vistos como el SDS. Los varios elementos de almacenamiento que comprenden la arquitectura física del SDS se pueden ubicar centralmente, o distribuir a través de una variedad de diversas ubicaciones.

La arquitectura del almacenamiento secundario del almacén de datos del sistema puede variar significativamente en diferentes realizaciones. En varias realizaciones, las bases de datos son utilizadas para almacenar y manipular los

datos; en algunas de tales realizaciones uno o más sistemas de manejo de base de datos relacionales, tales como DB2 (IBM, White Planes, NY), SQL Server (Microsoft Redmond, WA), ACCESS (Microsoft, Redmond, WA), ORACLE 8i (Oracle Corp., Redwood Shores, CA), Ingeres (Computer Associates, Islandia, NY) MySQL (MySQL AB, Sweeden) o Adaptive Server Enterprise (Sybase Inc., Emeryville, CA) se puede utilizar en conexión con una variedad de dispositivos de almacenamiento/servidores de archivo que pueden incluir una o más unidades magnéticas estándar y/o de disco óptico que utiliza cualquier interfaz apropiada que incluye, sin limitación, IDE y SCSI. En algunas realizaciones, se puede utilizar una biblioteca de cinta tal como el Exabyte X80 (Exabyte Corporation, Boulder, CO), una solución de red anexa de almacenamiento (SAN) tal como la disponible de (EMC, Inc., Hopkinton, MA), una solución de almacenamiento anexa de red (NAS) tal como una NetApp Filer 740 (Network Apliances, Sunnyvale, CA), o combinación es de las mismas. En otras realizaciones, el almacenamiento de datos puede utilizar sistemas de base de datos con otras arquitecturas tales como las orientadas a objeto, espaciales, relacional de objeto o jerárquica.

En lugar de o además de, aquellas aproximaciones de la organización discutidas anteriormente, ciertas realizaciones pueden utilizar otras ejecuciones de almacenamiento tales como tablas de direcciones calculadas o archivos planos o combinación es de tales arquitecturas. Tales Aproximaciones alternativas pueden utilizar servidores de datos diferentes de los sistemas de manejo de bases de datos tales como el servidor de consulta de la tabla de direcciones calculadas, el procedimiento y/o y el proceso y/o un servidor de recuperación de archivo plano, el procedimiento y/o el proceso. Además, el SDS puede utilizar una combinación de cualquiera de tales aproximaciones para organizar su arquitectura de almacenamiento secundaria.

Los componentes del hardware pueden tener cada uno un sistema operativo apropiado tal como WINDOWS/NT, WINDOWS 2000 o WINDOWS/XP Server, (Microsoft, Redmon, WA), Solaris, (Sun Microsystems, Palo Alto, CA), o LINUX (u otra variante de UNIX). En una realización preferida, los dispositivos 210A- D y /o el sistema 220 huésped incluye un sistema operativo LINUX (u otra variante de UNIX); aunque otras realizaciones pueden incluir un sistema operativo WINDOWS/XP (u otra familia de WINDOWS).

Dependiendo de la plataforma del sistema de hardware/operativo del ambiente total, se puede incluir el software de servidor apropiado para soportar el acceso deseado para el propósito de configuración, vigilancia y/o reporte. La funcionalidad del servidor de la red se puede suministrar por vía de un servidor de información de Internet (Microsoft, Redmon, WA), un Servidor Apache HTTP (Apache Software Foundation, Forest Hill, MD), un Servidor de la red iPlanet (iPlanet-E Commerce – A Sun – Netscape Aliance Mountain View, CA) u otra plataforma de la red adecuada. Los servicios de correo electrónico se pueden soportar por vía de un Exchange Server (Microsoft, Redmon, WA), sendmail u otro servidor de correo electrónico adecuado. Algunas realizaciones pueden incluir uno o más sistemas de respuesta de voz automatizados (AVR) que están además de, en lugar de, los servidores de acceso anteriormente mencionados. Tal sistema AVR podría soportar una interfaz manejada puramente por vos/teléfono al ambiente con una salida de copia en o papel suministrada electrónicamente a un dispositivo de salida en copia de papel adecuado (por ejemplo, impresora, facsímile, etc.), y enviada según sea necesario a través de un correo regular, mensajería rápida, correo interoficina, facsímil u otra aproximación de envío adecuada.

Algunas realizaciones preferidas de la presente invención incluyen los dispositivos 230A, 230B sensores de una forma tal como la descrita en la Figs. 7A-C. La Fig. 7A describe un dispositivo sensor que tiene la funcionalidad combinada de un punto de acceso y sensor. El dispositivo incluye una antena 705 de transceptor y una antena 710 de detección. La antena 705 del transceptor permite la recepción y la transmisión de señales inalámbricas de acuerdo a un protocolo predeterminado tal como una variante del IEEE 802.11. Las estaciones inalámbricas asociadas con la radio activa (antena del transceptor) que conecta a través del puerto 720 a una red alambrada tal como una interfaz de red a una Ethernet local y/o a una red inalámbrica adicional (transceptor no mostrado), un modem que permite la conexión a una red o la conexión directa a un sistema huésped o un sistema par o combinación es de los mismos. La antena 710 de detección permite la recepción de señales inalámbricas de acuerdo al protocolo sin impactar el desempeño del transceptor. La antena 710 de detección recibe todas las señales inalámbricas en paralelo con la antena 705 del transceptor. El sensor puede además incluir almacenamiento 715 de datos locales que sirve cono el SDS o una porción del mismo. Este almacenamiento 715 local contiene cualquier código operativo necesario y/o datos tales como los datos de seguridad acumulados, los datos de configuración de la red, la información de identificación del sensor y/o datos relacionados con comunicaciones de la red. Este almacenamiento local típicamente incluye DRAM, memoria FLASH o combinación es de las mismas. El sensor puede además incluir un procesador 725 local que sirve como el procesador del sistema, o una porción del mismo. Este procesador 725 local soporta el manejo de comunicación y la recolección de seguridad, y en alguna realización análisis de seguridad, funcionalidad. El procesador local puede ser cualquier microprocesador, ASIC, FPGA o combinación es de los mismos que tiene la potencia de cómputo capaz de manejar los dos componentes 705 y 710 inalámbricos y los componentes auxiliares del dispositivo (por ejemplo el almacenamiento 715 local, la interfaz 720 de red, etc.); por ejemplo un microprocesador Clase Pentium I (Intel) o más rápido es capaz de manejar las necesidades de cómputo. El dispositivo también incluye una conexión a una fuente de poder tal como la interface 730 de corriente alterna (AC) aunque otras realizaciones podrían además, o en su lugar, incluir una energía sobre la interfaz compatible Ethernet o un depósito para una o más baterías desechables y/o recargables.

La Fig. 7B describe una realización de un sensor autónomo. En esta realización, un transceptor inalámbrico para soportar la funcionalidad de punto de acceso no está incluido. La descripción anterior con respecto a la Fig. 7A suministra la descripción de los componentes numerados de manera similar en la Fig. 7B. Esta realización incluye una interfaz 735 de comunicación adicional. Esta interfaz adicional se puede utilizar para conectar dispositivos adicionales tales como un punto de acceso estándar. Esto sería útil para instalar un sensor en un sitio con un punto de acceso existente sin tener que correr otra línea de red. Cualquier dato enviado saliente del dispositivo conectado a la Interfaz 735 sería enviado por vía de la interfaz 720 de la red. Cualquier dato recibido en la interfaz 720 de la red dirigido al dispositivo se enviaría por vía de la interfaz 735.

La Fig. 7 describe una realización de punto de acceso modificado. En esta realización, no se suministra una antena separada para la vigilancia paralela de las señales inalámbricas. En su lugar, el transceptor 705 inalámbrico responde tanto al punto de acceso como a la funcionalidad de vigilancia. Esta funcionalidad se puede ejecutar en el software o en el hardware del procesador 725, local o como una lógica modificada dentro del transceptor mismo. Esta realización tiene la ventaja de que los puntos de acceso existentes con la capacidad de procesamiento local suficiente se puede modificar a través de la adición de un hardware o la actualización de un software para soportar la capacidad de vigilancia. Una desventaja es que el punto de acceso original puede no haber sido destinado a soportar ambas funcionalidades y, por lo tanto, la funcionalidad del punto de acceso se puede degradar en algunos casos.

Como se describió previamente, los sensores 230A-B y/o los dispositivos 210A-D en algunas realizaciones recolectan y envían datos relacionados con seguridad a un sistema 220 huésped para procesamiento y análisis adicional. Algunas de tales realizaciones suministran el procesamiento local de los datos de seguridad. Las Figs. 8A-B son diagramas de flujo que describen un proceso de recolección de datos de seguridad de ejemplo efectuado de acuerdo con la presente invención. En algunas realizaciones, este proceso se puede ejecutar mediante los sensores 230A-B y/o los dispositivos 210A-D.

En algunas realizaciones particulares utilizando la red compatible 802. 11, los sensores de hardware leen las ondas de radio 802. 11 y manejo de cinta y marcos de control, agrega estadísticas y envía información recolectada a un servidor backend. Un sensor de hardware puede tener varias realizaciones. Tres realizaciones tales como las descritas en las Figs. 7A-7C serían sensores (Fig. 7B) de hardware autónomos, una combinación del sensor Access Point 802.11/hardware (Fig. 7A), y un punto de acceso 802. 11 modificado capaz de manejo de cinta y marcos de control y enviarlos de regreso a un servidor central para análisis (Fig. 7C).

Un sensor de hardware típicamente incluirá al menos una radio 802. 11 capaz de leer ondas de radio 802. 11. Para suministrar la funcionalidad para asegurar una red inalámbrica, las cintas 802. 11 del sensor de hardware manejan y controlan los marcos fuera de las transmisiones de datos inalámbricas y envía en tiempo real datos en tanda de regreso a un servidor centralizado (por ejemplo un sistema 220 huésped) para análisis y procesamiento para determinar las intrusiones u otra actividad de la red tal como la vigilancia de la salud o el desempeño u efectuar tales análisis y procesar localmente en configuraciones interpares.

En las tres realizaciones anteriormente mencionadas, el sensor de hardware autónomo tendría una radio 802. 11 que opera en “modo promiscuo” con el fin de ser indetectable de las ondas de radio y aún leer un tráfico de red 802. 11. Al operar en modo promiscuo, el sensor de hardware no podría transmitir datos tales como manejo de baliza y estaría en modo de operación de solo lectura. El software del sensor incrustado en dispositivo leería los marcos 802. 11 de la red inalámbrica y las interrogaría para retirar los marcos de manejo y control de los marcos de datos, recolectar los datos y enviarlos a un servidor “back-end”. El proceso de recolectar los datos en una aproximación preferida es como sigue:

El hardware físico enciende y carga el sistema operativo (OS preferido: Linux en tiempo real o RTOS) a un estado operacional, etapa 800. La ejecución por primera vez del proceso sensor después del encendido (etapa 805), inicializa un temporizador para el manejo y control del almacenamiento temporal de los marcos (etapa 810). El temporizador permite que los marcos de manejo y control sean guardados almacenados temporalmente hasta que el temporizador alcanza un tiempo transcurrido predeterminado, en cuyo punto ellos serán enviados a un servidor o par para procesar o ser procesados localmente. Aunque otras realizaciones pueden enviar marcos de manejo y control no almacenados temporalmente y no se requeriría por lo tanto un temporizador, o cualquiera de las etapas del proceso que involucre el temporizador.

Un marco de paquete inalámbrico es entonces leído desde la red inalámbrica, etapa 820. Los marcos son leídos de tal manera que el contenido del marco se puede interrogar en un proceso corriente abajo. Este es también el punto 815 de entrada en el proceso para recuperar el siguiente marco después de la interrogación del presente marco.

El marco de paquete que lee por fuera de la red inalámbrica es interrogado para determinar si el marco es de un tipo redundante tal como los marcos de manejo y control, etapa 825. Si el marco es de un tipo redundante, el procesamiento continúa en el punto de entrada 830 en la Fig. 8B. Los marcos de manejo y control son radiodifundidos más frecuentemente que los marcos de datos y son de protocolo específico. La interrogación adicional del marco de manejo y control se efectúa para determinar si el marco es un marco de tipo redundante (es

decir un marco baliza), etapa 855. Sino, el control pasa de nuevo al punto 815 de entrada en la Fig. 8A. Los marcos de manejo y control tales como los marcos de baliza son radiodifundidos más frecuentemente que los marcos de datos y pueden ser almacenados temporalmente como un registro con un conteo de marco y para reducir el tráfico sobre la red en la medida en que los marcos son transmitidos a un servidor o a un par para reducir el "overhead" del procesamiento local. El almacenamiento temporal se puede lograr al mantener un conteo de marco para el tipo particular de marco (etapa 860) redundante y poblar una estructura de datos apropiada basada en el tipo (etapa 865) de marco redundante. Sí ha pasado un intervalo de tiempo apropiado o si se alcanza un tiempo particular (etapa 870), o si no se pretende un almacenamiento temporal, el procesamiento procede al punto 845 de entrada en la Fig. 8A para enviar la información de marco redundante al servidor central o par o para el procesamiento local dependiendo de la realización particular. Si el temporizador no dispara la transmisión o el procesamiento, el procesamiento continúa en el punto 815 de entrada para recuperar el siguiente marco en la Fig. 8A.

Si el marco no es de un tipo redundante, el procesamiento continúa en la etapa 835 donde los datos de cabecera son retirados del marco del paquete inalámbrico. Los datos de cabecera se utilizan para conseguir los datos de origen/destino así como también para mantener el estado.

En la etapa 840, la estructura de datos está poblada con la información pertinente que se relaciona con el estado de la estación inalámbrica y la actividad del protocolo así como también la información de origen y destino para procesamiento de línea de leída posterior por un servidor de análisis "back-end", por un par o un procesador local.

Una vez que se acumulan los datos y se procesan mediante el sensor remoto, la estructura de dato resultante pasa de nuevo al servidor central o aun par sobre IP o es localmente procesada para análisis de detección de intrusión (etapa 850). El proceso continúa al punto 815 de entrada con la recuperación del siguiente marco.

La realización de un sensor de hardware de combinación y el punto de acceso, una radio 802. 11 operaria como un punto de acceso normal 802. 11 que opera en el modo infraestructura que le permitiría a las estaciones inalámbricas asociar y pasar datos a través de la red alambrada. La radio 802. 11 adicional operaria en modo promiscuo justo como un sensor de hardware autónomo operaría. Esto le daría al dispositivo la capacidad de enviar y recibir datos como un punto de acceso 802. 11 normal mientras que utiliza la radio adicional para vigilar las ondas de radio contra intrusiones y vigilar la red inalámbrica para vigilar el desempeño y la salud.

La realización de un punto de acceso modificado para suministrar la capacidad de vigilancia utilizaría una radio 802. 11 única para enviar y recibir datos con estaciones inalámbricas pero utilizaría un mecanismo SNP para enviar trampas de regreso a un servidor "back-end" cuando ocurren eventos tales como intrusiones o ataques contra el punto de acceso. Este método no es tan efectivo como las realizaciones previamente mencionadas pero puede suministrar información adicional que no sea recolectada por los puntos de acceso operativos estándar.

En una realización preferida, los dispositivos 210A-D y el sistema 220 huésped se puede configurar local o remotamente, y la configuración puede ocurrir a través de una interfaz interactiva y/o a través de una interfaz de línea de comando. La interfaz interactiva es accesible localmente mientras que la interfaz de la línea de comando es accesible local o remotamente. El acceso remoto es preferiblemente otorgado a través del uso de un cliente con capa segura (SSH) que se comunica con un servidor SSH que corre sobre el dispositivo o el sistema huésped.

Mapeo y visualización de la topología de la red inalámbrica.

El manejo de una red inalámbrica difiere de muchas maneras del manejo de una red alambrada. Una diferencia importante es la naturaleza más dinámica de los nodos (ordenadores, PDA, teléfonos móviles 802. 11, etc.) en una red alambrada, las conexiones a la red ocurren solo en ubicaciones fijas. En una red inalámbrica, los nodos no están atados a una conectividad física a la red; una red inalámbrica no tiene los límites tradicionales y su topología puede cambiar a una velocidad muy alta.

Este cambio dinámico es debido a la capacidad de los usuarios de la red inalámbrica de deambular a través de múltiples redes así como también la capacidad de los protocolos de las redes modernas de soportar la creación instantánea de redes ad hoc. Dadas estas características, los patrones de conectividad y la topología de la red puede cambiar de momento a momento.

La Fig. 9 describe un proceso que soporta la captura, y en algunas realizaciones la visualización, de una topología de red inalámbrica durante el tiempo. Este mecanismo utiliza las capacidades de análisis de la indicación completa del estado del motor del comportamiento de la red para capturar y hacer seguimiento a los patrones de conectividad de los usuarios y las redes que se establecen durante el tiempo.

Los datos de la red se acumulan durante un periodo de tiempo definido (una época). Esta época puede variar en longitud dependiendo de la profundidad del análisis y la acumulación del estado deseado. En cualquier caso, al final de una época, se efectúa un análisis estadístico y de estado sobre los datos acumulados para generar una topología de red. Para propósitos de análisis, esta topología se puede entonces representar matemáticamente como una gráfica, con un conjunto de nodos y bordes que interconectan los nodos por el patrón observado. Esta topología

generada también se puede procesar adicionalmente para generar una visualización o para comparar con una topología de red anterior para evaluar la seguridad potencial y/o las violaciones de la política. La comparación de la topología en algunas realizaciones podría incluir comparación basada en reglas para la seguridad potencial y/o las violaciones de la política. Además, o en lugar de, la topología podría estar sometida a una comparación a base de una coincidencia patrón para identificar el estado de la topología que viola las restricciones de seguridad y/o política. Cualquier aproximación que coincida con el patrón adecuado se podría utilizar; en algunos casos, las redes neurales, y el análisis del léxico y/o el enmascaramiento de bytes se podrían incluir como partes de tal coincidencia de patrón. A través de la recolección de la información de estado relacionada con la actividad, los patrones de uso y conectividad, la topología se puede construir y actualizar durante el tiempo en la medida en que la información de nuevo es recolectada por el sistema. La información adicional también incluye la identidad del dispositivo y la clasificación que le permita a cada nodo en la red estar representado en términos de sus capacidades, su estado y sus patrones de uso. Adicionalmente, estos patrones también se pueden analizar por vía de un número de mecanismos que incluyen la coincidencia del patrón para discriminar entre actividad normal y anómala.

Esta información de topología se puede visualizar en algunas realizaciones a través del uso de representaciones gráficas con codificaciones para el estado, tráfico, seguridad; y conectividad. La Fig. 12 describe una interfaz de visualización de ejemplo que muestra una topología seguida.

Configuración del punto de acceso.

En algunas realizaciones preferidas de la presente invención, la interfaz interactiva se suministra para configurar el punto de acceso y varios componentes de hardware y suministrar una variedad de datos de configuración que incluyen valores umbral de varias clases. En una realización preferida, un área de programa de administración suministra tal interfaz y permite:

- la definición y configuración de las configuraciones y políticas del punto de acceso;
- definición de las identidades de los usuarios autorizados y de los tipos autorizados de modos de comportamiento
- creación y/o designación de los umbrales utilizados para disparar las alarmas de intrusión/detección para puntos de acceso autorizados;
- creación y/o designación de umbrales por omisión utilizados para disparar las alarmas de intrusión/detección para puntos de acceso no autorizados;
- configuración de las configuraciones de los varios componentes de hardware/software

El área del programa de administración, en una realización preferida, ofrece una interfaz de ventana estándar caracterizada por páginas con pestañas para la fácil navegación entre las funciones de configuración. Desde dentro de cada una de las páginas con pestañas, un botón de edición permite la modificación de los valores. Después de editar los datos, aceptar temporalmente guarda los cambios. Compromiso guarda permanentemente y aplica las ediciones (hasta que se edita de nuevo). Los cambios aceptados persisten hasta que el sistema es restablecido mientras que los cambios comprometidos persisten hasta que se reinicia.

Una realización preferida intenta automáticamente detectar y registrar todas las propiedades configuradas para todos los puntos de acceso que este observa. Las configuraciones constituyen las políticas “del punto de acceso” – cuando las propiedades del punto de acceso se desvían de aquellas registradas, se pueden generar una o más alarmas. Los valores para un punto de acceso se pueden modificar manualmente para alterar la generación de alarmas específicas. Las políticas de los puntos de acceso fuera de línea también se pueden crear en algunas realizaciones que utilizan una característica de agregar.

La tabla de adelante suministra un resumen de varias propiedades de los puntos de acceso desplegables y/o configurables en algunas realizaciones preferidas de la presente invención.

Valores	Descripción
ID del Punto de Acceso	La dirección MAC del punto de acceso
Nombre del Punto de Acceso	El nombre definido del usuario del punto de acceso
ID del Conjunto del Servicio Extendido	El nombre del conjunto de servicio extendido que indica la red inalámbrica a la cual pertenece el punto de acceso

Valores	Descripción
Vendedor del Punto de Acceso	El fabricante del punto de acceso. En algunas realizaciones, este se detecta al comparar los primeros tres bytes de su dirección MAC con una base de datos con los números OUI
Velocidades Soportadas	Las velocidades de las transferencias de datos que soporta el punto de acceso. En algunas realizaciones, este valor o (estos valores) se pueden editar para especificar las velocidades soportadas.
Modos de Autenticación	Si el punto de acceso acepta conexiones de red no autenticadas y/o también acepta compartir autenticación clave. (Si se detectan conexiones que se desvían de estas configuraciones, se puede generar una alarma)
WEP Configurada para Correr	Si o no el punto de acceso se configura para requerir encriptación WEP
Manejo del AP proveniente de la Red Inalámbrica	Si el punto de acceso se configura para permitirles a los usuarios administrar de manera directa sus configuraciones sobre la red inalámbrica.
Punto de Acceso Autorizado	Si el punto de acceso está autorizado a estar presente en el espacio aéreo. Los puntos de acceso no autorizados, cuando se detectan, puede generar alarmas. (En alguna realización, un cambio en este valor no tendrá efecto hasta que se reinicie el sistema)

Para cada punto de acceso, la pantalla de mantenimiento de estación o el menú puede permitir la especificación de las estaciones que están autorizadas para utilizarla. Una realización preferida de tal pantalla o menú, detecta automáticamente todas las estaciones dentro de la huella del conjunto de servicio básico del punto de acceso (BSS) e ingresa sus direcciones MAC en una Columna Observada. Tales estaciones se pueden indicar como un miembro autorizado del BSS al seleccionarlas en la columna observada y designarlas como válidas. Las estaciones designadas se mueven a una columna válida. (Las estaciones pueden, en algunas realizaciones, ser designadas como inválidas al seleccionar y marcarlas en una columna válida. Las estaciones no autodetectadas se pueden ingresar manualmente al especificar su dirección MC en un campo de entrada Ingresar Nueva Estación y disparar una característica agregar estación. Las autorizaciones de las estaciones también se pueden hacer por vía de importar archivo, exportación del servidor de control de acceso o por vía de la configuración directa a través de la configuración de un punto de acceso típico y el puerto de manejo.

Configuración de umbrales de punto de acceso y umbrales de estaciona agregada

Los sistemas y métodos de acuerdo con la presente invención generan alertas y si se detecta un tráfico de red que exceda el umbral. En una realización preferida, todos los puntos de acceso detectados o manualmente configurados fuera de línea se listan en una lista de “pick” de Elegir Ap. Los umbrales asociados con cada punto de acceso en la lista de “pick” se pueden editar al seleccionar el punto de acceso particular. Tales valores umbral pueden ser temporales (hasta el siguiente reinicio) o persistentes en todos los reinicios (hasta que se designe una edición adicional como persistente).

Valores	Descripción
Umbral de Fortaleza de Señal	Si la fortaleza de la señal para cualquier estación en el BSS es inferior que este valor, se puede generar una alarma.
# de Asociaciones por Minuto	Ingresar el número máximo de asociaciones por minuto a permitir con todas las estaciones combinadas. (Preferiblemente, este valor no es mayor que dos veces el número de estaciones en el BSS)
# de estaciones Asociadas	Ingresar el número máximo de estaciones a las que se le permite asociarse en cualquier momento con este punto de acceso. El número debe reflejar el número real de estaciones. Si se detecta un mayor número, se puede generar una alarma.

La siguiente tabla esboza un conjunto de umbrales utilizados en una realización preferida que se refieren a las características de la red que comprenden todas las estaciones y el tráfico en el BSS. En una realización preferida, se

debe tener especial cuidado cuando se crea el o los “umbrales de bite” que siguen inmediatamente. Varios factores manejan los valores ingresados para cada uno de:

• La “velocidad de transmisión” del punto de acceso cuantos datos puede transmitir la primera consideración. Si la velocidad de transmisión es de solo 1 megabytes por segundo, los umbrales serán muy inferiores que si la velocidad de transmisión es de 11 megabytes por segundo

• Todas las cuatro “direcciones” de tráfico (alambrada a alambrada, alambrada a inalámbrica, inalámbrica a alambrada, e inalámbrica) deben agregar hasta menos del 100% del ancho de banda disponible. Muchos administradores establecerán los umbrales individuales de tal manera que su valor combinado sea menor de 80% del ancho de banda disponible.

Valor	Descripción
# bytes en BSS Proveniente de la Malla Alambrada	Ingresar el número máximo de bytes de datos por minuto permitidas en el BSS desde la porción alambrada de su red. Si se detecta un mayor número, se puede generar una alarma
# de bytes del BSS a la Malla Alambrada	Ingresar el número máximo de bytes de datos por minuto permitidos por fuera del BSS a una porción alambrada de su red. Si se detecta un mayor número, se puede generar una alarma.
# de bytes entre Estaciones en BSS	Ingresar el número máximo de bytes de datos por minuto permitidos para ser transmitidos dentro del BSS desde todas las estaciones. Si se detecta un mayor número, se puede generar una alarma.
# de bytes desde la Malla Alambrada a la Malla alambrada	Ingresar el número máximo de bytes de datos por minuto permitidos para ser transmitidos desde una porción alambrada de la red a otra porción alambrada en la red, utilizando el punto de acceso como un puente. Si se detecta un mayor número, se puede generar una alarma.
Marcos de Datos Totales Vistos	Ingresar el número máximo de marcos de datos por minuto desde todas las estaciones combinadas a las que se les permite transmitir. Si se detecta un mayor número, se puede generar una alarma.
Marcos de Manejo Total Vistos	Ingresar el número máximo de marcos de manejo por minuto desde todas las estaciones combinadas a las que se les permite transmitir. Si se detecta un mayor número, se puede generar una arma
Marcos de Control Total Vistos	Ingresar el número máximo de marcos de control por minuto desde todas las estaciones combinadas a las que se les permite transmitir. Si se detecta un mayor número, se puede generar una alarma.
Marcos Ad hoc Total Vistos	Ingresar el número máximo de marcos ad hoc por minuto desde todas las estaciones combinadas a las que se les permite transmitir. Si se detecta un mayor número, se puede generar una alarma.

Umbrales de Estación Individual

La siguiente tabla esboza un conjunto de umbrales potenciales aplicados a cualquier estación individual en una realización preferida. Si una estación única alcanza uno de estos umbrales, se puede generar una alarma.

Columna	Descripción
Umbral de Fortaleza de Señal	Si la fortaleza de la señal para cualquier estación en el BSS es inferior que este valor, se puede generar una alarma.
# de Asociaciones por minuto	Ingresar el número máximo de asociaciones por minuto a cualquier estación a la que se le permite hacerlo con un punto de acceso. Si se detecta un mayor número, se puede generar una alarma.

Columna	Descripción
# de Bytes Transmitidos	Ingresar el número máximo de bytes de datos por minuto a la que se le permite transmitirla a cualquier estación. Si se detecta un número mayor, se puede generar una alarma
# de bytes Recibidos	Ingresar el número máximo de bytes por minuto a la que se le permite recibir a cualquier estación. si se detecta un mayor número se puede generar una alarma
# de Marcos de datos transmitidos	Ingresar el número máximo de marcos por minuto a la que se le permite transmitir a cualquier estación. Si se detecta un mayor número, se puede generar una alarma
# de marcos de Dato Recibidos	Ingresar un número máximo de marcos de datos por minuto a la que se le permite recibir a cualquier estación. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de manejo transmitidos	Ingresar el número máximo de marcos de manejo por minuto a la que se le permite transmitir a cualquier estación. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de manejo Recibidos	Ingresar el número máximo de marcos de manejo por minuto a la que se le permite recibir a cualquier estación. Si se detecta un mayor número, se puede generar una alarma.
# de Marcos de Control Transmitidos	Ingresar el número máximo de marcos de control por minuto a la que se le permite transmitir a cualquier estación. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Control Recibidos	Ingresar el número máximo de marcos de control por minuto a la que se le permite recibir a cualquier estación. Si se detecta un mayor número, se puede generar una alarma.
# de Marcos de Fragmentos Vistos	Ingresar el número máximo de marcos de fragmento por minuto desde cualquier estación a la que se le permita. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Error Desencriptados Vistos	Ingresar el número máximo de marcos de error de desencripción por minuto de cualquier estación a la que se le permita. Si se detecta un mayor número, se puede generar una alarma

Umbrales de la estación de puntos de acceso

La siguiente tabla esboza un conjunto de umbrales, en una realización preferida, aplicada al punto de acceso mismo, y típicamente será algo más que los umbrales de estación agregados

Columna	Descripción
Umbral de Fortaleza de la Señal	Si la fortaleza de la señal para cualquier marco es inferior que este valor se puede generar una alarma
# de Asociaciones por Minuto	Mientras que las estaciones deben asociarse con un punto de acceso, los puntos de acceso no se asocian con ellos mismos. Por lo tanto, este valor debe ser cero, indicando que no existe asociación.
# de Bytes Transmitidos	Ingresar el número máximo de bytes de datos por minuto que se le permite transmitir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma.
# de Bytes Recibidos	Ingresar el número máximo de bytes de datos por minuto que se le permite recibir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma

Columna	Descripción
# de Marcos de Datos Transmitidos	Ingresar el número máximo de marcos de datos por minuto que se le permite transmitir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma.
# de Marcos de Datos Recibidos	Ingresar el número máximo de marcos de dato por minuto que se le permite recibir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Manejo Transmitidos	Ingresar el número máximo de marcos de manejo por minuto que se le permite transmitir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Manejo Recibidos	Ingresar el número máximo de marcos de manejo por minuto que se le permite recibir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Control Transmitidos	Ingresar el número máximo de marcos de control por minuto que se le permite transmitir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma.
# de Marcos de Control Recibidos	Ingresar el número máximo de marcos de control por minuto que se le permite recibir a este punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Fragmento Vistos	Ingresar el número máximo de marcos de fragmento por minuto que puede ver este punto de acceso antes de generar una alarma
# de Marcos de Error Desencriptados Vistos	Ingresar el número máximo de marcos de error de desencripción por minuto que puede ver este punto de acceso antes de generar una alarma

Información umbral por omisión

En una realización preferida, cuando quiera que un punto de acceso se detecte o se ingrese manualmente, las configuraciones por omisión especificadas se aplican hasta que este es manualmente adecuado. Se asume que puntos de acceso nuevos o no autorizados son piratas potenciales, por lo tanto es preferible establecer umbrales por omisión muy bajos.

Umbrales de estación agregados

La tabla de adelante esboza un conjunto de umbrales que se refiere a las estadísticas combinadas para todas las estaciones en una realización preferida.

Columna	Descripción
Umbral de Fortaleza de la Señal	Si la fortaleza de la señal para cualquier estación en el BSS asociado con un punto de acceso desconocido es inferior que este valor, se puede generar una alarma
# de Asociaciones por minuto	Mientras que las estaciones se deben asociar con un punto de acceso, los puntos de acceso no se asocian con ellos mismos. Por lo tanto, este valor debe ser cero, indicando que este no se asocia
# de estaciones Asociadas	Ingresar el número máximo de estaciones a las que se le permite asociarse con puntos de acceso desconocidos. El número debe reflejar sus estaciones reales. Si se detecta un número mayor, se puede generar una alarma
# de Bytes en el BSS de una malla Alambrada	Ingresar el número máximo de bytes de datos por minuto permitidos en el BSS a través de los puntos de acceso desconocidos provenientes de la porción alambrada de su red. Si se detecta un mayor número, se puede generar una alarma

Columna	Descripción
# de Bytes Provenientes del BSS a la Malla Alambrada	Ingresar el número máximo de bytes de datos por minuto permitidos por fuera del BSS a través de los puntos de acceso no conocidos a una porción alambrada de su red. Si se detecta un mayor número, se puede generar una alarma
# de Bytes entre Estaciones en BSS	Ingresar el número máximo de bytes de datos por minuto que se le permite transmitir dentro del BSS desde todas las estaciones a través de los puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Bytes Provenientes de la Malla Alambrada a la Malla Alambrada	Ingresar el número máximo de bytes de datos por minuto que se le permite transmitir a través de puntos de acceso desconocidos de una porción alambrada de la red a una porción alambrada de la red, utilizando el punto de acceso como un puente. Si se detecta un mayor número, se puede generar una alarma
Marcos de Datos totales Vistos	Ingresar un número máximo de marcos de datos por minuto para todas las estaciones combinadas a las que se les permite transmitir a través de puntos de acceso desconocidos. Si se detecta un mayor números, se puede generar una alarma
Marcos de Manejo Totales Vistos	Ingresar el número máximo de marcos de manejo por minuto para todas las estaciones combinadas a las que se les permite transmitir a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
Marcos de Control Totales Vistos	Ingresar el número máximo de marcos de control por minuto para todas las estaciones combinadas a las que se les permite transmitir a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
Marcos Ad Hoc Totales Vistos	Ingresar el número máximo de marcos ad hoc por minuto para todas las estaciones combinadas a las que se les permite transmitir a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma

Umbrales de estación individual

El conjunto de umbrales esbozados en la tabla de adelante aplica a cualquier estación individual en una realización preferida, y típicamente será inferior que los umbrales de estación agregados.

Columna	Descripción
Umbral de Fortaleza de la Señal	Si la fortaleza de la señal para cualquier estación asociada con un punto de acceso desconocido es inferior que este valor, se puede generar una alarma
# de Asociaciones por Minuto	Ingresar el número máximo de asociaciones por minuto que se le permite hacer a cualquier estación con un punto de acceso desconocido. Si se detecta un mayor número, se puede generar una alarma
# de Bytes Transmitidos	Ingresar el número máximo de bytes de datos por minuto que se le permite transmitir a cualquier estación a través de un punto de acceso desconocido. Si se detecta un mayor número, se puede generar una alarma
# de Bytes Recibidos	Ingresar el número máximo de bytes de datos por minuto que se le permite recibir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Datos Transmitidos	Ingresar el número máximo de marcos de datos por minuto que se le permite transmitir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma

Columna	Descripción
# de Marcos de Datos Recibidos	Ingresar el número máximo de marcos de datos por minuto que se le permite recibir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Manejo Transmitidos	Ingresar el número máximo de marcos de manejo por minuto que se le permite transmitir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Manejo Recibidos	Ingresar el número de marcos de manejo por minuto que se le permita recibir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Control Transmitidos	Ingresar el número máximo de marcos de control por minuto que se le permite transmitir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Control Recibidos	Ingresar el número máximo de marcos de control por minuto que se le permite recibir a cualquier estación a través de puntos de acceso desconocidos. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Fragmento vistos	Ingresar el número máximo de marcos de fragmento por minuto que se le permite a cualquier estación. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Error de Desencripción Vistos	Ingresar el número máximo de marcos de error desencriptados por minuto que se le permite a cualquier estación. Si se detecta un mayor número, se puede generar una alarma

Umbrales de la estación de punto de acceso

El conjunto de umbrales en la tabla de adelante aplica a todos los puntos de acceso no autorizados en una realización preferida.

Columna	Descripción
Umbral de Fortaleza de la Señal	Si la fortaleza de la señal para cualquier punto de acceso es inferior que este valor, se puede generar una alarma
# de Asociaciones por Minuto	Ingresar el número máximo de asociaciones por minuto entre cualquier punto de acceso y las estaciones. (se recomienda que este valor no sea mayor que dos veces el número de las estaciones en su BSS).
# de Bytes Transmitidos	Ingresar el número máximo de bytes de datos por minuto que se le permite transmitir desde cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Bytes Recibidos	Ingresar el número máximo de bytes de datos por minuto que se le permite recibir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Datos Transmitidos	Ingresar el número máximo de marcos de datos por minuto que se le permite transmitir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Datos Recibidos	Ingresar el número máximo de marcos de datos por minuto que se le permite recibir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Manejo Transmitidos	Ingresar el número máximo de marcos de manejo por minuto que se le permite transmitir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma

Columna	Descripción
# de Marcos de Manejo Recibidos	Ingresar el número máximo de marcos de manejo por minuto que se le permita recibir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Control Transmitidos	Ingresar el número máximo de marcos de control por minuto que se le permite transmitir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Control Recibidos	Ingresar el número máximo de marcos de control por minuto que se le permite recibir a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Fragmento vistos	Ingresar el número máximo de marcos de fragmento por minuto que se le permite a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma
# de Marcos de Error de Desencripción Vistos	Ingresar el número máximo de marcos de error desencriptados por minuto que se le permite a cualquier punto de acceso. Si se detecta un mayor número, se puede generar una alarma

Algunas realizaciones pueden permitir la autoconfiguración de algunos o todos los umbrales discutidos anteriormente. Tal autoconfiguración podría ocurrir a través del modo de aprendizaje en el cual los sistemas y métodos de acuerdo con la presente invención vigilan el tráfico sobre la red de ordenador inalámbrica durante las primeras horas o días después de la instalación. En tal modo de aprendizaje, las notificaciones de alarma se pueden deshabilitar, se espera que, al inicio, la generación de alarmas será de varios cientos o miles por día dependiendo del tráfico real de la red, hasta que se determinen los umbrales de acuerdo con la actividad normal de la red. Una vez que una fotografía precisa del tráfico de red normal se haya capturado, y que los umbrales reflejen la actividad normal, un cambio a un modo de operaciones normal posibilita las notificaciones de alarma.

En una realización preferida, una interfaz de línea de comando se suministra para configurar las configuraciones que no estén disponibles dentro de la interfaz de usuario gráfica. Por ejemplo, la dirección IP de un componente de hardware se puede cambiar, su reloj del sistema reiniciar o establecer en “sync” con un servidor de tiempo de la red. En otras realizaciones, la interfaz de usuario gráfica y/o la interfaz de línea de comando pueden permitir un traslapo significativo de la capacidad de configuración. Además, algunas realizaciones solo tienen una u otro tipo de interfaz. Finalmente, algunas realizaciones no suministran interfaz interactiva para configuración y están limitadas a leer los datos de configuración de un archivo, derivar los datos de configuración de vigilancias pasadas de la red de ordenador inalámbrica o de otra manera recibir estos datos. La interfaz de la línea de comando en una realización preferida se puede acceder sobre el componente de hardware tal como a través de una capa de comando tal como un Terminal Linux Gnome o sobre la red utilizando un cliente SSH (preferiblemente, versión 2).

En una realización preferida, una capa de comando abre automáticamente sobre el componente de hardware después de la inscripción. Un ícono terminal puede aparecer sobre la barra de tareas en la parte inferior de la pantalla. Pinchar el icono abre la ventana terminal adicional. En la indicación de la línea de comando, el comando es ingresado para lanzar la interfaz de la línea de comando.

Un cliente SSH es lanzado y conectado a la dirección IP de los componentes del hardware. La identidad del usuario que hace la conexión se verifica. En la indicación de la línea de comando, ingresar el siguiente comando para lanzar la interfaz de la línea de comando:

Interfaz de la línea de comando

En una realización preferida, la pantalla desplegada en la ventana terminal suministra cinco “áreas de programa”:

.• Red-ofrece opciones para cambiar la dirección IP, los servidores DNS, el nombre del huésped, el nombre de dominio, el servidor de correo, ARP, y crear listas de “permitir “ y “denegar”

• Fecha -permite editar el tiempo y la fecha, configurar la zona de tiempo, y la configuración de un servidor NTP.

• Servicio -suministra herramientas para la sintonía fina de los parámetros del componente de hardware, configurar el manejo de datos, y reinscribir y apagar el componente.

• Usuario -permite la creación, edición, y supresión de cuentas de usuario a las que se les permite acceso a la interfaz de usuario gráfica.

• ayuda-guía sobre el uso de la aplicación, y tópicos de ayuda detallados.

Red

Abriendo el área de programa de configuración de la red, están disponibles los siguientes comandos en una realización preferida:

Comando	Descripción
IP	Configurar dirección IP Permite la modificación de la dirección IP, enmascara la submalla, y la compuerta por omisión para el componente de hardware en el cual se comenzó sesión. La pantalla de “configuración IP” abre, desplegando la configuración de red real y permite modificación.
DNS	Definir los servidores DNS Agregar o suprimir un nameserver DRS. La “pantalla nameserver” abre, desplegando su dirección IP de los servidores DNS corrientes y permite la adición, supresión y modificación. Nota: múltiples servidores DNS pueden en algunas realizaciones tener un “orden” para procesar solicitudes DNS. El primer servidor en la lista, (identificado por el numeral 1) es el primero en ofrecer resolución de nombre; el segundo servidor en la lista (identificado con el numeral 2) es el segundo para procesar la solicitud si el primero no es capaz de hacerlo así. Con el fin de cambiar el orden de preferencia de múltiples servidores, todos deben ser suprimidos y reingresados en el orden deseado para ellos procesar las solicitudes DNS
HNAME	Establecer el hostname Cambiar el nombre del componente de hardware. La pantalla hostname “despliega” su hostname real y permite la modificación. Tener en cuenta que cuando se quiera cambiar el hostname su nombre también debe ser modificado en todos los dispositivos a los que se refiere este (por ejemplo los servidores DNS)
DNAME	Establecer el nombre de dominio Cambiar el dominio al cual pertenece el componente de hardware. La pantalla de nombre de dominio despliega su nombre de dominio corriente y permite la modificación Tener en mente que cuando quiera que se cambie el nombre de dominio este se debe modificar en todos los dispositivos a los que se refiere este (por ejemplo los servidores DNS)
MRELAY	Configurar huésped de relevo de correo Configurar un componente de hardware para enviar alarmas por correo electrónico. La pantalla de huésped de relevo de correo aparece y permite la entrada de “hostnames” calificados. En una realización, los huéspedes de relevo de correo pueden ser denominados por su dirección IP o por un “hostname” completamente cualificado (por ejemplo myhostname.mydomainname.com) o un servidor de correo para procesar mensajes de alarma de correo electrónico. Nota: el servidor de correo se debe configurar para permitir que este aparato releve el correo electrónico a través de este, o al menos para dirigir su correo a otro servidor de correo que lo relevará.

Comando	Descripción
ARP	Configurar tabla ARP permanente Crear una tabla ARP permanente. La pantalla de tabla ARP despliega sus registros ARP reales y permite la modificación. Con el fin de proteger las conexiones entre este componente de hardware y los administradores remotos que son pirateados por “la explosión” del ARP del hombre en el medio (que redirige el tráfico para esta dirección IP a una dirección MAC alternativa), es preferible crear registros ARP permanentes para puertas de acceso y otras máquinas importantes.
HALLOW	Archivo configure /etc./host.allow Especificar a qué maquinas se les permite conectar el componente de hardware. La pantalla de lista permitida despliega su lista real de las máquinas permitidas y permite modificación. Las máquinas permitidas a las que se les permite conectar a estos componentes de hardware se pueden especificar. Solo aquellas cuya dirección IP submalla, “hostname” completamente calificado, o nombre de dominio coincida con una entrada en esta lista se le permite conectar a este componente de hardware para correr los programas y las rutinas administrativas disponibles.
HDENY	Archivo config/etc./host.deny Identificar las maquinas que no puedan conectar con el componente de hardware. La pantalla de lista de denegación despliega su lista real de máquinas denegadas y permite la modificación. Las maquinas a las que no se le permite conectar con este componente de hardware se pueden especificar. Cualquiera cuya dirección IP, submalla, “hostname” completamente calificada, o nombre de dominio coincida con una entrada en la lista no se le permite conectar con este componente de hardware. Nota: HALLOW, en una realización preferida, toma precedencia sobre HDENY. Por ejemplo, si 123.456.789.963 está sobre la lista permitida, aun la submalla 123.456.789 está sobre la lista denegada, la máquina individual anterior se le permite conectar al aparato.

Fecha

Abriendo el área de programa de configuraciones de fecha, los siguientes comandos están disponibles en una realización preferida.

Comando	Descripción
TIME	Configuración de tiempo/fecha Permite la configuración de tiempo/fecha para el componente de hardware.
TZ	Establecer zona horaria Permite la configuración de la zona horaria para el componente de hardware.

Comando	Descripción
NTP	Habilitar/deshabilitar NTP Permite la configuración del componente de hardware para usar en el servidor de tiempo de red
Nota: si usted cambia el tiempo del sistema porque, por ejemplo, usted cambio la ubicación del aparato de la costa este a la oeste de los Estados Unidos, usted también debe ubicar el servidor de tiempo de red o nuevo en la misma zona horaria.	

Servicios

Abriendo el conjunto de parámetros del aparato, configurar el manejo de datos, y reestablecer o desconectar el área del sistema, los siguientes comandos están disponibles en una realización preferida:

Comando	Descripción
TUNE	Afinar los parámetros del aparato Permitir a los usuarios modificar algunos de los valores núcleo relacionado con la funcionalidad del ambiente.
DMGT	Manejo de datos Le permite a los usuarios modificar como se almacena el ambiente de sus datos
REBOOT	Sistema de reinscripción Permite el reinicio elegante de componente de hardware
HALT	Sistema de detención Permite la desconexión elegante del componente de hardware.

Usuarios

Abriendo el área de programas de usuarios, están disponibles los siguientes comandos en una realización preferida

Comando	Descripción
NEWU	Crear usuario
EDITU	Editar usuario
DELU	Suprimir usuario

La funcionalidad de estas características puede en una realización preferida coincidir con una funcionalidad similar suministrada en una instalación de manejo de usuario Linux Estándar.

Varios métodos y funciones como se exhiben en varias realizaciones de acuerdo con la presente invención se describieron anteriormente y adelante con respecto al mejoramiento de seguridad de la red. En algunas realizaciones, uno o más procesadores dentro de las arquitecturas de los ambientes como se describió anteriormente pueden ejecutar las etapas en tales métodos y suministrar tal funcionalidad. La funcionalidad puede esparcirse a través de múltiples elementos de procesamiento. En otras realizaciones, cualquier dispositivo, medio o combinación de dispositivos y/o medios de almacenamiento leíbles por ordenador que incluyen almacenamiento primario tal como RAM, ROM, memoria caché, etc. o almacenamiento secundario tal como medios magnéticos que incluyen discos y cintas fijos y removibles, medios ópticos que incluyen discos fijos y removibles sean de solo lectura

o de lectura y escritura; medios en papel que incluyen tarjetas perforadas y cintas de papel; y otros almacenamientos secundarios serán conocidos por aquellos medianamente versados en la técnica, pueden almacenar instrucciones que luego de la ejecución por uno más procesadores originen que uno o más procesadores ejecuten las etapas en tales métodos y suministren tal funcionalidad.

Evaluación de la vulnerabilidad e identificación de la amenaza

La evaluación de la vulnerabilidad se logra al analizar el tráfico WLAN, y descubrir los puntos de acceso y las estaciones de trabajo. El sistema determina cuantos bytes de estaciones de datos se envían y reciben, la fortaleza de la señal media para un día completo o la fortaleza de la señal alta/baja durante cada minuto. Se puede distinguir entre un tráfico de red interna a la red inalámbrica y un tráfico que se origine desde o destinado a la red física, alambrada y cuyas estaciones sean solos remitentes y receptores de datos más grandes. El sistema produce resúmenes amplios de datos que reportan valores altos, bajos y medios para una variedad de parámetros de tráfico, y vistas detalladas que muestran instantáneos de su tráfico minuto a minuto. Los parámetros de tráfico incluyen la descomposición del tráfico marco (control, manejo, datos, y marcos de error) y la información de enrutamiento de la red. El sistema determina si cualquier tráfico no ha sido encriptado, los usuarios son autenticados, y todo el hardware se configura adecuadamente. El sistema detecta despliegues de malintencionados al identificar y ubicar WLAN no autorizados y redes ad hoc (redes interpares) que violan la política de compañía y ponen en riesgo la seguridad. El sistema identifica tráfico/WLAN sospechoso a través de canales y frecuencias no autorizadas, las cuales pueden ser una señal común de intrusos que acceden a su WLAN o empleados que abusan de sus privilegios de red.

Los sistemas y métodos de acuerdo con una realización preferida utilizan una auditoria del hardware inalámbrico existente y efectúan una inspección de las ondas de radio que rodean la red inalámbrica antes de activar la detección de intrusión. De esta manera, se puede determinar el nivel de actividad de la línea base.

Etapa: 1 Auditoria de Hardware

Identificar cada punto de acceso en la red de ordenador inalámbrico. Obtener o determinar para cada una de sus direcciones MAC, nombre de un Conjunto de Servicio Extendido, fabricante, velocidades de transmisión soportadas, modos de autenticación, y si o no este se configura para correr Privacidad Equivalente Alambrada (WEP) y manejo administrativo inalámbrico. Además, identifica cada estación de trabajo equipada con una tarjeta de interfaz de red inalámbrica, y registra la dirección MAC de cada dispositivo. Toma nota de cualquiera de las características físicas en el ambiente (paredes, dispositivos electrónicos competentes tales como hornos microondas, teléfonos inalámbricos, etc.) que podrían interferir con las señales inalámbricas.

La auditoría de hardware sirve como línea base contra la cual los sistemas y métodos de acuerdo con la presente invención se pueden comparar. Esto es, todos los puntos de acceso y las estaciones inalámbricas se deben detectar mediante varias de las realizaciones de la presente invención. (Si no se detecta un punto de acceso o estación, luego de las etapas de los problemas lógicos) de otro lado, es probable que más dispositivos de los esperados serán detectados. Algunos de estos pueden ser estaciones o puntos de acceso no identificado o de los cuales nadie estaba enterado. Otros pueden ser dispositivos “malintencionados”- instalaciones subrepticias o no autorizadas en la red – o equipos inofensivos que pertenecen a compañías vecinas, y otros pueden ser piratas reales. Una vez que los sistemas y métodos de acuerdo con la presente invención están en modo de detección de intrusión, todos los puntos y estaciones de acceso detectadas se pueden reportar.

Etapa 2: Perímetro de inspección

Preferiblemente un componente de hardware móvil de acuerdo con la presente invención deambula el perímetro de la red de ordenador inalámbrica en un estado encendido (lo que le permite recolectar datos en la medida en que este se mueve), o colocado en una ubicación central durante 12 a 24 horas para recolectar una mayor cantidad de datos. El beneficio de una inspección “deambulante” es que esta genera una fotografía aproximadamente inmediata del “espacio aéreo” inalámbrico existente. El beneficio de una inspección “estacionaria” es que durante un mayor periodo de tiempo, es mayor la certidumbre de detectar dispositivos que solo operan intermitentemente o piratas que intentan penetrar la red en horas no hábiles. La repetición de la inspección, sea ambulante o estacionaria, debe ocurrir en todos los 11 canales.

Recolección de datos estacionarios

Dependiendo del tamaño de la red inalámbrica, el componente del equipo se puede colocar en cuatro esquinas o en puntos intermedios en la huella de Conjunto de Servicio Extendido. En cada sitio, al componente se le debe permitir vigilar pasivamente el tráfico de la red durante 12-24 horas. La copia en papel de los datos de la red se debe preservar antes de cada movimiento.

Recolección de datos deambulantes

Simplemente deambulando alrededor del perímetro de la red inalámbrica con el componente de hardware encendido y abierto en una pantalla de revisión. Los varios puntos y estaciones de acceso dentro de la red de ordenador inalámbrico se pueden detectar. Comparar esta información con la auditoria de hardware hecha antes de la recolección de estos datos. Repetir esta inspección deambulante para cada uno de los once canales.

Etapa 3: Configurada para “Reconocer” esta red.

Cada punto de acceso detectado se debe diseñar como autorizado o no autorizado. Cada estación observada se debe diseñar como válida o no.

Etapa 4: Colocar los componentes de Hardware en ubicaciones discretas a través de la red inalámbrica

Dejar un componente en cada ubicación desde 1 – 3 días. Cada día, imprimir los reportes y preservar la información capturada. Con base en esta información, se pueden sintonizar los umbrales relacionados con el punto y la estación de acceso específico para distinguir entre patrones de tráficos normales y anormales.

El motor del sistema de detección de intrusión (IDS) escucha el tráfico de la red inalámbrica. La Fig. 3 describe un proceso preferido que sigue el IDS para evaluar los datos asociados con el tráfico recibido. En el proceso de ejemplo descrito, todos los paquetes pasan a través de cuatro sistemas de detección: el ensayo basado en firma, el ensayo basado en protocolo, el ensayo basado en anomalía, y los ensayos basados en desviación de la política; otras realizaciones pueden utilizar una o más de estos ensayos u otros ensayos, en combinaciones variantes.

Inicialmente, la información de configuración es recibida en la etapa 305, típicamente incluyendo datos por omisión de la red y criterios de riesgo. Esta información se puede recuperar de un archivo, derivar u obtener de la vigilancia de la red y/o ingresar interactivamente al resultado del proceso. El sistema lee o recibe marcos del paso 310 de la red inalámbrica. Los marcos recibidos son interrogados como sigue.

La información dentro del marco se interroga para determinar si se ha identificado una firma de ataque conocida en el paso 325. La capa de enlace de datos que codifica firmas ataca patrones como combinación es de secuencias y estados de paquete. Por ejemplo, las ondas activas emiten un patrón o secuencia de solicitudes de red. Esta secuencia se puede reconocer por su firma de secuencia de paquete. Si la firma de ataque se identifica, el sistema de detección de intrusión señala un manejador de alarma para suministrar una alerta al administrador en la etapa 345.

Si no se identifica una forma de ataque, la información de marco se pasa a través de un motor de violación de protocolo para determinar si el protocolo utilizado en el marco es autorizado en la etapa 330. El análisis del protocolo examina si el uso del protocolo es legítimo o no. Por ejemplo, emitir un gran número de solicitudes de asociación o desasociación en un corto intervalo no es un uso legítimo del protocolo. Si el protocolo utilizado en el marco esta por fuera del conjunto del protocolo autorizado, el sistema de detección de intrusión señala un manejador de alarma para suministrar una alerta al administrador en la etapa 345.

Si la prueba de protocolo pasa, a la etapa 335, el IDS revisa los datos marco para anomalía estadísticas contra el SDS, o la base de datos estadística mantenida allí. La detección basada en la anomalía computa tales valores como la media, la media diferente de cero, la desviación estándar la correlación y el pico para cada franja de tiempo durante el día. Esto se puede utilizar para crear datos estadísticos normalizados para cada franja de tiempo y usuario. La actividad habitual es luego vigilada y comparada con el vector de estadísticas registrado. Si la diferencia es mayor que el umbral configurable, se genera una alerta. En lugar de o, además de, esta aproximación, la prueba Bayes se puede aplicar para deducir la probabilidad de que el vector de estadísticas habitual sea un ataque opuesto a una secuencia legítima. Si existe una anomalía, el sistema de detección de intrusión señala un manejador de alarma para suministrar una alerta al administrador en la etapa 345.

Si no se detecta una anomalía, el sistema interroga el marco para determinar si la política predefinida se ha violado en la etapa 340. La política de prueba compara la actividad observada con el conjunto configurable de reglas de actividad almacenados en el SDS. Por ejemplo, una regla puede declarar que solamente el huésped específico con la dirección específica y las tarjetas de red específicas puedan acceder la red. Si una política predefinida se ha violado, el sistema de detección de intrusión señala un manejador de alarma para suministrar una alerta al administrador en la etapa 345.

Las pruebas esbozadas anteriormente y descritas en la Fig. 3 se efectúan serialmente. En otras realizaciones, una o más de estas pruebas pueden ocurrir en paralelo. Además, solo ocurren pruebas subsecuentes si una prueba anterior se ha pasado. En una realización adicional preferida, todas las pruebas ocurren sin importar el resultado de una prueba anterior; por lo tanto, un marco de lectura simple podría generar potencialmente una alarma para cada prueba efectuada en este.

Las alertas pueden estar en cualquier forma adecuada suministrada a cualquier plataforma adecuada que incluye, sin limitación, un pantallazo a un monitor, un aviso a un buscapersonas, una llamada de voz saliente a un teléfono,

un mensaje SMS a un teléfono móvil, un mensaje de correo electrónico a una dirección valida, enviado a una página de red disponible por vía de un servidor de red apropiado o una alerta WAP a un dispositivo habilitado con WAP. Varios tipos de pantallazos y reportes se pueden utilizar para suministrar información con relación a las alarmas generadas.

En alguna realización, la salida de todas las pruebas IDS son entonces comparadas y el nivel de confianza computado en la etapa 345. En una de tales realizaciones, en el caso donde solamente se detecta una anomalía estadística, esta es marcada con una alerta de desempeño de nivel inferior. En el caso donde una o más de otras violaciones se detectan, la alarma se eleva a una alarma de intrusión.

Algunas realizaciones pueden utilizar una variedad de almacenes de datos para ejecutar el proceso anterior para hacer seguimiento a los datos a través de múltiples iteraciones del proceso; tales almacenes de datos pueden en una realización preferida ser parte de un SDS tal como se describió anteriormente. Algunas de tales realizaciones pueden incluir una base de datos estadística, una base de datos de estación y/o un almacén de datos de estado. En tales realizaciones, pueden ocurrir algunas o todas las siguientes etapas descritas en la Fig. 3

En la etapa 315, se actualiza la base de datos de la estación. Esta base de datos contiene, en una realización preferida, por estación y por punto de acceso registros con la información que describe la dirección del dispositivo, el estado de comunicaciones, marcas de tiempo de la primera y última actividad, conteo de los bytes de transmisiones y la información de política local que describe si el dispositivo es autorizado o no para uso en la red vigilada.

En la etapa 320 se actualiza la información de estado. El estado se refiere a si el dispositivo ha sido visto o no antes y si o no la estación es información de estado no autenticada y no asociada, autenticada, autenticada y asociada o desconocida, asociada con una red de ordenador inalámbrica.

En la etapa 350, se hace la determinación de si el intervalo estadístico particular ha sido completo. Si es así, la estadística en el SDS se actualiza en la etapa 355, y el procesamiento continúa con el siguiente marco en la etapa 310. De otra manera, el procesamiento simple continúa en la etapa 310 con la siguiente lectura o recepción de un marco.

Un versión modificada y mejorada de la aproximación anterior se utiliza donde el tráfico de la red se vigila desde múltiples dispositivos de entrada tal como las realizaciones descritas en las Figs. 2B-E. La Fig. 4 describe este proceso mejorado que inicia en la etapa 405.

La etapa 410 es análoga a la etapa 305 proveniente del proceso de la Fig. 3. En la etapa 410, se recibe la información de configuración. Como anteriormente, este se hace típicamente a través de un sistema de archivos de configuración de sistema de lectura, vigilar la red y/o la entrada interactiva a la salida del proceso. Esta información incluye típicamente datos por omisión de la red y criterios de riesgo tales como, datos de configuración del punto de acceso (Dirección MAC del punto de acceso, nombre del Punto de Acceso, etc.), datos de configuración de la estación y varios valores de umbral.

En la etapa 430, el marco de paquete inalámbrico se recibe de cada dispositivo de entrada (por ejemplo componentes de hardware 210A-D, sistema 220 huésped y/o los sensores 230A, 230B). Los marcos son leídos de tal manera que se puede interrogar el contenido del marco.

Cada marco leído es interrogado por un sistema de detección de intrusión multidimensional (IDS) tal como se detalló anteriormente con respecto a la Fig. 3, y las salidas de todas las pruebas IDS son entonces comparadas con un nivel de confianza computado en la etapa 435. Como con el proceso anterior, otros resultados solos, o en combinación con cada uno de los otros en combinación con uno o más de aquellos descritos anteriormente se pueden utilizar en otras realizaciones.

En la etapa 440, en el caso donde solamente se detecta anomalía estadística esta se marca como una alerta de desempeño de nivel inferior. En el caso donde, además de la anomalía estadística, se ha detectado una de las otras violaciones, la alarma se eleva a una alarma de intrusión y un manejador de alarma se alerta en la etapa 444. Otras realizaciones no confían en el resultado de la prueba agregada pero determina el estado de alarma en los resultados de prueba única. Además, algunas realizaciones pueden utilizar otros tipos de prueba y combinación es de resultados para determinar el tipo y la severidad de las alarmas generadas.

Si una alarma no es detectada en la etapa 440, una prueba para ver si el intervalo predeterminado para recoger las estadísticas se ha alcanzado ocurre en la etapa 460. Si al final ha ocurrido el intervalo de recogida de estadísticas preconfiguradas, el SDS se actualiza en la etapa 470 para reflejar las estadísticas recogidas provenientes de los marcos recibidos sobre el intervalo. Las estadísticas son recogidas por el tráfico de vigilancia entre los nodos de la red, las estadísticas minuto a minuto acerca de los tipos de marco BSS y los volúmenes de tráfico, resumen las estadísticas de transmisión para todas las estaciones asociadas con los puntos de acceso, las estadísticas de transmisión del minuto presente para todas las estaciones, y las estadísticas de transmisión minuto a minuto detalladas para cualquier estación individual en la red de ordenador inalámbrica.

La fusión de datos ocurre sobre una base de tanda al agregar los datos provenientes de múltiples bases de datos. Este proceso inicia en la etapa 414. El proceso integra datos estadísticos provenientes de multiplex bases de datos que es generado a través de la vigilancia marco y los motores de detección de intrusión. Esta aproximación suministra una metodología para manejar los datos recibidos de los dispositivos de entrada tal como los dispositivos de hardware 210A-D y/o los sensores 230A, 230B desplegados en múltiples sitios para agregar datos de empresa en un sistema central único tal como el huésped 220.

La base de datos de Perfil de Ataque y de Estación se lee en la etapa 418 para iniciar el bucle de procesamiento para integrar las bases de datos provenientes de fuentes separadas. La correlación y el patrón de reconocimiento se efectúan en la etapa 420 para actualizar los perfiles de ataque y estación en la etapa 424. El bucle de procesamiento luego se duerme en la etapa 428 hasta que el siguiente intervalo de bucle de procesamiento tiene lugar con base en el intervalo o disparo de tiempo preconfigurado.

Después de que el manejador de alarma es señalado en la etapa 444, el ataque y la base de datos del perfil de la estación es leído en la etapa 448; en esta etapa, los ataques existentes son consultados y el estado de seguridad de la estación existente es consultado. En la etapa 450, este dato es comparado con la alarma recientemente generada. Si esta es suficientemente similar, no ocurre ninguna nueva notificación externa en la etapa 454. Sino, se genera un nuevo mensaje de notificación en la etapa 454 y la pantalla de la consola y/o el mensaje externo de la alarma ocurre en la etapa 458.

En algunas realizaciones, la exploración de las ondas de radio para la actividad de la red puede ser de naturaleza adaptativa. En una configuración típica, los canales de la red inalámbrica son explorados para actividad de acuerdo con un patrón predefinido. De acuerdo con una aproximación adaptativa, el patrón predefinido puede servir como un patrón inicial y/o de línea base. Este patrón puede ser entonces adaptado con base en la actividad presente de los canales explorados. La Fig. 11 describe un diagrama de flujo de un proceso para efectuar exploración adaptativa.

Este mecanismo le permite al sistema explorar determinísticamente todos los canales inalámbricos a través del multiplexado basado en tiempo aunque también le permite al sistema ajustarse adaptativamente al gasto de tiempo sobre un canal dado con base en la actividad corriente o pasada. Un escenario típico sería vigilar un conjunto fijo de canales y periódicamente efectuar una exploración de trasfondo de los canales restantes; la Fig. 14 describe una interfaz de ejemplo para configurar tal línea base o el patrón de exploración por omisión. Si se observa cualquier actividad en un canal que se espera que este ocioso o si se descubre actividad no autorizada, el sistema se adapta al agregar este canal a su patrón de exploración primario. Si la actividad disminuye entonces, este canal se retirará del patrón de exploración primario y luego se explorará durante el modo de exploración de trasfondo. El sistema puede utilizar umbrales preconfigurados o umbrales ingresados por el usuario para determinar el punto de disparo en el cual iniciar o detener la vigilancia dinámica del canal. Adicionalmente, se pueden incluir los controles automatizados lo que se asegurará en el canal si se ha detectado una violación de seguridad por un motor de análisis multidimensional subyacente.

Además, las realizaciones mejoradas pueden utilizar receptores multicanal en los cuales puede ocurrir una exploración adaptativa únicamente por el receptor. Esto permite, por ejemplo, que los canales múltiples o que las bandas de frecuencia múltiples se puedan explorar y vigilar en paralelo.

Como se describió anteriormente, los sistemas y métodos de acuerdo con la presente invención pueden generar automáticamente alarmas cuando quiera que ciertos eventos o condiciones ocurren dentro de su red inalámbrica. En algunas realizaciones, se puede suministrar un manejador de alarma que suministra una interfaz para visualización.

La siguiente tabla identifica las alarmas, los subtipos de alarma y las severidades disponibles en una realización preferida denominada como AirDefense Mobile.

Tipo de alarma	Subtipo de alarma	Nivel de alarma
Ataque DoS	Desautenticar El AirDefense Mobile detecta cuando un pirata pretende tener un punto de acceso y radiodifundir un mensaje de “desautenticar”. Esto forza a todas las estaciones a reautenticarse generando tráfico de red excesivo y originando conectividad inconsistente y transferencia de datos.	Crítico

Tipo de alarma	Subtipo de alarma	Nivel de alarma
	Disociar El AirDefense Mobile detecta cuando un pirata pretende tener un punto de acceso y radiodifundir un mensaje de “desasociar”. Este forza todas las estaciones a reasociarsen con el punto de acceso, generando tráfico de red excesiva, y originando conectividad inconsistente y transferencia de datos.	Crítico
Estación no autorizada	No está en la lista permitida AirDefense Mobile detecta una estación cuya dirección MAC no está en su lista valida (una lista valida es mantenida por el sistema.)	Crítico
Umbral	Errores GLB CRC AirDefense Mobile detecta si los errores CLC excedieron los limites configurados (errores CRC los errores CRC son generados cuando los “checksums” fallan en marcos individuales.)	Mayor
	Conteo de asociación BSS AirDefense Mobile detecta cuando el número de asociación dentro del BSS completo, en cualquier minuto dado excede el número especificado en la información de configuración.	Mayor
	Fortaleza de la señal BSS AirDefense Mobile detecta cuando la fortaleza de la señal en cualquier punto de acceso cae por debajo de un umbral especificado.	Crítico
	Fragmentos BSS	Menor
	AirDefense Mobile detecta cuando el número de marcos fragmentados dentro de algún minuto excede un umbral especificado.	
	Errores de desencriptación BSS AirDefense Mobile detecta cuando el número de marcos de error desencriptados dentro de cualquier minuto excede un umbral especificado.	Mayor
	Estaciones de asociación BSS AirDefense Mobile detecta cuando el número total de estaciones asociadas en un BSS completo, en cualquier minuto dado, excede un número especificado.	Menor
	BSS tbw dentro AirDefense Mobile detecta cuando, durante cualquier minuto, el número de bytes de datos que ingresan al BSS proveniente de una porción alambrada de su red excede un umbral establecido.	Menor
	BSS tbw fuera AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de bytes de datos que van del BSS a la porción alambrada de su red excede un umbral establecido.	Menor

Tipo de alarma	Subtipo de alarma	Nivel de alarma
	BSS tbw intra AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de bytes de datos que se originan desde y que están destinados al BSS exceden un umbral especificado.	Menor
	BSS tbw a través AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de bytes de datos que se origina de una porción alambrada de la red salta a través del BSS a otra porción alambrada de la red excede un umbral establecido.	Menor
	Datos BSS AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de marcos de datos en el BSS excede un umbral especificado.	Mayor
	BSS mgt AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de marcos de manejo en el BSS excede un umbral especificado.	Mayor
	BSS ctl AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de marcos de control en el BSS excede un umbral establecido.	Mayor
	BCC ad hoc AirDefense Mobile detecta cuando, durante cualquier minuto, el número total de marcos ad hoc en el BSS excede un umbral especificado. Nota: las tarjetas adaptadoras de red inalámbrica de menor calidad generaran aleatoriamente marcos ad hoc. El umbral (1) por omisión del AirDefense Mobile puede originar que todos estos marcos espurios generen una alarma. Después de vigilar la red durante una semana o dos, puede ser aconsejable establecer el umbral en un número o un poco mayor que lo que normalmente genera la red.	Crítico
	Conteo de asociaciones STA AirDefense Mobile detecta cuando, durante cualquier minuto, cuando cualquier estación de asocia con un punto de acceso más veces de las suministradas por un umbral especificado.	Mayor
	Fortaleza de las señales STA AirDefense Mobile detecta cuando, durante cualquier minuto, cuando cualquier fortaleza de la señal de la estación cae por debajo de un valor especificado.	Crítico
	Fragmentos STA AirDefense Mobile detecta cuando, durante cualquier minuto, cuando cualquier estación genera más marcos fragmentados que un valor especificado.	Menor

Tipo de alarma	Subtipo de alarma	Nivel de alarma
	Errores de desencriptacion STA AirDefense Mobile detecta cuando, durante cualquier minuto, cuando cualquier estación genera más errores de desencriptación que un umbral establecido.	Mayor
	STA tbw recibido AirDefense Mobile detecta cuando, durante cualquier minuto, cuando cualquier estación recibe más bytes de datos que un umbral predetermidado.	Menor
	STA tbw transmitido AirDefense Mobile detecta cuando, durante cualquier minuto, cuando cualquier estación transmite más bytes de datos que las especificadas en el umbral establecido.	Menor
	Datos recibidos STA AirDefense Mobile detecta cuando, en cualquier minuto, cuando cualquier estación recibe más marcos de datos que un umbral especificado.	Mayor
	Datos transmitidos STA AirDefense Mobile detecta cuando, en cualquier minuto, cuando cualquier estación transmite más marcos de datos que un umbral especificado.	Mayor
	STA mg recibido AirDefense Mobile detecta cuando, en cualquier minuto, cuando cualquier estación recibe más marcos de manejo que un umbral especificado.	Mayor
	STA mgt transmitido AirDefense Mobile detecta cuando, en cualquier minuto, cuando cualquier estación transmite más marcos de manejo que un umbral especificado.	Mayor
	STA ctl recibo	Mayor
	AirDefense Mobile detecta cuando, en cualquier minuto, cuando cualquier estación recibe más marcos de control que un umbral especificado.	
	Transmisión STA ctl AirDefense Mobile detecta cuando, en cualquier minuto, cuando una estación transmite más marcos de control que un umbral establecido.	Mayor
Robo de ID	Fuera de secuencia AirDefense Mobile detecta cuando los marcos son transmitidos fuera de secuencia. Esto sugiere que alguien ha falseado una estación y está enviando datos al mismo tiempo como la estación legitima.	Crítico

Tipo de alarma	Subtipo de alarma	Nivel de alarma
	Vendedor fuera de carácter AirDefense Mobile compara cada una de las transmisiones de la estación contra una base de datos interna del vendedor conocida “perfiles de transmisión” o “firmas”. Si el tráfico de red real no coincide con el perfil del vendedor asociado con el NIC inalámbrico de la estación, el AirDefense Mobile asume el tráfico se origina de una estación no autorizada que utiliza un NIC falso.	Crítico
	Fortaleza de señal anómala AirDefense Mobile hace seguimiento a una fortaleza de señal alta, baja y media de cada estación muchas veces en un minuto durante el día. Cuando quiera que éste detecta que la fortaleza de la señal de la estación se desvía de la norma, este genera una alarma.	Crítico
Modo de Punto de Acceso	Modo WEP cambiado AirDefense Mobile detecta cuando el valor WEP en una baliza de punto de acceso difiere del valor que este se supone que debe ser. (AirDefense Mobile autodetectó la propiedad WEP o fue manualmente ingresada)	Crítico
	Velocidad cambiada AirDefense Mobile detecta cuando los valores de velocidad de transmisión soportados en una baliza de punto de acceso difieren del valor que éste se supone que debe ser. (AirDefense Mobile autodetectó la propiedad de velocidad, o fue manualmente ingresada)	Crítico
	Canal cambiado AirDefense Mobile detecta cuando quiera que el punto de acceso cambia los canales. (el canal se identifica en información de configuración)	Crítico
	CF cambiado AirDefense Mobile detecta cuando el valor de coordinación del punto en una baliza de AP cambia. Un cambio en este campo puede indicar que el punto de acceso fue reconfigurado, aunque este no es necesariamente un problema. (El campo de coordinación de punto se refiere al modo del punto de acceso de evitar colisión.)	
	Essid cambiado AirDefense Mobile detecta cuando la radiodifusión del punto de acceso de su BSS ID extendido cambia. La información ESSID se almacena como información de configuración.	
Administración de AP no Autorizado	AirDefense Mobile detecta cuando las sesiones de administración están siendo conducidas directamente con el punto de acceso.	Crítico
Marco Mgt. Aleatorio	Sta tx ap mgt fr AirDefense Mobile detecta cuando una estación está transmitiendo un marco de manejo reservado para el uso del punto de acceso.	Crítico

Tipo de alarma	Subtipo de alarma	Nivel de alarma
	Aptx ilegal mgt fr AirDefense Mobile detecta cuando el punto de acceso transmite un marco de manejo ilegal.	Crítico
	Fuera del marco spec AirDefense Mobile detecta cuando el punto de acceso transmite un marco que no sigue los estándares 802.11b.	Crítico
	Otro marco falso AirDefense Mobile detecta cuando un punto de acceso transmite cualquier marco que éste no entiende.	Crítico
Malla Ad Hoc Detectada	AirDefense Mobile detecta cuando las estaciones están directamente transmitiendo y recibiendo a y desde cada una de las otras sin utilizar un punto de acceso autorizado. Nota: a diferencia de todas las otras alarmas que son generadas cada vez que se detecta un evento de red en un minuto, AirDefense Mobile solo generara una alarma de Red Ad Hoc una vez en el periodo de 24 horas corriente para cada dirección MAC.	Crítico
Velocidad de Baliza AP	AirDefense Mobile detecta cuando la velocidad de baliza del punto de acceso cambió.	Crítico

Los presentes sistemas y métodos le permiten al usuario final especificar y ejecutar las restricciones de seguridad y política asociadas con el despliegue de una red inalámbrica particular. Una vez configurada con tal información, la actividad de la red se vigila de manera continua para determinar si la actividad está dentro de las guías especificadas por las restricciones establecidas.

Si se encuentra que la actividad no cumple con las restricciones establecidas, se genera una alarma en tiempo real y se reporta al usuario a través de una serie de mecanismos. Estos mecanismos pueden incluir Web, Email, SNMP y una notificación Syslog. En algunas realizaciones, la respuesta no está limitada a la notificación. Estas realizaciones pueden incluir aplicación automatizada y/o medidas defensivas activas tal como se discute adelante.

Aplicación de política automatizada

Algunas realizaciones soportan aplicaciones automatizadas de restricciones. En tales realizaciones, pueden ocurrir intentos para rectificar la desviación de la política a través de la reconfiguración del dispositivo o dispositivos afectados automáticamente luego de la detección de la desviación. Estos intentos de reconfiguración intentan ejecutar la política especificada dentro de los dispositivos relevantes.

Este problema se puede visualizar como una forma de un bucle de control de retroalimentación. En muchos casos, tal bucle opera al comparar la entrada de referencia a una salida medida, computar su diferencia, y utilizar esta diferencia para ajustar la salida deseada. Esto continúa para impulsar la salida deseada para cumplir con la entrada de referencia.

La FIG. 10 describe un proceso de ejemplo que incluye aplicación de política automatizada. Ocurre la vigilancia normal de actividad de la red. La actividad vigilada es revisada para cumplimiento de las restricciones establecidas. Si una restricción es violada, se genera una notificación (alerta) y se envía a un usuario y/u otros sistemas. Un procedimiento asociado con la alerta se dispara lo que intenta manual o atónitamente rectificar la causa subyacente de la violación. Si el procedimiento rectifica exitosamente la causa de la violación, la alerta disparada se puede cancelar, actualizar o modificar de otra manera para indicar el estado presente de la violación.

La resolución automática de la violación de política puede emplear una interfaz de manejo y control sobre el equipo vigilado para efectuar el cambio deseado. Esta interfaz puede estar en la forma de un HTTP, HTTPS, SNMP o una interfaz de línea de comando especifica del vendedor alcanzable por vía Telnet, SSH u otra interfaz de inicio de sesión remota; además, o en lugar de, las interfaces alternativas se pueden suministrar por vía de voz automatizada y/o sistemas de reconocimiento de tono para manejar la configuración basada en teléfono del ambiente. Múltiples de

tales interfaces podrían estar disponibles de manera simultánea. Un ejemplo de una interfaz basada en la red se describe en las FIGS. 13a-B.

Defensa activa

En algunas realizaciones de la presente invención, uno o más mecanismos de defensa activos se pueden disparar en respuesta a las condiciones de alarma, además de, o en lugar de, el proceso de notificación descrito anteriormente. El sistema puede suministrar defensa activa de los ataques al radiodifundir datos en la red inalámbrica así como también ser capaz de atrapar y/o mapear las estaciones de trabajo del intruso al triangular la ubicación de la estación de trabajo del intruso con relación a los puntos de acceso de la red inalámbrica. Esta también puede intentar alterar la configuración del punto de acceso de manera que le haga difícil o imposible al atacante objetivo continuar con las comunicaciones.

Al introducir los errores CRC en la corriente inalámbrica, el sistema pude derrotar activamente un atacante que está vigilando la corriente de patrones para romper la encriptación. Los errores CRC son introducidos al transmitir al mismo tiempo que el intruso detectado. Debido a la naturaleza del medio compartido de la red de ordenador inalámbrico, causa que la transmisión del paquete se corrompa, evitando que el intruso se comunique exitosamente con la red.

Al introducir “chaf”, el sistema puede derrotar activamente el atacante al ubicar marcos aleatorios en la corriente de tal manera que los patrones de encriptación se vuelvan indetectables. El “chaf” es una forma de transmisión de paquetes aleatorizada que se diseña para reducir la probabilidad de que un análisis estadístico de la secuencia de paquete resulte en la ruptura de la clave de encriptación. Esto se hace al emitir una transmisión de trasfondo de baja velocidad de los paquetes que son emitidos utilizando las mismas características (por ejemplo, dirección, vector de inicialización, etc.) del tráfico legítimamente observado pero con una carga útil aleatorizada.

El sistema puede bloquear una red inalámbrica al interferir, una técnica para evitar cualquier acceso no autorizado al punto de acceso inalámbrico al introducir suficiente ruido en la red inalámbrica de tal manera que las estaciones de trabajo no puedan conectarse físicamente a la red inalámbrica. La interferencia es una transmisión de capa física que se efectúa para afectar todas las comunicaciones inalámbricas no deseadas. Esto es equivalente a introducir una señal de ruido en la parte superior de una transmisión de señal no deseada de tal manera que cualquier receptor no pueda recibir exitosamente la transmisión.

En una aproximación de dispositivo físico, una realización utilizaría un sensor autónomo para ejecutar cualquiera de los mecanismos de defensa activo. El cambio de canal dinámico puede ser utilizado para reencaminar el tráfico autorizado a un canal de comunicación diferente para evitar un intruso detectado en un canal particular. En esta aproximación, la solicitud de cambio de canal es transmitida al punto de acceso que se cree que está comprometido y las estaciones autorizadas utilizan el nuevo canal para comunicarse con el punto de acceso. Esta aproximación se puede utilizar para evitar los problemas que origina la interferencia en la comunicación entre el punto de acceso y sus estaciones autorizadas.

Algunas realizaciones que incluyen un cambio de canal dinámico pueden además utilizar un equipo trampa que engañe al atacante al pensar que el canal original es aun valido y suministre información forense necesaria para identificar el atacante. La Figura 5 describe un diagrama de flujo de un proceso que inicia en la etapa 510 utilizada en algunas de tales realizaciones que incorporan el equipo trampa.

En la etapa 520, se recibe la información de configuración. Esta etapa es la misma de las etapas previamente descritas 305 y 410 en las Figs. 3 y 4 respectivamente. La etapa 530 representa un bucle de espera que espera hasta que el ataque ha sido detectado. Típicamente, un sistema de detección de intrusión genera una señal que dispara la partida de este bucle; en algunas realizaciones preferidas, el sistema de detección de intrusión contiene el hardware y/o ejecuta el proceso descrito anteriormente. La señal del sistema de detección de intrusión típicamente incluye un indicador del punto de acceso que se cree que está bajo ataque.

En el caso de que un ataque haya sido detectado en 530, el procesamiento es pasado a la etapa 540 para activar el equipo trampa. Una trampa se inicia en la etapa 580. La trampa se inicializa así misma con la identidad del punto de acceso vigilado que se considera que va ser atacado. Esta identidad típicamente incluye la dirección MAC, el identificador del conjunto de servicio, el modo de encriptación, el modelo de red y los modos de transmisión. Una vez inicializado, la trampa se mueve a la etapa 590, el intruso trampa se procesa. Este proceso es designado para engañar lógicamente al atacante identificador al creer que la comunicación está aún ocurriendo con el punto de acceso original. Esto se logra a través de una emulación completa de la identidad del punto de acceso original y el comportamiento. Al mantener la comunicación con el atacante, se crea la trampa de tal manera que la proximidad física del atacante se asegura en tanto que continúe la comunicación. Opcionalmente, se puede asumir una nueva identidad de tal manera que un punto de acceso que aparece más vulnerable pueda ser presentado al atacante. Esto se hace al emular de nuevo la funcionalidad del punto de acceso, pero en este caso con la identidad y conjunto de características que parezcan vulnerables. Esta apariencia de vulnerabilidad puede ser creada a través del uso de

modos de encriptación débiles o sin estos o la apariencia de modos de fabricación por omisión con claves conocidas y las ID de usuario.

En la etapa 550 se envía un paquete de control al punto de acceso original para cambiar los canales o suspender la transmisión mientras que la trampa es acoplada. Este paquete encapsula un mensaje que indica la anterior solicitud y puede ser enviado fuera de banda al punto de acceso. En banda se refiere a la transmisión sobre el aire de la interfaz de red inalámbrica del punto de acceso mientras que una transmisión fuera de banda se refiere a una transmisión de la interfaz lateral alambrada del punto de acceso.

Procesar el bucle principal que regresa a la detección de ataque en 530.

La triangulación determina la ubicación del atacante al mapear su posición relativa dentro de los puntos de acceso inalámbricos desplegados. El proceso de mapeo y detección de la localización de acuerdo con una o más de las realizaciones preferidas de la presente invención tal como se describió en la Figs. 6A-B se discute con mayor detalle adelante.

El proceso de la Fig. 6A se utiliza para crear una base de datos interna de las direcciones IP y/o los nombres mapeados a las direcciones MAC correspondientes. Cada transacción de protocolo de resolución de dirección (ARP) se detecta en la etapa 605. En la etapa 610, la información en la transacción detectada se utiliza para actualizar la base de datos interna. Algunas realizaciones pueden efectuar la identificación y el procesamiento de localización tal como se describió en la Fig. 6B sin referencia a tal base de datos interna. La base de datos se crea y se mantiene en una realización preferida para hacer la identificación de la estación y el proceso de localización más fácil y más eficiente.

La Fig. 6B describe un proceso para identificar y ubicar una estación dentro de una red inalámbrica. En algunas realizaciones, este proceso se puede utilizar para precisar la ubicación del potencial atacante; en algunas de tales realizaciones, la activación del proceso se dispara mediante un sistema de detección de intrusión. En una realización preferida, el proceso es disparado por uno de los sistemas de detección de intrusión y los métodos descritos en detalle anteriormente.

En la etapa 620, ocurre una búsqueda en la base de datos interna, tal como la creada por vía del proceso descrito en la Fig. 6A, sobre la dirección MAC corriente para determinar si un IP o mapeo de nombra ya está disponible. Si se encuentra, la base de datos interna es actualizada en la etapa 640 y la ejecución procede a la etapa 645 para solicitarle al arreglo de sensor inalámbrico, iniciar la posición o resolución de localización. Como se indicó anteriormente, la base de datos interna es una aproximación para adquirir la información deseada. Algunas realizaciones pueden pasar esta etapa y utilizar el sensor de cableado o la aproximación de protocolo de resolución de dirección inversa (RARP) discutida adelante.

De otra manera, se puede consultar un sensor de red cableado opcional por el mapeo del nombre en la etapa 625. Este sensor es preferiblemente desplegado dentro de una red alambrada en una localización conveniente para olfatear el DHCP, LDAP, DNS u otros protocolos de mapeo de servicio/nombre. Si se encuentra, la base de datos interna se actualiza en la etapa 640 y la ejecución procede a la etapa 645 para solicitarle al arreglo de sensor inalámbrico, iniciar la posición y resolución de localización. Algunas realizaciones pueden no incluir tal sensor de red alambrado, en cuyo caso se pasa esta etapa.

Si el nombre aún no se ha encontrado, la ejecución procede a la etapa 630 donde se emite una solicitud RARP. Esta solicitud le solicita a la población receptora la dirección IP y la dirección MAC en cuestión. Si se encuentra, la base de datos interna se actualiza en la etapa 640 y la ejecución procede a la etapa 645 para solicitarle al arreglo de sensor inalámbrico iniciar la posición o resolución de ubicación.

Si no se encuentra, el mapeo del nombre/IP no está disponible al momento corriente para esta dirección MAC. En algunas realizaciones, el mapeo del nombre/IP puede no ser deseado pero la localización o información de posición es en cuyo caso el proceso puede iniciar en tales realizaciones en la etapa 645.

La etapa 645 inicia la posición o resolución de localización con una solicitud al arreglo de sensor inalámbrico. Cada sensor se le solicita el seguimiento de información sobre la dirección MAC corriente en cuestión. Esta información de seguimiento identifica si el MAC es actualmente observable por un sensor dado, el sensor ID, y la fortaleza de señal asociada con el MAC en cuestión. El arreglo de sensor puede incluir no solo dispositivos de sensor (por ejemplo 230A, 230B) sino también otros nuevos inalámbricos accesibles desde este proceso tal como los dispositivos 210A-D y/o el sistema 220 huésped.

De los datos recibidos por vía de la solicitud, la posición relativa de la parrilla de sensores se calcula en la etapa 650 al computar la distancia de la “fortaleza de señal” a cada sensor. Esta distancia es computada como la raíz cuadrada de la suma de los cuadrados de los valores de fortaleza de señal de los tres sensores. La posición es luego estimada para estar dentro de la proximidad de los sensores determinados por tener una distancia de fortaleza de señal más pequeña con la dirección MAC en cuestión por la computación anterior. Una vez que se seleccione el

conjunto de sensores, la posición se refina adicionalmente al seleccionar la posición como dentro de la proximidad del sensor dentro del anterior conjunto con la fortaleza de señal más fuerte. En algunas realizaciones, el proceso finaliza en este punto regresando la información de posición.

En realizaciones que mantienen la base de datos en posición, esta base de datos es actualizada en la etapa 660 con la posición de la dirección MAC en cuestión. El proceso entonces finaliza en la etapa 670.

Análisis y manejo de la red Encriptada.

Las técnicas utilizadas para vigilar las WLAN pueden aplicar en general para vigilar y analizar cualquier enlace de red que utiliza la encriptación de la carga útil o en la capa IP y por encima de solo los WLAN. En este caso, se observan la capa1 y la capa 2 y se toman decisiones en estas capas en términos de firma, protocolo, política y análisis de anomalía estadística para evaluar la salud y seguridad de la red. Esta técnica es así aplicable a cualquier red (alambrada o inalámbrica) que exhiba las características de encriptación anteriores del tráfico de red. En otras palabras, la IDS multidimensional implementada por nuestro marco es más ampliamente aplicable para manejar y asegurar cualquier encriptada. En este caso, un WLAN que corre el WEP es una instancia particular de una red encriptada.

Las realizaciones descritas anteriormente son dadas como ejemplos ilustrativos solamente. Se apreciará fácilmente por aquellos expertos en la técnica que muchas desviaciones se pueden hacer de las realizaciones específicas descritas en esta especificación sin apartarse de la invención. De acuerdo con esto, el alcance de la invención va a ser determinado por las reivindicaciones de adelante en lugar de estar limitado por las realizaciones específicamente descritas anteriormente.

REIVINDICACIONES

1. Un sistema de seguridad de red, el sistema comprende:

(a) Un almacén (110) de datos de sistema capaz de almacenar datos de criterio de riesgo, datos por omisión de red, y desempeño de la red y datos de uso;

(b) una primera interfaz de comunicación que comprende un receptor que recibe comunicaciones de llegada desde un canal de comunicación asociado con la interfaz de comunicación;

(c) un procesador (120) de sistema que comprende uno o más elementos de procesamiento, en donde el procesador (120) de sistema está en comunicación con el almacén (110) de datos del sistema y está programado o adaptado para efectuar las etapas de:

(i) recibir (310) datos que corresponden a un marco transmitido sobre la red de ordenador inalámbrica encriptada y una señal utilizada para transmitir el marco por vía de la interfaz de comunicación

(ii) detectar (325, 330, 335, 340) una violación dentro de la corriente de datos encriptada al aplicar una pluralidad de pruebas que comprenden una prueba (335) de anomalía estadística que compara los datos recibidos con los datos estadísticos en el almacén (110) de datos del sistema o la información derivada de ésta y efectúa detección basada en anomalía con base en la comparación entre los datos recibidos y los datos estadísticos, en donde la pluralidad de pruebas además comprende una prueba (340) de política que compara los datos recibidos con la política predeterminada, y en donde los datos estadísticos comprenden cualquier media, media no cero, desviación estándar, autocorrelación, y pico para cada franja de tiempo y una pluralidad de umbrales.

(iii) Generar (345) una señal de alarma si se detectó la violación;

en donde la primera interfaz de comunicación comprende además un transmisor que transmite comunicaciones de salida al canal de comunicaciones y en donde el procesador (120) del sistema es programado o adaptado para efectuar la etapa de disparar una defensa activa de la red de ordenador inalámbrica en respuesta a una alarma generada; y

en donde la defensa activa disparada es:

1) Introducir errores CRC;

2) transmitir marcos que comprenden datos aleatorios, o

3) activar una defensa de equipo trampa al:

(a) determinar de los datos recibidos el canal utilizado para transmitir la señal, un punto de acceso al cual la señal fue dirigida y una estación que origina la señal;

(b) reconfigurar el punto de acceso y las estaciones autorizadas para comunicación utilizando un canal diferente del canal determinado; y

(c) interactuar con la estación que origina la señal que utiliza el canal determinado.

2. El sistema de la reivindicación 1, en donde el almacén (110) de datos del sistema comprende un almacén de datos estadísticos que almacena los datos históricos con relación a la red de ordenador inalámbrica.

3. El sistema de la reivindicación 2, en donde la prueba de anomalía estadística compara los datos recibidos dentro de los datos por omisión de la red en el almacén (110) de datos del sistema, y la información derivada de esta, y los datos de criterios de riesgo almacenados en el almacén (110) de datos del sistema.

4. El sistema de la reivindicación 2, en donde el procesador (120) del sistema está programado o adaptado además para efectuar la etapa caracterizada por actualizar (355) el almacén de datos estadísticos con base en los datos recibidos.

5. El sistema de cualquier reivindicación previa, en donde el primer receptor de la interfaz de la comunicación recibe señales que corresponden al marco transmitido entre estaciones y los puntos (180) de acceso dentro de la red de ordenador inalámbrica y envía los datos que corresponden al marco al procesador (120) del sistema.

6. El sistema de la reivindicación 5, en donde el primer receptor de la interfaz de la comunicación es un receptor inalámbrico.

7. El sistema de la reivindicación 5 o reivindicación 6, en donde las señales recibidas por el primer receptor de la interfaz de comunicación se origina desde un punto (180) de acceso dentro de la red de ordenador inalámbrica, de una estación (170) dentro de la red de ordenador inalámbrica, o desde uno o más sensores (230) ubicados dentro de un área servida por la red de ordenador inalámbrica.

8. El sistema de la reivindicación 7, que comprende además uno o más sensores (230) ubicados dentro de un área servida por la red inalámbrica, en donde cada uno de los uno o más sensores comprende un receptor inalámbrico capaz de recibir marcos transmitidos sobre la red de ordenador inalámbrica y un transmisor (705) capaz de transmitir datos asociados con los marcos recibidos sobre el canal de comunicación a la primera interfaz de comunicación.

9. El sistema de la reivindicación 8, en donde:

(i) Cada sensor (230) comprende además al menos un elemento (725) del procesamiento del procesador (120) del sistema; y

(ii) El al menos un elemento (725) de procesamiento es programado o adaptado para hacer que el transmisor del sensor envíe datos asociados con los marcos recibidos, en respuesta a la recepción o los marcos recibidos por el receptor inalámbrico del sensor.

10. El sistema de la reivindicación 9, en donde cada uno de los transmisores (705) del sensor es un transmisor inalámbrico o en donde cada sensor comprende además un transmisor inalámbrico, y en donde cada al menos un procesador (725) del sensor es además programado o adaptado para efectuar la etapa de disparar una defensa activa de la red de ordenador inalámbrica en respuesta a una alarma generada.

11. El sistema de cualquier reivindicación previa, que comprende además una carcasa de dispositivo que aloja la primera interfaz de comunicación y al menos un elemento de procesamiento del procesador (120) del sistema formando de esta manera un primer dispositivo, y uno o más dispositivos adicionales, en donde cada dispositivo adicional comprende una carcasa, una interfaz de comunicación del dispositivo que permite la comunicación por vía del canal de comunicación y al menos un elemento de procesamiento del procesador (120) del sistema, en donde las señales recibidas por cualquiera de los primeros o de las respectivas interfaces de comunicación de los dispositivos adicionales se originan desde un punto de acceso dentro de la red del ordenador inalámbrica, desde una estación dentro de la red de ordenador inalámbrica, o desde un dispositivo diferente.

12. El sistema de la reivindicación 11, que comprende además uno o más sensores (230) ubicados dentro de un área servida por la red inalámbrica, en donde cada uno de los uno o más sensores (230) comprende un receptor inalámbrico capaz de recibir marcos transmitidos sobre la red de ordenador inalámbrica y un transmisor (705) capaz de transmitir datos asociados con los marcos recibidos sobre el canal de comunicación a la primera interfaz de comunicación, en donde las señales recibidas por cualquiera de los primeros o la interfaz de comunicación respectiva de los dispositivos adicionales puede también originarse desde los uno o más sensores (230).

13. El sistema de una cualquiera de las reivindicaciones previas, en donde cada alarma generada comprende un tipo o una severidad.

14. El sistema de la reivindicación 13, en donde el procesador (120) del sistema que dispara una defensa activa comprende la etapa de seleccionar una defensa activa con base en el tipo o la severidad de la alarma generada a la cual responde la etapa de disparo.

15. El sistema de la reivindicación 13 o 14, en donde la defensa activa disparada también incluye:

(i) Interferir las transmisiones inalámbricas; o

(ii) Bloquear la red de ordenador inalámbrica.

16. El sistema de cualquiera de las reivindicaciones previas, en donde el procesador (120) del sistema está además programado o adaptado para efectuar las etapas que comprenden recibir (410) información de configuración y almacenar (470) la información de configuración recibida en el almacén (110) de datos del sistema.

17. El sistema de la reivindicación 16, en donde la información de configuración es recibida por el procesador (120) del sistema desde un archivo de configuración, de una interfaz de entrada de datos interactiva o desde una línea de comando.

18. El sistema de la reivindicación 16 o 17, en donde la información de configuración recibida comprende datos por omisión de la red y criterios de riesgo.

19. El sistema de cualquier reivindicación previa, en donde el almacén (110) de datos del sistema comprende un almacén de datos de estación y en donde el procesador (120) del sistema está además programado o adaptado

para efectuar la etapa que comprende actualizar los datos de la estación almacenados con base en los datos recibidos.

20. El sistema de cualquiera de las reivindicaciones 1-18, en donde el almacén (110) de datos del sistema comprende un almacén de datos del punto de acceso y en donde el procesador (120) del sistema está además programado o adaptado para efectuar la etapa que comprende actualizar el almacén de datos de punto de acceso con base en los datos recibidos.

21. El sistema de cualquiera de las reivindicaciones previas, en donde el procesador (120) del sistema está además programado o adaptado para efectuar la etapa que comprende notificar (444) un administrador de la alarma generada si se detectó la violación.

22. El sistema de cualquiera de las reivindicaciones previas, en donde la pluralidad de pruebas aplicada por el procesador (120) del sistema comprende además al menos una prueba seleccionada del grupo que consiste de prueba de firma, y prueba de protocolo.

23. El sistema de cualquiera de las reivindicaciones previas, en donde el procesador (120) del sistema está además programado adaptado para efectuar la etapa que comprende mapear la identidad de la estación.

24. El sistema de cualquiera de las reivindicaciones previas, en donde el procesador (120) del sistema está además programado o adaptado para efectuar la etapa que comprende mapear la localización de la estación.

FIG. 1 (TÉCNICA ANTERIOR)

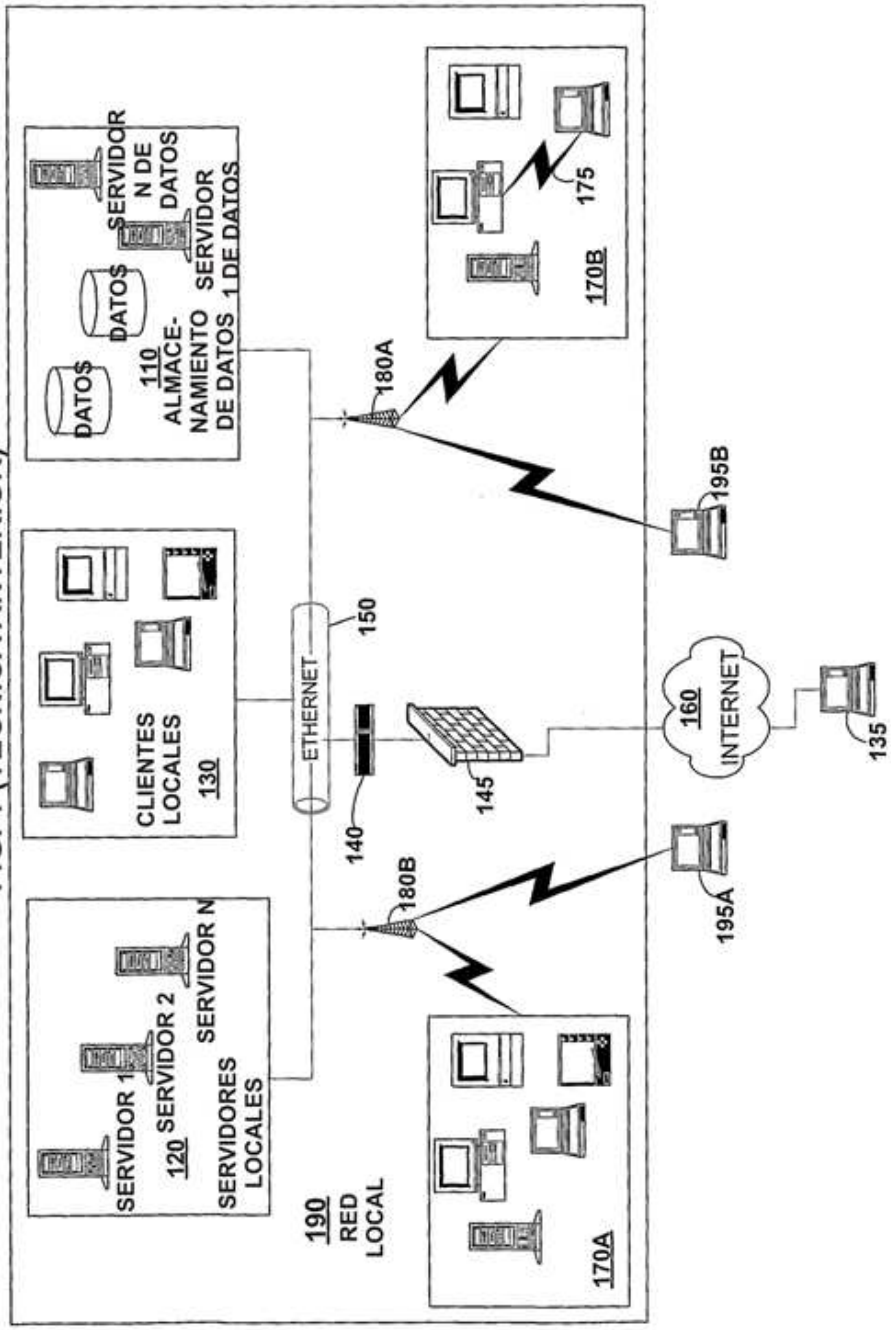
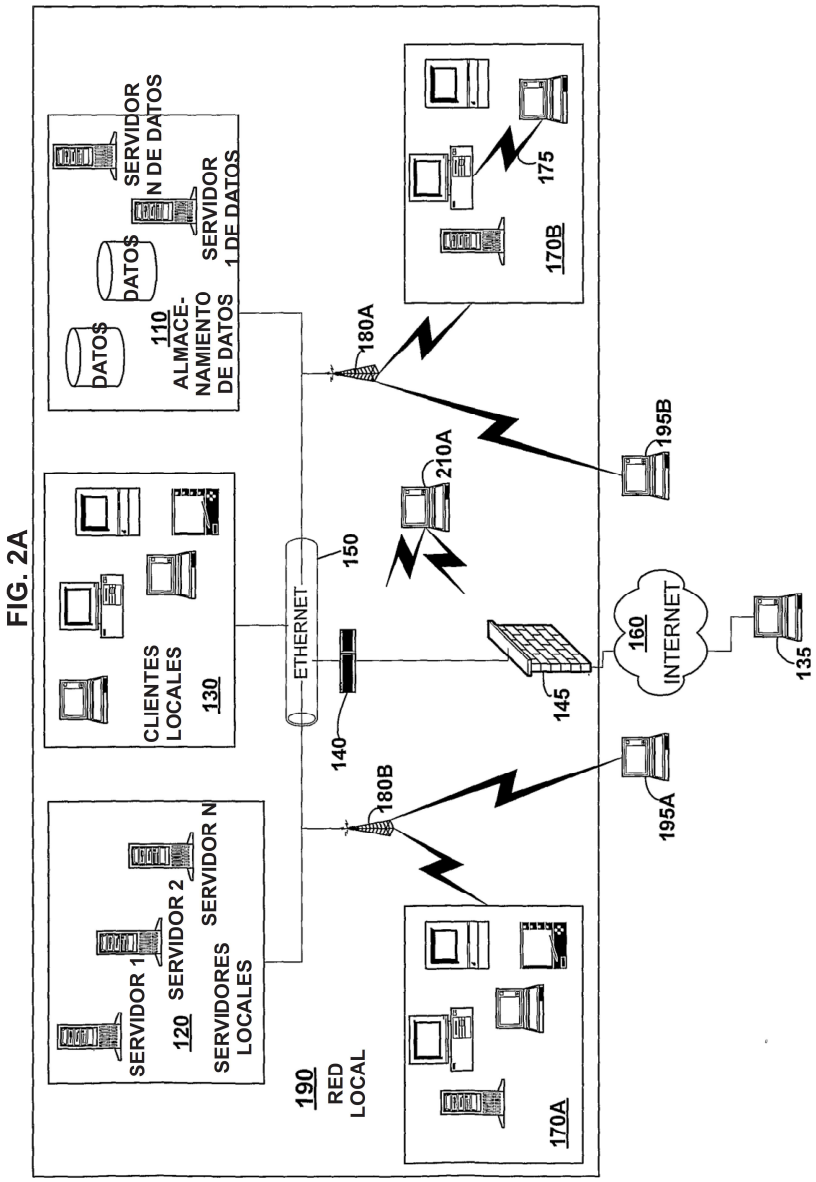


FIG. 2A


SERVIDOR N DE DATOS
SERVIDOR 1 DE DATOS
DATOS
DATOS
110 ALMACE-NAMIENTO DE DATOS
180A
170B
175
195B
210A
CLIENTES LOCALES 130
150
ETHERNET
160 INTERNET
135
145
140
180B
195A
SERVIDOR 1
SERVIDOR 2
SERVIDOR N
120 SERVIDORES LOCALES
190 RED LOCAL
170A

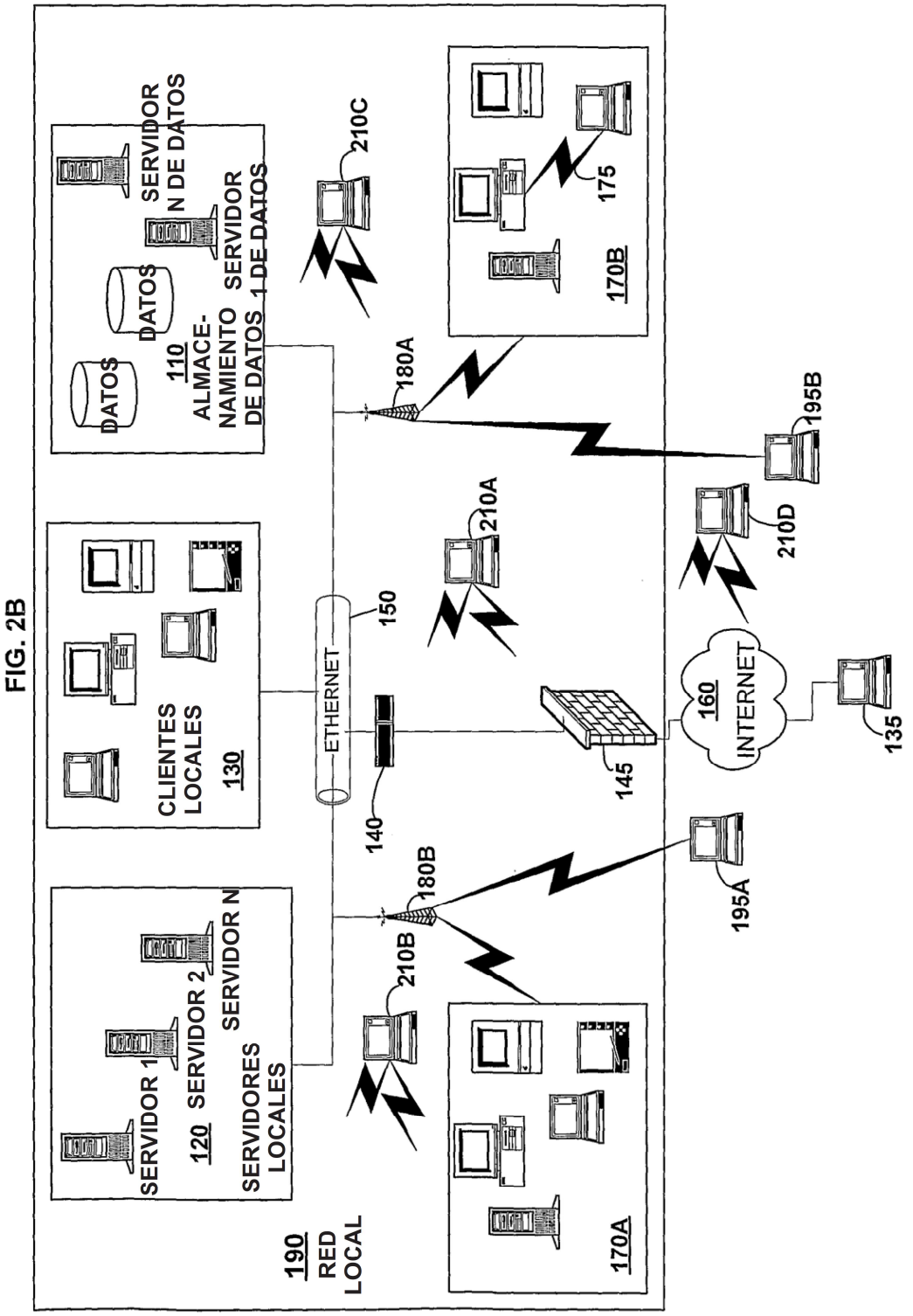

190
RED
LOCAL
SERVIDORES
LOCALES
SERVIDOR 1
120 SERVIDOR 2
SERVIDOR N
CLIENTES
LOCALES
130
110
ALMACE-
NAMIENTO
DE DATOS
DATOS
DATOS
SERVIDOR
1 DE DATOS
SERVIDOR
N DE DATOS
ETHERNET
150
140
145
160
INTERNET
135
170A
170B
175
180A
180B
210A
210B
210C
210D
195A
195B

FIG. 2B

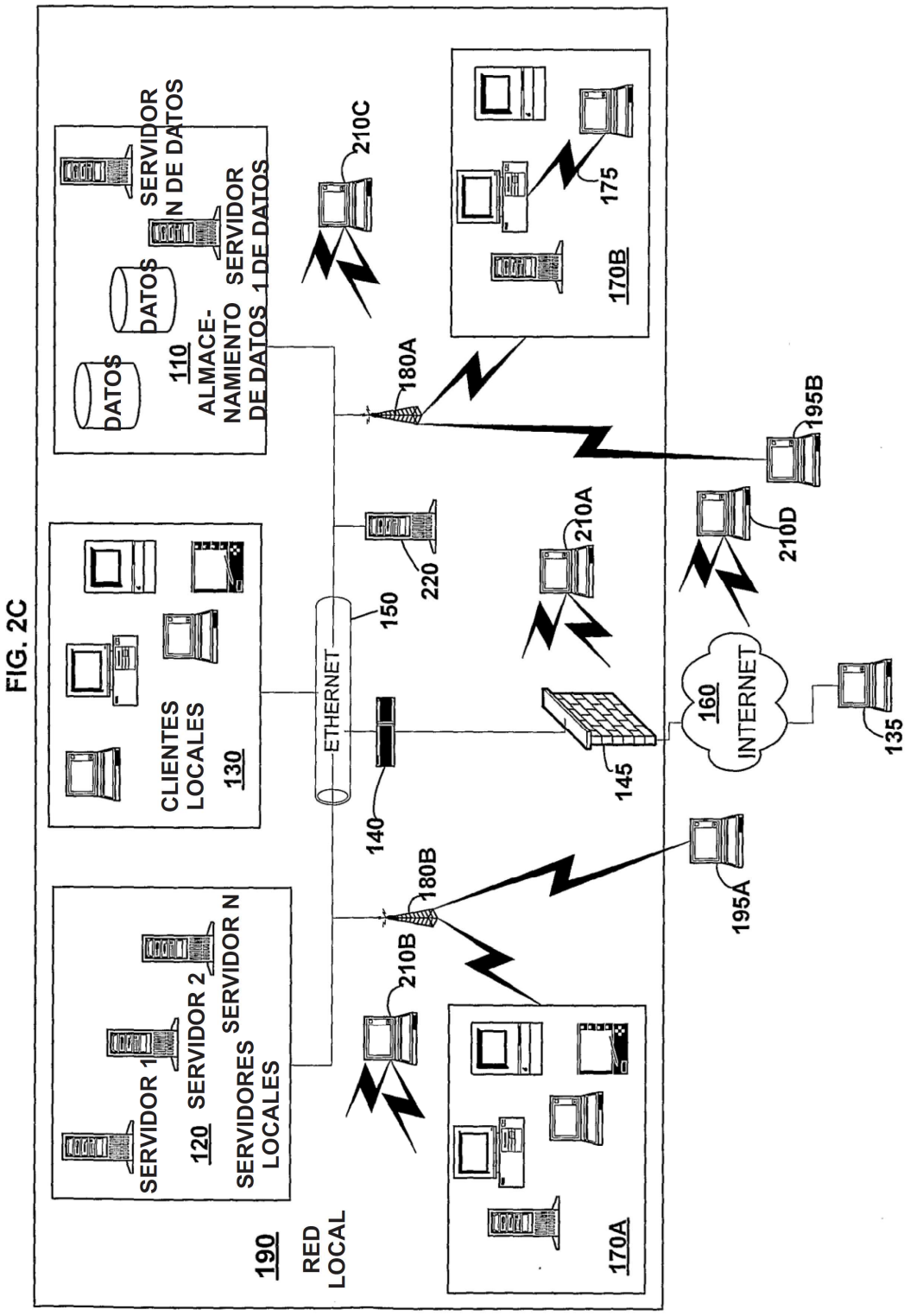

190
RED LOCAL
SERVIDOR 1
120 SERVIDOR 2
SERVIDOR N
SERVIDORES LOCALES
CLIENTES LOCALES
130
110 ALMACE-NAMIENTO DE DATOS
SERVIDOR 1 DE DATOS
SERVIDOR N DE DATOS
DATOS
DATOS
DATOS
ETHERNET
150
140
220
145
160 INTERNET
135
180A
180B
210A
210B
210C
210D
170A
170B
175
195A
195B

FIG. 2C

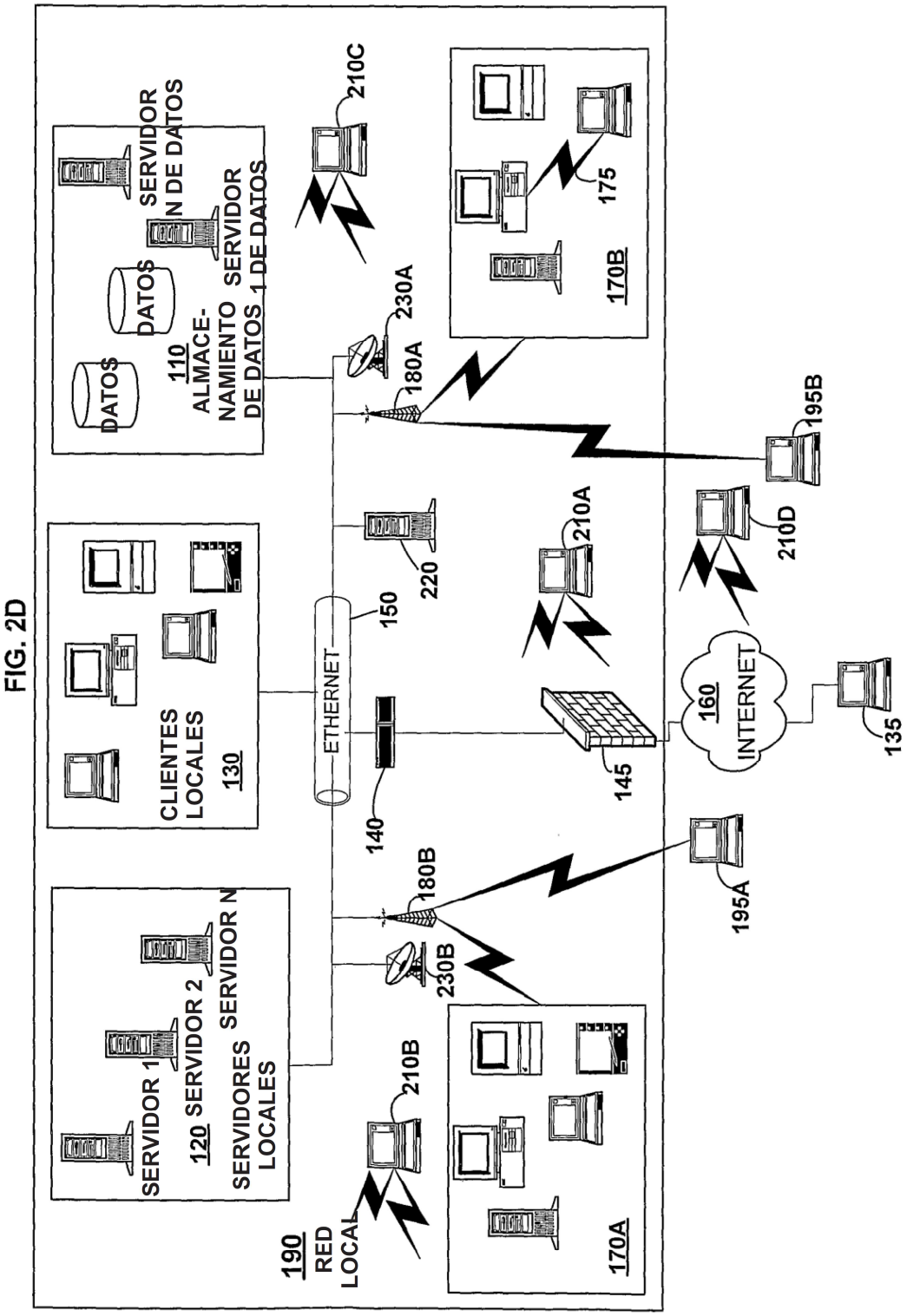

190
RED LOCAL
SERVIDORES LOCALES
SERVIDOR 1
120 SERVIDOR 2
SERVIDOR N
CLIENTES LOCALES
130
110 ALMACE-NAMIENTO DE DATOS
SERVIDOR 1 DE DATOS
SERVIDOR N DE DATOS
DATOS
DATOS
DATOS
ETHERNET
150
140
145
160 INTERNET
135
170A
170B
175
180A
180B
195A
195B
210A
210B
210C
210D
220
230A
230B

FIG. 2D

FIG. 2E

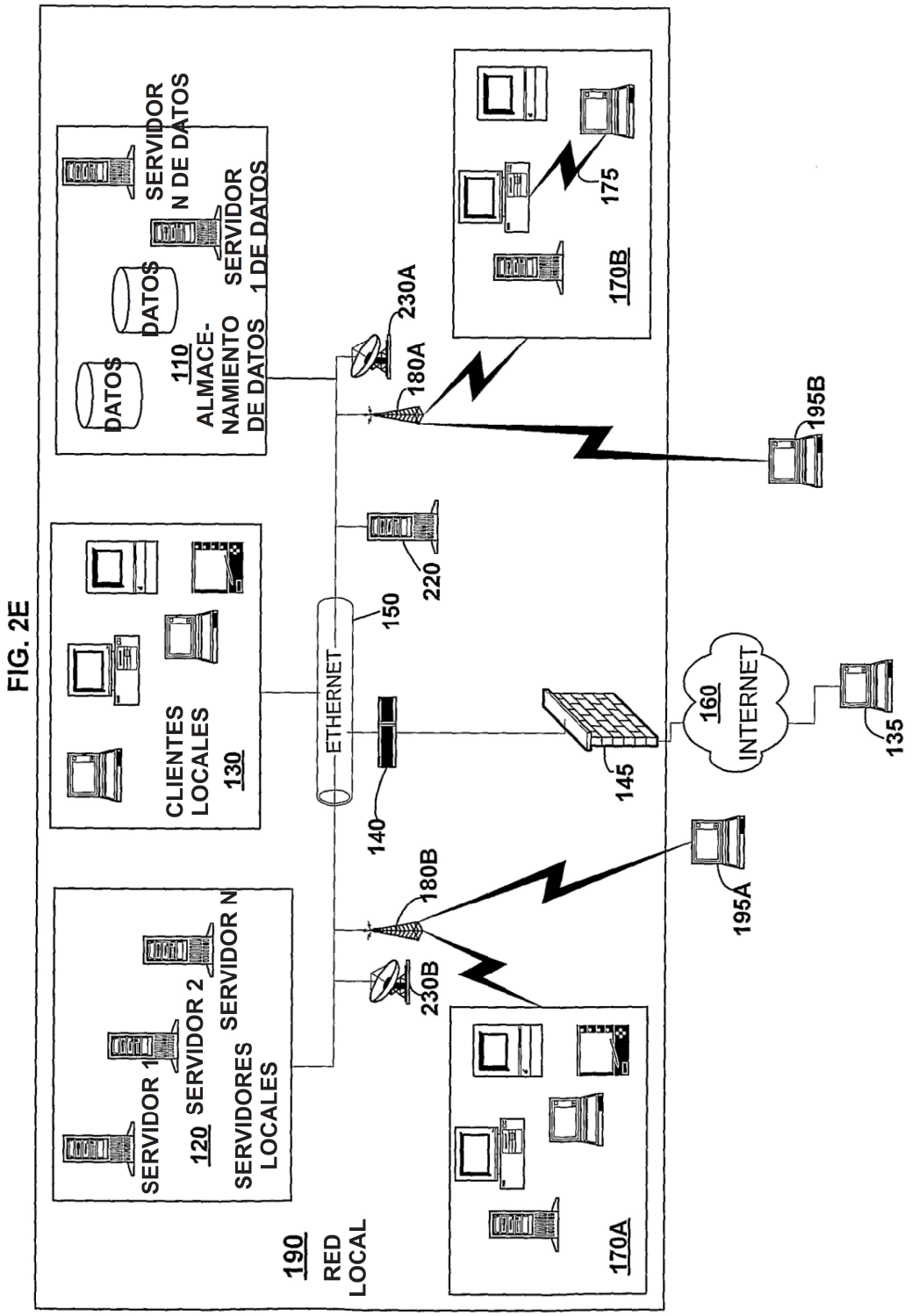

190
RED LOCAL
SERVIDORES LOCALES
120
SERVIDOR 1
SERVIDOR 2
SERVIDOR N
CLIENTES LOCALES
130
ALMACE-NAMIENTO DE DATOS
110
DATOS
DATOS
SERVIDOR 1 DE DATOS
SERVIDOR N DE DATOS
ETHERNET
150
140
145
160
INTERNET
135
170A
170B
175
180A
180B
195A
195B
220
230A
230B

FIG. 3

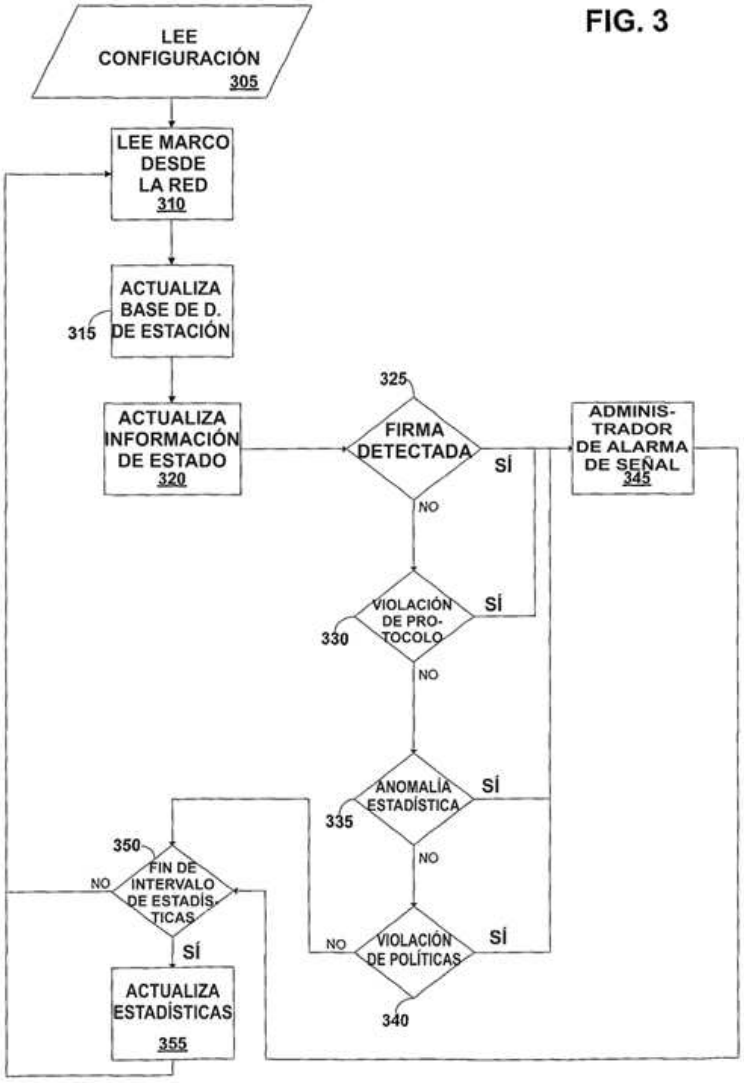

LEE CONFIGURACIÓN 305
LEE MARCO DESDE LA RED 310
ACTUALIZA BASE DE D. DE ESTACIÓN 315
ACTUALIZA INFORMACIÓN DE ESTADO 320
325
FIRMA DETECTADA
SÍ
NO
ADMINIS-TRADOR DE ALARMA DE SEÑAL 345
VIOLACIÓN DE PRO-TOCOLO 330
SÍ
NO
ANOMALÍA ESTADÍSTICA 335
SÍ
NO
VIOLACIÓN DE POLÍTICAS
SÍ
NO
340
350
FIN DE INTERVALO DE ESTADÍS-TICAS
NO
SÍ
ACTUALIZA ESTADÍSTICAS 355

FIG. 4

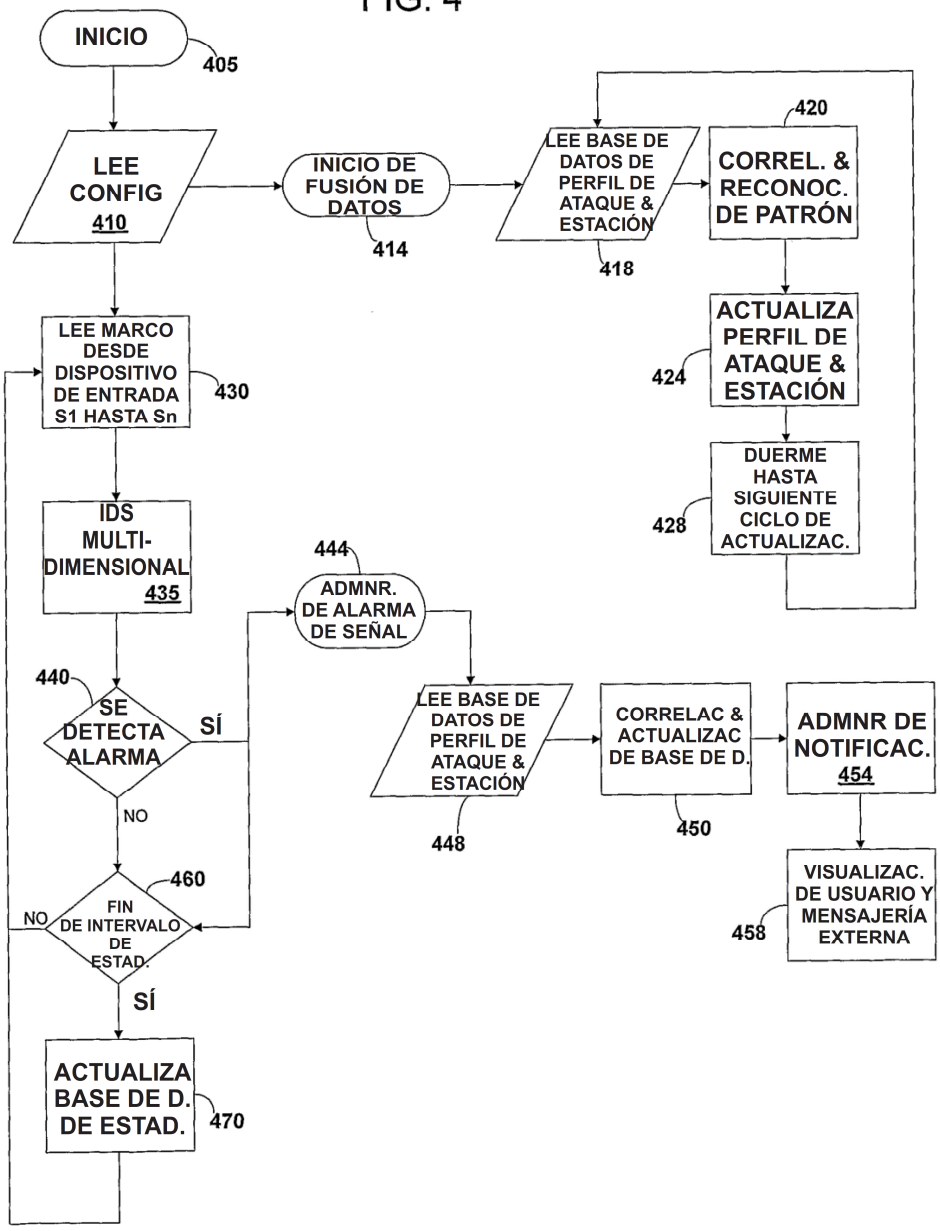

INICIO
405
LEE CONFIG 410
INICIO DE FUSIÓN DE DATOS
414
LEE BASE DE DATOS DE PERFIL DE ATAQUE & ESTACIÓN
418
420
CORREL. & RECONOC. DE PATRÓN
ACTUALIZA PERFIL DE ATAQUE & ESTACIÓN
424
DUERME HASTA SIGUIENTE CICLO DE ACTUALIZAC.
428
LEE MARCO DESDE DISPOSITIVO DE ENTRADA S1 HASTA Sn
430
IDS MULTI-DIMENSIONAL 435
444
ADMNR. DE ALARMA DE SEÑAL
440
SE DETECTA ALARMA
SÍ
NO
LEE BASE DE DATOS DE PERFIL DE ATAQUE & ESTACIÓN
448
CORRELAC & ACTUALIZAC DE BASE DE D.
450
ADMNR DE NOTIFICAC. 454
VISUALIZAC. DE USUARIO Y MENSAJERÍA EXTERNA
458
460
FIN DE INTERVALO DE ESTAD.
NO
SÍ
ACTUALIZA BASE DE D. DE ESTAD.
470

FIG. 5

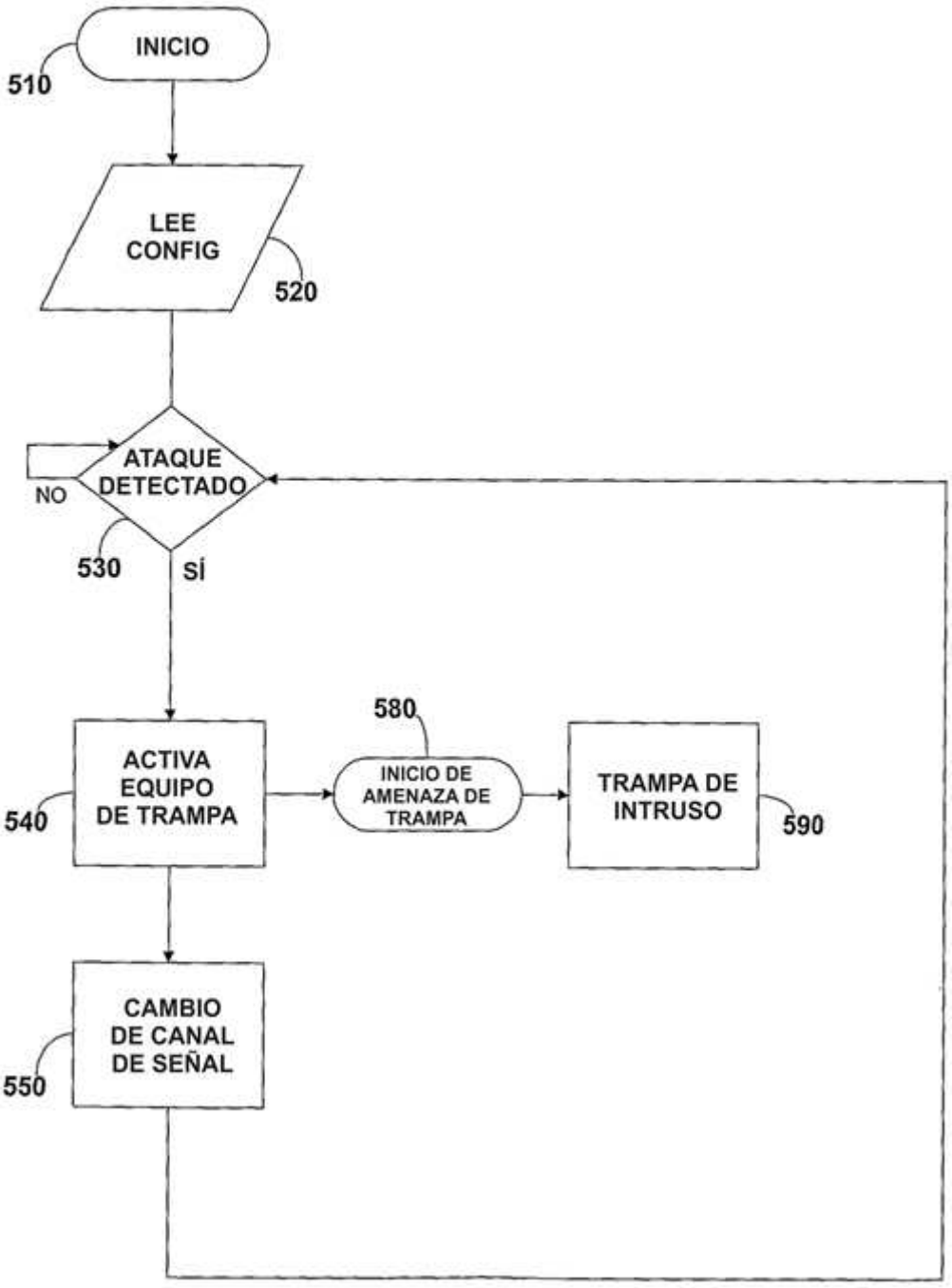

INICIO
510
LEE CONFIG
520
ATAQUE DETECTADO
NO
530
SÍ
580
ACTIVA EQUIPO DE TRAMPA
540
INICIO DE AMENAZA DE TRAMPA
TRAMPA DE INTRUSO
590
CAMBIO DE CANAL DE SEÑAL
550

FIG. 6A


ARP DETECTADO
605
SÍ
ACTUALIZA BASE DE D. DE BÚSQUEDA DE NOMBRE INTERNO
610

FIG. 6B

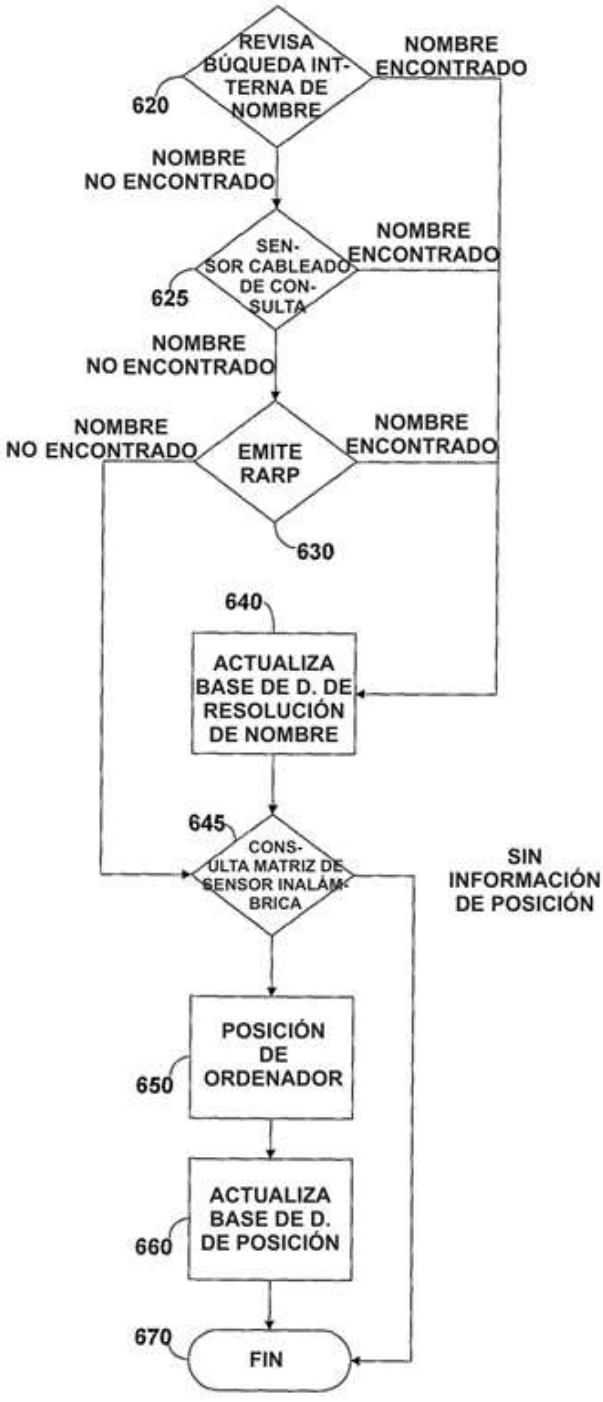

REVISA BÚQUEDA INTERNA DE NOMBRE
620
NOMBRE ENCONTRADO
NOMBRE NO ENCONTRADO
SENSOR CABLEADO DE CONSULTA
625
NOMBRE ENCONTRADO
NOMBRE NO ENCONTRADO
EMITE RARP
630
NOMBRE NO ENCONTRADO
NOMBRE ENCONTRADO
640
ACTUALIZA BASE DE D. DE RESOLUCIÓN DE NOMBRE
645
CONSULTA MATRIZ DE SENSOR INALÁMBRICA
SIN INFORMACIÓN DE POSICIÓN
POSICIÓN DE ORDENADOR
650
ACTUALIZA BASE DE D. DE POSICIÓN
660
670
FIN

FIG. 7A

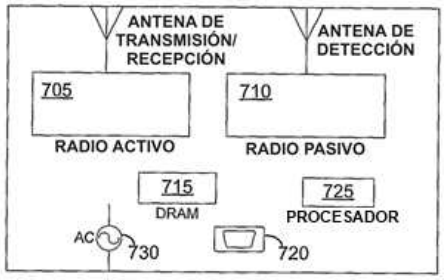


FIG. 7B

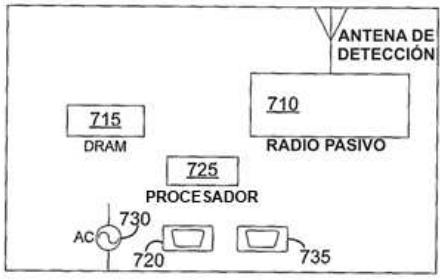


FIG. 7C

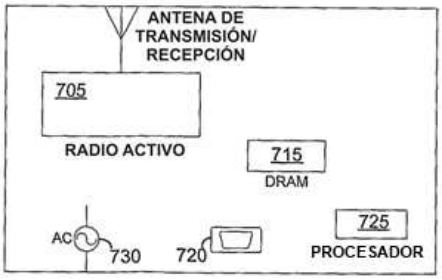


FIG 8A

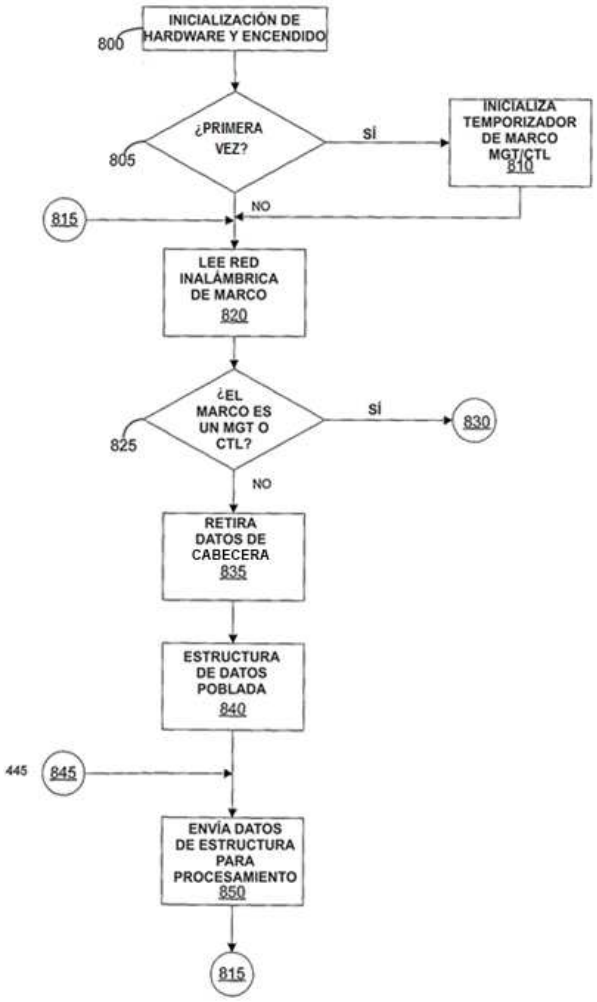

INICIALIZACIÓN DE HARDWARE Y ENCENDIDO
800
¿PRIMERA VEZ?
805
SÍ
INICIALIZA TEMPORIZADOR DE MARCO MGT/CTL
810
NO
815
LEE RED INALÁMBRICA DE MARCO
820
¿EL MARCO ES UN MGT O CTL?
825
SÍ
830
NO
RETIRA DATOS DE CABECERA
835
ESTRUCTURA DE DATOS POBLADA
840
445
845
ENVÍA DATOS DE ESTRUCTURA PARA PROCESAMIENTO
850
815

FIG 8B

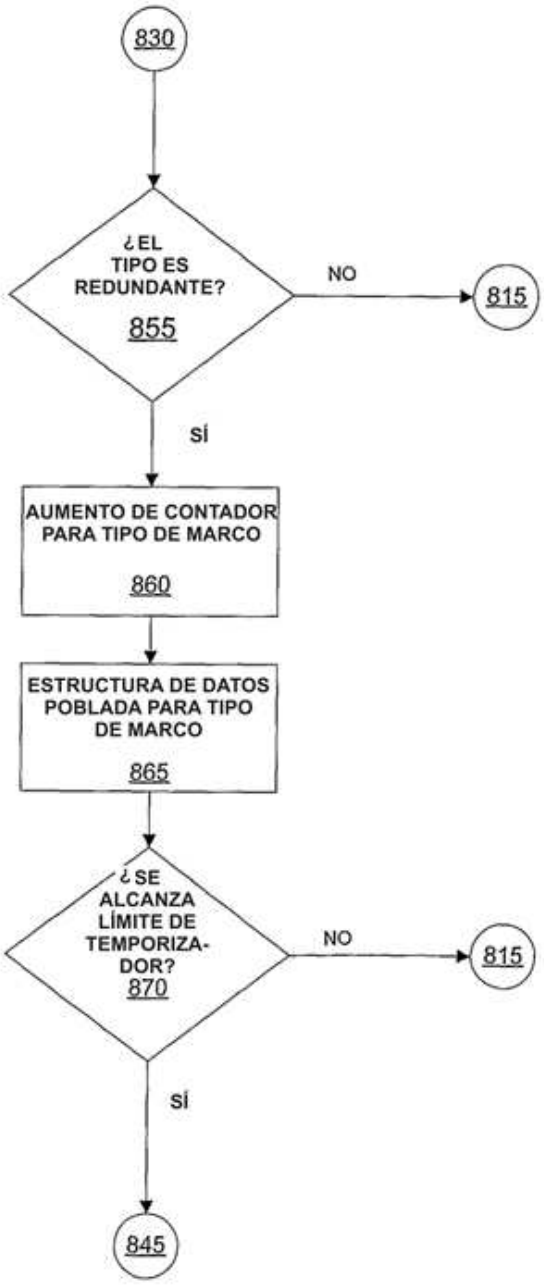

830
¿EL TIPO ES REDUNDANTE?
855
NO
815
SÍ
AUMENTO DE CONTADOR PARA TIPO DE MARCO
860
ESTRUCTURA DE DATOS POBLADA PARA TIPO DE MARCO
865
¿SE ALCANZA LÍMITE DE TEMPORIZA-DOR?
870
NO
815
SÍ
845

FIG. 9

Alerta y Seguimiento de Topología de Red Dinámica

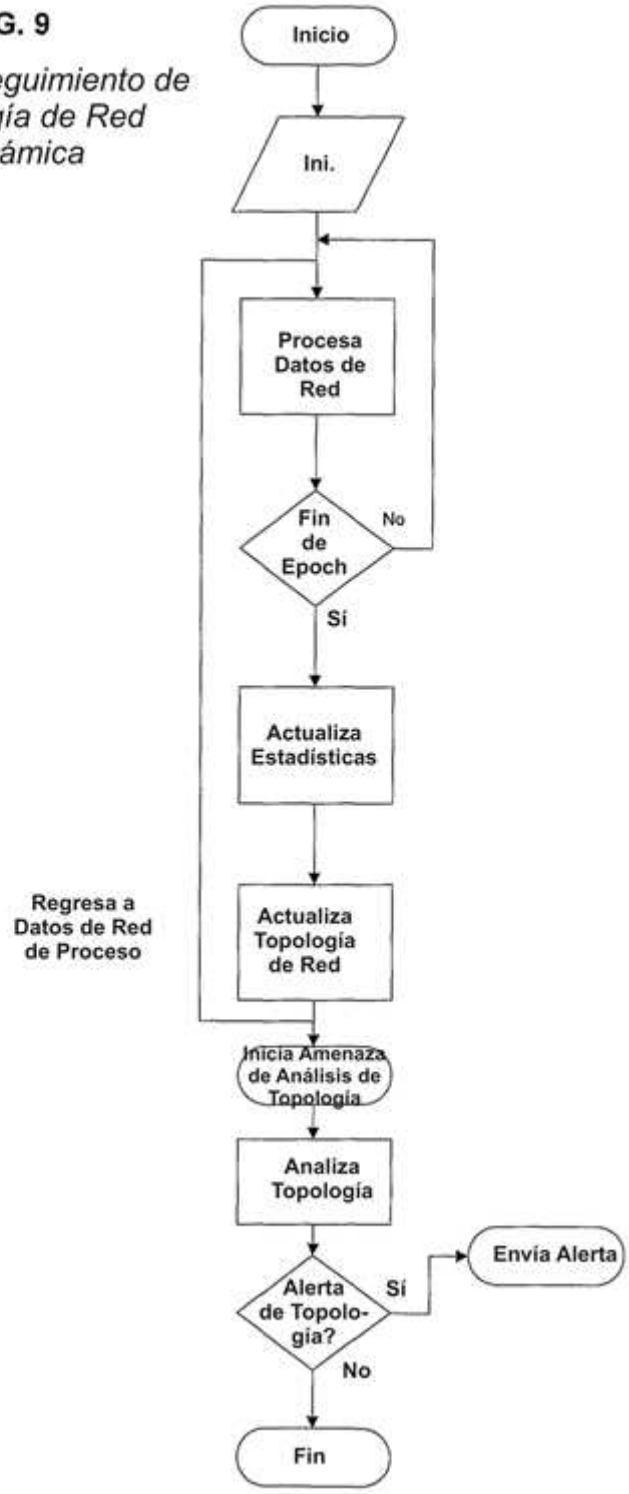


FIG. 10

Aplicación de Política Automatizada

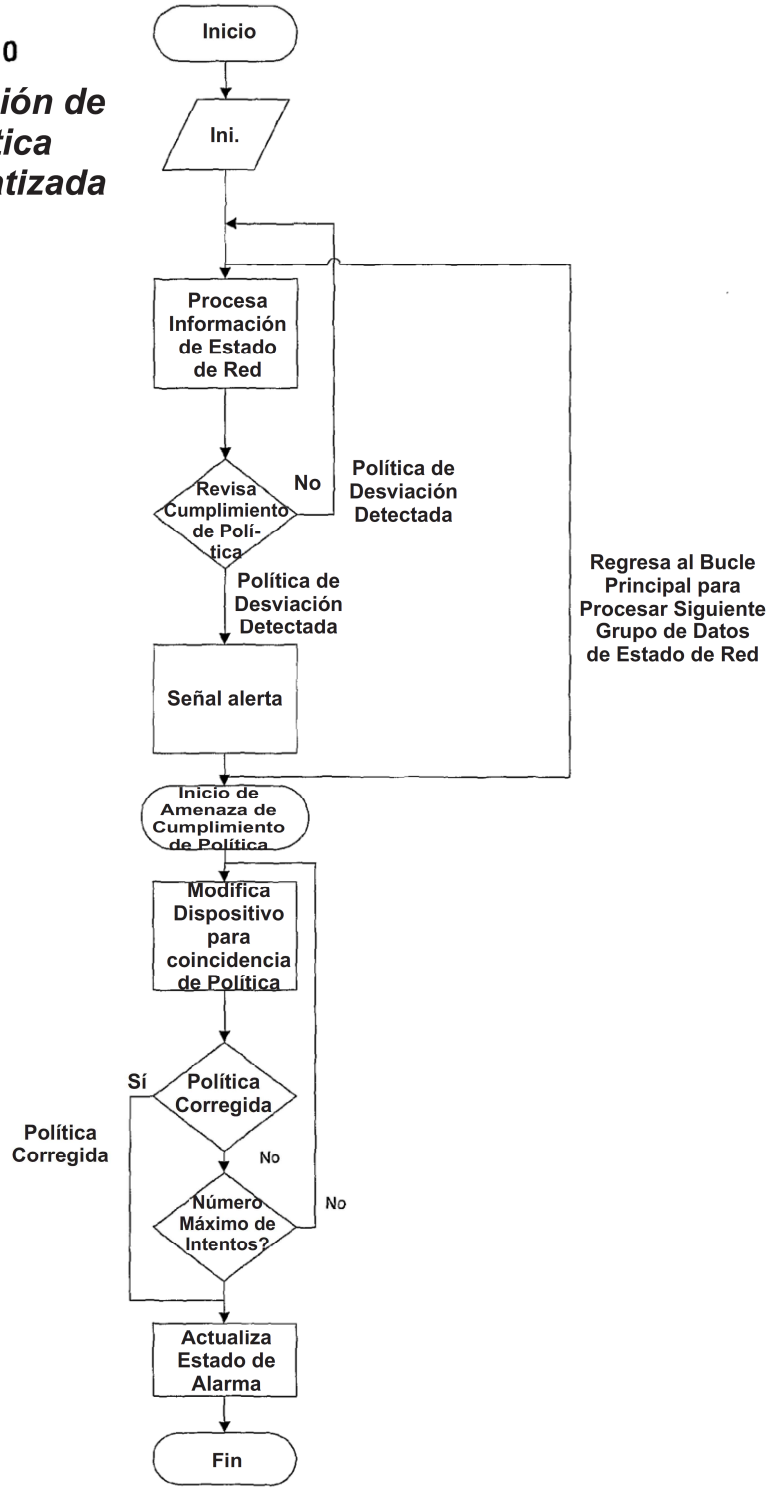


FIG. 11

Exploración Adaptativa

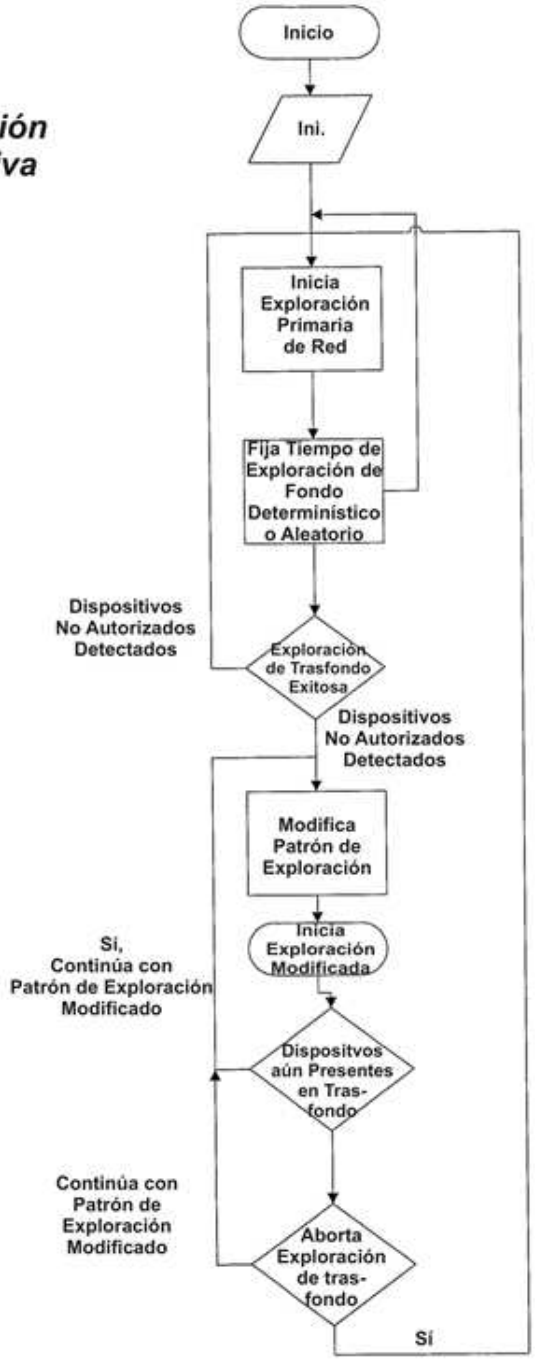


FIG. 12

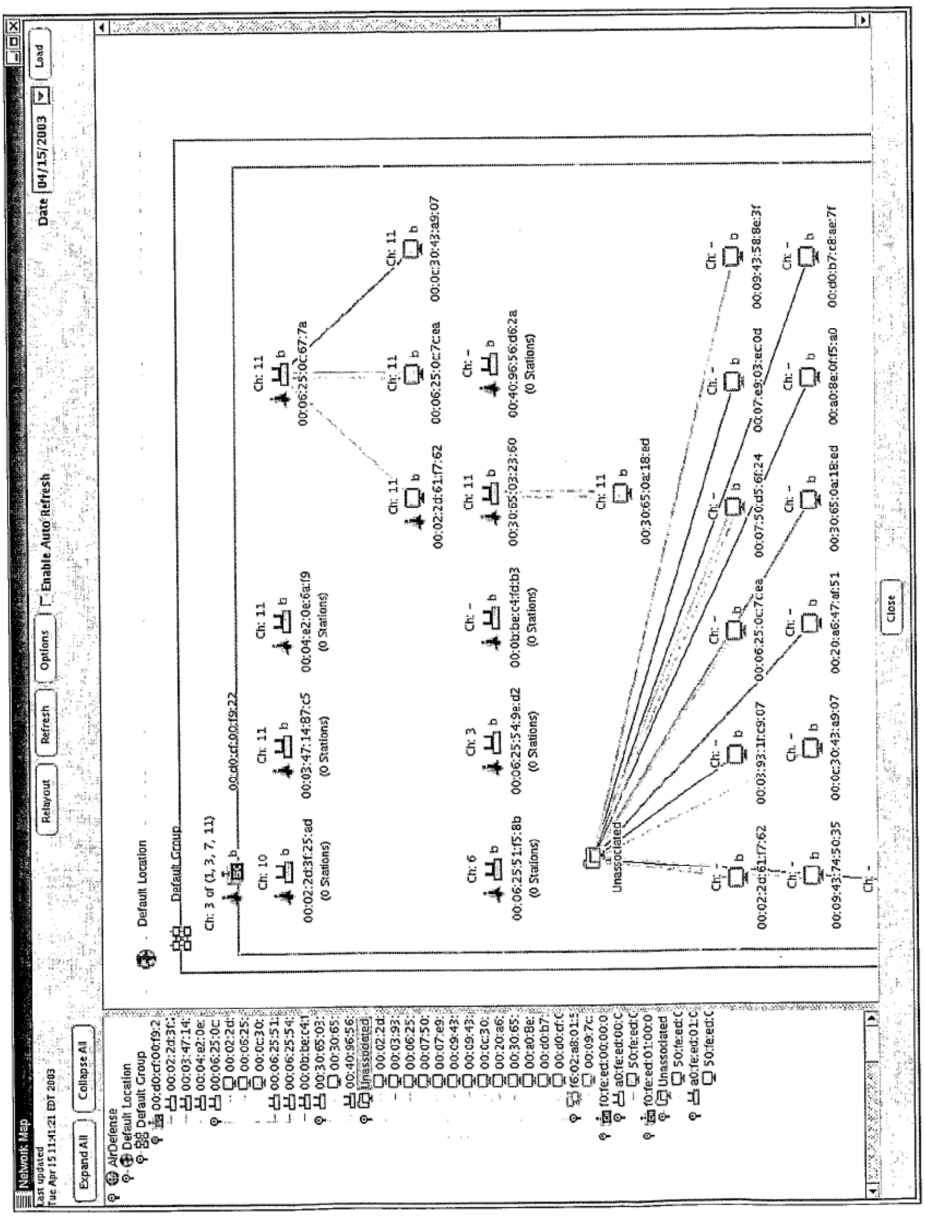

Network Map
Last updated
Tue Apr 15 11:41:21 EDT 2003
Expand All
Collapse All
Relayout
Refresh
Options
Enable Auto Refresh
Date 04/15/2003
Load
Default Location
Default Group
Ch: 3 of (1, 3, 7, 11)
00:d0:cf:00:f9:22
Ch: 10
00:02:2d:3f:25:ad
(0 Stations)
Ch: 11
00:03:47:14:87:c5
(0 Stations)
00:04:a2:0e:6a:f9
(0 Stations)
00:06:25:0c:67:7a
00:02:2d:61:f7:62
00:06:25:0c:7c:ea
00:0c:30:43:a9:07
Ch: 6
00:06:25:51:f5:8b
(0 Stations)
Ch: 3
00:06:25:54:9a:d2
(0 Stations)
00:0b:be:c4:fd:b3
(0 Stations)
00:30:65:03:23:60
00:40:96:56:d6:2a
(0 Stations)
Unassociated
00:30:65:0a:18:ed
00:02:2d:61:f7:62
00:03:93:1f:c9:07
00:06:25:0c:7c:ea
00:07:50:d5:6f:24
00:07:e8:03:ac:0d
00:09:43:74:50:35
00:0c:30:43:a9:07
00:20:a6:47:af:51
00:30:65:0a:18:ed
00:a0:8e:0f:f5:a0
00:d0:b7:c8:ae:7f
Close

FIG. 13A

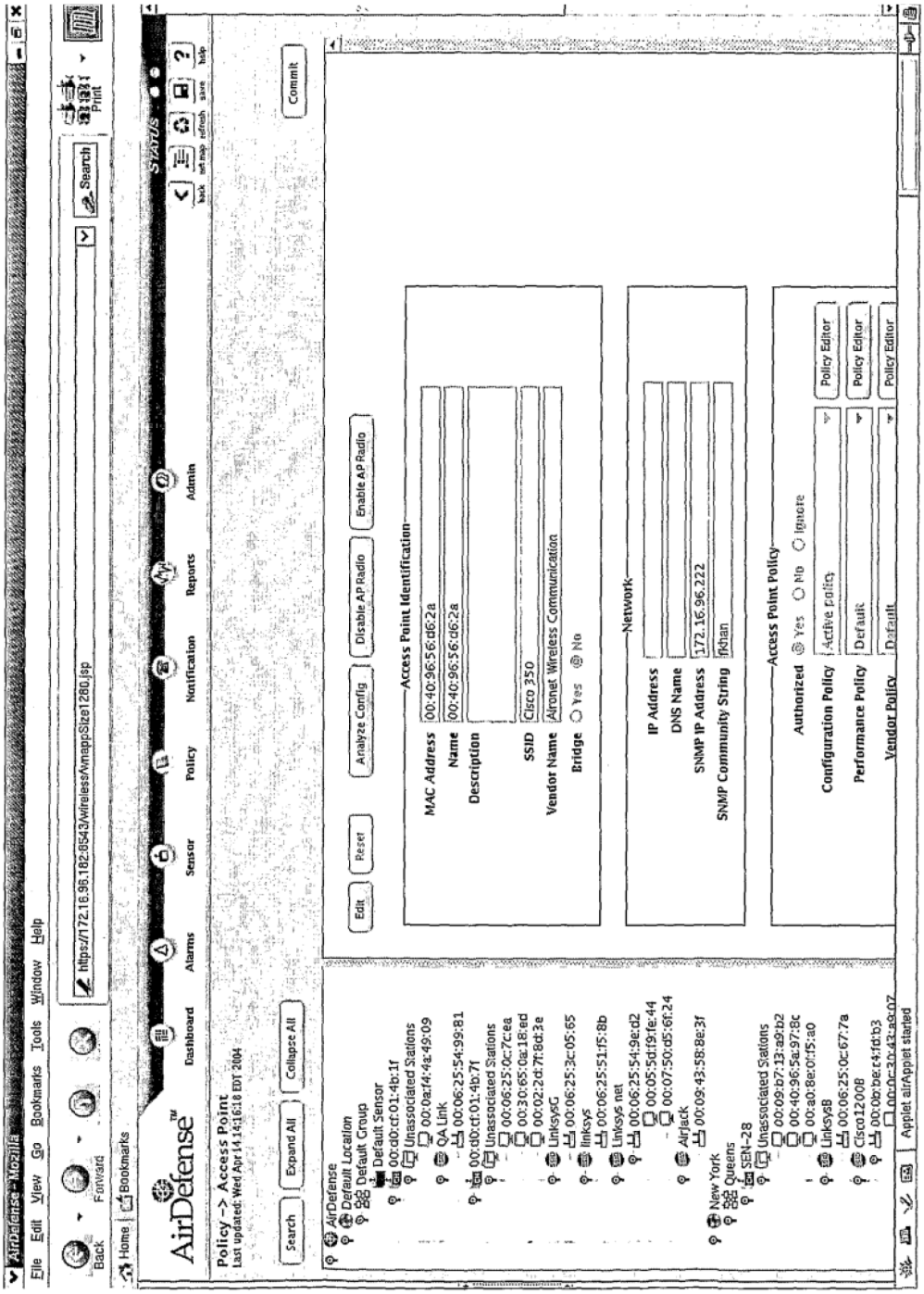

AirDefense Mozilla
File Edit View Go Bookmarks Tools Window Help
Back Forward
https://172.16.96.182:8543/wireless/AmappSize1280.jsp
Search
Print
Home Bookmarks
AirDefense
Dashboard Alarms Sensor Policy Notification Reports Admin
STATUS
Policy --> Access Point
Last updated: Wed Apr 14 14:16:16 EDT 2004
Search Expand All Collapse All
Commit
Edit Reset Analyze Config Disable AP Radio Enable AP Radio
Access Point Identification
MAC Address 00:40:96:56:d6:2a
Name 00:40:96:56:d6:2a
Description
SSID Cisco 350
Vendor Name Aironet Wireless Communication
Bridge Yes No
Network
IP Address
DNS Name
SNMP IP Address 172.16.96.222
SNMP Community String ikhan
Access Point Policy
Authorized Yes No Ignore
Configuration Policy Active policy Policy Editor
Performance Policy Default Policy Editor
Vendor Policy Default Policy Editor
AirDefense
Default Location
Default Group
Default Sensor
00:d0:cf:01:4b:1f
Unassociated Stations
00:0a:f4:4a:49:09
A Link
00:06:25:54:99:81
00:d0:cf:01:4b:7f
Unassociated Stations
00:06:25:0c:7c:ea
00:30:65:0a:18:ed
00:02:2d:7f:8d:3e
LinksysG
00:06:25:3c:05:65
linksys
00:06:25:51:f5:8b
Linksys net
00:06:25:54:9e:d2
00:05:5d:f9:fe:44
00:07:50:d5:6f:24
Airjack
00:09:43:58:8e:3f
New York
Queens
SEN-28
Unassociated Stations
00:09:b7:13:a9:b2
00:40:96:5a:97:8c
00:a0:8e:0f:f5:a0
Linksy8
00:06:25:0c:67:7a
Cisco1200B
00:0b:be:c4:fd:b3
00:0c:30:43:a6:07
Applet airApplet started

FIG. 13B

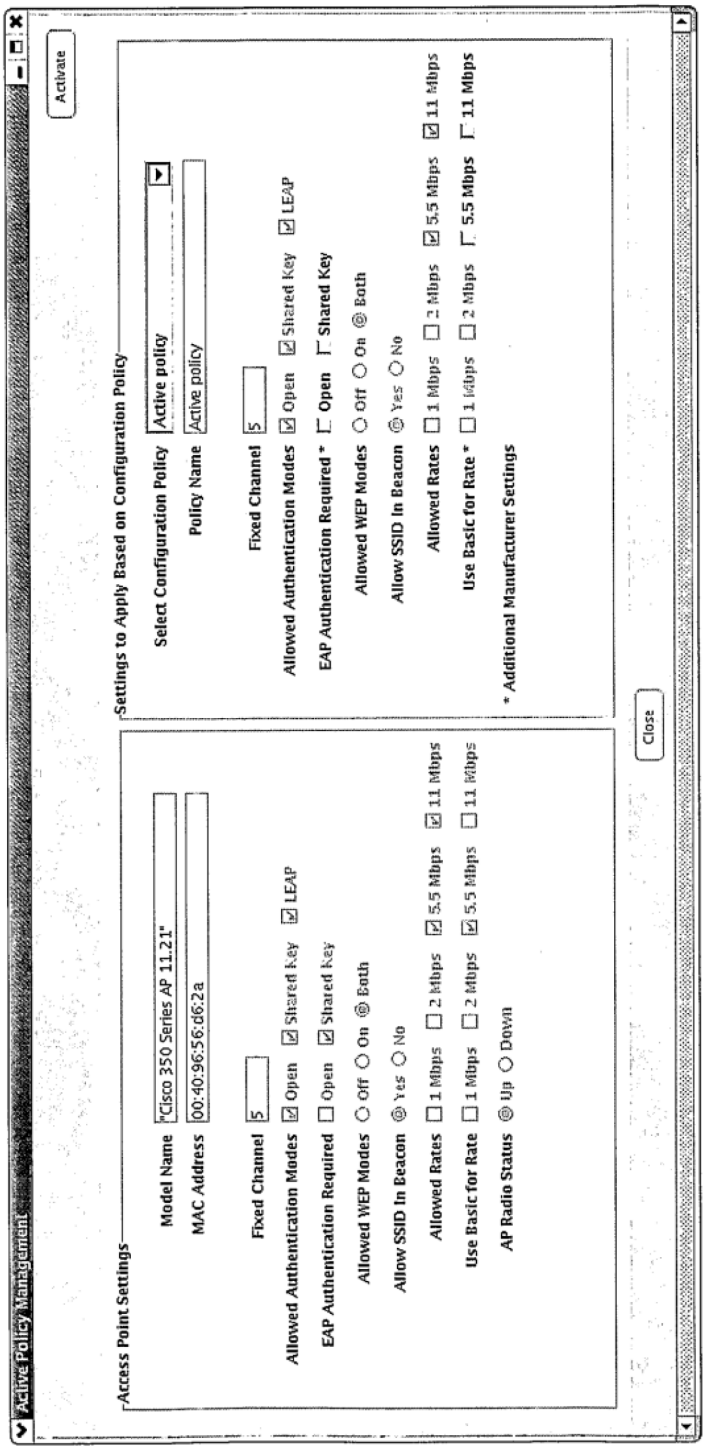
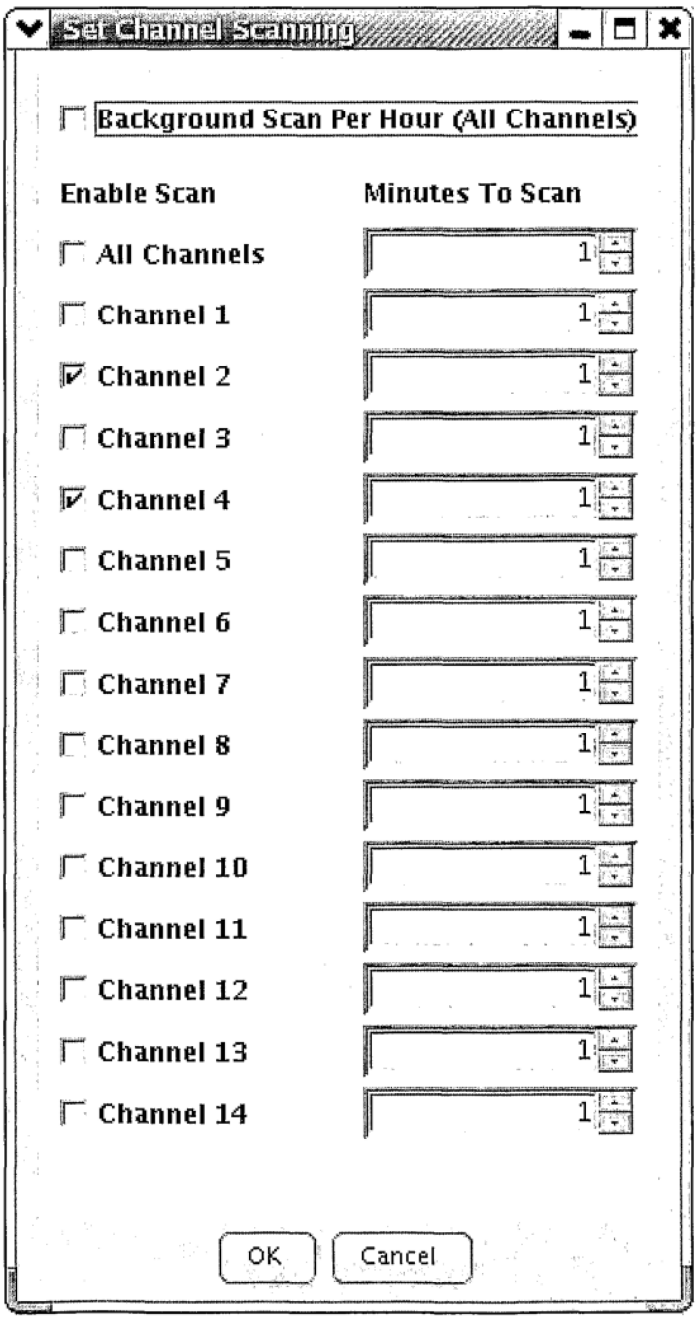

Active Policy Management
Activate
Access Point Settings
Model Name "Cisco 350 Series AP 11.21"
MAC Address 00:40:96:56:d6:2a
Fixed Channel 5
Allowed Authentication Modes Open Shared Key LEAP
EAP Authentication Required Open Shared Key
Allowed WEP Modes Off On Both
Allow SSID In Beacon Yes No
Allowed Rates 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps
Use Basic for Rate 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps
AP Radio Status Up Down
Close
Settings to Apply Based on Configuration Policy
Select Configuration Policy Active policy
Policy Name Active policy
Fixed Channel 5
Allowed Authentication Modes Open Shared Key LEAP
EAP Authentication Required * Open Shared Key
Allowed WEP Modes Off On Both
Allow SSID In Beacon Yes No
Allowed Rates 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps
Use Basic for Rate * 1 Mbps 2 Mbps 5.5 Mbps 11 Mbps
* Additional Manufacturer Settings

FIG. 14


Set Channel Scanning
Background Scan Per Hour (All Channels)
Enable Scan
Minutes To Scan
All Channels
Channel 1
Channel 2
Channel 3
Channel 4
Channel 5
Channel 6
Channel 7
Channel 8
Channel 9
Channel 10
Channel 11
Channel 12
Channel 13
Channel 14
1
OK
Cancel