



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 279 479**

51 Int. Cl.:
H04L 12/24 (2006.01)
H04L 12/26 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Número de solicitud europea: **05100630 .2**
86 Fecha de presentación : **31.01.2005**
87 Número de publicación de la solicitud: **1560366**
87 Fecha de publicación de la solicitud: **03.08.2005**

54 Título: **Detección de fallo y diagnóstico.**

30 Prioridad: **30.01.2004 US 540738**
30.06.2004 US 881695

45 Fecha de publicación de la mención BOPI:
16.08.2007

45 Fecha de la publicación del folleto de la patente:
16.08.2007

73 Titular/es: **MICROSOFT CORPORATION**
One Microsoft Way
Redmond, Washington 98052-6399, US

72 Inventor/es: **Zhou, Lidong;**
Qiu, Lili;
Bahl, Paramvir y
Rao, Ananth Rajagopala

74 Agente: **Carpintero López, Francisco**

ES 2 279 479 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Detección de fallo y diagnóstico.

5 **Campo técnico**

La presente invención se refiere en general al campo de las redes alámbricas e inalámbricas, y más concretamente se refiere a una estructura de depuración de una red para la detección y diagnóstico de fallos en una red.

10 **Antecedentes**

La gestión de una red, aunque es un ingrediente clave en un despliegue satisfactorio de una red inalámbrica multirreflejo, ha recibido una atención limitada tanto por parte de la industria como de los colectivos dedicados a la investigación. La depuración de una red es un aspecto de la gestión de una red que responde del mantenimiento de la “salud” de la red y asegura un funcionamiento continuado y sin obstáculos. La depuración de una red ya sea alámbrica o inalámbrica, se complica por los obstáculos ocasionados por las interacciones entre diferentes entidades de red, entre diferentes fallos, etc.

La depuración de una red inalámbrica multirreflejo ltiple se complica también por una diversidad de factores adicionales. Por ejemplo, las típicas redes inalámbricas multirreflejo son en general propensas a enlazar errores ocasionados por las fluctuaciones en la propagación de la señal. Las fluctuaciones en la propagación de la señal pueden ser provocadas por una diversidad de factores, como por ejemplo condiciones fluctuantes del entorno. Estas fluctuaciones producen una topología de red dinámica e impredecible. La movilidad de los nodos agrava más aún estos factores, ya que los nodos pueden estar situados en una diversidad de emplazamientos mientras están conectados a la red, incrementado con ello la naturaleza dinámica e impredecible de la red. Adicionalmente, la capacidad de las redes inalámbricas de multirreflejo está en general limitada debido a la escasez de recursos (por ejemplo, anchura de banda, potencia de batería, etc.), la cual limita la cantidad de sobregasto del tráfico de gestión que la red puede tolerar. Así mismo, una red inalámbrica puede ser vulnerable a ataques de enlaces procedentes de partes malintencionadas. Los agresores, por ejemplo, pueden inyectar información falsa para perturbar o interferir con el esfuerzo de gestión de la red.

Las técnicas teóricas y heurísticas tradicionales que se utilizaron tradicionalmente para llevar a cabo la depuración de una red típicamente no captan el rendimiento de una red como implementado en un entorno “real”. Por ejemplo, el comportamiento de una red puede estar dirigido por una interacción de nodos, uno respecto de otro, así como por las fuentes de ruido exteriores situadas en las inmediaciones de los nodos. Las técnicas teóricas o heurísticas tradicionales no ofrecen una respuesta suficiente a la interacción entre los diferentes componentes de la red con su entorno circundante y, por consiguiente, no captan el rendimiento de dicha red.

En consecuencia, se necesita una estructura para la depuración de una red que proporcione una detección y un diagnóstico de los fallos mejoradas.

Sumario

Se describe una estructura de depuración de una red. La estructura puede emplear una simulación de una red real para detectar y diagnosticar fallos en el funcionamiento de la red real. Por ejemplo una simulación de red puede ser activada por los datos que describen la operación de la red real. En la práctica, los datos no analizados que se recogen para su uso en la activación de la simulación de red pueden contener errores por diversas razones, como por ejemplo debido a errores en el hardware, en el software y/o en la red. Para asegurar que los datos utilizados para activar la simulación de red son coherentes, los datos en bruto deben ser limpiados. Por ejemplo, cada nodo de una red puede proporcionar datos para su uso en la activación de la simulación de red. Los datos suministrados por un nodo particular pueden describir no solo la operación de ese nodo particular, sino también la operación de uno o más nodos vecinos. Por consiguiente, los datos obtenidos de los nodos de la red pueden ser redundantes. Los datos redundantes son a continuación comparados, uno con otro, para identificar cualquier incoherencia, la cual puede entonces ser rectificadada de diversas formas, como por ejemplo promediando los datos, mediante la retirada de los datos incoherentes, etc.

La simulación de red puede entonces estimar el rendimiento de la red en base a estos datos. El rendimiento estimado de la red es comparado con el rendimiento observado de la red del rendimiento real de la red para detectar si la red real está rindiendo de acuerdo con lo esperado. Si no, se detecta un fallo en la operación de la red real. En otras palabras, puede utilizarse una diferencia entre el rendimiento estimado de la red, de acuerdo con lo indicado por la red real para detectar la presencia de fallos en la red real. La simulación de red puede entonces ser utilizada para el diagnóstico de los fallos inyectando de forma selectiva uno o más fallos dentro de la simulación de red hasta que el rendimiento de la red de la simulación de red se aproxime al rendimiento de red de la red real.

Una vez que se identifica el conjunto de uno o más fallos producidos en el rendimiento de la red aproximado, pueden identificarse e implementarse una o más modificaciones para corregir los fallos. Por ejemplo la simulación de red puede entonces ser utilizada para efectuar un análisis ¿Qué pasaría si ...?, de forma que puedan llevarse a cabo modificaciones en la red simulada para verificar si la modificación corrige el fallo y/o mejora de cualquier otra forma

el rendimiento de la red. Así, la simulación de red puede proporcionar una retroalimentación cuantitativa sobre el impacto en el funcionamiento de la red de una diversidad de modificaciones que pueden llevarse a cabo en la red, como por ejemplo las modificaciones efectuadas para corregir los fallos y/o mejorar el rendimiento de la red.

5 El documento US-A-5 922 051 divulga una red informática que tiene una pluralidad de nodos asociados con ella, un sistema de gestión de tráfico de datos para gestionar el tráfico de datos entre la pluralidad de nodos, comprendiendo 1) un circuito de sondeo que recupere la información del tráfico de los nodos procedente de la pluralidad de nodos; y 2) una lógica de proceso que compare la primera información seleccionada de tráfico de los nodos asociada con un segundo nodo seleccionado entre la pluralidad de nodos con un primer nivel de umbral para detectar una tendencia en 10 la primera información seleccionada de tráfico de los nodos con respecto al primer nivel de umbral.

El documento US 2003/0093709 A1, da a conocer un sistema para soportar la depuración de una red, que incluye: un medio de almacenaje para almacenar periódicamente los datos de regulación/configuración y los datos sobre la calidad de servicio de los dispositivos que constituyen la red en base a un esquema de IDs de dispositivos, IDs de 15 interfaces, y un número de versión de la CONFIG respectiva; un medio de verificación para verificar los datos sobre la calidad de servicio de los dispositivos mediante la comparación de los datos sobre la calidad de servicio con los valores de umbral respectivos; un medio de identificación para identificar el dispositivo defectuoso en base al esquema cuando los datos sobre la calidad de servicio de al menos un dispositivo vayan más allá de un respectivo valor de umbral, en el que el medio de almacenaje almacena también el resultado identificado para la depuración de la red. Así, 20 el sistema puede estimar un factor de un cambio de la condición operativa del sistema de red y repararlo de acuerdo con ello.

En el documento WO 03/094538 A, se da a conocer un procedimiento para simular una red que transporta una mezcla heterogénea de tráfico con el fin de evaluar la calidad del rendimiento de la red. Se proporcionan parámetros e información para definir la configuración de la red y definir cómo se comparten los recursos de la red entre tipos 25 de tráfico para la ejecución de una simulación. Así mismo, determinados conjuntos de parámetros definen las características de los tipos individuales de tráfico. Durante la ejecución de una simulación, los tipos individuales de tráfico son generados con unas características definidas utilizando uno o más modelos. Los tipos individuales de tráfico son a continuación agregados para generar una mezcla de tráfico conjunta, heterogénea. Cuando se ha generado la mezcla 30 de tráfico, se asignan los recursos de la red. Se recogen entonces las estadísticas para cada ejecución de simulación para indicar la ejecución de la red simulada cuando está cargada con la mezcla heterogénea de tráfico.

Constituye el objeto de la presente invención proporcionar un procedimiento y un sistema mejorados que comprenda una estructura de depuración para la detección y diagnóstico de fallos en la red. 35

Este objeto se consigue con el contenido de las reivindicaciones independientes 1, 11 y 22.

Formas de realización preferentes se expondrán con mayor detalle en conexión con los dibujos que se acompañan.

40 **Breve descripción de los dibujos**

La Fig. 1 es una ilustración de un entorno en una implementación ejemplar que muestra una red que incorpora una pluralidad de nodos.

45 La Fig. 2 es una ilustración de una implementación ejemplar que muestra un módulo de análisis de la Fig. 1 con mayor detalle.

La Fig. 3 es una ilustración de una red que incorpora una topología de mallas de siete por tres.

50 La Fig. 4 es una ilustración de una implementación ejemplar que muestra un sistema que incluye un simulador y una simulación de red de la Fig. 2.

La Fig. 5 es un diagrama de flujo que representa un procedimiento en una implementación ejemplar en la cual son inicialmente diagnosticados fallos del mismo tipo, uno respecto del otro. 55

La Fig. 6 es una ilustración de un árbol de decisión en una implementación ejemplar que puede utilizarse para determinar un tipo de fallo basado en la diferencia entre la ejecución estimada y la observada.

60 La Fig. 7 es un diagrama de flujo que representa un procedimiento en una implementación ejemplar en la cual se diagnostican fallos de tipos diferentes, uno respecto de otro, utilizando un algoritmo de diagnóstico interactivo.

La Fig. 8 es una ilustración de una red en una implementación ejemplar en la cual la pluralidad de nodos de la Fig. 1 incluye unos módulos agente que son ejecutables para ejecutar una verificación de nodos vecinos.

65 La Fig. 9 es un diagrama de flujo que representa un procedimiento en una implementación ejemplar en la cual se comparan los informes que describen los nodos vecinos para localizar los nodos que fallan en una red.

ES 2 279 479 T3

La Fig. 10 es un diagrama de flujo que representa un procedimiento en una implementación ejemplar en la cual se lleva a cabo un análisis ¿Qué pasaría si ...? En base a una simulación en línea activada por trazas.

La Fig. 11 es un diagrama de flujo que representa un procedimiento en una implementación ejemplar en la cual se derivan unas modificaciones en una red en base a un diagnóstico de un flujo perjudicial.

La Fig. 12 es una ilustración de una red que incluye una pluralidad de flujos, siendo uno de ellos un flujo perjudicial.

La Fig. 13 es una ilustración en una implementación ejemplar que muestra una interfaz gráfica de usuario (GUI) suministrada por un nodo gestor que permite que un administrador de red visualice una red y emita solicitudes de gestión a la red.

Se utilizan los mismos números a lo largo de la divulgación y en las figuras para hacer referencia a los mismos componentes y características.

Descripción detallada

Perspectiva General

Se describe una estructura de depuración de red para su uso en redes alámbricas y/o inalámbricas para mantener la eficacia y fiabilidad de las operaciones de la red. La estructura descrita en la presente memoria puede emplear una simulación de red en línea activada por trazas para detectar los fallos y para llevar a cabo un análisis de las causas originarias de los fallos. La simulación de red es “en línea” porque puede obtener datos sobre la calidad de servicio de la red a partir de una red “real”.

La estructura puede ser aplicada para diagnosticar una amplia variedad de problemas de ejecución (esto es, fallos), como por ejemplo los fallos ocasionados por caída de paquetes, congestión de enlaces, comportamiento irregular del control de acceso al medio (MAC), ruido exterior, etc. La estructura puede también utilizarse para evaluar configuraciones de red alternativas para mejorar el rendimiento de la red. Aunque la exposición que sigue describe la estructura en una red inalámbrica ejemplar, la estructura puede también emplearse en redes alámbricas.

Entorno Ejemplar

Como se expuso anteriormente, la gestión de red ha recibido una atención limitada tanto por parte de la industria como por parte de los colectivos dedicados a la investigación. La implementación de una gestión de red puede implicar una verificación continua del funcionamiento de la red, la recogida de información acerca de los nodos y de los enlaces de la red, la eliminación de las incongruencias y del ruido procedentes de los datos transmitidos, el análisis de los datos, y la ejecución de las acciones apropiadas para mejorar la fiabilidad y el rendimiento de la red.

La depuración de una red es un aspecto de la gestión de red responsable del mantenimiento de la “salud” de la red y para asegurar su rendimiento continuado y sin obstáculos. La depuración de una red, ya sea alámbrica o inalámbrica puede complicarse por una pluralidad de interacciones, como por ejemplo las interacciones ocasionadas entre entidades de red diferentes, las interacciones entre fallos, etc. La depuración de una red inalámbrica de reflexión múltiple se complica así mismo por una diversidad de factores adicionales. Por ejemplo, las típicas redes inalámbricas multirreflejo son en general propensas a enlazar errores ocasionados por fluctuaciones en la propagación de la señal, lo cual determina una topología de la red dinámica e impredecible. Así mismo, la capacidad de las redes inalámbricas multirreflejo está genéricamente limitada por la escasez de recursos (por ejemplo, anchura de banda, potencia de la batería, etc.), la cual también limita la cantidad de sobregasto de tráfico de gestión que la red puede tolerar.

Se describe una estructura que da respuesta a estas complicaciones. La estructura puede utilizar una simulación en línea activada por trazas para detectar los fallos y efectuar el análisis de la causa originaria. La simulación puede ser utilizada para reproducir situaciones que tuvieron lugar en la red que provocaron un fallo, y por consiguiente identificar y rectificar estos fallos.

La Fig. 1 es una ilustración de un entorno en una implementación ejemplar que muestra una red 100 que incorpora una pluralidad de nodos 102 (1), 102 (2), 102 (3), ... 102 (n), ... 102 (N). La pluralidad de nodos 102 (1) a 102 (N) de la Fig. 1 implementa una estructura ejemplar que utiliza una simulación de la red 100 para la detección de los fallos, el diagnóstico y el análisis ¿Qué pasaría si ...?. La estructura tiene una pluralidad de propiedades beneficiosas. Primeramente, la estructura es flexible. Debido a que la simulación es personalizable en sumo grado y puede ser aplicada a una amplia variedad de redes implementadas en diferentes entornos, el diagnóstico de los fallos incorporado sobre el simulador puede ser configurado para heredar esta flexibilidad. En segundo lugar, una simulación permite captar una diversidad de interacciones complicadas. Por ejemplo, las interacciones pueden ser captadas dentro de la red, entre la red y el entorno, así como entre fallos diferentes que ocurran durante la operación de la red. Por consiguiente, la estructura, mediante el empleo de la simulación, proporciona un diagnóstico sistemático de una amplia gama de fallos, incluyendo combinaciones de los mismos. En tercer lugar, la estructura es extensible en el sentido de que la capacidad para detectar nuevos fallos puede incorporarse dentro de la estructura modelando los fallos en la simulación con independencia de otros fallos del sistema. La interacción entre los nuevos fallos y los fallos preexistentes que son modelados en la estructura es captada implícitamente mediante la ejecución de la simulación. En cuarto lugar, la

reproducción de la red dentro de un simulador facilita el análisis ¿Qué pasaría si ...?, lo cual proporciona una retroalimentación cuantitativa sobre el impacto de ejecución de las modificaciones que pueden llevarse a cabo en la red. Por ejemplo, adoptarse medidas correctoras para corregir un fallo en la operación de una red, puede efectuarse una modificación para incrementar el rendimiento de una red, etc.

5

La estructura puede utilizar uno o más simuladores entre una pluralidad de simuladores de red existentes para simular la red 100, como por ejemplo QUALNET (QUALNET es una marca de Scalable Network Technologies, Inc. de Los Angeles, CA), OPNET MODELER (OPNET MODELER es una marca de OPNET Technologies, Inc. de Washington D.C.), etc. Las trazas que son suministradas a los simuladores son obtenidas de la red que está siendo diagnosticada, esto es, una red “real”. El uso de trazas procedentes de la red elimina la dependencia de la estructura respecto de modelos teóricos genéricos que pueden no captar los matices del hardware, software, y del entorno de la concreta red en cuestión, mejorando de esta forma la precisión de la estructura.

10

La estructura puede también emplear un plan de diagnóstico de los fallos para efectuar un análisis de la causa generadora. Por ejemplo, el plan puede utilizar datos estimados del rendimiento de la red emitidos por el simulador en línea activado por trazas, como línea de base del rendimiento esperado de la red real. La desviación del rendimiento esperado se utiliza entonces para indicar un fallo potencial. Así mismo, el plan puede selectivamente inyectar una serie de datos candidato en un simulador para efectuar el análisis de la causa generadora reduciendo el diagnóstico de los fallos a un problema de búsqueda de un conjunto de fallos. Una causa originaria puede, por consiguiente, ser identificada en base a los fallos que, al ser inyectados, provocan que la simulación se aproxime al rendimiento observado de la red real. Por consiguiente, la estructura puede emplear un algoritmo de búsqueda para detectar y diagnosticar fallos como por ejemplo caída de paquetes, congestión de enlaces, fuentes de ruido externas, comportamiento irregular del MAC, etc. Estos fallos pueden tener un impacto relativamente duradero sobre el rendimiento, y son más difíciles de detectar que los errores de fallo y parada, como por ejemplo cuando un nodo se apaga debido a un corte de la energía o de la batería.

15

20

25

De esta forma, la estructura puede utilizar una simulación como herramienta analítica para la depuración y el análisis de configuraciones de red alternativas y potencialmente incrementadoras del rendimiento. En las secciones siguientes, se identifican las trazas de red, las cuales, cuando se suministran a un simulador, suministran una simulación de red que proporciona una ilustración precisa del comportamiento efectivo de la red. También se describe una técnica que reduce o elimina los datos erróneos derivados de las trazas, cuya exposición más detallada puede encontrarse en relación con las Figs. 8 y 9. En consecuencia, el simulador se suministra con datos de alta calidad. Adicionalmente, se describe un algoritmo de búsqueda que resulta efectivo para el diagnóstico de múltiples fallos de la red, cuya exposición más detallada puede encontrarse en relación con la Fig. 7. El simulador puede también utilizarse para llevar a cabo un análisis ¿Qué pasaría si ...? Y cuantificar el beneficio sobre la calidad de servicio sobre posibles acciones sobre la red actual, cuya exposición más detallada puede encontrarse en relación con las Figs. 10 a 13.

30

35

La estructura de depuración puede ser empleada en una amplia variedad de configuraciones de red. Un ejemplo del tipo indicado se ilustra mediante la red 100 de la Fig. 1, la cual se representa como una red inalámbrica en malla. Una red en malla puede emplear una diversidad de disposiciones, como por ejemplo una topología total en malla o una tipología parcial en malla. En una topología total en malla, cada nodo está directamente conectado a cada uno de los otros nodos de la red. En una topología parcial en malla, cada nodo está conectado a al menos otro nodo, pero no necesariamente a cada uno de los otros nodos de la red.

40

45

Una red en malla, por ejemplo, puede ser utilizada como tecnología que permita que los vecinos, de manera cooperante, constituyan una red en malla inalámbrica colectiva autogestionada. Cada vecino puede proporcionar uno o más de entre la pluralidad de nodos 102 (1) a 102 (N) de la red 100. En una red del tipo indicado, los vecinos pueden, por ejemplo, compartir una pasarela 104 de Internet efectiva en cuanto al coste.

50

55

60

En un ejemplo de una red en malla como la utilizada en un vecindario, las encaminadoras que se utilizan para acoplar en comunicación la pluralidad de nodos 102 (1) a 102 (N) se alojan dentro de una casa y se enchufan en terminales eléctricos. Por consiguiente, cada una de las encaminadoras en este ejemplo tiene una movilidad limitada. La estabilidad relativa de dicha red, sin embargo, hace que la depuración de la red sea incluso más importante porque los fallos pueden tener una influencia duradera en el rendimiento de la red. Debe destacarse que la falta de movilidad de la encaminadora, en este ejemplo no reduce el dinamismo de la topología de la red porque los enlaces inalámbricos pueden ser accesibles o inaccesibles debido a cambios del entorno. En otro ejemplo, los nodos de la red en malla pueden ser móviles, como por ejemplo utilizando dispositivos de computación móviles con capacidades de comunicación inalámbrica, como asistentes digitales personales (PDA), computadoras personales de tableta (PCs), computadoras portátiles, etc.

65

Así mismo, el crecimiento de una red en malla de comunidad es orgánica en cuanto a que los usuarios compran e instalan el equipo para unirse a la red en malla. Las redes en malla tradicionales carecían de una entidad centralizada responsable de la administración de la red. Sin embargo, las capacidades de autogestionabilidad y autorregenerantes suministradas a través de la estructura descrita en la presente memoria pueden ser proporcionadas de forma que cada nodo 102 (1) a 12 (N) implemente las capacidades de depuración. En la implementación ilustrada, se proporciona un solo nodo con capacidades de gestión.

ES 2 279 479 T3

En la red 100 ilustrada en la Fig. 1, cada uno de los nodos tiene un procesador, una memoria, y un dispositivo de conexión a la red, un ejemplo de los cuales se muestra mediante el nodo 102(n) que incluye un procesador 106(n) una memoria 108(n), y un dispositivo 110(n) de conexión a la red. Los procesadores (por ejemplo, los procesadores 106 (n), 106(N)) no están limitados por los materiales con los cuales están formados o por los mecanismos de procesamiento empleados dentro de ellos. Por ejemplo, los procesadores pueden estar compuestos de semiconductor (s) y/o transistores (por ejemplo circuitos integrados electrónicos (ICs)). En dicho contexto, las instrucciones ejecutables por los procesadores pueden ser instrucciones ejecutables electrónicamente. Alternativamente, los mecanismos de o para los procesadores, y por tanto de o para un nodo, pueden incluir, sin que ello suponga limitación computación cuántica, computación óptica, computación mecánica (por ejemplo utilizando nanotecnología), etc.

La memoria (por ejemplo, la memoria 108 (n), 108 (N)) incluye unos medios de almacenaje de la computadora en forma de memoria volátil y/o no volátil, como por ejemplo memoria de solo lectura (ROM) o memoria de acceso aleatorio (RAM), etc. La memoria puede también incluir otros medios de almacenaje de la computadora volátiles/no volátiles, desmontables/no desmontables. La memoria proporciona el almacenaje de las instrucciones legibles por computadora, las estructuras de los datos, los componentes del software, y otros datos para los nodos.

Los dispositivos de conexión a la red (por ejemplo, los dispositivos 110 (n), 110 (N) de conexión a la red) pueden adoptar una diversidad de configuraciones para acoplar en comunicación los nodos a la red 100. Cuando se utiliza en un entorno de red de área local (LAN), por ejemplo, el nodo 102 (n) está conectado en comunicación con el LAN a través de una interfaz o adaptador de red, que puede ser alámbrico o inalámbrico. Cuando se utiliza en un entorno de red de área amplia (WAN), el dispositivo de conexión a la red puede estar configurado como un módem u otro medio para establecer comunicaciones, como por ejemplo una conexión alámbrica sobre una línea de suscriptor digital (DSL), una conexión inalámbrica suministrada por satélite, etc. Las conexiones lógicas se representan en la Fig. 1 mediante el empleo de flechas. Aunque la red 100 mostrada en la Fig. 1 es una red en malla inalámbrica, puede emplearse una diversidad de redes distintas, como por ejemplo Internet, intrarredes, etc.

Los nodos 102 (n), 102 (N) ilustran una arquitectura de gestión ejemplar compuesta por módulos de software. En general, cualquiera de las funciones descritas en la presente memoria puede ser implementada usando software, firmware (por ejemplo circuitería lógica fija), procesamiento manual, o una combinación de estas implementaciones. Los términos “módulo”, “funcionalidad”, y “lógica”, tal como se utilizan en la presente memoria representan software, firmware o una combinación de software y firmware. En el caso de una implementación de software, el módulo, la funcionalidad, o la lógica representa un código de programa que efectúa las tareas específicas cuando son ejecutadas en un procesador, como por ejemplo una o más unidades de procesamiento centrales (CPUs). El código de programa puede ser almacenado en uno o más dispositivos de memoria legibles por computadora. Las características de la estructura descrita más adelante son independientes de la plataforma, significándose con ello que las técnicas de depuración pueden ser implementadas en una diversidad de plataformas de computación comerciales incorporando una diversidad de procesadores.

Se proporciona un módulo agente 112 (n) para su ejecución sobre cada nodo 102 (n) de la red 100. El módulo agente 112 (n) se ilustra siendo ejecutado sobre el procesador 106 (n) y puede ser almacenado en la memoria 108 (n). El módulo agente 112 (n) incluye un módulo 114 (n) de recogida de datos (en adelante “módulo de recogida”) que, cuando es ejecutado, puede reunir datos procedentes de diversas capas de protocolo y/o partir del dispositivo de conexión 110 (n) a la red. En la red ilustrada 100 de la Fig. 1, el módulo agente 112 (n) informa de estos datos al nodo 102 (N) que tiene la función de la gestión, el cual en adelante será designado como nodo gestor. El nodo gestor 102 (n) realiza un análisis de los datos (por ejemplo, mediante la implementación de una simulación que acepta los datos como entrada) y adopta las acciones apropiadas para depurar la red. La gestión de la red puede ser centralizada colocando el gestor sobre un único nodo tal como se ilustra en la red 100 de la Fig. 1 o distribuirse de forma que la pluralidad de los nodos de una red incluya cada uno la función de la gestión.

Los módulos agente 112 (n), 112 (N), cuando son ejecutados sobre los respectivos procesadores 106 (n), 106 (N), recogen y comunican los datos que describen su visión (local) del comportamiento de la red al nodo gestor 102 (N). Ejemplos de datos enviados pueden incluir una estadística del tráfico, la potencia de la señal de los paquetes recibidos sobre diversos enlaces, los conteos de retransmisión sobre cada enlace, etc.

El nodo gestor 102 (N) incluye un módulo gestor 116 (N) que puede almacenarse en la memoria 108 (N) y que puede ejecutarse sobre el procesador 106 (N) para procesar los datos procedentes de los agentes 112 (n), 112 (N) para depurar la red 100. El módulo gestor 116 (N), por ejemplo, incluye un simulador de red 118 (N) (en adelante “simulador”) que puede ejecutarse en el procesador 106 (N) y puede almacenarse en la memoria 108 (N) para simular la red 100.

Los datos recibidos por el nodo gestor 102 (N) procedentes de diversos agentes 112 (n), 112 (N) pueden producir una visión incoherente de la red 100. Dichas incoherencias pueden ser el resultado de cambios topológicos y del entorno, de errores de medición, de nodos de comportamiento irregular. Por consiguiente, el nodo gestor 102 (N) incluye un módulo 120 (N) de limpieza de datos (en adelante “módulo de limpieza”) que puede ejecutarse en el procesador 106 (N) para resolver dichas incoherencias. La salida de los datos limpiados procedente del módulo de limpieza 120 (N) se incorpora para su procesamiento por un módulo 122 (N) de análisis de la causa originaria (en adelante “módulo de análisis”) cuya exposición más detallada puede encontrarse en relación con la figura siguiente. Aunque el nodo gestor 102 (N) se ilustra incluyendo el módulo agente 112 (N) y el módulo gestor 116 (N), en otra

ES 2 279 479 T3

implementación el nodo gestor 102 (N) es un nodo gestor dedicado en el sentido de que no incluye el módulo agente 112 (N). Así mismo, como se expuso anteriormente, la funcionalidad del módulo gestor 116 (N) puede suministrarse por más de un nodo de la red 100.

5 La Fig. 2 es una ilustración de una implementación ejemplar 200 que muestra el módulo de análisis 122 (N) de la Fig. 1 con mayor detalle. Una vez que han sido resueltas las incongruencias en los datos mediante el módulo de limpieza 120 (N) de la Fig. 1, los datos limpiados son alimentados en el módulo de análisis 122 (N) para su investigación adicional.

10 El módulo de análisis 122 (N) utiliza una simulación en línea activada por trazas para determinar las causas originarias de las discrepancias respecto del rendimiento esperado de la red indicado por la ejecución de red simulada. En la exposición que sigue, el rendimiento de red esperado y el rendimiento de red simulado son utilizados de manera intercambiable para indicar el rendimiento de red tal como es suministrado por una simulación de red. El módulo de análisis 122 (N) puede utilizar los datos limpiados 202 obtenidos de una utilería de trazas, ejemplos de dichos datos se ilustran en la Fig. 2 como potencia de la señal recibida de enlace (RSS) 204, emplazamiento 206 de enlace, y actualización de encaminamiento 208, par activar simulaciones en línea y establecer el rendimiento esperado bajo la configuración de red ofrecida y los patrones de tráfico.

20 El módulo de análisis 122 (N) se ilustra incluyendo una simulación de red 210 que se proporciona mediante la ejecución del simulador 118 (N). La simulación 210 puede proporcionarse mediante la ejecución de uno o más módulos de software que proporcionen simulaciones de características de una red, de las que se ilustran ejemplos en la Fig. 2 mediante un módulo 212 de inyección de interferencias, un módulo 214 simulador de tráfico, y un módulo 216 de cambio de topología. El módulo 212 de inyección de interferencias puede ejecutarse para simular fuentes de ruido externas inyectando el efecto de ruido externo en la simulación de red 210. El módulo 214 simulador de tráfico puede ejecutarse para asegurar que el tráfico de la simulación de red 210 se aproxime al de la red real. El módulo 216 de cambio de topología puede ejecutarse para simular cambios en la topología, como por ejemplo añadiendo y/o suprimiendo nodos en la simulación de red 210.

30 El módulo de análisis 122 (N) detecta los fallos en la red 100 de la Fig. 1 comparando la ejecución esperada tal como se indica mediante la simulación de red 210 con la ejecución observada. Cuando se observan las discrepancias, el módulo de análisis 122 (N) determina la causa generadora de las discrepancias buscando uno o más fallos almacenados en el directorio 218 de fallos que produzcan la mejor correspondencia entre la ejecución de red simulada y observada.

35 El módulo de análisis 122 (N), por ejemplo, puede recibir los datos observados 220 procedentes de uno o más módulos agente 112 (n) de la Fig. 1 que describe una pérdida de velocidad, el caudal, y el ruido 220, el cual se ilustra en la Fig 2 como “pérdida de velocidad, caudal, y ruido 220”. La simulación de red 210 computa los datos esperados 222 que describen una pérdida de velocidad esperada, un caudal esperado, y un ruido esperado, lo cual se ilustra en la Fig. 2 como “pérdida de velocidad, caudal, y ruido esperados 222”. Los datos observados 222 son comunicados a través de una demora 224 hasta un comparador 226, de forma que el comparador 226 recibe los datos observados y esperados 220, 222 simultáneamente. El comparador 226 determina entonces si los datos observados 220 exceden a los datos esperados 222. Si es así, el comparador 226 emite de salida un mensaje de error 228 para su comunicación al administrador de red y comunica el error al directorio de fallos 218 para determinar una causa originaria del error.

45 Después de que la causa originaria del error ha sido indicada mediante la selección de una o más de los fallos procedentes del directorio de fallos 218, el módulo de análisis 122 (N) puede simular una o más acciones alternativas para rectificar el fallo. Las acciones alternativas pueden ser simuladas bajo el modelo de tráfico actual y la topología de red tal como se suministra por el simulador de tráfico 214 y por el módulo de cambio de topología 216, respectivamente. En base a las simulaciones, el módulo de análisis 122 (N) puede sugerir una o más acciones apropiadas para paliar los fallos y potenciar el rendimiento global de la red, un ejemplo de lo cual se ilustra como fallo de nodo de enlace 230 de la Fig. 2. Por ejemplo, el administrador de red puede ser notificado si existen sospechas de fallo en el software o en el hardware, la topología puede ser modificada por medio de un ajuste de la potencia de transmisión si se detecta una conectividad deficiente, las enaminadoras pueden emplear unas limitaciones de velocidad para aliviar la congestión, etc.

55 El empleo de la simulación de red 210 para un diagnóstico en línea ofrece una pluralidad de beneficios respecto de las técnicas de diagnóstico teóricas o heurísticas tradicionales. Por ejemplo, la simulación de red 210 puede proporcionar una comprensión incrementada en el comportamiento de la red respecto de las técnicas teóricas o heurísticas tradicionales. Una red inalámbrica operativa, por ejemplo, es un sistema complejo de piezas intrincadas, como por ejemplo flujos de tráfico, protocolos de integración en red, algoritmos de procesamiento de señales, hardware, propa- gación de radiofrecuencia, etc. Adicionalmente pueden tener lugar interacciones entre todas las piezas de la red. Las interacciones entre fallos pueden ser eficazmente diagnosticadas y tratadas mediante la selección de uno o más fallos tomados del directorio de fallos 218 que produce una simulación de red 210 que se corresponde con el comportamiento efectivo de la red “real”.

65 Así mismo, el comportamiento de la red puede ser dirigido mediante interacciones de los nodos, uno respecto de otro, así como mediante fuentes de ruido externo situadas en las inmediaciones de los nodos. Las técnicas teóricas y heurísticas tradicionales no captan el comportamiento de dichas redes y no tratan suficientemente las interacciones producidas entre los diferentes componentes de la red.

ES 2 279 479 T3

Como ejemplo, considérese una red 300 de topología de mallas de siete por tres mostrada en la Fig. 3. Se ilustran cinco flujos en la red 300 y se designan como F_1 302, F_2 304, F_3 306, F_4 308, y F_5 310. En el ejemplo ilustrado, cada uno de los flujos 302 a 310 tiene una cantidad de tráfico que comunicar. Por ejemplo, cada uno de los flujos 302 a 310 puede recibir cantidades sustancialmente similares de datos procedentes de las aplicaciones respectivas.

Adicionalmente, en este ejemplo, los nodos adyacente pueden “oírse” entre sí y el alcance de interferencia es dos veces el alcance de comunicación. El tráfico entre el nodo A 312 y el nodo O 314, por ejemplo, interfiere con el tráfico entre los nodos C y Q 316, 318. De modo similar, el tráfico entre los nodos G y U 320, 322 interfiere con el tráfico entre los nodos E y S 324, 326. Sin embargo, el tráfico entre G y U 320, 322 y el tráfico entre los nodos A y/o 312, 314 no interfiere con el tráfico entre los nodos D y R 328, 330.

La tabla siguiente describe un ejemplo de caudal de los flujos 302 a 310 cuando cada flujo envía un tráfico con una tasa de bits constante (CBR) a una velocidad de once Mbps.

F_1	F_2	F_3	F_4	F_5
2,50 Mbps	0,23 Mbps	2,09 Mbps	0,17 Mbps	2,53 Mbps

Como se muestra en la tabla superior, el flujo F_3 306 recibe un caudal más alto que los flujos F_2 304 y F_4 308. En otras palabras, el flujo F_3 306 consume una porción más alta de anchura de banda que los otros flujos de la red 300.

Tradicionalmente, la aplicación de técnicas heurísticas puede llevar a la conclusión de que el flujo F_3 306 recibe una cuota de la anchura de banda indebidamente mayor. Mediante el uso de una simulación en línea de activación de trazas, sin embargo, el nodo gestor 102 (N) puede concluir que este es un comportamiento normal. Por ejemplo, la simulación de red puede tomar en consideración la calidad de los enlaces y, por consiguiente, determinar que los flujos F_1 302 y F_5 310 interfieren con los flujos F_2 304 y F_4 308. Por consiguiente, el flujo F_3 306 está provisto de una anchura de banda adicional debido a la falta de interferencia de los flujos F_1 302 y F_5 310, por oposición a los flujos F_2 304 y F_4 308. De esta forma, la simulación puede determinar que, aún cuando todos los flujos pueden tener la misma velocidad de envío de nivel de aplicación, se espera el caudal observado. Una heurística simple, sin embargo, puede llegar a la conclusión errónea de que los nodos D y R 328, 330 se comportan irregularmente.

La simulación de red se utiliza por el módulo de análisis 122 (N) para gestionar la red sabiendo “qué esperar” de la red dados los flujos de tráfico y cualidades de enlace actuales. En otras palabras, el módulo de análisis 122 (N) puede hacer comentarios sobre lo que constituye el comportamiento normal en base a las estimaciones suministradas por la simulación de red. En el ejemplo anterior, aún cuando F_3 306 utilice una cuota mayor de la anchura de banda de la red 300 que los demás flujos de la red 300, ello no será considerado como fallo por el módulo gestor porque el comportamiento es esperado. Cuando el comportamiento observado se desvía del comportamiento esperado, el módulo gestor puede invocar los algoritmos de búsqueda de fallos que utiliza el directorio de fallos 218 de la Fig. 2 para determinar la causa originaria de la desviación.

Así mismo, aunque sería posible aplicar una propuesta de diagnóstico tradicional de fallos basado en firmas o basado en normas en un tipo concreto de red y bajo un entorno y configuración específicos, las simples firmas o normas son insuficientes para captar la complejidad intrínseca del diagnóstico de fallos en configuraciones generales. Por contra, un simulador es personalizable en gran medida y puede ser aplicado, con las apropiadas configuraciones de parámetros, en una amplia gama de redes que están configuradas para su uso en diferentes entornos. El diagnóstico de los fallos incorporado en dicho simulador hereda esta generalidad.

Otra ventaja adicional de la propuesta basada en la simulación, es la capacidad de llevar a cabo un análisis ¿Qué pasaría si ...?. Esto es, modificando los parámetros o llevando a cabo determinadas acciones en el simulador, un simulador puede predecir la ejecución para un escenario imaginario. En base a estos datos, un módulo gestor puede instruir a los módulos agente (por ejemplo al módulo agente 112 (n) de la Fig. 1) para adoptar una acción apropiada para optimizar el rendimiento de la red. Como se expuso anteriormente, dicho análisis ¿Qué pasaría si? es valioso porque puede ser difícil prever las consecuencias de una acción correctora debido a la interacción de múltiples factores en la red. Por ejemplo, la potencia transmisora puede incrementarse para mejorar la calidad de los enlaces, pero el incremento puede también crear una interferencia adicional que afecte a otros nodos de la red.

Detección y Diagnóstico de Fallos

Se describe una propuesta de diagnóstico a base de simulación que proporciona la creación de un entorno dentro de un simulador (por ejemplo, una simulación de red 210) que se aproxime a la funcionalidad de una red real. El entorno creado (esto es, la simulación de red) puede entonces ser utilizado para determinar los comportamientos esperados de la red real así como determinar cuándo se presentan las discrepancias en la operación de la red real. Para encontrar

una causa originaria de estas discrepancias, el módulo gestor es ejecutado para buscar sobre un espacio de faltas para determinar qué falta o conjunto de faltas puede reproducir la ejecución de red que se aproxime a la ejecución de red que se ha observado en la red real. La red simulada puede reproducir una pluralidad de aspectos de la red, como por ejemplo la topología, el comportamiento del encaminamiento, los modelos de tráfico de la red observados en la red real, etc.

Utilizando la simulación en línea activada por trazas como bloque funcional, se describe un algoritmo de diagnóstico que puede ejecutarse para encontrar las causas originarias de los fallos. El algoritmo de diagnóstico, por ejemplo, puede en primer término estimar el rendimiento de la red bajo un determinado conjunto de fallos. A continuación, en base a las diferencias existente entre la ejecución estimada y observada, el algoritmo de diagnóstico busca un espacio de fallos para reproducir cualquier discrepancia observada. En una implementación, el algoritmo de diagnóstico puede diagnosticar múltiples fallos del mismo tipo (por ejemplo topología de red), así como diagnosticar la presencia de múltiples tipos de fallos, (por ejemplo, ruido y topología).

Los fallos pueden ser diagnosticados aún cuando los datos de la trazas para activar la simulación contengan errores. Por ejemplo los datos suministrados por el módulo agente 112 (n) de la Fig. 1 pueden contener errores debido a varias razones, como por ejemplo errores de medición, información falsa, errores en el software/hardware, errores en la ejecución del nodo 102 (n), errores en la comunicación de la red, etc. El módulo de limpieza 120 (N) es ejecutado por el nodo gestor 102 (n) para reducir o eliminar los datos erróneos procedentes de la traza, de forma que la calidad de los datos de traza se utiliza para activar el diagnóstico de los fallos en base a la simulación. Una exposición más detallada de la ejecución del módulo de limpieza 120 (N) puede encontrarse en relación con las Figs. 8 y 9.

Simulación activada por Trazas

La Fig. 4 es una ilustración de una implementación ejemplar que muestra un sistema 400 que incluye el simulador 118 (N) y la simulación de red 210 de la Fig. 2. Los datos de traza obtenidos mediante la operación de red de la red real y examina los efectos de un conjunto determinado de fallos en la red real. Una diversidad de datos de traza pueden ser recogidos para su introducción en un simulador, ejemplos de los cuales se describen a continuación:

Topología de Red 402

Los datos de la topología de red 402 describen la topología de la red, como por ejemplo qué nodos son miembros actualmente de la red y los enlaces correspondientes entre los nodos. Cada nodo de la red, por ejemplo, puede estar configurado para informar sobre el estatus (por ejemplo, conectado o desconectado) de los nodos vecinos y de los nodos referenciados en una o más tablas de encaminamiento del nodo. De esta forma, la pertenencia del nodo a la red puede ser comunicada al nodo gestor 102 (N) de la Fig. 1. En una implementación, únicamente se informa de cambios de vecinos o caminos. Estos datos pueden utilizarse para activar una simulación de camino, la cual se describe con mayor detalle en relación con la simulación de camino de la Fig. 4.

Estadística 404 del Tráfico

Los datos de la estadística 404 del tráfico pueden ser utilizados para describir las cantidades de datos que son comunicadas a través de la red y de los nodos concretos que comunican esos datos. La estadística de tráfico 404 puede ser utilizada como entrada por el módulo simulador de tráfico 214 de la Fig. 2, de forma que la simulación de red 210 tenga un flujo de tráfico que se aproxime al de la red real. Cada nodo de la red puede mantener uno o más contadores que describan el volumen de tráfico enviado a y recibido desde sus vecinos inmediatos. Estos datos son utilizados para activar una simulación de tráfico de caminos suministrada por el módulo de simulación de tráfico 214, lo que se describe con mayor detalle en relación con la Fig. 4.

Medio Físico 406

Los datos del medio físico 406 pueden describir los efectos producidos sobre la ejecución de red del medio físico que se utiliza para implementar la red. Por ejemplo, una red inalámbrica en cada nodo puede informar sobre su nivel de ruido y de la potencia de la señal de los enlaces inalámbricos procedentes de sus nodos vecinos. En una implementación, las variaciones de la potencia de la señal son periódicamente captadas mediante premedicación de tiempos, desviación característica, u otro agregado estadístico.

Operación de Red 408

Los datos de la operación de red 408 describen la operación de red 408 de la red real. Como se expuso anteriormente, la operación de red observada es comparada con la salida de la operación de red estimada procedente de la simulación de red para detectar las discrepancias de las operaciones de red. La operación de red puede incluir tanto la operación de enlaces como la operación de extremo a extremo, las cuales pueden ser ambas medidas empleando una diversidad de medidas, como por ejemplo velocidad de pérdida de paquetes, demora, y caudal. La descripción siguiente se centra sobre la operación del nivel de enlace.

La recogida de datos puede implicar dos etapas: 1) la recogida de los datos de ejecución en bruto en un nodo local y 2) la distribución de los datos recogidos hasta los puntos de recogida para su análisis. Puede utilizarse una diversidad de herramientas para la recogida local de datos, como por ejemplo protocolos nativos de encaminamiento y husmeadores de paquetes.

5 En una implementación, aún cuando la distribución de datos hasta el módulo gestor introduce una sobrecarga de la red, la sobrecarga de la red es baja y tiene escaso impacto sobre el tráfico de datos de la red. Adicionalmente, la sobrecarga de la red puede ser reducida utilizando la compresión, la codificación delta, la multidifusión, cambios adaptadores de una escala temporal y/o espacial de distribución, etc. Por ejemplo, un conjunto mínimo de datos es
10 recogido e intercambiado durante la operación normal de una red. Una vez que surge la necesidad de datos adicionales (por ejemplo, cuando la información que está siendo recogida indica una discrepancia), el módulo gestor puede solicitar información adicional e incrementar la frecuencia de la recogida de datos para el subconjunto de los datos que necesitan una verificación incrementada.

15 *Metodología de la Simulación*

Las características de la red que son modeladas por el simulador pueden ser clasificadas en diversas categorías, como por ejemplo carga de tráfico, encaminamiento, señal inalámbrica, fallos, etc. Las siguientes secciones describen
20 ejemplos de simulación de cada una de estas categorías ejemplares como módulos individuales que son utilizados para hacer que el simulador simule las correspondientes características de la red.

Simulador 410 de la Carga de Tráfico

Una simulación de red generada por un simulador puede configurarse de forma que proporcione una estructura de
25 tráfico que se aproxime a la estructura de tráfico de la red real. Un ejemplo de una propuesta de simulación de carga de tráfico implica la simulación de demandas de aplicación de extremo a extremo. Sin embargo, una red de N nodos puede incluir potencialmente N^2 demandas. Así mismo, las demandas de aplicación de extremo a extremo pueden ser difíciles de obtener dada la heterogeneidad de las demandas de aplicación y el uso de protocolos de transporte diferentes, como por ejemplo un protocolo de control de transmisión (TCP), un protocolo de datagrama de usuario
30 (UDP), un protocolo de transporte rápido (RTP), etc.

En una implementación, el módulo de simulador de carga 410 es una porción del módulo simulador de tráfico 214 de la Fig. 2 y proporciona una simulación de tráfico en base a los enlaces que se utiliza para la escalabilidad para
35 evitar la necesidad de obtener demandas de aplicación de extremo a extremo. La simulación de tráfico en base a los enlaces, una vez implementada, puede ajustar una velocidad de envío en nivel de aplicación en cada enlace para hacer coincidir los goteos de tráfico al nivel de los enlaces observados de la red real. De esta forma, son abstraídas capas de orden superior (por ejemplo una capa de transporte, una capa de aplicación, etc), lo que posibilita que la simulación se concentre sobre el tamaño de los paquetes y sobre la velocidad del tráfico.

40 La adaptación de la velocidad de envío sobre una base por enlace en un simulador puede no ser trivial cuando la velocidad de envío sobre un enlace no puede ser directamente controlada, como por ejemplo cuando solo se puede ajustar la velocidad de envío en nivel de aplicación y hay que afrontar el protocolo de control de acceso al medio (MAC). Por ejemplo, cuando una velocidad de envío de aplicación de un enlace se fija en un Mbps, la velocidad de envío real (por el aire) puede ser más baja debido al retraso en la capa MAC o más alta debido a la retransmisión del
45 nivel MAC. La cuestión se complica aún más mediante la interferencia, lo que introduce una interdependencia entre las velocidades de envío sobre enlaces diferentes.

Una técnica de búsqueda interactiva puede ser utilizada para afrontar estas cuestiones mediante la determinación de la velocidad de envío en cada enlace. Puede utilizarse una pluralidad de técnicas de búsqueda interactiva, como por
50 ejemplo i) el incremento multiplicativo y la reducción multiplicativa, y ii) el incremento aditivo y la reducción aditiva. Como se muestra en el siguiente procedimiento representado utilizando un pseudocódigo ejemplar, cada enlace trata individualmente de reducir la diferencia entre la velocidad de envío actual en el simulador y la velocidad de envío efectiva en la red real.

55 mientras (no sea convergido y $i < \text{maxIterations}$)

$i = i + 1$

si (option == multiplicative)

60 para cada enlace (j)

$\text{prevRatio} = \text{targetMacSent}(j) / \text{simMacSent}(j);$

65 $\text{currRatio} = (1 - \alpha) + \alpha * \text{prevRatio};$

$\text{simAppSent.}(j) = \text{prevAppSent}(j) * \text{currRatio};$

si no // aditivo

para cada enlace (j)

5 diff = targetMacSent (j) - prevMacSent (j);

simAppSent (j) = prevAppSent (j) + α * diff;

ejecutar simulación utilizando simAppSent como entrada

10

determinar simMacSent para todos los enlaces a partir de los resultados de la simulación

conducido = isConverge (simMacSent, targetMacSent)

15

Así, el pseudocódigo expuesto ilustra un ejemplo de búsqueda de la velocidad de envío de nivel de aplicación utilizando ya sea incremento - multiplicativo/decremento multiplicativo ya sea incremento - aditivo/decremento - aditivo. En el procedimiento ejemplar expuesto, es inducido un parámetro α , en el que $\alpha \leq 1$ (por ejemplo, $\alpha = 0,5$) para amortiguar la oscilación. El proceso se reitera hasta que o bien la velocidad se aproxima a la velocidad escogida como objetivo (designada como targetMacSent) o bien hasta que se alcance un número máximo de iteraciones.

20

Simulador de Camino 412

El encaminamiento juega un papel importante en la prestación de una red, particularmente en redes inalámbricas multirreflejo. Una propuesta de simulación de camino implica la simulación de un protocolo de encaminamiento utilizado en la red real dentro del simulador. Con el fin de reproducir el mismo comportamiento de encaminamiento como en una red real, se obtienen trazas de paquetes detalladas para establecer el encaminamiento.

25

Los caminos efectivos adoptados por los paquetes pueden ser utilizados como entrada para el módulo del simulador 412 de caminos, cuando los caminos no fluctúan frecuentemente, los cambios de encaminamiento pueden ser rastreados en lugar de recoger los caminos sobre una base de paquete por paquete en el gestor. Con este fin, el módulo del simulador 412 de caminos puede ser activado por trazas. Por ejemplo, el módulo de simulación de caminos puede ser implementado dentro del simulador 118 (N), como por ejemplo un simulador QUALNET (QUALNET es una marca de Scalable Network Technologies, Inc. de Los Angeles, CA). El módulo del simulador 412 de caminos acepta las actualizaciones de del encaminamiento y las correspondientes estampillas de tiempo como entradas, y a continuación se asegura de que los paquetes de la simulación de red siguen el mismo camino que en la red real.

30

35

Simulador 414 de la Potencia de la Señal

La potencia de la señal tiene un impacto en el rendimiento de la red alámbrica e inalámbrica. Debido a las variaciones producidas a través de los distintos dispositivos (por ejemplo tarjetas inalámbricas) y entornos de conexión a la red, puede ser difícil derivar un modelo de propagación general que capte todos estos factores. Para afrontar esta cuestión, puede ser activado un simulador 414 de la potencia de la señal a partir de la medición real de la fuerza de la señal de la red real, tal como el obtenido a partir de los mismos dispositivos de conexión a la red.

40

Inyección 416 de Fallos

La estructura puede incluir un módulo de inyección 416 de fallos que puede ejecutarse para inyectar diferentes tipos de fallos dentro del simulador, como por ejemplo caída de paquetes en los anfitriones, fuentes externas de ruido, comportamiento irregular MAC, etc. De esta forma, el módulo de análisis puede examinar el impacto de los fallos en la red. La caída de paquetes en los anfitriones, por ejemplo, tiene lugar cuando un nodo de comportamiento irregular deja caer una porción del tráfico desde uno o más nodos vecinos, por ejemplo debido a errores en el software/hardware, sobrefluje de báfer, caídas malintencionadas, etc. La capacidad para detectar dichas caídas de paquetes de los anfitriones terminales resulta útil, puesto que posibilita que el gestor diferencie las pérdidas ocasionadas por los anfitriones de las pérdidas ocasionadas por la red.

50

55

La estructura, mediante la ejecución del modulo de inyección 416 de fallos, también soporta la capacidad de inyectar fuentes externas de ruido en la red. Así, la estructura puede proporcionar una simulación que replique el efecto de las fuentes de ruido situadas fuera de la red (esto es, no son suministradas por un nodo) pero que sin embargo afectan a la red.

60

Un comportamiento irregular del MAC tiene lugar cuando un nodo defectuoso no sigue la etiqueta del MAC y obtiene una participación improcedente de la anchura de banda del canal. Por ejemplo en el IEEE 802.11, un nodo incorrecto puede escoger una ventana de competencia (CW) más pequeña para enviar tráfico de manera agresiva.

65

La congestión de enlaces puede también ser simulada por la estructura suministrando una carga de transmisión de datos elevada en la red simulada. A diferencia de los otros tipos de fallos, la congestión de enlaces es implícitamente captada por la estadística del tráfico reunida a partir de cada nodo. Por consiguiente, la simulación activada por trazas

puede directamente evaluar el impacto de la congestión de enlaces en la red real. Una exposición más detallada del diagnóstico de los fallos puede encontrarse en la sección siguiente.

Diagnóstico de los Fallos

Las causas originarias de los fallos y de los problemas de rendimiento pueden ser diagnosticados mediante la ejecución del módulo de análisis 122 (N) de la Fig. 2. Aplicando los fallos a la simulación de la red, el diagnóstico de las discrepancias de la red puede reducirse a buscar un conjunto de fallos que, cuando son inyectados dentro de la red simulada, dan como resultado un rendimiento estimado por la red simulada que se aproxima al rendimiento observado de la red real. Más formalmente expresado, dados los parámetros de red NS el Conjunto de Fallos se descubre de forma que:

$$\text{SimPerf (NS; FaultSet)} \approx \text{RealPerf},$$

donde el rendimiento de la red es un valor funcional que puede ser cuantificado utilizando diferentes métricas.

El espacio de búsqueda de un fallo puede contener una multitud de dimensiones de búsqueda debido a las diferentes combinaciones de fallos que pueden afrontarse. En una implementación el módulo de análisis 122 (N) es optimizado mediante una búsqueda eficiente debido a la comprensión de que tipos diferentes de fallos a menudo modifican algunas métricas concretas del rendimiento de la red. Por ejemplo, la caída de paquetes en los anfitriones genéricamente afecta a la velocidad de la pérdida de los enlaces, pero no afecta a otros parámetros del rendimiento de la red. Por consiguiente, los parámetros del rendimiento de la red pueden ser utilizados para diagnosticar el rendimiento de la red advirtiendo las diferencias entre el rendimiento de la red observada y estimada indicadas por los parámetros.

En una implementación, no es necesario proporcionar un modelo predictivo a los fines del diagnóstico de los fallos. Antes bien, es suficiente simular lo que sucedió en la red después del hecho. Por ejemplo, los módulos agente pueden periódicamente transmitir información acerca de las condiciones de los enlaces y de las estructuras del tráfico hasta el módulo gestor. Esta información es procesada y a continuación alimentada en el simulador para crear una simulación de red que pueda ser utilizada para determinar la probable causa originaria del fallo.

Diagnóstico inicial

La Fig. 5 es un diagrama de flujo que representa un procedimiento 500 en una implementación ejemplar en la cual los fallos del mismo tipo, uno respecto de otro, son inicialmente diagnosticados. Para facilitar la descripción, la exposición que sigue afecta a tres tipos ejemplares de fallos: 1) caída de paquetes en los anfitriones; 2) ruido externo; y 3) comportamiento irregular del MAC. Es evidente, sin embargo, que existen múltiples fallos y combinaciones de fallos que pueden también tratarse de manera similar. La exposición que sigue incluye procedimientos que pueden ser implementados utilizando los sistemas y procedimientos descritos. Aspectos de cada uno de los procedimientos pueden ser implementados en hardware, firmware o software o combinaciones de los mismos. Los procedimientos se muestran como conjunto de bloques que especifican las operaciones desarrolladas por uno o más dispositivos y no están necesariamente limitados a las órdenes mostradas para llevar a cabo las operaciones por los respectivos bloques.

Como se expuso anteriormente, una simulación activada por trazas, cuando es alimentada con los parámetros de red actuales de una red real, puede ser utilizadas para establecer el rendimiento de red estimado de la red. En base a las diferencias entre el rendimiento de red estimado y el rendimiento de red observado, el tipo de fallos puede ser determinado utilizando un árbol de decisión, un ejemplo del cual se representa en la Fig. 6.

Debido a una diversidad de factores, el rendimiento de red estimado es improbable que sea idéntico al rendimiento de red observado, incluso en ausencia de fallos, por consiguiente, las discrepancias en el rendimiento de red pueden determinarse utilizando un umbral. Por ejemplo, una discrepancia puede ser determinada en base a si una diferencia entre los valores de rendimiento de red estimados y observados (esto es, real) excede de un umbral correspondiente. El umbral puede ser computado de diversas maneras, como por ejemplo observando la diferencia histórica entre el rendimiento de red simulado y efectivo.

Un sistema de clasificación de los fallos, un ejemplo del cual se representa en la Fig. 6, está configurado para determinar el tipo de fallo que provocó la discrepancia apreciando que fallos diferentes exhiben comportamientos respectivos diferentes. Aunque los comportamientos exhibidos por cada uno de los fallos pueden también superponerse (por ejemplo, tanto las fuentes de ruido como la caída de paquetes en los anfitriones incrementa las tasas de pérdida, el descenso de una ventana de competencia incrementa la cantidad de tráfico y por tanto incrementa el ruido de interferencia, etc.), los fallos pueden ordenarse por categorías verificando el respectivo comportamiento diferencial. Por ejemplo, una fuente externa de ruido incrementa los niveles de ruido experimentados por los nodos vecinos, pero no incrementa las velocidades de envío de cualquier nodo. Por consiguiente, la fuente externa de ruido puede ser diferenciada del comportamiento irregular del MAC y de la caída de paquetes en los anfitriones.

A continuación se hará de nuevo referencia a la Fig. 5. La exposición que sigue incluye paréntesis que incorporan un texto en letra cursiva los cuales describen indicaciones alternativas como se utilizan en el pseudocódigo ejemplar que se incluye en la exposición de las figuras relacionadas. En el bloque 502, el módulo de análisis selecciona uno

ES 2 279 479 T3

o más fallos entre una pluralidad de fallos, por ejemplo entre el directorio de fallos 318 de la Fig. 2. En una primera interacción del procedimiento 500, ninguno entre la pluralidad de fallos es seleccionado para derivar un rendimiento esperado de la red bajo condiciones operativas normales, esto es, sin fallos. En otra implementación, el procedimiento 500 de la Fig. 5 se utiliza para llevar a cabo un diagnóstico inicial y es no iterativo, esto es, es un procedimiento de “un paso”. En dicha implementación, el bloque 502 puede ser eliminado del procedimiento 500 y disponerse en el conjunto de fallos como un conjunto vacío { }.

En el bloque 504, el conjunto de fallos (FS) y los parámetros de red (NS) se suministran como entrada a una simulación de red. Pueden suministrarse múltiples parámetros de red, como por ejemplo potencia de la señal, estadística de tráfico, tablas de encaminamiento, etc.

En el bloque 506, el rendimiento esperado (SimPerf) se predice ejecutando la simulación de red con las entradas suministradas. En el bloque de decisión 506, se toma la decisión de si la diferencia (Diff) entre el rendimiento esperado (SimPerf) y el rendimiento real (RealPerf) es mayor que un umbral. Si la diferencia es mayor que el umbral (bloque 506), se determina (bloque 510) el tipo de fallo (TF). Una exposición adicional de la determinación de un tipo de fallo puede encontrarse en relación con la Fig. 6

Después de que se ha determinado el tipo de fallo, los fallos son situados (bloque 512) encontrando un conjunto de nodos y enlaces que tienen diferencias entre el rendimiento de red observado y esperado que exceda un umbral para un concreto tipo de fallo (bloque 514). El tipo de fallo determina qué métrica de rendimiento de red se utiliza para cuantificar la diferencia de rendimiento. Por ejemplo, una caída de paquetes puede ser identificada encontrando enlaces que tengan diferencias significativas entre las velocidades índices de pérdidas esperados y observados.

En el bloque 516, se determina la magnitud del fallo. Una función (designada como “g()”), por ejemplo, puede ser utilizada para trazar un mapa del impacto de un fallo en una correspondiente magnitud. Por ejemplo, en un escenario de caída de paquetes en anfitriones terminales, la función g() es una función de identidad, puesto que la diferencia en velocidad de pérdida de un enlace puede ser directamente trazada sobre el mapa respecto de un cambio de velocidad de caída de los paquetes sobre un enlace (magnitud del fallo). En un escenario de fallo de ruido externo, la función g() es una función de propagación de una señal de ruido. Los bloques 510 a 516 pueden ser repetidos para cada enlace o nodo. El fallo con una correspondiente magnitud puede entonces ser añadido al conjunto de fallos en la referencia 516.

La exposición que sigue representa un pseudocódigo ejemplar que puede ser ejecutado para implementar un procedimiento similar al procedimiento 500 de la Fig. 5, el cual se muestra como sigue:

```
suponiendo que NS designa los parámetros de red (p. ej., potencia de señal, estadística de tráfico, tabla de
encaminamiento)
suponiendo que RealPerf designa el rendimiento de red real
FaultSet = { }
Predict SimPerf ejecutando simulación con entrada (NS; FaultSet)
si | Diff (SimPerf , RealPerf) | > threshold
    determinar el tipo de fallo ft utilizando un árbol de decisión para cada enlace o nodo i
    si (| Diffa (SimPerf (i), RealPerf (i)) | > threshold)
        add fault (ft, i) with
            magnitud (i) = g (Diffft (SimPerf (i), RealPerf (i)))
```

El pseudocódigo describe un algoritmo de diagnóstico que puede ser utilizado para detectar si se ha producido un fallo. El siguiente procedimiento es un ejemplo de un algoritmo que puede utilizarse para determinar el tipo de fallo detectado.

La Fig. 6 es un diagrama de flujo que representa un procedimiento 600 en una implementación ejemplar en la cual un árbol de decisión es utilizado para determinar un tipo de fallo. El procedimiento 600 representado en la Fig. 6 puede o no corresponder al bloque 510 de la Fig. 5. En el bloque de decisión 602, se toma una determinación en cuanto a si el valor absoluto de una cantidad simulada de paquetes enviados (SimSent) menos una cantidad real de paquetes enviados (RealSent) es mayor que un umbral, designado como ThreshSentDiff. Si es así, se envía un fallo que indica que la ventana de competencia (CW) está fijada demasiado baja (bloque 604).

ES 2 279 479 T3

Si el umbral del bloque 602 no es sobrepasado, entonces en el bloque de decisión 606, se toma una determinación en cuanto a si hay una discrepancia esto es un diferencial de ruido de umbral, ThreshNoiseDiff, ha sido sobrepasado), entre el ruido real (RealNoise) indicado sobre la red real y el ruido esperado (SimNoise) de la red simulada. Si es así, se determina un fallo de ruido (bloque 608)

Si el umbral de ruido no ha sido sobrepasado (bloque 606) entonces, en el bloque de decisión 610, se toma una determinación en cuanto a si la pérdida de paquetes simulada (SimLoss), esto es, la pérdida de paquetes esperada, difiere de la pérdida de paquetes real (RealSim) en más de una diferencia de pérdida de umbral (ThreshLossDiff). Si es así, se ha tropezado con un fallo de caída de paquetes (bloque 612). En otro caso, el nodo está operando normalmente (bloque 614). Es evidente que puede también determinarse de manera similar una pluralidad de otros tipos de fallo.

La Fig. 7 es un diagrama de flujo que representa un procedimiento 700 en una implementación ejemplar en la cual fallos de diferentes tipos, uno respecto de otro, son diagnosticados utilizando un algoritmo iterativo de diagnóstico. En general, en una red puede tropezarse con múltiples fallos interactuantes. Aún cuando los fallos son del mismo tipo, puede tropezarse con interacciones, las cuales pueden hacer que resulte insuficiente un algoritmo de diagnóstico de un paso. Por consiguiente, puede implementarse, como se muestra en la Fig. 7, un algoritmo de diagnóstico iterativo para encontrar las causas originarias. El algoritmo incluye dos etapas: i) una etapa de diagnóstico inicial similar al procedimiento 500 de la Fig. 5, y ii) refinamientos iterativos.

Durante la etapa de diagnóstico inicial, un algoritmo de diagnóstico de un paso se aplica para derivar un conjunto inicial de fallos. Durante la segunda etapa, el conjunto de fallos es refinado de manera iterativa i) ajustando la magnitud de los fallos que han sido ya insertados dentro del conjunto de fallos, y ii) añadiendo un nuevo fallo al conjunto, en caso necesario. El procedimiento 700 puede ser reiterado hasta que el cambio en el conjunto de fallos sea desdeñable, por ejemplo cuando los tipos de fallo y los emplazamientos no cambian, las magnitudes del cambio de los fallos son cantidades mínimas, etc.

Una propuesta iterativa puede también utilizarse para buscar las magnitudes de los fallos. A un nivel alto, esta propuesta es similar a la simulación en base a enlaces, descrita en relación a la Fig. 5, en la que la diferencia entre los valores escogido como objetivo y actuales se utilizaron como retroalimentación para avanzar progresivamente hacia el blanco.

En el bloque 702, por ejemplo, el rendimiento de red esperado se estima con arreglo al conjunto de fallos existente para cada iteración. Por ejemplo, el rendimiento de red esperado puede ser estimado mediante simulación de la red que utiliza los parámetros de red obtenidos a partir de la red real. Los parámetros de red se suministran mediante la ejecución de los módulos agente sobre cada nodo. Los parámetros de red suministrados por cada nodo pueden describir el rendimiento de red local del nodo así como el rendimiento de red de los nodos vecinos.

En el bloque 704, se computa la diferencia entre el rendimiento de red estimado (con arreglo al conjunto de fallos existente) y el rendimiento real. La diferencia, por ejemplo, puede ser computada por un nodo gestor mediante la ejecución de un módulo gestor. El módulo gestor, una vez ejecutado, compara el rendimiento de red estimado (esto es, esperado) obtenido a partir de la red simulada con un rendimiento de red real (esto es, observado) tal como se indica mediante los parámetros de red adicionales obtenidos de la pluralidad de agentes.

El procedimiento 700 de la Fig. 7 primero hace un diagnóstico de fallos inicial de modo similar al procedimiento 500 descrito en relación con la Fig. 5. En el bloque de decisión 706, por ejemplo, se toma una determinación en cuanto a si la diferencia computada es mayor que un umbral correspondiente. Si no, el conjunto de fallos es transmitido (bloque 708). En este ejemplo, debido a que la diferencia computada no es mayor que el umbral, ello indica al módulo de análisis que la red está operando normalmente. Sin embargo, si la diferencia computada es mayor que el umbral correspondiente (bloque 706), se determina el tipo de fallo (bloque 710). El tipo de fallo puede determinarse de varias maneras, de lo cual se describe un ejemplo en relación con la Fig. 6.

En el bloque 712, la diferencia se traduce en un cambio en las magnitudes del fallo y las magnitudes del fallo son ajustadas de acuerdo con el cambio computado (bloque 714). Por ejemplo, la función $g()$, como se expuso anteriormente con relación a la Fig. 5, puede ser utilizada para computar una magnitud de fallo para cada uno de los fallos en base a las respectivas diferencias entre el rendimiento de red esperado y real. De esta forma, los fallos pueden ser comparados uno con otro, para determinar qué fallo tiene un efecto sobre el rendimiento de la red que se corresponda con la discrepancia observada. En una implementación, la magnitud de fallo mayor se utiliza primeramente para explicar la discrepancia, y de esta forma identificar un fallo concreto que provocó la discrepancia. En otra implementación, las magnitudes de los fallos se comparan para localizar un fallo que se traduzca en una diferencia que aproxime la diferencia computada. Por ejemplo, cada pluralidad de fallos puede tener diferencias respectivas entre el rendimiento de red esperado y real. Uno o más de los fallos puede ser seleccionado adaptando las respectivas diferencias con la diferencia computada en el rendimiento de red. En el bloque 716 son eliminados los fallos con magnitudes que estén por debajo de un umbral correspondiente, optimizando de esta manera el conjunto de fallos.

En el bloque de decisión 718 se toma una determinación en cuanto a si el rendimiento esperado de la red que utiliza el conjunto de fallos actual es convergente con el rendimiento de red real. Por ejemplo, el módulo de análisis puede almacenar datos heurísticos que describan una o más iteraciones previas de conjuntos de fallos y los valores de rendimiento resultantes de la simulación de red. La diferencia entre los valores escogido como objetivo (esto es, los

ES 2 279 479 T3

valores de rendimiento de red reales) y los valores actuales (esto es, los valores de rendimiento de red simulados) se utiliza como retroalimentación por el modulo de análisis para progresivamente “desplazar” la simulación de red para aproximarse la red real.

5 Si el rendimiento esperado no es convergente con el rendimiento de red real (bloque 718), un nuevo candidato de fallo se añade al conjunto de fallos. Además de buscar las magnitudes correctas de los fallos, por ejemplo, la pertenencia al conjunto de fallos puede ser iterativamente refinada seleccionando nuevos candidatos de fallo que puedan explicar de manera óptima la diferencia entre el rendimiento de red esperado y el real (bloque 720). Estos nuevos fallos son añadidos al conjunto de fallos (bloque 722). El conjunto de fallos que incluye el nuevo candidato de
10 fallo es entonces utilizado como entrada para una simulación de red y para estimar el rendimiento de red esperado con arreglo al conjunto de fallos existente (bloque 702). En una implementación, un fallo es añadido durante cada iteración del procedimiento 700 el cual puede explicar la mayor discrepancia, controlando de esta forma falsos positivos. El procedimiento 700 puede entonces ser repetido hasta que el rendimiento esperado de la red simulada se aproxime al rendimiento real de la red real. De esta forma, la red simulada puede ser desplazada mediante la inclusión de fallos,
15 de manera que proporcione una representación precisa de los fallos que provocan el rendimiento de red observado en la red real.

La exposición siguiente ilustra un pseudocódigo ejemplar que puede ser utilizado para obtener el procedimiento 700 de la Fig. 7.

20 1) supongamos que NS designa los parámetros de red
(p. ej., potencia de señal, estadística de tráfico, y tablas de encaminamiento)
25 supongamos que RealPerf designa el rendimiento de red real
2) FaultSet = { }
3) Predecir SimPerf ejecutando simulación con la entrada (NS; FaultSet)
30 4) Si $| \text{Diff} (\text{SimPerf}, \text{RealPerf}) | > \text{threshold}$
ir a (5)
35 si no
ir a (7)
40 5) Diagnostico inicial: inicializar FaultSet aplicando el algoritmo de la Fig. 5
6) Mientras que (no sea convergido)
a) ajustar magnitud de fallo
45 para cada tipo de fallo f_t en FaultSet (en el orden del árbol de decisión en la Fig. 6).
para cada fallo i en (FaultSet, f_t)
magnitud (i) = $g (\text{Diff}_{f_t} (\text{SimPerf} (i), \text{RealPerf} (i)))$
50 si $(| \text{magnitud} (i) | > \text{threshold})$
suprimir el fallo (f_t, i)
55 b) añadir nuevo candidato a fallos, en caso necesario
para cada tipo de fallo f_{tt} (en el orden del árbol de decisión de la Fig. 6)
i) encontrar un fallo i s.t. no está en Faultset y tiene el mayor $| \text{Diff}_{f_t} (\text{SimPerf} (i); \text{RealPerf} (i)) |$
60 ii) si $| \text{Diff}_{f_t} (\text{SimPerf} (i), \text{RealPerf} (i)) | > \text{threshold}$
añadir (f_t, i) para FaultSet whit $\text{magnitud} (i) = g (\text{Diff}_{f_t} (\text{SimPerf} (i), \text{RealPerf} (i)))$
65 c) simular
7) Transmitir FaultSet

Así, el pseudocódigo expuesto describe un algoritmo de diagnóstico ejemplar que está configurado para diagnosticar fallos de múltiples tipos.

Eliminando Errores en los Datos de Traza

5

En las secciones anteriores, se describió un diagnóstico de fallo en el cual los datos de traza se utilizaron para activar una simulación en línea. En la práctica, los datos en bruto de la traza que son recogidos por los módulos agente, una vez ejecutados sobre los respectivos nodos, pueden contener errores por varias razones de acuerdo con lo anteriormente expuesto, debido por ejemplo a errores en el hardware, software y/o de la red. Por consiguiente, el módulo de limpieza 120 (N) de la Fig. 1 puede ser ejecutado para limpiar los datos de traza “en bruto” recibidos por la pluralidad de agentes para proporcionar unos datos de traza limpios como entrada al simulador 118 (N) para un diagnóstico de los fallos.

10

La Fig. 8 es una ilustración de una red 800 en una implementación ejemplar en la cual la pluralidad de nodos 102 (1) - 102 (N) de la Fig. 1 incluye unos módulos agente que son ejecutables para llevar a cabo la verificación de los vecinos. Los módulos agente son ejecutados sobre cada uno de los nodos en la verificación de vecinos de rendimiento de red, que es una técnica en la cual cada uno de la pluralidad de nodos 102 (1) - 102 (N) informa del rendimiento y de la estadística del tráfico no solo para sus propios enlaces entrantes/salientes, sino también para otros enlaces existentes dentro de su ámbito de comunicación. La verificación de vecinos puede llevarse a cabo de diversas formas. Por ejemplo, un módulo agente sobre un primer nodo puede ser ejecutado para examinar un segundo nodo en la red para obtener unos datos de rendimiento de red por parte del segundo nodo. En otro ejemplo, el primer nodo recibe una comunicación del segundo nodo, como por ejemplo un pronóstico, que incluye los datos de rendimiento de red. En un ejemplo adicional, el primer nodo verifica los datos enviados por el segundo nodo para su comunicación a través de la red para verificar el rendimiento de red. El primer nodo, por ejemplo, puede operar de un modo “promiscuo” que permita que un dispositivo de conexión a la red del nodo intercepte y lea cada paquete de datos que llega en ese particular nodo en su totalidad.

25

Debido a la verificación de vecinos, múltiples informes, procedentes de diferentes fuentes (esto es, nodos) son susceptibles de ser presentados en cada enlace. El nodo 102 (3), por ejemplo, puede obtener un informe 802 (2) del nodo 102 (2) que describa la prestación de red del nodo 102 (2), así como el rendimiento de red de los nodos 102 (1), 102 (n). Los paréntesis utilizados en los nodos de referencia de los informes en la Fig. 8 están seleccionados para mostrar la correspondencia del informe con su respectivo nodo, por ejemplo, el nodo 102 (2) y el informe 802 (2).

35

El nodo 102 (3) incluye los datos de rendimiento de red procedentes del informe 802 (2) (el cual se ilustra en línea de puntos en la Fig. 8) en el informe 802 (3) que se forma para su comunicación al nodo gestor 102 (N). El informe 802 (3) puede también incluir datos de rendimiento de red obtenidos por el nodo 102 (3) por los nodos de verificación 102 (2), 102 (1). En una implementación, el informe 802 (3) es optimizado mediante la ejecución de un módulo agente para eliminar la información redundante. Por ejemplo, el módulo agente del nodo 102 (3) puede eliminar la información que sea coherente y repetida por los nodos 102 (2), 102 (3) en los respectivos informes 802 (2), 802 (3), pero mantener los datos que describen cualquier incoherencia de los datos. Así mismo, el nodo 102 (n) puede ejecutar el módulo de recogida 114 (n) para obtener unos datos de rendimiento de red de los nodos 102 (2), 102 (3). Los datos de rendimiento de red están configurados como informe 802 (n) para su comunicación al nodo gestor 102 (N).

40

Los informes redundantes pueden utilizarse por el nodo gestor 102 (N) para detectar una o más incongruencias en el rendimiento de red. Por ejemplo, los informes 802 (2), 802 (3) pueden ser comparados entre sí mediante la ejecución del módulo de limpieza 120 (N) por el nodo gestor 102 (N) para encontrar las incongruencias en los datos de rendimiento de red descritos dentro de aquél. Las incongruencias pueden encontrarse de diversas maneras, un ejemplo de las cuales se describe en la figura siguiente.

45

La Fig. 9 es un diagrama de flujo que representa un procedimiento 900 en una implementación ejemplar en el cual los informes que describen los nodos vecinos son comparados para localizar un nodo de comportamiento irregular dentro de una red. En esta implementación, el procedimiento 900 identifica los nodos de comportamiento irregular como el conjunto de nodos mínimo que puede explicar la discrepancia de los informes.

55

El procedimiento 900 descrito en relación con la Fig. 9, un nodo de envío i informa de un número de paquetes enviados y de un número de acuses de recibo de nivel MAC recibidos para un enlace dirigido 1 como $(sent_i(1), ack_i(1))$. Un nodo de recepción j informa del número de paquetes recibidos en el enlace designado como $recv_j(1)$. Así mismo, un vecino k inmediato del nodo de envío o recepción informa también del número de paquetes y de los acuses de recibo en el nivel MAC que son enviados o recibidos sobre el enlace, indicados como $(sent_k(1), recv_k(1), ack_k(1))$. Una incongruencia en los informes se define como uno de los casos siguientes.

60

En el bloque de decisión 902, se toma una determinación en cuanto a si un número de paquetes recibido sobre un enlace, tal como se informa mediante su destino, es significativamente mayor (tal como se describe mediante un umbral) que el número de paquetes enviados sobre el mismo enlace, de acuerdo con lo informado por su fuente. Esto es, para el enlace 1 desde el nodo i hasta el nodo j , y dado un umbral t , se lleva a cabo la siguiente determinación:

65

$$recv_j(1) - sent_i(1) > t$$

ES 2 279 479 T3

el umbral t es utilizado, dado que la comunicación de los informes por los respectivos nodos no está típicamente sincronizada. Si el número de paquetes recibidos es significativamente mayor que el número de paquetes enviados, entonces se detecta una incongruencia en los informes, lo que se describirá con mayor detalle con relación al bloque 912. Si los números de los paquetes recibidos y enviados por los respectivos nodos se corresponden, entonces el procedimiento 900 progresa hasta el bloque 904.

En el bloque de decisión 904, se toma una determinación acerca de si un número de acuses de recibo de nivel MAC transmitido sobre un enlace, como transmitidos por su fuente, se corresponde con un número de paquetes recibidos sobre ese enlace, como transmitidos por su destino. En otras palabras, para el enlace l desde el nodo i hasta el nodo j , y dado un umbral t , se determina lo siguiente:

$$| \text{ack}_i(l) - \text{rcv}_j(l) | > t$$

así, si el número de acuses de recibo no se corresponde, (esto es se aproxima) al número de paquetes recibidos (bloque 904), entonces se aprecia una incongruencia en los informes. Si los números de los acuses de recibo y de los paquetes recibidos se corresponden (bloque 904), entonces el procedimiento 900 progresa hasta el bloque 906.

En el bloque de decisión 906, se toma una determinación en cuanto a si un número de paquetes recibidos sobre un enlace, según se transmitió por un vecino de su destino, es significativamente mayor que el número de paquetes enviados sobre el enlace, según se transmitió por su fuente. Esto es, para el enlace l desde el nodo i hasta el nodo j , en el cual el vecino del nodo j es el nodo k , y dado un umbral t , se determina lo siguiente:

$$\text{rcv}_k(l) - \text{sent}_i(l) > t$$

así, si el número de paquetes recibidos se corresponde (esto es, se aproxima) al número de paquetes enviados (bloque 906), entonces se consigna una incongruencia en los informes. En otro caso el procedimiento 900 continúa hasta el bloque 908.

En el bloque de decisión 908, se toma una determinación en cuanto a si un número de paquetes enviados sobre un enlace, según se transmitió mediante un vecino de su fuente, es significativamente mayor que un número de paquetes enviados sobre el mismo enlace, según lo transmitido por su fuente. En otras palabras, para el enlace l desde el nodo i hasta el nodo j , en el cual el nodo el vecino de k es el nodo i y dado un umbral t , se determina lo siguiente:

$$\text{sent}_k(l) - \text{sent}_i(l) > t$$

como se muestra en la ecuación, si el número de paquetes enviados se aproxima al número de paquetes enviados (bloque 908), según lo indicado, respectivamente, por los nodos de fuente y vecinos, entonces se observa una incongruencia en los informes. En otro caso, los informes son congruentes (bloque 910).

En el bloque de decisión 912 se adopta una determinación en cuanto a si un par incongruente de nodos está ya incluido en el gráfico de incongruencia. Si no, los nodos son añadidos a un gráfico de incongruencia (bloque 914). Si el par incongruente de nodos está ya en el gráfico de incongruencia (bloque 912) o ha sido añadidos al gráfico de incongruencia (bloque 912), un borde es añadido entre los nodos en el gráfico de incongruencia (bloque 916).

Después de que han sido identificados cada uno de los pares incongruentes, a continuación, en el bloque 918 un conjunto más pequeño (esto es, un número menor) de nodos se encuentra en el gráfico de incongruencia que puede explicar las incongruencias explicadas. Por ejemplo, se puede adoptar la presunción de que la mayoría de los nodos de la red envían informes fiables. Por consiguiente, se puede encontrar el conjunto más pequeño de nodos que puede explicar las incongruencias explicadas. Esto puede conseguirse, por ejemplo, encontrando el conjunto más pequeño de vértices que cubra el gráfico incongruente, donde los vértices identificados representan los nodos de comportamiento irregular.

El conjunto más pequeño de vértices puede encontrarse mediante la utilización de un problema de recubrimiento de vértices mínimo, que es conocido como NP duro protector de la red. Un algoritmo voraz es aplicado, el cual repetidamente pica y retira el nodo con la mayoría de los bordes y de los bordes incidentes respecto de un gráfico de incongruencia actual hasta que no quedan bordes.

Un historia de informes puede utilizarse para mejorar en mayor medida la precisión de la detección de incongruencias. Por ejemplo, en el bloque 920 puede añadirse un nuevo informe para poner al día el gráfico de incongruencias sin suprimir la información anterior. Los pares incongruentes de nodos del nuevo informe pueden entonces ser procesados utilizando los bloques 912 a 918 del procedimiento 900. Por ejemplo, el mismo algoritmo voraz del bloque 918 puede ser reaplicado para identificar los nodos de comportamiento irregular.

Análisis ¿Qué Pasaría Si ...?

En las secciones previas, se inyectaron selectivamente unos fallos en una simulación de red para identificar qué fallos, caso de existir, pueden haber provocado una diferencia entre el comportamiento de la red esperado y observado. La simulación de red puede también ser utilizada para llevar a cabo un análisis “¿Qué pasaría si ...?” para mejorar el funcionamiento de la red. El análisis ¿Qué pasaría si ...? posibilita que el módulo gestor, una vez ejecutado, determine el efecto de posibles diferentes configuraciones de los nodos y de la red sobre el rendimiento de la red. El resultado del análisis ¿Qué pasaría si ...? es un conjunto de acciones que permite que el módulo gestor opere la red de manera eficiente, por ejemplo, haciendo que el módulo agente sobre los nodos seleccionados dentro de la red configure el nodo respectivo de acuerdo con ello.

El análisis ¿Qué pasaría si ...?, por ejemplo, puede llevarse a cabo mediante el uso de una simulación en línea activada por trazas, según lo anteriormente descrito. Las trazas ejemplares son identificadas en la exposición que sigue en las cuales pueden determinar que las recogidas activen el simulador (por ejemplo, el simulador 118 (N) de la Fig. 2). Por ejemplo, el simulador puede ser utilizado para suministrar una simulación de red de una red real. La simulación de red puede ser reconfigurada para probar diferentes configuraciones de red y nodos y determinar qué configuración produce el mejor comportamiento global de la red con respecto a las condiciones existentes del tráfico. El módulo gestor puede entonces determinar un conjunto de acciones para su implementación mediante nodos concretos dentro de la red en base a la configuración.

Las técnicas tradicionales que fueron empleadas para el análisis ¿Qué pasaría si ...?, empleaban modelos de red simplificados y derivaban analíticamente el comportamiento esperado. La simulación en línea activada por trazas, sin embargo, tiene ventajas respecto del análisis teórico porque el uso de un simulador ofrece una comprensión mejorada del comportamiento de la red de lo que puede conseguir por sí misma la técnica teórica o heurística. Por ejemplo, una red inalámbrica operativa es un sistema complejo con muchas piezas intrincadas incluyendo flujos de tráfico, protocolos integrados en la red, algoritmos de procesamiento de señales, hardware, propagación de RF, y sobre todo la interacción entre cada una de estas piezas. Así mismo, el comportamiento de la red puede estar determinado por la interacción entre nodos con un alcance mutuo y por las fuentes de ruido de las inmediaciones. Ni las técnicas teóricas ni las heurísticas captan el comportamiento de dichas redes y las interacciones entre los diferentes componentes.

La Fig. 10 es un diagrama de flujo que representa un procedimiento 1000 en una implementación ejemplar en la cual el análisis ¿Qué pasaría si ...? se lleva a cabo en base a una simulación en línea activada por trazas. En un nivel alto, el procedimiento 1000 reproduce primero una red real que usa una simulación de red. Las consecuencias de modificaciones en la red, al ser aplicadas a la red real, son entonces determinadas aplicando aquellos cambios en la simulación de red para cuantificar las simplificaciones en el comportamiento de la red.

En el bloque 1002, se selecciona una o más entre una pluralidad de modificaciones, mediante la ejecución del módulo gestor. Las modificaciones pueden seleccionarse de diversas formas. Por ejemplo, las modificaciones pueden ser consideradas por el módulo gestor como un fallo que provoca un incremento en lugar de un decremento en el comportamiento de la red. En este caso las modificaciones pueden ser almacenadas en el directorio de fallos 218 de la Fig. 2 y dispuestos en base a tipo. En el bloque 1004, el módulo de análisis proporciona unos parámetros de red de una red real y un conjunto de modificaciones que incluye las modificaciones seleccionadas en una simulación de red como entrada.

En el bloque 1006, el rendimiento esperado de la red es predicho en base a las entradas. Por ejemplo, el simulador puede crear una simulación de red en base a los parámetros de la red de red real y del conjunto de modificaciones. La simulación de red, según lo anteriormente descrito, puede entonces ser utilizada para determinar las consecuencias de las modificaciones sobre la red real.

En el bloque de decisión 1008, se toma una determinación en cuanto a si la diferencia entre el rendimiento esperado de la simulación de red y el rendimiento real de una red real es mayor que un umbral. La simulación de red, por ejemplo, puede proporcionar una salida de los valores de comportamiento de red simulados que son comparados con los valores de rendimiento de red reales obtenidos a partir de los módulos agente 122 (n) de la Fig. 1. Si la diferencia entre el rendimiento de red esperado real es inferior que el umbral (bloque 1008), puede seleccionarse una nueva modificación (bloque 1002) y determinarse el efecto de la modificación según lo anteriormente descrito.

El módulo de análisis, una vez ejecutado, deriva una o más acciones que van a realizarse con módulos agente de la red para implementar la modificación (bloque 1008). El módulo de análisis, por ejemplo, puede incluir un directorio de acciones que se representa gráficamente incorporando las correspondientes modificaciones. El módulo de análisis puede entonces obtener las correspondientes acciones en base a las modificaciones.

En el bloque 1010, el módulo de análisis constituye una comunicación que describe las una o más acciones para su comunicación a los correspondientes módulos agente. Los correspondientes módulos agente pueden entonces provocar que los respectivos nodos de la red implementen las acciones descritas dentro de aquellos. Así, los módulos gestor y agente pueden ser utilizados para efectuar un análisis ¿Qué pasaría si ...? en base a la simulación en línea activada por trazas de manera similar a la detección de fallos. El análisis ¿Qué pasaría si ...? puede ser utilizado para corregir fallos y mejorar en rendimiento de la red.

En otra implementación ejemplar, la simulación se utiliza para determinar una modificación que va a efectuarse sobre una red para mejorar el rendimiento de la red, por ejemplo utilizando una propuesta iterativa para efectuar el análisis ¿Qué pasaría si ...?. Esta propuesta es similar a la simulación descrita en relación con las Figs. 5 y 7. Así, el refinamiento de la iteración podría ser utilizado cuando se necesitarán múltiples acciones de modificación.

5

La Fig. 11 es un diagrama de flujo que representa un procedimiento 1100 en una implementación ejemplar en la cual las modificaciones en una red se derivan en base a un diagnóstico de un flujo perjudicial. En el bloque 1102, un módulo gestor (por ejemplo un módulo gestor 116 (N) de las Figs. 1 y 2) se ejecuta para determinar que uno o más flujos de una red están experimentando unos valores de rendimiento total inferiores que sus correspondientes valores de rendimiento total elegidos como objetivo esperados. En el bloque 1104, el módulo gestor determina cuáles, caso de existir, de los flujos de la red son un “flujo perjudicial”. Un flujo perjudicial es un tipo de fallo cuya presencia provoca una seria degradación en el rendimiento total de la red, y es diferente de los fallos previos en el sentido de que el flujo perjudicial puede ser en sí mismo sano, pero no interactúa bien con otros flujos en competencia.

10

En el bloque 1106, por ejemplo, los parámetros de red son recogidos y describen las solicitudes de extremo a extremo escogidas como objetivo y el protocolo de encaminamiento que está en uso. Debe destacarse que estos parámetros de red pueden ser diferentes de las trazas utilizadas para la depuración, porque el procedimiento 1100 examina cómo la red (por ejemplo, las cargas de enlaces y el encaminamiento) reaccionarán a los cambios en la configuración de la red.

15

20

En el bloque 1108, el efecto sobre el rendimiento total agregado de la red es examinado en base a la eliminación, de uno en uno, de cada flujo respecto de una simulación de red. En una implementación, un flujo perjudicial es identificado como el flujo cuya eliminación produce la mejora global más significativa en el rendimiento de la red. Por ejemplo, una red 1200 se muestra en la Fig. 12 incluyendo una pluralidad de flujos 1202 a 1216. El flujo ocho 1216 (ilustrado como F_8 en la Fig. 12) cruza cada uno de los demás flujos 1202 a 1214 en la red ilustrada 1200. Por consiguiente, la eliminación del flujo ocho 1208 puede dar como resultado el mayor incremento en el rendimiento final, por oposición a la eliminación de cualquiera de los demás flujos 1202 a 1214. En otras palabras, la presencia del flujo ocho 1216 provoca la mayor cantidad de daño en el rendimiento de la red 1200. De esta forma, puede determinarse una modificación (por ejemplo la eliminación o reducción de la influencia del flujo ocho 1216 sobre los demás flujos del sistema) en la red 1200, lo que se traduce en el mayor incremento en el rendimiento de la red.

25

30

En el bloque 1110, una o más acciones son derivadas en base a la modificación que puede utilizarse para mejorar el rendimiento de la red. Acciones ejemplares pueden incluir limitación de velocidad, reencaminamiento, y control de la topología del flujo ocho 1216. La simulación de red posibilita que el módulo gestor evalúe también con precisión el beneficio de estas acciones. Por ejemplo, la tabla siguiente muestra un caudal esperado para unas acciones correctoras ejemplares.

35

40

Acción	Caudal total (Mbps)
Inacción	1,064
Reducir la velocidad del flujo ocho en la mitad	1,148
Encaminar flujo ocho vía frontera de malla	1,217
Incrementar transmisión de potencia hasta 20 dBm	0,990
Incrementar transmisión de potencia hasta 25 dBm	1,661

45

50

Como se muestra en la tabla, un incremento en la potencia de transmisión de hasta 25 dBm produce el mayor caudal entre las cuatro acciones ejemplares (y una inacción) objeto de consideración, puesto que reduce el número de reflejos requeridos para alcanzar un destino. En base a estos resultados, el módulo gestor constituye una comunicación que provoca que uno o más de los agentes en los respectivos nodos incremente la potencia para paliar el problema de rendimiento de la red.

55

60 *Implementación de Estructura Ejemplar*

Un ejemplo de la estructura descrita ha sido implementada en una plataforma WINDOWS XP (WINDOWS XP es una marca de Microsoft Corp., Redmond WA). En esta sección se describen componentes de la implementación ejemplar, principios de diseño, y sus características.

65

La estructura ejemplar en este caso incluye dos componentes separados: módulos agente y módulos gestor. Según lo anteriormente descrito en relación con la Fig. 1, el módulo agente es ejecutado en cada nodo de la red para transmitir

ES 2 279 479 T3

datos locales, ya sea periódicamente o tras petición. Un módulo gestor recoge los datos relevantes procedentes de los módulos agente y es ejecutado para analizar los datos, por ejemplo mediante ejecución de un módulo de análisis incluido según lo descrito en la Fig. 2.

5 La estructura ejemplar emplea principios de diseño de simplicidad y extensibilidad, por ejemplo, los datos agrupados y propagados para su verificación y gestión pueden formularse en contadores de rendimiento soportados en WINDOWS (WINDOWS, es una marca de Microsoft Corp., Redmond WA). Los contadores de rendimiento pueden suministrarse como (nombre, valor) pares agrupados por categorías.

10 La estructura descrita es también extensible. La adición a los datos que están siendo verificados implica la creación de una nueva categoría de contadores de rendimiento y la escritura de un módulo que ponga al día los valores del contador de rendimiento a medida que la información cambia. Los datos de rendimiento relacionados con el protocolo de control de transmisión (TCP), con el protocolo de datagrama de usuario (UDP), con el protocolo de Internet (IP), y con la interfaz de programación de aplicación a distancia de estaciones de trabajo (WRAPI) pueden incorporarse en
15 la estructura con poco trabajo adicional.

Los valores de estos contadores de rendimiento pueden ser de solo lectura o que pueden escribirse. Los contadores que pueden escribirse, por ejemplo, ofrecen un modo de que un nodo gestor autorizado cambie los valores e inflencie el comportamiento de un nodo con el fin de fijar problemas e iniciar experimentos a distancia, como por ejemplo mediante la comunicación de un módulo gestor con un módulo agente que esté siendo ejecutado sobre nodos respectivos
20 diferentes.

Cada nodo gestor puede también estar equipado con una interfaz gráfica de usuario (GUI) 1300 del que se ilustra un ejemplo en la Fig. 13, para interactuar con los administradores de la red. La GUI posibilita que un administrador visualice la red así como emita solicitudes de gestión a través del módulo gestor. La GUI 1300 despliega una topología para un banco de pruebas ejemplar de la red. La GUI 1300 en este caso representa una ventana de gestor con agentes desplegados sobre un banco de pruebas de 23 nodos. El módulo gestor puede desplegar la topología en base a las coordenadas relativas de los nodos, ya sea directamente obtenidos o inferidos. La GUI 1300 puede también permitir que el administrador cierre zoom sobre una parte concreta de la red para una información más detallada y para pinchar sobre un enlace para obtener una representación de los datos del rendimiento de la red acerca de un enlace concreto en un formato de tabla.
25
30

35

40

45

50

55

60

65

REIVINDICACIONES

1. Procedimiento para la detección y diagnóstico de fallos en una red que comprende:

5 detectar una discrepancia en el funcionamiento de una red mediante:

el suministro de datos que describan la red a una simulación de red (210) para que la simulación de red proporcione una estimación del rendimiento de red (504); y

10 la determinación de si la estimación del rendimiento de red difiere del rendimiento de red observado de la red (508); y

15 el diagnóstico de una causa originaria de la discrepancia inyectando uno o más fallos de una pluralidad de fallos en la simulación de red hasta que la estimación del rendimiento de red se aproxime al rendimiento de red observado (510, 512, 514, 516).

20 2. Procedimiento según lo descrito en la reivindicación 1, en el que la determinación incluye verificar si la estimación del rendimiento de red difiere del rendimiento de red observado de la red en más de un correspondiente umbral.

3. Procedimiento según lo descrito en la reivindicación 1, en el que el diagnóstico incluye:

traducir la diferencia entre los rendimientos esperado y observado de red en una magnitud de fallo; y

25 determinar si la magnitud de fallo desplaza la simulación de red hasta aproximar el rendimiento de red observado de la red.

4. Procedimiento según lo descrito en la reivindicación 1, en el que el diagnóstico incluye:

30 trasducir la diferencia entre los rendimientos de red estimados y observados en una magnitud de fallo;

determinar si la magnitud de fallo es inferior a un correspondiente umbral; y

35 cuando la magnitud de fallo es inferior al correspondiente umbral, suprimir dicho fallo correspondiente del conjunto de fallos utilizado como entrada para la simulación de red.

5. Procedimiento según lo descrito en la reivindicación 1, en el que el diagnóstico incluye:

40 efectuar un diagnóstico inicial para generar un conjunto inicial de fallos; y

refinar de manera iterativa el conjunto inicial de fallos para llegar a un conjunto actual de fallos que, cuando se utilizan como entrada por la simulación de red, provoca la estimación del rendimiento de red suministrado por la simulación de red para aproximar el rendimiento de red observado.

45 6. Procedimiento según lo descrito en la reivindicación 1, en el que la red es una red inalámbrica multirreflejo.

7. Procedimiento según lo descrito en la reivindicación 1, en el que la red es una red alámbrica.

50 8. Procedimiento según lo descrito en la reivindicación 1, en el que los datos describen un camino formado por una serie de reflejos tomados por un paquete de datos a través de la red entre un nodo originario y un nodo objetivo de la red.

55 9. Procedimiento según lo descrito en la reivindicación 1, en el que los datos incluyen datos de traza que son seleccionados entre el grupo compuesto por:

una topología de red incluyendo encaminamientos;

una estadística de tráfico, un medio físico; y

60 un rendimiento de red.

65 10. Uno o más medios legibles por computadora que comprenden unas instrucciones ejecutables por computadora que, una vez ejecutadas por una computadora, dirigen la computadora para llevar a cabo el procedimiento de la reivindicación 1.

11. Sistema para la detección y diagnóstico de fallos en una red que comprende una pluralidad de nodos (102) que están comunicativamente acoplados, uno con otro, para formar dicha red, en el que:

ES 2 279 479 T3

uno o más de dichos nodos incluye un módulo agente (112 (N)) que es ejecutable sobre él para:

recoger los parámetros de red; y

5 establecer una comunicación que incluya los parámetros de red para su comunicación sobre la red; y

al menos dicho nodo incluye un módulo gestor (116 (N)) que es ejecutable sobre él para:

recibir la comunicación

10 generar una simulación de la red en base a los parámetros de red obtenidos de la comunicación para que la simulación de red proporcione una estimación del rendimiento de red; y

15 detectar un fallo (510, 512, 514, 516) en el funcionamiento de la red comparando una estimación del rendimiento de red con una observación de rendimiento de red de la red (508).

12. Sistema según lo descrito en la reivindicación 11, en el que al menos dichos dos nodos incluyen un respectivo dicho módulo gestor.

20 13. Sistema según lo descrito en la reivindicación 11, en el que cada dicho nodo incluye un respectivo dicho módulo agente.

14. Sistema según lo descrito en la reivindicación 11, en el que el módulo gestor es así mismo ejecutable para:

25 derivar una acción correctora en base al fallo detectado; y

provocar que el módulo agente lleve a cabo la acción correctora.

30 15. Sistema según lo descrito en la reivindicación 11, en el que el fallo en el funcionamiento de la red es detectado determinando si una diferencia entre la estimación y la observación es mayor que un correspondiente umbral.

35 16. Sistema según lo descrito en la reivindicación 11, en el que el módulo gestor es así mismo ejecutable para diagnosticar el fallo inyectando uno o más entre una pluralidad de dichos fallos en la simulación de red hasta que la estimación se aproxime a la observación.

17. Sistema según lo descrito en la reivindicación 11, en el que el módulo gestor es así mismo ejecutable para diagnosticar el fallo mediante:

40 la traducción de una diferencia entre la estimación y la observación de una magnitud de fallo; y

la determinación de si la magnitud de fallo desplaza la estimación proporcionada por la simulación de red para aproximar la observación.

45 18. Sistema según lo descrito en la reivindicación 11, en el que el módulo gestor es así mismo ejecutable para diagnosticar el fallo mediante:

la traducción de una diferencia entre la estimación y la observación en una magnitud de fallo; y

50 la determinación de si la magnitud de fallo es inferior a un correspondiente umbral; y

cuando la magnitud de fallo es inferior a la del correspondiente umbral, eliminar dicho correspondiente fallo de un conjunto de fallos que se utiliza como entrada por la simulación generada para producir la estimación.

55 19. Sistema según lo descrito en la reivindicación 11, en el que el módulo gestor es así mismo ejecutable para diagnosticar el fallo mediante:

la realización de un diagnóstico inicial para generar un conjunto inicial de fallos;

60 el refinamiento de manera iterativa del conjunto inicial de fallos para llegar a un conjunto de fallos en curso que, cuando se utilizan como entrada por la simulación de red, provoquen que la estimación se aproxime a la observación.

20. Sistema según lo descrito en la reivindicación 11, en el que la red es una red en malla.

65 21. Sistema según lo descrito en la reivindicación 11, en el que los parámetros de red describen un camino formado por una serie de reflejos adoptados por un paquete de datos a través de la red entre dicho nodo originario y dicho nodo objetivo de la red.

ES 2 279 479 T3

22. Nodo (102) de una red que tiene unos medios para la detección y el diagnóstico de fallos en dicha red, comprendiendo dicho nodo:

5 un medio para la operación (102 (N)) de gestión de una red que tiene una pluralidad de medios para encaminar paquetes de datos, en el que:

cada uno de dichos medios de encaminamiento está acoplado de manera comunicativa con otro de dichos medios de encaminamiento; y

10 el medio de gestión incluye así mismo un medio para suministrar los parámetros de red obtenidos de la red a un medio para simular la red (210);

recibir una salida del medio de simulación el cual estima el rendimiento de red de la red; y

15 detectar un fallo (510, 512, 514, 516) comparando la salida con una observación del rendimiento de red de la red (508).

23. Nodo según lo descrito en la reivindicación 22, en el que el medio de gestión incluye así mismo un medio para diagnosticar el fallo.

20 24. Nodo según lo descrito en la reivindicación 22, en el que la red es una red en malla.

25 25. Nodo según lo descrito en la reivindicación 22, en el que el medio de gestión incluye así mismo un medio para derivar una acción correctora en base al fallo detectado.

30

35

40

45

50

55

60

65

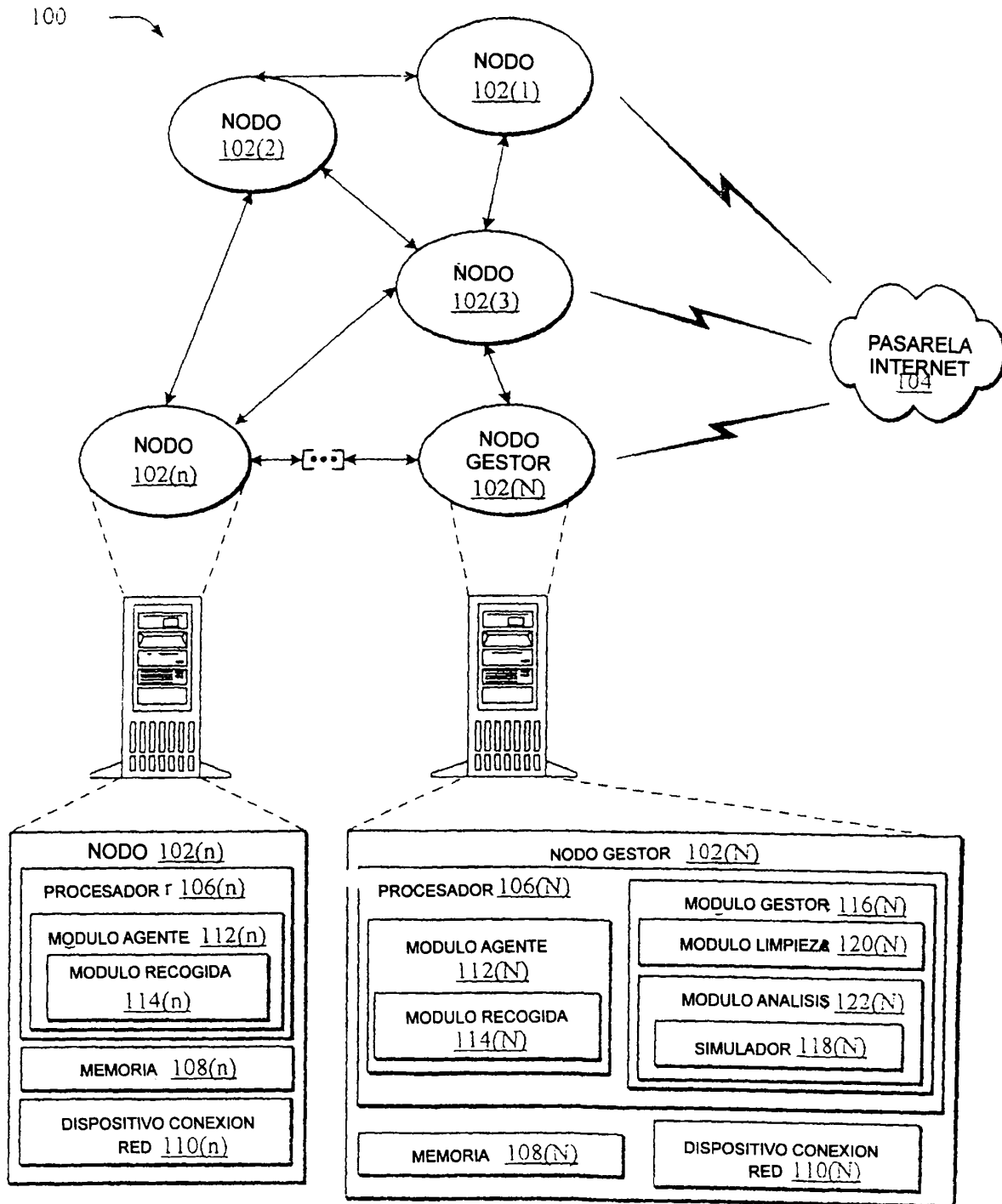


Fig. 1

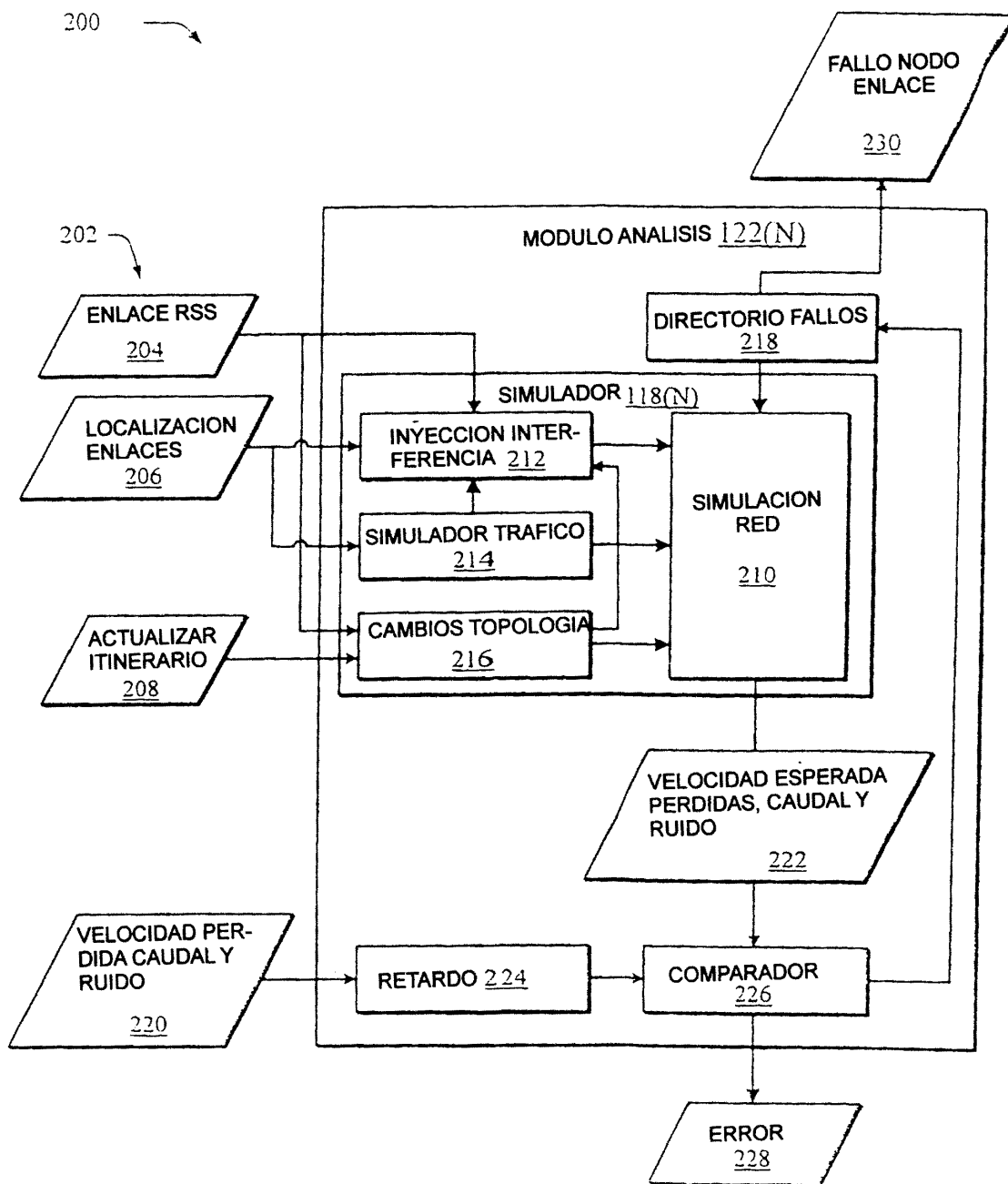


Fig. 2

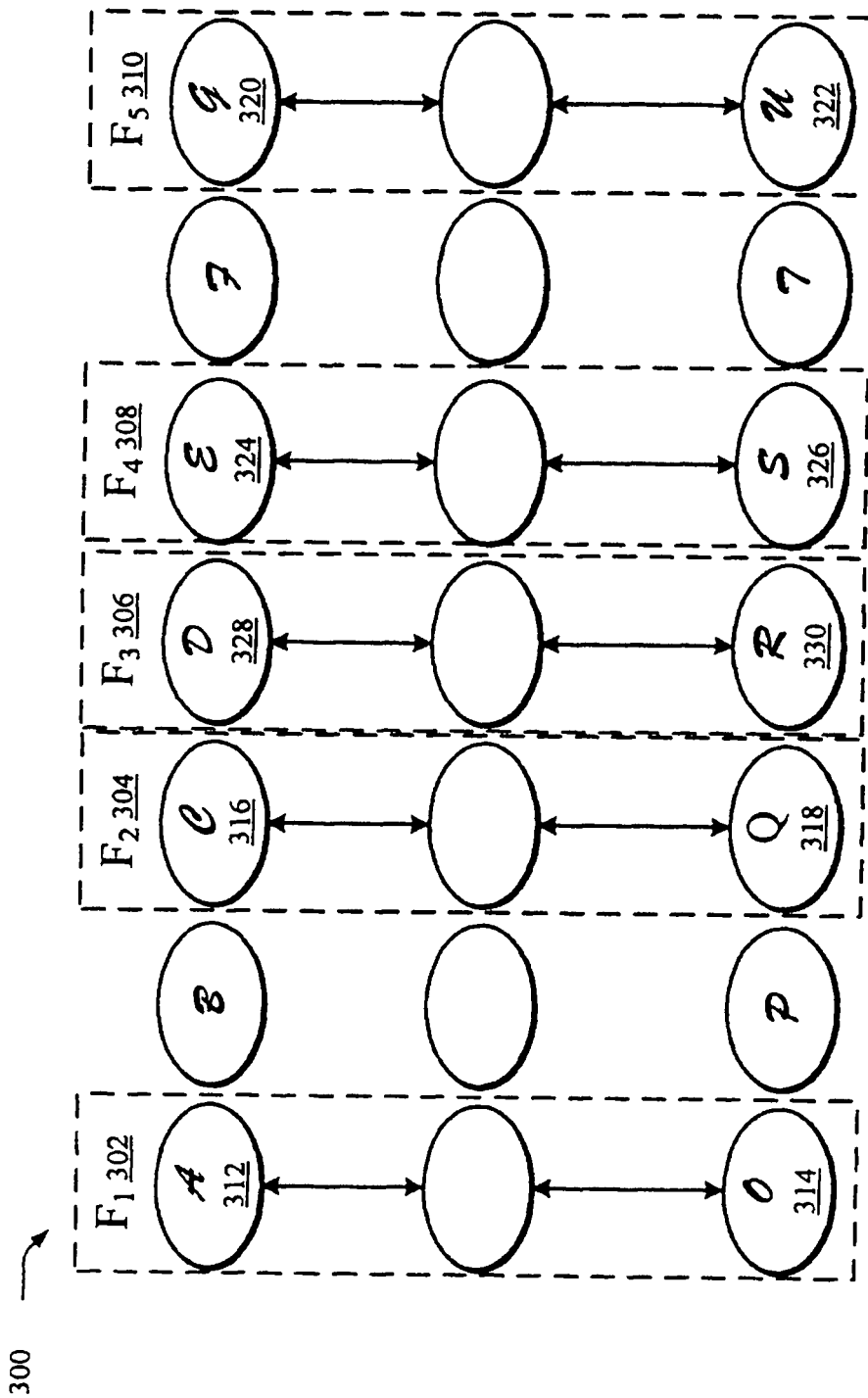


Fig. 3

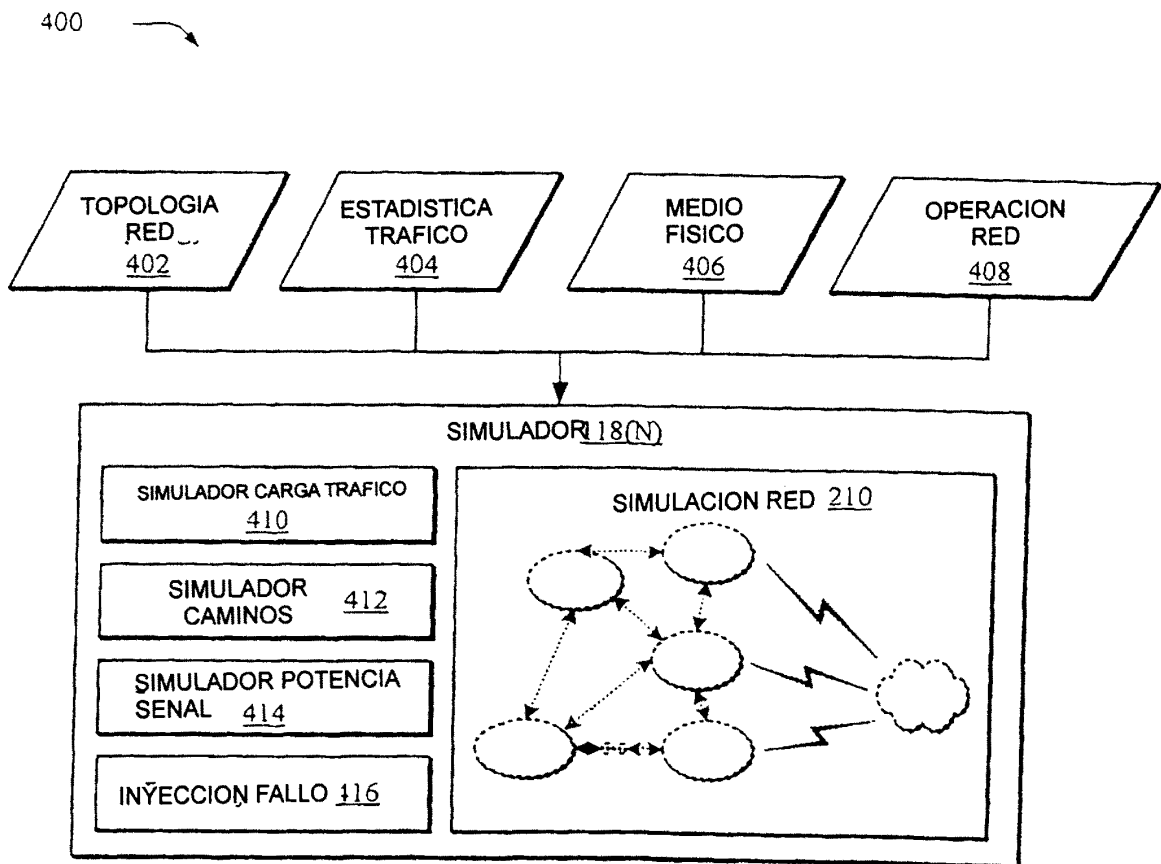


Fig. 4

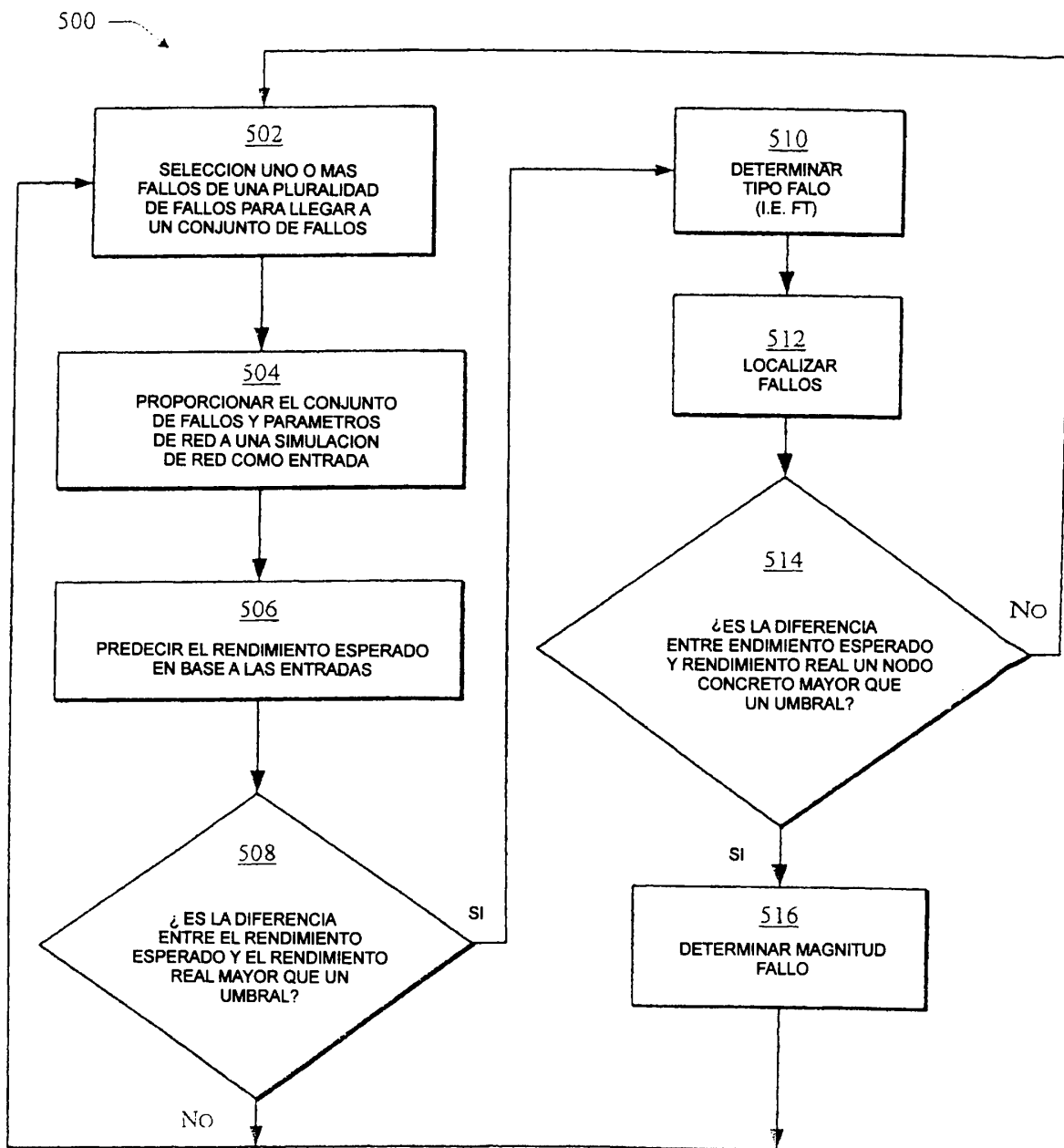


Fig. 5

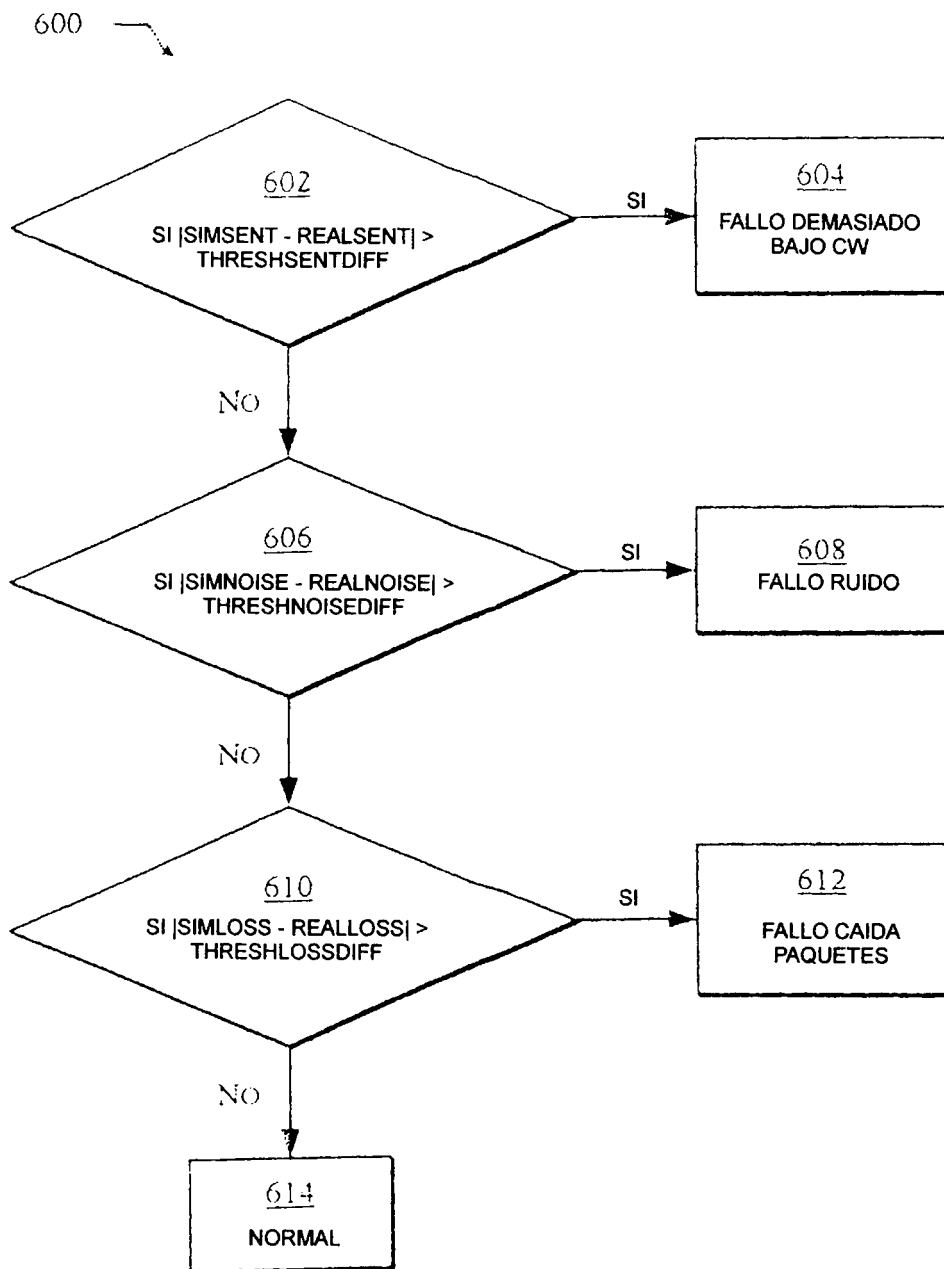


Fig. 6

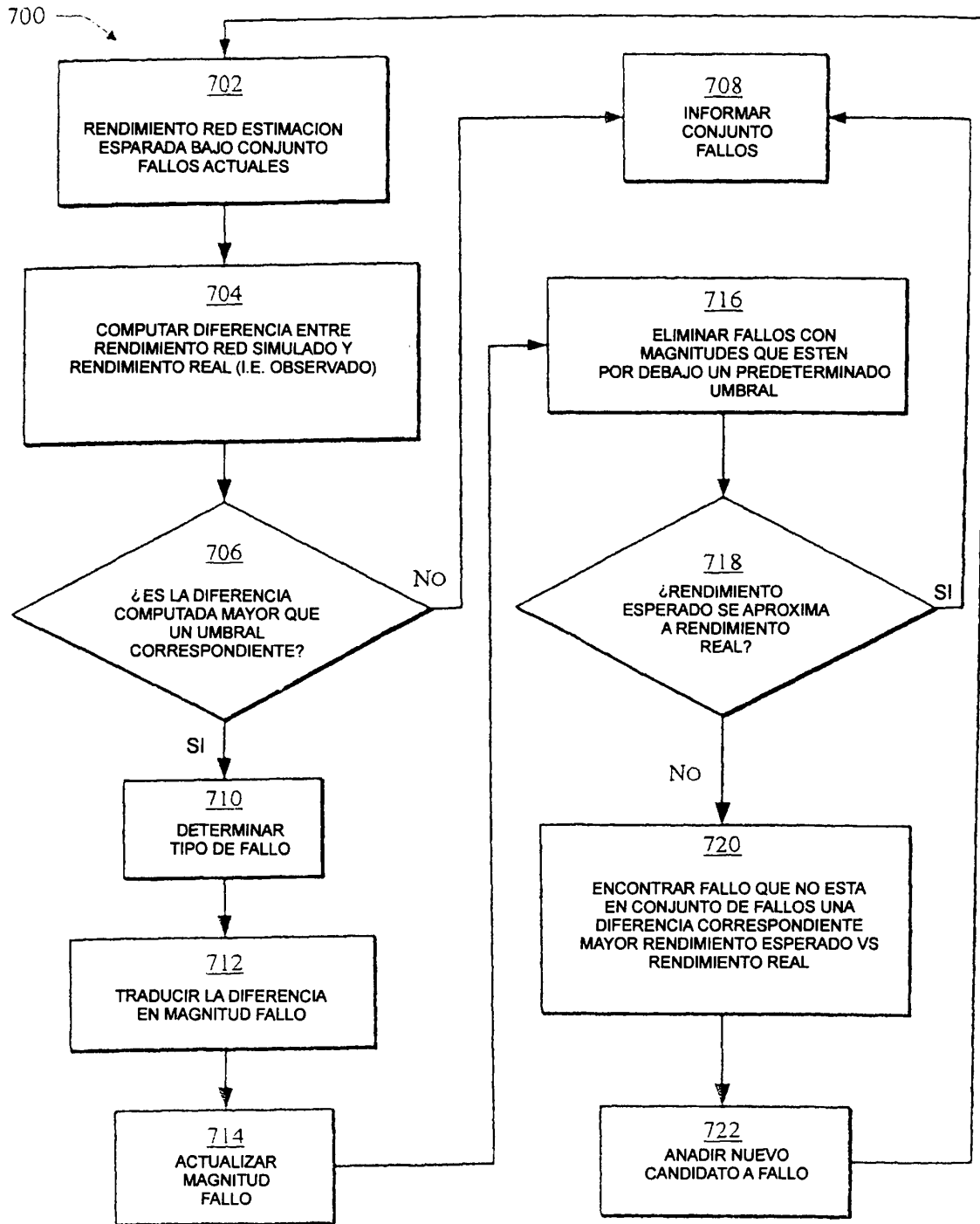


Fig. 7

800

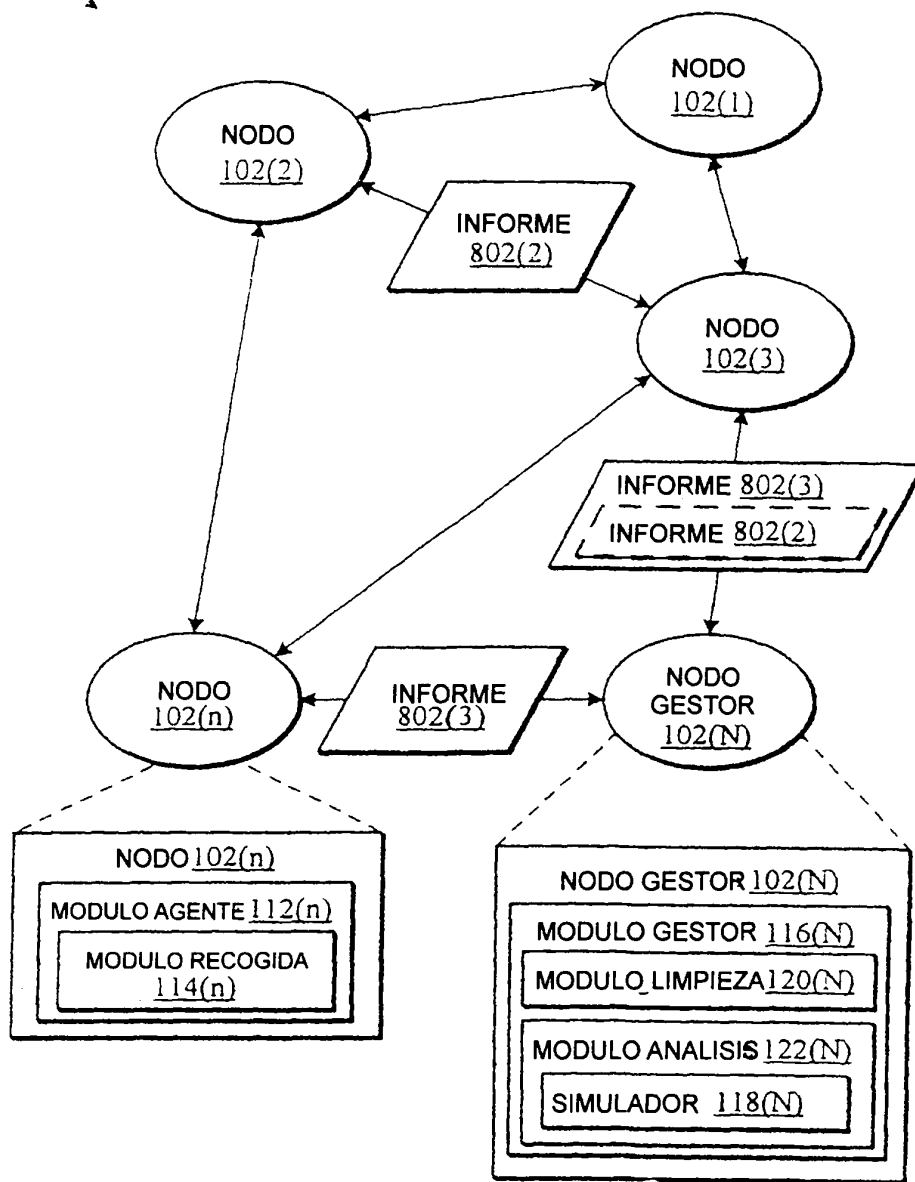


Fig. 8

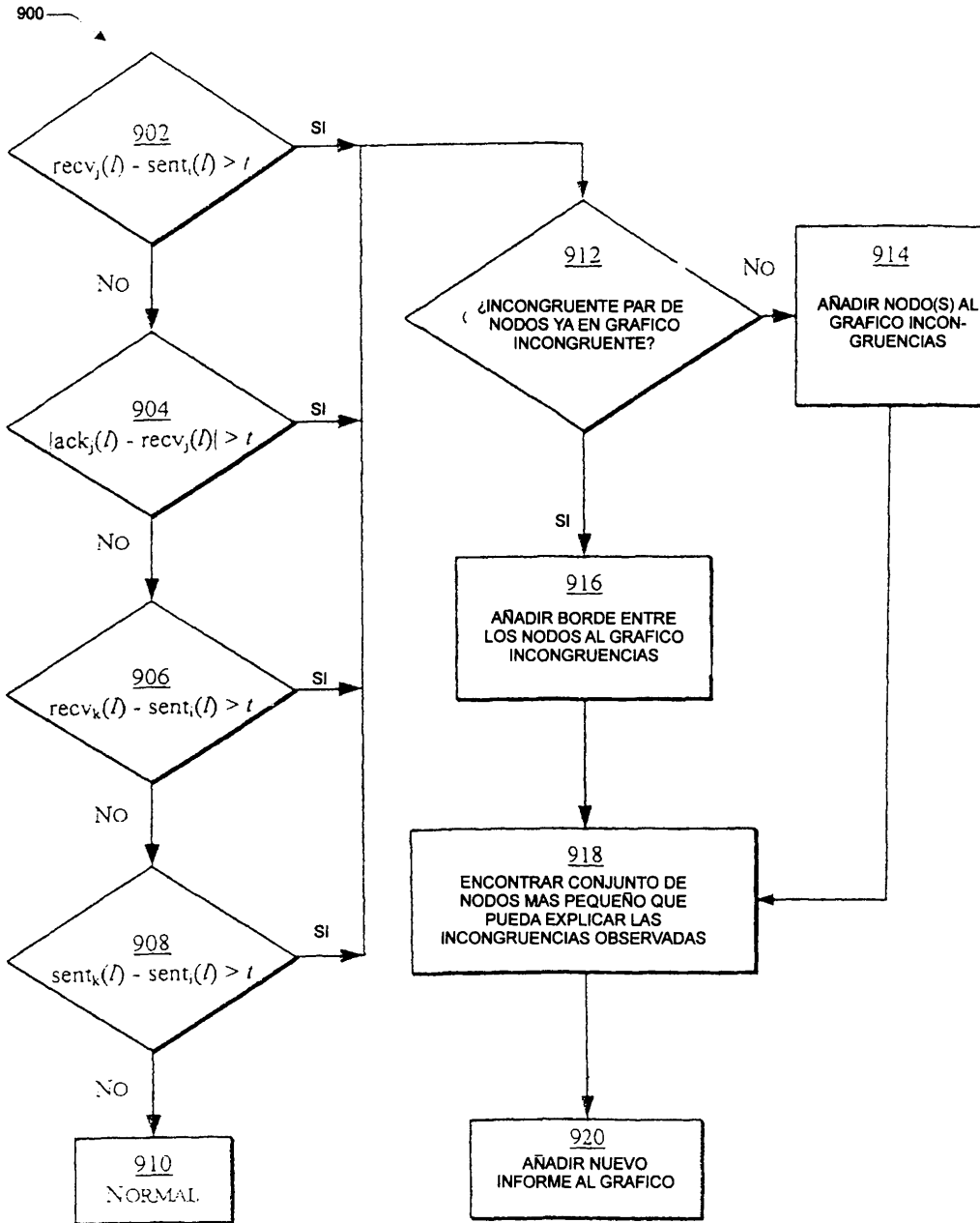


Fig. 9

1000

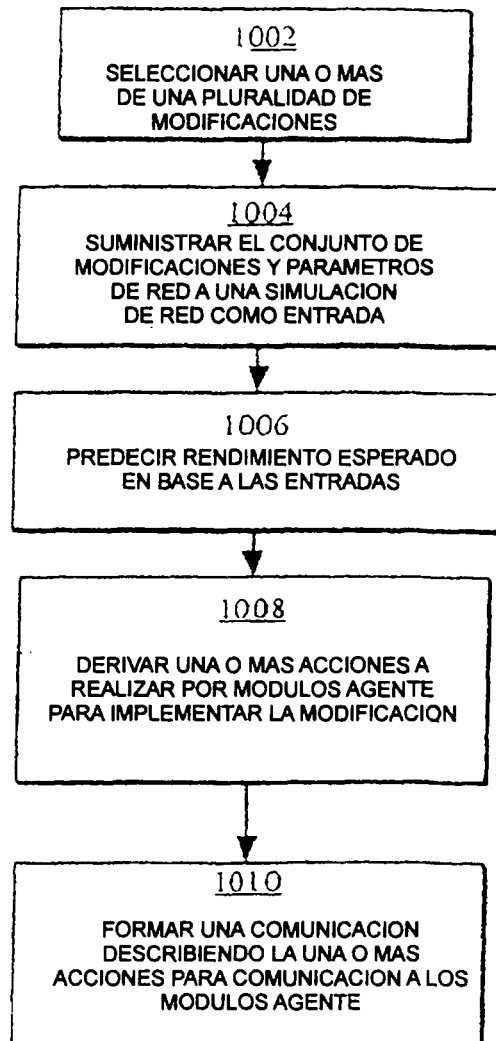


Fig.
10

1100

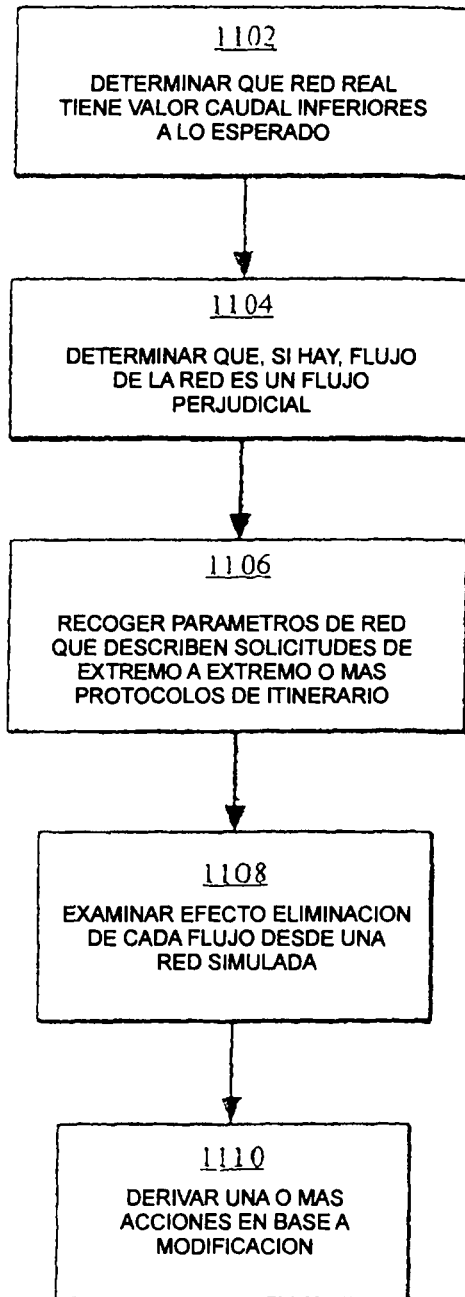


Fig.
11

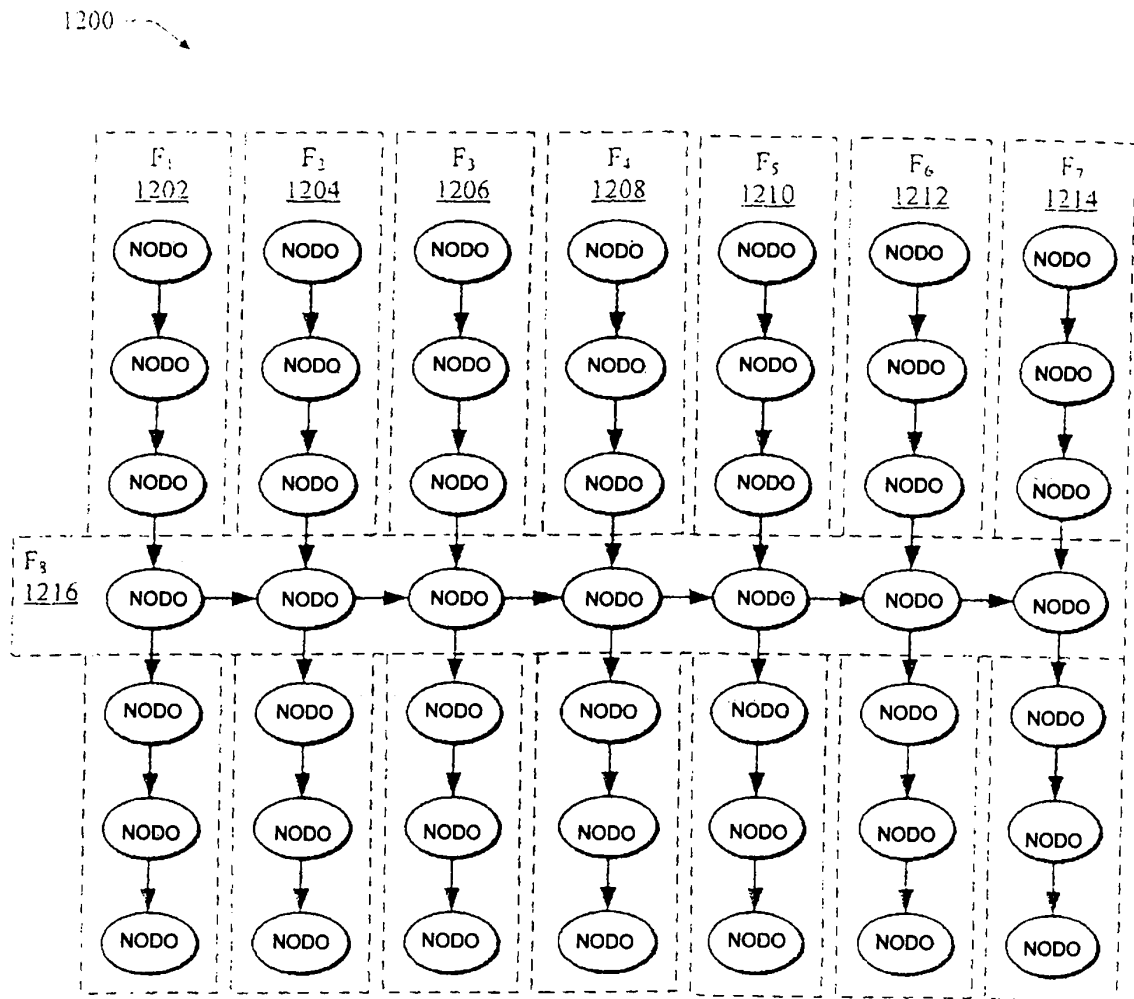


Fig.
12

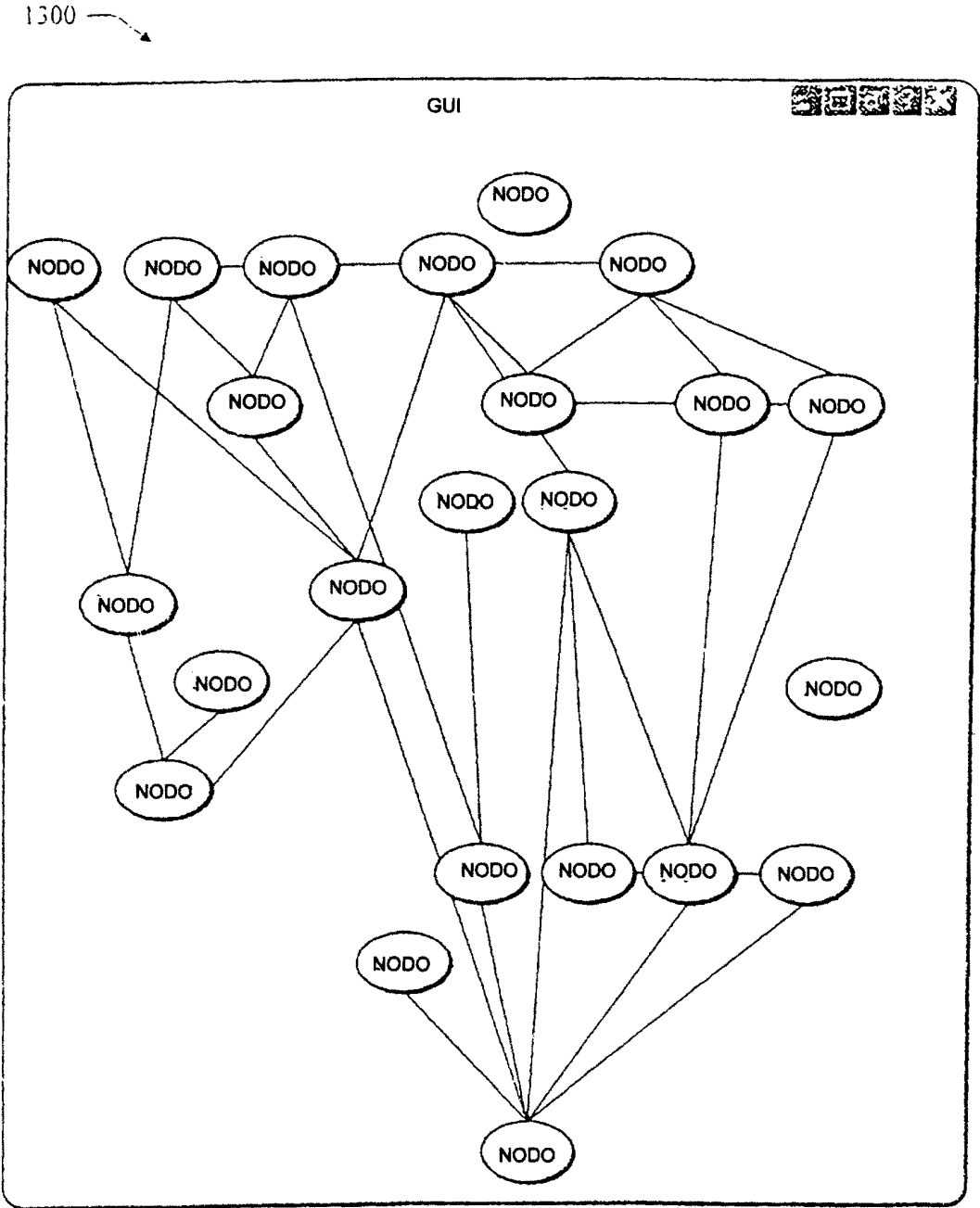


Fig.
13