(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 812 152**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.10.2017 E 17196825 (8)**

(97) Fecha y número de publicación de la concesión europea: **20.05.2020 EP 3474489**

(54) Título: **Un método y un sistema para habilitar una (re)configuración de una red de telecomunicaciones**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
16.03.2021

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

SOBANIA, ALEXANDER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Un método y un sistema para habilitar una (re)configuración de una red de telecomunicaciones

La presente invención se refiere a un método y un sistema apropiado para mantener, asegurar y/o garantizar el correcto funcionamiento de una red de telecomunicaciones.

Tanto el método como el sistema se basan en datos de la red.

En general, una red de telecomunicaciones es una colección de nodos terminales. Los enlaces están conectados para permitir la telecomunicación entre los nodos terminales. Los enlaces de transmisión conectan los nodos terminales entre sí. Los nodos terminales usan conmutación de circuitos, conmutación de mensajes o conmutación de paquetes para pasar la señal a través de los enlaces y nodos correctos para llegar al nodo terminal de destino correcto. Cada nodo terminal en la red de telecomunicaciones generalmente tiene una dirección única, por lo que los mensajes o las conexiones se pueden encaminar a los destinatarios correctos. La colección de direcciones en la red se llama espacio de direcciones. Ejemplos de redes de telecomunicaciones son las redes de ordenadores, Internet, la red telefónica, etc.

La transparencia del estado actual de una red de telecomunicaciones es muy importante y se utilizan muchas fuentes de datos diferentes para identificar el estado actual de la red respectiva. Una vez que el estado de la red cambia de un comportamiento normal a uno anormal de la red, el operador de red respectivo tiene que reaccionar para evitar interrupciones y el impacto en los servidores y/o clientes.

Además, el comportamiento normal puede causar problemas, dependiendo de una situación y una configuración de la red subyacente que deben identificarse y evaluarse.

En una red de telecomunicaciones, un evento es una acción (por ejemplo, un accionamiento del ratón, una pulsación del teclado, un mensaje de otro programa) o una circunstancia reconocida por software, que a menudo se origina de forma asíncrona desde un entorno externo que puede ser manejado por el software.

Tradicionalmente, los eventos que son controlados continuamente por una unidad central dentro de la red a través del Protocolo de Gestión de Red Simple (SNMP) se utilizan para identificar problemas en la red respectiva. Las nuevas tecnologías de datos masivos permiten a los operadores enriquecer SNMP y también utilizar registros, KPI (Indicador Clave de Rendimiento) y datos de configuración para identificar eventos. Los datos de red (es decir, datos sin procesar o datos de origen) rara vez se usan y, en caso de que se usen, se basan en KPI y umbrales predefinidos para esos KPI. Un indicador clave de rendimiento es un tipo de medición del rendimiento. Con frecuencia, los KPI evalúan lo satisfactorio de una actividad particular, tal como un programa en el que participan. Cada indicador clave de rendimiento define un conjunto de valores contra los cuales se debe medir. Un registro o un archivo de registros es un archivo que registra eventos que ocurren en un sistema operativo o en otras ejecuciones de software o en mensajes entre diferentes usuarios de un software de comunicación dentro de la red.

Sin embargo, las redes de telecomunicaciones se vuelven más dinámicas y divergentes, lo que dificulta que un operador obtenga información importante sobre el estado de una red de telecomunicaciones subyacente y procesarla. Una vez que se identifican los problemas, un operador tiene que encontrar una causa raíz y, según su experiencia, decidir cómo solucionar los problemas respectivos para que la red vuelva a un estado normal o de funcionamiento adecuado. Las diferentes soluciones de funciones de red virtual exponen los datos en una variedad de formatos y encriptan una serie de interfaces que hacen que sea muy difícil para los operadores administrar su red.

Además, una topología de red de una red de telecomunicaciones es una herramienta importante para planificar el funcionamiento y para la optimización de redes. Sin embargo, tradicionalmente, las topologías se mantienen manualmente o, en el caso de que se generen automáticamente, se limitan a capas específicas tales como, por ejemplo, capa 3, es decir, la capa de red dentro del modelo OSI de 7 capas de red de telecomunicaciones. Los datos de red de sondeo pasivo o captura de tráfico que podrían usarse para modelar topologías siempre se recopilaron y almacenaron en productos protegidos y, por lo tanto, nunca se aprovecharon para construir topologías en más de diversas capas de red del modelo OSI de 7 capas.

Las nuevas tecnologías de datos masivos permiten un enfoque diferente para tratar los datos de la red y, por lo tanto, también podrían usarse para modelar topologías que combinen múltiples capas y dominios tecnológicos.

En relación con el primer problema mencionado anteriormente, se debe afirmar que los filtros y correlaciones mantenidos manualmente para datos SNMP para resaltar un comportamiento anormal en una red de telecomunicaciones serán muy difíciles de mantener en el futuro debido a las redes dinámicas y divergentes.

Las herramientas que aplican análisis más inteligentes en diferentes fuentes de datos como SNMP, registros, KPI y datos en depósito se enfrentan al desafío de que las fuentes de datos tradicionales son específicas del proveedor o

del dominio de la tecnología y requieren una cierta magnitud de "normalización". Tal "normalización" tiene muchas desventajas, por ejemplo, la consistencia del formato de datos, la correlación de datos, los problemas de sincronización de datos, etc., para un operador y vuelve a hacer que los datos sean específicos en función de la definición específica basada en la "normalización". La analítica no se puede transferir a otras capas de "normalización". Una vez que se identifica el comportamiento anormal dentro de una red, el operador de red respectivo tiene que encontrar la causa raíz basándose en su propio conocimiento o en diversas fuentes, como, por ejemplo, el conocimiento de bases de datos.

El comportamiento anormal puede ocurrir en muchas capas del modelo OSI de 7 capas de la red de telecomunicaciones respectiva, lo que hace que a veces sea muy difícil de identificar.

En cuanto a la segunda cuestión mencionada anteriormente, se tiene que asegurar además que una topología de red que es mantiene manualmente suele estar limitada para fines específicos y solo cubre los nodos relevantes de este propósito específico, por ejemplo, la planificación de redes IP. Dado que existen diversos dominios tecnológicos y diversas capas de red, una variedad de topologías conducen a la falta de transparencia de la red y alta complejidad. Los cambios dentro de una topología son difíciles de rastrear y resolución de problemas de extremo a extremo es muy compleja. Las topologías de red que se generan automáticamente se centran en ciertas capas de red dentro de las 7 capas del modelo OSI y a menudo se generan al descubrir activamente la red, por ejemplo, por medio de mensajes ICMP (Protocolo de Mensajes de Control de Internet). Esos mensajes ICMP están bloqueados la mayor parte del tiempo en la red de telecomunicaciones por razones de seguridad. Los sondeos pasivos y la captura de tráfico generalmente se aplican para un caso de uso específico cuando los datos se almacenan en un formato protegido. Debido al alto rendimiento en las redes de telecomunicaciones, las herramientas se optimizan para el caso de uso específico, y los datos no están disponibles para otros fines. Por lo tanto, la diversidad de esas herramientas hace que sea muy difícil extraer automáticamente una topología subyacente o construir automáticamente topologías de extremo a extremo.

El documento US 2006/0023638 Al describe un sistema de análisis de red proactivo que abarca un recopilador de flujo de datos que captura datos como capturas de paquetes. El analizador de tráfico del US 2006/0023638 Al se caracteriza por que puede identificar para el administrador de la red lo que ha sucedido o está sucediendo al revelar actividad no autorizada de la utilización, los patrones de tráfico y el espacio de direcciones de la red. Sin embargo, el recopilador de flujo de datos de captura de paquetes de la red proporcionado no captura datos de red sin procesar de al menos una función de red, como un componente de red, una herramienta de red, un interfaz de red y/o una aplicación de red. Además, no se proporciona acceso a dichos datos de red sin procesar (datos fuente o datos atómicos).

En este contexto, era un objeto de la presente invención proporcionar la posibilidad de permitir una configuración o una reconfiguración de una red de telecomunicaciones por medio de datos de red pasivos surgidos de forma general para usar esos datos para el modelado de topologías y/o la automatización de la red.

Se presenta un método con las características de la reivindicación independiente 1 y un sistema con las características de la reivindicación independiente 13. Realizaciones adicionales se indican en las respectivas reivindicaciones dependientes y en la siguiente descripción.

La invención se dirige a un método para mantener, asegurar y/o garantizar el funcionamiento correcto/deseado de una red de telecomunicaciones, comprendiendo el método al menos las siguientes etapas:

- extraer, capturar y recopilar datos de red sin procesar de al menos una función de red, tales como un componente de red, una herramienta de red, un interfaz de red y/o una aplicación de red,
- duplicar los datos de red sin procesar capturados,
- convertir los datos de red sin procesar capturados duplicados en un formato interpretable por personas,
- almacenar los datos de red sin procesar convertidos en un almacenamiento de datos que soporte procesamiento paralelo y escalado horizontal, y
- hacer que los datos de red sin procesar almacenados estén disponibles por medio de al menos un interfaz de programación de aplicaciones para un despliegue adicional en cuanto a la automatización de la red, en particular con respecto a la detección de fallos y al reacondicionamiento de la red de telecomunicaciones, y para el modelado de topología de la red de telecomunicaciones,
- recuperar por medio del al menos un interfaz de programación de aplicaciones al menos un subconjunto de los datos de red sin procesar disponibles, dependiendo el subconjunto depende del despliegue posterior, y
- buscar los datos de red sin procesar recuperados para datos que sean indicativos y utilizables para un caso de uso específico, en cuanto a detección de fallos y/o modelado de topología,
- analizar los datos de red sin procesar recuperados con respecto a los parámetros del protocolo, e
- identificar en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, en al menos una causa raíz de problemas que perturban/afectan el estado actual de trabajo de la red de telecomunicaciones,
- indicar al menos la causa raíz identificada a un operador de la red de telecomunicaciones por medio de un interfaz de usuarios.

El método propuesto se puede usar para una red de telecomunicaciones virtualizada.

En el contexto de la presente descripción, el término "configuración" y/o "reconfiguración" se refiere a cualquier tipo de reconfiguración, mantenimiento, apoyo y/o garantía del funcionamiento correcto/deseado de la red de telecomunicaciones. El término "despliegue" cubre la automatización de la red, particularmente con respecto a la detección de fallos y el reacondicionamiento de la red de telecomunicaciones subyacente, y el modelado de topología de la red de telecomunicaciones.

El término "indicador específico del despliegue" se refiere a esos datos entre los datos de red sin procesar disponibles que son indicativos y utilizables para un caso de uso específico. En el caso del modelado de topología, existen datos específicos, como la dirección MAC y/o la dirección IP de un componente de red, que pueden utilizarse para identificar un rol de dicho componente de red dentro de la red de telecomunicaciones. En caso de detección de fallos, los datos de tráfico, por ejemplo, pueden usarse para identificar un fallo específico dentro de la red de telecomunicaciones.

De acuerdo con una realización, la red de telecomunicaciones está mapeada lógicamente en una arquitectura de red por capas, comprendiendo la arquitectura de red por capas al menos una capa de función de red, una capa de conversión, una capa de almacenamiento y una capa de aplicación, interrelacionándose las capas por medio de los interfaces de red respectivos, y en donde la al menos una función de red, se ejecuta en la capa de función de red, realizándose la conversión de los datos de red sin procesar capturados duplicados en un formato interpretable por personas dentro de la capa de conversión, y los datos de red sin procesar convertidos se almacenan en la capa de almacenamiento de datos, y los datos de red sin procesar almacenados se hacen disponibles en la capa de aplicación por medio de al menos un interfaz de programación de aplicaciones para un despliegue adicional en cuanto a la automatización de redes y al modelado de topología de la red de telecomunicaciones. La búsqueda de los datos de red sin procesar recuperados para los datos que son indicativos y utilizables para un caso de uso específico, como para la detección de fallos y/o el modelado de topología, se puede realizar en una capa de análisis de la arquitectura de red en capas.

Los datos de red sin procesar (abreviatura: datos sin procesar), también llamados datos de origen o datos atómicos, son datos que no se han procesado para su uso. A veces se hace una distinción entre los datos y la información en el sentido de que la información es un producto final del procesamiento de datos. Aunque los datos sin procesar tienen el potencial de convertirse en información, requieren extracción selectiva, organización y, a veces, análisis y formato para su presentación. Los datos sin procesar son datos que no han sufrido ninguna forma de transformación o agregación y aún contienen datos de operaciones de red base en su forma más pura. Esto no quiere decir que el formato de los datos no haya cambiado. Los datos sin procesar se refieren a cualquier objeto de datos que no se haya sometido a un procesamiento exhaustivo, ya sea manualmente o mediante software computarizado automático. Los datos sin procesar se pueden recopilar de varios procesos y recursos de IT, y particularmente de un protocolo de red que generalmente comprende datos normalizados sin procesar, particularmente dentro de los encabezados respectivos de las diferentes capas OSI de la red de telecomunicaciones subyacente. Estos datos capturados se pueden escribir en un archivo con herramientas como tcpdump. tcpdump es una herramienta de análisis de red (rastreador de paquetes). Con tcpdump, no existe un interfaz gráfico de usuario, pero tcpdump se inicia directamente dentro de la consola de un ordenador. Rastrea el tráfico de la red y analiza los paquetes de la red extrayendo, por ejemplo, direcciones IP/nombres de los servidores involucrados y mostrando servicios que producen el tráfico de datos/red. tcpdump registra el tráfico de red por medio de un interfaz y muestra/indica todos los paquetes que se transmiten a través de la red. Por lo tanto, la tarjeta Ethernet (es decir, la tarjeta de interfaz de red) se configura en un modo denominado promiscuo. Los datos de red extraídos se escriben en un archivo tcpdump y luego se convierten en un formato interpretable por el personal, es decir, en un archivo de texto interpretable por el personal. En general, los datos sin procesar son principalmente datos en depósito no estructurados o sin formato que pueden estar en forma de archivos, imágenes visuales, registros de bases de datos o cualquier otro dato digital.

En general, un formato interpretable por el personal es una representación de datos o información que el personal puede leer de forma natural. En ordenadores, los datos interpretables por el personal a menudo se codifican como un archivo en lugar de presentarse en una representación binaria. Se puede usar JSON (Notación de Objeto de Script Java), por ejemplo, que es un formato de archivo normalizado abierto que utiliza texto interpretable por el personal para transmitir objetos de datos que consisten en pares de atributos y tipos de datos matriciales o cualquier otro valor disponible en serie. Es un formato de datos muy común utilizado para la comunicación asíncrona de navegador-servidor. Es un formato de datos independiente del idioma.

Una arquitectura de red en capas propuesta por una realización del presente método supera los silos derivados de soluciones específicas. Dentro de cada capa, las funciones disponibles son mutuamente excluyentes para garantizar que no haya duplicación de funciones entre capas. Cada capa por lo tanto contiene un conjunto de funciones singularmente segregado. Del mismo modo, los datos no se duplican en las capas. Los datos almacenados y manejados en cada capa son distintos de los datos en todas las demás capas.

De acuerdo con el método propuesto, los datos sin procesar se extraen, se recopilan, se analizan y se pueden procesar y utilizar para sacar conclusiones, hacer proyecciones o extraer información significativa. Como ya se indicó, los

componentes de red y/o protocolos de red pueden ser cualquier recurso de IT o cualquier proceso dentro de la red. Particularmente, tales componentes de red y/o herramientas de red pueden ser un interfaz de red, un controlador de interfaz de red y/o cualquier punto de reflejo de tráfico. Los datos de la red se pueden capturar con herramientas como tcpdump o hardware especializado optimizadas para un alto rendimiento. Las herramientas de software pueden capturar los datos en el recurso de IT en sí y almacenarlos en un archivo, mientras que el hardware requiere un dispositivo adicional para reflejar o duplicar el tráfico.

Un controlador de interfaz de red, es decir, una tarjeta de interfaz de red (NIC) es un componente de hardware de ordenador que conecta el mismo a una red de telecomunicaciones. Un controlador de interfaz de red generalmente realiza una circuitería electrónica requerida para comunicarse usando una capa física específica y una norma de capa de enlace de datos tal como Ethernet, Canal de Fibra o WiFi. Esto proporciona una base para una pila de protocolos de red completa, permitiendo la comunicación entre pequeños grupos de ordenadores en la misma red de área local o comunicaciones de red a gran escala a través de protocolos encaminables, como Protocolo de Internet (IP). Un controlador de interfaz de red permite que los ordenadores se comuniquen a través de una red de telecomunicaciones mediante el uso de cables o de forma inalámbrica. Es tanto un dispositivo de capa física como de capa de enlace de datos, ya que proporciona acceso físico a un medio de red y proporciona un sistema de direccionamiento de bajo nivel mediante el uso de direcciones MAC (Control de Acceso a los Medios) que se asignan de forma exclusiva a los interfaces de red.

Un interfaz de red es generalmente un interfaz de un sistema entre dos partes de equipos o capas de protocolo en una red de telecomunicaciones. Un interfaz de red generalmente tiene alguna forma de dirección de red. Esto puede consistir en una ID de nodo y un número de puerto, o puede ser una ID de nodo única por derecho propio. En general, los interfaces de red proporcionan funciones normalizadas, tales como mensajes de etapa, conexión y desconexión, etc. Un puerto de ordenador, por ejemplo, es un interfaz de red para otros ordenadores o periféricos.

Un punto de reflejo de tráfico dentro de una red de telecomunicaciones debe entenderse como un punto dentro de la red, por ejemplo, un conmutador de red que se utiliza para enviar una copia de paquetes de red, visto en un puerto de conmutador a una conexión de supervisión de red en otro puerto conmutador. Los puntos de reflejo de tráfico se utilizan para supervisar el tráfico de red para, por ejemplo, analizar datos de depuración o errores de diagnóstico en la red de telecomunicaciones. El tráfico entrante o saliente o ambos pueden reflejarse en interfaces simples o múltiples.

De acuerdo con una realización del presente método, los datos de red sin procesar son proporcionados directamente por la al menos una función de red a través de un interfaz o por medio de al menos un agente de rastreo que se ejecuta en una máquina virtual, particularmente en la capa de función de red mencionada anteriormente.

De acuerdo con una realización adicional, los datos de red sin procesar se capturan mediante un mecanismo de extracción o mediante un mecanismo de inserción.

Los datos sin procesar se capturan directamente desde al menos una función de red o mediante un agente de rastreo que se ejecuta en una máquina virtual, particularmente dentro de la capa de función de red mencionada anteriormente. Si bien se considera que un mecanismo de inserción para capturar datos es lo más probable, la arquitectura no excluye la opción para que los operadores creen un mecanismo de extracción. De acuerdo con un mecanismo de inserción, los datos de red sin procesar se capturan y se envían a conversión y almacenamiento y finalmente a herramientas de análisis a través de al menos un API. De acuerdo con el mecanismo de inserción, los datos sin procesar duplicados de la red están (deberán estar) disponibles instantáneamente. De acuerdo con un mecanismo de extracción, los datos de red sin procesar se duplican y luego se extraen mediante un elemento de conversión, por ejemplo, la capa de conversión.

De acuerdo con el mecanismo de inserción y extracción, los datos de red sin procesar duplicados son continuos y no se interrumpen ni retrasan antes de ponerse a disposición de otros elementos /capas, particularmente para una herramienta de análisis.

A efectos de claridad, el término "datos de la red sin procesar", por brevedad también denominado "datos sin procesar", abarca la señalización, el encaminamiento y datos similares. La integridad de los datos y su naturaleza "sin procesar" en el punto de captura se conserva hasta su almacenamiento dentro del almacenamiento de datos, particularmente en la arquitectura de red en capas propuesta. En ningún momento los datos recopilados se modifican, aumentan o agregan hasta su almacenamiento dentro del almacenamiento de datos, particularmente a través de las capas hasta la capa de almacenamiento. Los metadatos, por ejemplo, la marca horaria puede asociarse con los datos sin procesar de la red siempre que garanticen la integridad de los datos sin procesar capturados.

Los datos de red sin procesar se pueden re empaquetar. Con fines de almacenamiento y uso por parte de las aplicaciones, los datos se pueden desencriptar y formatear. Tales procesos aún conservan la integridad del contenido original de datos sin procesar.

El método comprende las siguientes etapas:

- analizar los datos de red sin procesar almacenados con respecto a parámetros específicos, como los parámetros de protocolo, e
- identificar en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, al menos una causa raíz de problemas que perturben/afecten el estado actual de funcionamiento de la red de telecomunicaciones.

De acuerdo con una posible realización del método propuesto, estas etapas del método se realizan dentro de una capa de procesamiento/análisis de datos de la arquitectura en capas propuesta.

La captura de datos sin procesar tiene lugar a través de medios 'pasivos' que no debería afectar el tráfico de red. La captura de datos se produce solo una vez y está disponible para diferentes aplicaciones, por ejemplo, análisis. Todos los datos sin procesar almacenados se pueden usar múltiples veces simultáneamente o en diferentes momentos por las mismas o diferentes aplicaciones.

Mediante el uso de API normalizados o API abiertos, se ofrecen datos sin procesar para análisis y otras aplicaciones. Los API aseguran que los usos analíticos y de otro tipo de los datos sin procesar puedan funcionar en todo el almacenamiento de datos, es decir, en toda la capa de almacenamiento.

Cuando la red de telecomunicaciones se mapea lógicamente en una arquitectura de red en capas como se mencionó anteriormente, las diferentes capas se definen de la siguiente manera:

La capa de función de red se define como la capa donde se realizan todas las funciones de red. Cualquier función de red u otra forma de software que se ejecute en esta capa en una máquina virtual (VM) o en contenedores hace que sus datos estén disponibles en una capa de conversión. Los datos hacia/desde la máquina virtual son proporcionados directamente por una función de red a través de un interfaz o permitiendo la instalación de agentes para recopilar los datos de la VM/contenedora.

Todos los paquetes de red que salen o entran en la máquina virtual se proporcionan hasta la capa de conversión en formato sin procesar. Donde los datos están encriptados, la función de red los desencripta como parte del proceso. En la transferencia y el almacenamiento, los datos también pueden estar en estado encriptado.

Para asegurar que los datos se transfieran fácilmente, no se realiza ninguna modificación o agregación. Los datos originales permanecen en su estado no modificado.

La captura de los datos sin procesar es 'pasiva' por duplicación. Cualquier mal funcionamiento del proceso de duplicación no afecta el entorno de producción.

Eso significa que el método propuesto es utilizar datos de red pasivos, es decir, datos de red sin procesar, para identificar "situaciones" en una red de telecomunicaciones.

En la capa de conversión, los datos recibidos de la 'capa de red' se convierten a un formato adecuado para el almacenamiento. Este proceso se realiza sin ninguna modificación o agregación de los datos sin procesar originales. Los metadatos pueden ser opcionalmente añadidos en este punto.

La capa de conversión es capaz de analizar (y por lo tanto comprender) todos los protocolos relevantes, incluidos los protocolos que se han desarrollado específicamente para los requisitos de rastreo de los operadores individuales. La conversión se hace posible utilizando herramientas apropiadas conocidas en la técnica.

La capa de almacenamiento es donde se encuentran los datos convertidos para su posterior análisis. Preferiblemente, se usa un API para mover datos de la capa de conversión a la capa de almacenamiento. Lógicamente, la capa de almacenamiento de datos aparece como un sistema centralizado y admite procesamiento paralelo y escalado horizontal. Físicamente, los datos pueden almacenarse de manera distribuida o centralizada. Por razones de eficiencia, es posible que los datos almacenados estén indexados.

De acuerdo con una realización adicional del método propuesto, la arquitectura de red en capas comprende además una capa de exposición que hace que los datos almacenados estén disponibles para la capa de aplicación a través de API específicos. Los mecanismos de búsqueda y recuento basados en los datos indexados están disponibles para numerosas aplicaciones.

Dentro de la capa de aplicaciones, cualquier aplicación puede hacer uso del API de 'capa de exposición' disponible para diferentes propósitos, por ejemplo, analítica. De acuerdo con una realización adicional del método propuesto, la arquitectura de red en capas comprende además una capa analítica/una capa de análisis.

Los protocolos en, por ejemplo, 3GPP (Proyecto de Asociación de Tercera Generación) están normalizados y, por lo tanto, se pueden utilizar para identificar anomalías en una red de telecomunicaciones, por ejemplo, tasa de caída de llamadas. Más allá del comportamiento anormal de la red, también el comportamiento normal puede causar problemas como, por ejemplo, una configuración en un cortafuegos que bloquee el tráfico o un ataque DoS. Una vez identificadas, esas situaciones/problemas pueden compararse con eventos históricos para identificar una causa raíz respectiva. Además, la información relevante normalizada del protocolo podría ser aprovechada para identificar tales situaciones/problemas. Situaciones que los operadores definirían como comportamiento de red normal, pero que son inusuales, como, por ejemplo, DoS, también se pueden identificar y resaltar para el operador de red. DoS significa "denegación de servicios", lo que indica que una máquina o un recurso de red no está disponible para sus usuarios previstos interrumpiendo temporal o indefinidamente los servicios de un anfitrión conectado a Internet. La denegación de servicio generalmente se logra dejando flotante una red de telecomunicaciones específica con una solicitud superflua en un intento de sobrecargar la red de telecomunicaciones.

Como se pueden identificar situaciones/problemas cuando se analizan los datos de red sin procesar extraídos y recopilados con respecto a parámetros específicos en diferentes capas de red entre las capas del modelo OSI de 7 capas, es posible identificar en la red al menos una causa raíz de las situaciones/problemas que perturban y/o afectan el estado actual de funcionamiento de la red de telecomunicaciones. Una vez identificada, la al menos una causa raíz identificada se le puede indicar a un operador de la red, por ejemplo, a través de una pantalla o cualquier dispositivo de salida acústica. Una vez que un dispositivo captura el tráfico de la red, es decir, los datos de la red, incluye automáticamente todas las capas dentro de un paquete. Por ejemplo, si un servidor web captura el tráfico http, todas las capas OSI a continuación también son visibles dentro del paquete. Los parámetros que se consideren dependerán de la tecnología de la red. Además, de acuerdo con una realización adicional del método propuesto, el método comprende además las etapas:

activar un motor de flujo de trabajo que contiene una biblioteca de acciones, estando vinculada cada acción a al menos una causa raíz y que se puede utilizar para devolver la red al estado de funcionamiento deseado, y realizar al menos una acción de la biblioteca vinculada a la al menos una causa raíz identificada.

Eso significa que es posible que las acciones que sean propuestas se puedan activar o incluso activar automáticamente, lo que da lugar a un mayor grado de automatización de la red de telecomunicaciones subyacente. Esas acciones también pueden ser acciones proactivas como la solicitud de validación de un cliente para nuevas fuentes de red. El número de acciones posibles comprende, además, por ejemplo, un reinicio de la red de telecomunicaciones, un re-encaminamiento del tráfico dentro de la red de telecomunicaciones cuando la causa raíz identificada se correlaciona con la ruta de tráfico original, una reinstalación de la red de telecomunicaciones, etc.

Las etapas para identificar problemas y activar las acciones se pueden aplicar en todas las capas OSI (en términos) del modelo de red de telecomunicaciones. Por lo tanto, el método planteado es genérico y puede transferirse ya que los datos de red sin procesar están altamente normalizados. El enfoque de normalización mencionado anteriormente puede evitarse y la información principal de la red de telecomunicaciones sin la dependencia del proveedor o de la tecnología puede ser aprovechada.

De acuerdo con una realización adicional del método propuesto, la etapa de identificar en la red la al menos una causa raíz comprende reconocer al menos un mensaje de red que sea indicativo de al menos una causa raíz.

Como ya se mencionó anteriormente, la red es la fuente principal para los datos de red sin procesar. Los datos de red sin procesar se pueden recopilar desde el interfaz de red, el controlador de interfaz de red o cualquier punto de reflejo de tráfico. Los datos de red sin procesar deben almacenarse en un formato interpretable por el personal y estar disponibles a través del API. Un interfaz de programación de aplicaciones (API) es un conjunto de definiciones de subrutinas, protocolos y herramientas para crear software de aplicación. Generalmente, es un conjunto de métodos claramente definidos de comunicación entre varios componentes de software. Un API permite a un operador obtener acceso a los datos sin procesar extraídos y recopilados. De acuerdo con el método propuesto, los API a través de los cuales se ponen a disposición los datos sin procesar están relacionados con el almacenamiento de datos, es decir, la capa de almacenamiento de datos en la que los datos sin procesar se han almacenado después de haber sido extraídos y recopilados.

Un módulo de aprendizaje automático, es decir, un algoritmo respectivo, aprovecha los datos de red sin procesar a través del API que está relacionado con el almacenamiento de datos. El módulo de aprendizaje automático identifica situaciones/problemas en la red de telecomunicaciones considerando parámetros en diferentes capas de las capas OSI. Si se puede identificar una causa raíz basándose en la información de datos de la red, el módulo de aprendizaje automático puede activar un motor de flujo de trabajo que contenga una biblioteca de acciones que se utilizan para volver a poner la red de telecomunicaciones en un estado normal de funcionamiento. En caso de que la red de telecomunicaciones se asigne lógicamente a la estructura en capas mencionada anteriormente, el módulo de aprendizaje automático se está ejecutando, por ejemplo, sobre una capa de análisis en la parte superior de la capa de aplicación.

El método propuesto puede, por ejemplo, usarse en el siguiente escenario.

Una interrupción de un HSS (Servidor de Abonado Doméstico) puede tener muchas causas raíz. Podría ser, por ejemplo, una comunicación hacia la CNTDB (Base de Datos de Tecnología de Red Común) que falle, un fallo de la red o la autenticación que no funcione, porque el módulo de encriptado que autoriza la SIM (Módulo de Identidad del Abonado) no funciona. Todas las causas raíz diferentes serán visibles en la red con diferentes mensajes de red. El fallo de la red también podría deberse a un problema con un encaminador IP o un cortafuegos IP mal configurado. Si se identifica un cortafuegos mal configurado, se podría activar una acción para corregir la configuración. En caso de que haya problemas con un emplazamiento de CNTDB, podría evaluarse la causa raíz de los problemas de CNTDB y el tráfico puede redirigirse. Al observarse una cantidad inusual de fuentes IP a un determinado destino IP, el tráfico hacia el destino IP podría bloquearse desde ciertos enlaces.

Por ejemplo, si una nueva fuente de tráfico de una lista en blanco es visible en la red, pero aún no está configurada, podría activarse un mecanismo para informar proactivamente al usuario sobre este tráfico y requerir una validación que active una reconfiguración de la lista en blanco.

El método propuesto proporcionará a un operador de red transparencia en su red de telecomunicaciones no solo enfocándose en los errores, sino también considerando situaciones/problemas inusuales. Las fuentes de datos para la transparencia se reducen drásticamente y, por lo tanto, también se han evitado todos los problemas de normalización de los datos. El método propuesto puede utilizar la fuente de datos más fiable y evaluar las situaciones/problemas en todas las capas OSI. Esto permitirá un nuevo grado de automatización para protocolos normalizados y de los elementos que los usan. El aprendizaje automático, es decir, un módulo de aprendizaje automático como se mencionó anteriormente, permitirá una comparación histórica más amplia con problemas conocidos y podrá activar acciones para solucionarlos. El tiempo de inactividad de la red de telecomunicaciones puede reducirse y la resolución de problemas puede ser mucho más eficiente. Todos los análisis se desarrollan y los datos de la red se pueden transferir a cualquier otra organización utilizando los mismos protocolos. Solo podría variar la acción en el motor de flujo de trabajo que se combina con un determinado problema que perturba/afecta el estado de funcionamiento actual de la red de telecomunicaciones.

De acuerdo con otra realización, el método propuesto comprende además la siguiente etapa:

modelar, basándose en los datos de red sin procesar recuperados, extraídos y recopilados, una topología de red que combine múltiples capas de protocolo y dominios tecnológicos de la red de telecomunicaciones.

El método propuesto permite recopilar los datos de red sin procesar de la red y hacer que los datos de red sin procesar estén disponibles a través del API para un uso más amplio. Esos datos ahora se pueden usar para crear automáticamente al menos una topología de red que cubra múltiples capas de protocolo y dominios tecnológicos y, por lo tanto, permita una vista fiable de extremo a extremo. Se puede usar una combinación de diferentes capas y campos de protocolo en esas capas de protocolo para determinar el propósito de un elemento de red, una posición y una relación del elemento de red con otros elementos de red. Esto se puede hacer en diferentes capas del modelo OSI, también en capas superiores a la capa 3 del modelo OSI.

De acuerdo con otra realización del método propuesto, el método comprende además la etapa de revisar campos específicos de los datos de red sin procesar que son significativos para la topología de red subyacente. A modo de ejemplo, se revisa al menos uno de los siguientes elementos: información de Ethernet, tal como direcciones MAC Ethernet, información IP, como direcciones IP, información UDP, información de geolocalización, información GTPv2. Todos los paquetes que se transfieren a través de la red pueden ser buscados por identificadores LTE y agruparse según la identidad/similitud de los identificadores LTE localizados. Esos grupos pueden analizarse más a fondo en relación con más detalles, como direcciones IP, etc.

El método comprende además las etapas de:

identificar, a partir de los campos revisados, los roles de los respectivos componentes de la red, tal como por ejemplo, Núcleo de Paquetes Evolucionado (EPC), Entidad de Gestión de la Movilidad (MME) o Subsistema Multimedios IP (IMS), Función de Control de Sesión de Llamada (CSCF) y
determinar, en función de los roles identificados de los componentes de la red y de los campos revisados, la topología de la red.

Para revisar campos específicos de los datos de red sin procesar, incluso los protocolos utilizados podrían ser suficientes. Si un nodo está utilizando ciertos protocolos, existe una gran probabilidad de que tenga una funcionalidad específica.

Se proporciona un módulo de modelado de topología que revisa campos relevantes de los datos de red sin procesar en diferentes capas de protocolo del modelo OSI de 7 capas y aplica algoritmos para determinar la topología de red subyacente. Cada aplicación o nodo tiene que identificar el mensaje relevante por sí mismo. Esto se puede hacer a

través de un campo de protocolo único como el título global o una combinación de campos como la dirección IP y el puerto TCP. La primera etapa es identificar patrones comunes en paquetes como la misma dirección IP con el mismo puerto y título global, lo que probablemente sea indicativo de un nodo específico. Al agrupar esos patrones se puede hacer una primera agrupación. El mismo título global puede usar una dirección IP diferente para una mayor comunicación, por lo que un enlace entre algunos grupos debe ser visualizado. En general, una combinación de aprendizaje supervisado y no supervisado puede proporcionar los resultados. Con el aprendizaje supervisado, los ejemplos se etiquetarán y con el aprendizaje no supervisado, los grupos se construirán automáticamente.

Se aportará un ejemplo considerando el núcleo empaquetado evolucionado (EPC) LTE incluyendo la red troncal IP. Una vez que los mensajes del EPC son capturados y disponibles a través de la capa de almacenamiento, contienen información de Ethernet, IP, UDP y GTPv2. La dirección MAC de Ethernet es única y se puede utilizar para determinar el dispositivo de hardware. La dirección IP se puede usar para determinar el rol y la relación en una red IP. La IP y/o UDP ofrece información de geolocalización que habilita el nodo para ser colocado en una posición adecuada. Un nodo EPC puede tener múltiples direcciones IP y, por lo tanto, la información GDPv2, por ejemplo, GTPC-TEID, debe aplicarse para identificar el rol en la red EPC. Otros protocolos que también se usan dentro del mismo contexto pueden identificarse como el rol exacto como, por ejemplo, MME de un nodo. Sobre la base de la identificación de los diferentes roles de los diferentes componentes de la red, se puede derivar la topología de red subyacente.

El método propuesto permite al operador de una red tener siempre una vista actualizada de la red de telecomunicaciones y en capas de extremo a extremo. Como ya se mencionó anteriormente, el método propuesto ofrece beneficios significativos para escenarios de solución de problemas donde también, por ejemplo, los cortafuegos pueden hacerse transparentes incluso cuando la solución de problemas se lleva a cabo en una capa de GDPv2. La topología de la red se puede correlacionar con el tráfico real y las topologías históricas para identificar cambios en la red de telecomunicaciones. Se evitan errores manuales en inventarios y otras bases de datos y se reduce el mantenimiento de los mismos. El método propuesto no depende de protocolos de descubrimiento activos y se puede aprovechar para fines de planificación en todas las capas de red de acuerdo con el modelo OSI. Las oportunidades de optimización se pueden identificar rápidamente y la planificación de la capacidad se puede hacer con la ayuda del rendimiento del tráfico y la visualización de la ruta del tráfico.

La presente invención también se refiere a un sistema para mantener, asegurar y/o garantizar el funcionamiento correcto/deseado de una red de telecomunicaciones, en el que el sistema comprende un medio interpretable por ordenador con un código de programa, que se configura, cuando se ejecuta en una unidad de ordenador, para activar al menos las siguientes etapas:

- extraer, capturar y recopilar de datos de red sin procesar desde al menos una función de red, como un componente de red, una herramienta de red, un interfaz de red y/o una aplicación de red,
- duplicar los datos de red sin procesar capturados,
- convertir los datos de red sin procesar capturados duplicados en un formato interpretable por el personal,
- almacenar los datos de red sin procesar convertidos en un almacenamiento de datos que admite procesamiento paralelo y escalado horizontal,
- hacer que los datos de red sin procesar almacenados estén disponibles a través de al menos un interfaz de programación de aplicaciones para un despliegue adicional como para la automatización de la red con respecto a la detección de fallos y al reacondicionamiento de la red de telecomunicaciones, y para la modelización de la red de telecomunicaciones, y
- recuperar a través de al menos un interfaz de programación de aplicaciones al menos un subconjunto de los datos de red sin procesar disponibles, dependiendo el subconjunto de la realización posterior, y
- buscar en los datos de red sin procesar recuperados datos que sean indicativos y que puedan utilizarse para la detección de fallos y/o el modelado de topología,
- analizar los datos de red sin procesar recuperados con respecto a los parámetros del protocolo, e
- identificar en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, en al menos una causa raíz de problemas que perturben/afecten el estado actual de funcionamiento de la red de telecomunicaciones,
- indicando la al menos una causa raíz identificada a un operador de la red de telecomunicaciones a través de un interfaz de usuario.

El sistema puede usarse, por ejemplo, para una red de telecomunicaciones virtual. De acuerdo con una realización del sistema propuesto, La red de telecomunicaciones se mapea lógicamente en una red en capas, comprendiendo la red en capas al menos una capa de función de red, una capa de conversión, una capa de almacenamiento y una capa de aplicación, estando las capas interrelacionadas a través de interfaces de red respectivos en los que el sistema comprende un medio interpretable por ordenador con un código de programa, que se configura, cuando se ejecuta en una unidad de ordenador, para activar al menos las siguientes etapas:

- extraer, capturar y recopilar datos de red sin procesar de al menos una función de red tal como un componente de red, una herramienta de red, un interfaz de red y/o una aplicación de red, en donde la al menos una función de red se ejecuta en la capa de funciones de red,

- duplicar los datos de red sin procesar capturados,
- convertir los datos de red sin procesar capturados duplicados en un formato interpretable por el personal dentro de la capa de conversión,
- almacenar los datos de red sin procesar convertidos en un almacenamiento de datos que admite procesamiento paralelo y escalado horizontal,
- hacer que los datos de red sin procesar almacenados estén disponibles en la capa de aplicación a través de al menos un interfaz de programación de aplicaciones para un despliegue adicional como para la automatización de la red con respecto a la detección de fallos y reacondicionamiento de la red de telecomunicaciones, y para el modelado de topología de la red de telecomunicaciones, y
- recuperar a través del al menos un interfaz de programación de aplicaciones al menos un subconjunto de los datos de red sin procesar disponibles, dependiendo el subconjunto del despliegue posterior, y
- buscar, en una capa de análisis, los datos de red sin procesar recuperados para datos que sean indicativos y utilizables para la detección de fallos y/o el modelado de la topología,
- analizar los datos de red sin procesar recuperados con respecto a los parámetros del protocolo, e
- identificar en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, en al menos una causa raíz de problemas que perturben/afecten el estado actual de funcionamiento de la red de telecomunicaciones,
- indicar al menos una causa raíz identificada a un operador de la red de telecomunicaciones a través de un interfaz de usuario.

Otras realizaciones de la presente invención se describen en el presente documento, a modo de ejemplo, junto con las siguientes figuras, en las que

La figura 1 muestra un diagrama de flujo que ilustra un flujo del método de acuerdo con diversas realizaciones del método propuesto;
La figura 2 muestra un escenario que puede usarse al determinar una topología de una red de telecomunicaciones subyacente de acuerdo con una realización del método propuesto.

Aunque se describen varias realizaciones de la invención junto con las figuras, debe ser evidente que diversas modificaciones, alteraciones y adaptaciones a esas realizaciones se le pueden ocurrir a una persona experta en la técnica con el logro de parte o la totalidad de las ventajas de la presente invención. Por lo tanto, se pretende cubrir todas esas modificaciones, alteraciones y adaptaciones sin apartarse del alcance de la presente invención tal como se define en las reivindicaciones adjuntas.

La figura 1 muestra un diagrama de flujo 100 de posibles realizaciones del método reivindicado.

En una primera etapa 110, se extraen y recopilan datos de la red sin procesar de al menos una función de red, tal como componentes de red y/o herramientas de red (protocolos de red) de una red de telecomunicaciones. Tales componentes de la red y/o herramientas de red se pueden elegir del grupo que comprende al menos un interfaz de red, un controlador de interfaz de red y/o cualquier punto de duplicación de tráfico. Un interfaz de red es un interfaz entre dos equipos o capas de protocolo en la red de telecomunicaciones. El interfaz de red generalmente tiene alguna forma de dirección de red que también se puede elegir como fuente de datos para los datos sin procesar que se van a extraer y recopilar. La dirección de red puede consistir en una ID de nodo y un número de puerto, o puede ser una ID de nodo única por derecho propio. Los interfaces de red proporcionan funciones normalizadas, como pasar mensajes, conectarse y desconectarse, etc. Además, a partir de estas funciones normalizadas, los datos sin procesar pueden extraerse y utilizarse para su posterior utilización. Un controlador de interfaz de red, también conocido como una tarjeta de interfaz de red o un adaptador de red, es un componente de hardware de ordenador que lo conecta a la red de telecomunicaciones. El controlador de interfaz de red realiza el circuito electrónico requerido para comunicarse utilizando una capa física específica y una norma de capa de enlace de datos, tales como Internet, Canal de Fibra o WiFi.

En otra segunda etapa 120, los datos de red sin procesar extraídos y recopilados se duplican y los datos duplicados se almacenan en un formato interpretable por el personal como JSON en una capa/biblioteca de almacenamiento de datos. En otra etapa adicional 130, los datos de red sin procesar extraídos y recopilados se ponen a disposición a través de al menos un interfaz de programación de aplicaciones que está relacionado con el almacenamiento de datos/biblioteca. Los datos de red sin procesar extraídos y recopilados se proporcionan a través del al menos un interfaz de programación de aplicaciones para un despliegue adicional para la (re) configuración de la red de telecomunicaciones. En general, hay más de un interfaz de programación de aplicaciones que están relacionadas con el almacenamiento de datos y que pueden proporcionar u ofrecer acceso a los datos de red sin procesar que se almacenan en el almacenamiento de datos/biblioteca. De acuerdo con una realización del método propuesto, los datos de red sin procesar extraídos y recopilados se recuperan en una etapa adicional 131 a través del al menos un interfaz de programación de aplicaciones. Los datos de red sin procesar extraídos y recopilados se analizan con respecto a parámetros clave específicos como son los bits de control TCP (Protocolo de Control de la Transmisión) o códigos de causas GTP (Protocolo de Túnel GPRS) en diferentes capas de red de entre las siete capas de acuerdo con el modelo OSI de 7 capas de la red de telecomunicaciones subyacente. Basándose en los datos de red sin procesar extraídos y

recopilados, se identifica al menos una causa raíz de problemas/asuntos que perturban y/o afectan el estado de funcionamiento actual de la red de telecomunicaciones. Una cantidad anormal de ciertos códigos de causas GTP o retransmisiones TCP, es decir, bits de control TCP, indica un problema en la red. O una gran cantidad anormal de direcciones IP de origen con el mismo destino IP indica un ataque DoS.

De acuerdo con otra etapa adicional133, la al menos una causa raíz identificada se le indica a un operador de la red de telecomunicaciones por medio de una pantalla o de cualquier otro dispositivo de salida adecuado. El dispositivo de salida también puede tener una salida visual y/o acústica. En una etapa 132, que es alternativa a la etapa 133 o complementaria a la etapa 133 posible que un motor de flujo de trabajo que contenga o tenga acceso a una biblioteca de acciones, cada acción vinculada con al menos una causa raíz y utilizable para devolver la red a una estación de trabajo deseable, se activa de modo que al menos una acción de la biblioteca que está vinculada a al menos una causa raíz identificada se interprete y se realice automáticamente en una etapa adicional 134. Debido a la al menos una acción, la red de telecomunicaciones vuelve a su estado normal de funcionamiento. De acuerdo con una posible realización, la etapa de identificar en la red de telecomunicaciones la al menos una causa raíz comprende reconocer al menos un mensaje de red que sea indicativo de la al menos una causa raíz.

En una realización adicional del método propuesto, los campos clave específicos de los datos de red sin procesar se revisan en la etapa 141, en la que los campos específicos revisados son importantes para la topología de red de la red de telecomunicaciones subyacente. En la etapa 142, los roles de los componentes de red respectivos de la red de telecomunicaciones subyacente se identifican a partir de los campos revisados y en una etapa 143, una topología de red de la red de telecomunicaciones subyacente finalmente se determina y se deriva de los roles identificados de los componentes de la red.

Para identificar y caracterizar los roles específicos de los componentes de red específicos, se revisa al menos uno de los siguientes elementos:

- Información de Ethernet, tal como direcciones MAC de Ethernet
- Información de IP, tal como direcciones IP
- Información UDP
- Información de geolocalización e información de GDPv2.

Estos son solo ejemplos muy limitados; véase también la lista de identificadores LTE. Sin embargo, el método propuesto no se limita a LTE, ya que todas las redes usan algunos tipos de identificadores.
La figura 2 muestra un escenario de ejemplo dentro de una red de telecomunicaciones que puede usarse para determinar una topología de la red de telecomunicaciones.

Si una MME 210 (entidad de gestión de la movilidad) y un eNodoB 220 (nodo B evolucionado) intercambian un mensaje S1-MME (un mensaje de señalización LTE con protocolo de aplicación (AP)) como se indica mediante una flecha doble, tal mensaje S1-MME contiene identificadores en múltiples capas OSI (Ethernet, IP y S1-AP). Contiene un identificador MME 211, una dirección IP 212 de la MME 210, una dirección MAC 213 de la MME 210, un identificador eNodeB 221, una dirección IP 222 del eNodeB 220 y una dirección MAC 223 del eNodeB 220. Cada paquete capturado es un documento que contiene toda esa información. Una consulta simple para contar todos los documentos en los que los identificadores MAC, IP y S1-AP sean iguales, proporcionará una visión general del flujo de mensajes entre estos dos nodos diferentes. En la siguiente etapa, se solicita que enumeren para cada identificador S1-AP todos los diferentes identificadores IP. Esto dará como resultado una lista con toda la comunicación IP para dicho nodo determinado.

El siguiente enlace proporciona una visión general de los identificadores LTE y su uso: https://de.slideshare.net/allabout4g/lte-identifiers. Esos identificadores LTE pueden usarse para identificar diferentes roles de diferentes nodos con el sistema de telecomunicaciones y, por lo tanto, para modelar la topología de la red de telecomunicaciones.

Además, los protocolos utilizados identifican la función lógica del nodo como, por ejemplo, MME o HSS (Servidor de Abonado Doméstico). Dependiendo de dónde, es decir, en qué capa OSI, se han capturado los paquetes, pueden ser exactamente los mismos en la capa superior, pero pueden tener cambios en la capa inferior, como, por ejemplo, dirección MAC. Esto indica que un dispositivo ha estado involucrado en la comunicación como, por ejemplo, un cortafuegos.

REIVINDICACIONES

1. Un método para mantener, asegurar y/o garantizar el funcionamiento correcto/deseable de una red de telecomunicaciones, que comprende al menos las siguientes etapas:

- extraer, capturar y recopilar (110) datos de red sin procesar de al menos una función de red, como un componente de red, una herramienta de red, un interfaz de red y/o una aplicación de red,
- duplicar (120) los datos de red sin procesar capturados,
- convertir (120) los datos de red sin procesar capturados duplicados en un formato interpretable por el personal,
- almacenar (120) los datos de red sin procesar convertidos en un almacenamiento de datos que soporte procesamiento paralelo y escalado horizontal, y
- hacer que (130) los datos de red sin procesar almacenados estén disponibles por medio de al menos un Interfaz de programación de aplicaciones para un despliegue adicional en cuanto a la automatización de la red, particularmente con respecto a la detección de fallos y reacondicionamiento de la red de telecomunicaciones, y para el modelo de topología de la red de telecomunicaciones,
- recuperar a través de al menos una interfaz de programación de aplicaciones al menos un subconjunto de los datos de red sin procesar disponibles, dependiendo el subconjunto del despliegue adicional,
- buscar los datos de red sin procesar recuperados para datos que sean indicativos y utilizables para un caso de uso específico, como para la detección de fallos y/o el modelo de topología,
- analizar (131) los datos de red sin procesar recuperados con respecto a los parámetros del protocolo, e
- identificar (131) en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, al menos una causa raíz de problemas que perturban/afectan el estado de funcionamiento actual de la red de telecomunicaciones,
- indicar (133) la al menos una causa raíz identificada a un operador de la red de telecomunicaciones a través de un interfaz de usuario.

2. El método de acuerdo con la reivindicación 1, en el que los datos de red sin procesar son proporcionados directamente por la al menos una función de red a través de un interfaz o por medio de al menos un agente de rastreo que se ejecuta en una máquina virtual.

3. El método de acuerdo con la reivindicación 1 o 2, en el que los datos de red sin procesar se capturan mediante un mecanismo de extracción o mediante un mecanismo de empuje.

4. El método de acuerdo con las reivindicaciones 1 a 3, en el que los datos de red sin procesar se extraen y se recopilan desde un interfaz de red, un controlador de interfaz de red y/o cualquier punto de duplicación de tráfico de la red de telecomunicaciones.

5. El método de acuerdo con cualquiera de los anteriores reivindicaciones en el que la red de telecomunicaciones está mapeada lógicamente en una red en capas, comprendiendo la red en capas al menos una capa de función de red, una capa de conversión, una capa de almacenamiento y una capa de aplicaciones, estando las capas interrelacionadas a través de los interfaces de red respectivos, y en el que la al menos una función de red se ejecuta en la capa de función de red, se realiza la conversión de los datos de red sin procesar capturados duplicados en un formato interpretable por el personal dentro de la capa de conversión, y los datos de red sin procesar convertidos se almacenan en la capa de almacenamiento de datos, y los datos de red sin procesar almacenados se ponen a disposición en la capa de aplicación a través de al menos un interfaz de programación de aplicaciones para un despliegue adicional como para la automatización de la red y para el modelado de topologías de la red de telecomunicaciones.

6. Método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además la etapa de:

- activar (132) un motor de flujo de trabajo que contiene una biblioteca de acciones, estando vinculada cada acción a al menos una causa raíz y se puede utilizar para volver a poner la red de telecomunicaciones en un estado de trabajo deseable, y
- realizar (132) al menos una acción de la biblioteca que está vinculada a la al menos una causa raíz identificada.

7. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en el que la etapa de identificar en la red de telecomunicaciones la al menos una causa raíz comprende reconocer al menos un mensaje de red que sea indicativo de la al menos una causa raíz.

8. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, que comprende además las siguientes etapas:

- modelar, basándose en los datos de red sin procesar recuperados, una topología de red de la red de telecomunicaciones combinando múltiples capas de protocolo y dominios tecnológicos de la red de telecomunicaciones.

9. El método de acuerdo con la reivindicación 8, que comprende además la siguiente etapa:

- revisar (141) campos específicos, como dirección IP o título global, a partir de los datos sin procesar de la red, que sean significativos para la topología de la red,
- identificar (142), de los campos revisados, los roles de los componentes de red respectivos dentro de la red de telecomunicaciones; y
- determinar (143), basándose en los roles identificados de los componentes de red y los campos revisados, la topología de red de la red de telecomunicaciones.

10. El método de acuerdo con la reivindicación 8 o 9, en el que se revisa al menos uno de los siguientes elementos: información de Ethernet, tal como direcciones MAC de Ethernet, información IP, tal como direcciones IP, información UDP, información de geolocalización, información GTPv2.

11. Un sistema para mantener, asegurar y/o garantizar un funcionamiento correcto/deseable de una red de telecomunicaciones en el que el sistema comprende un medio interpretable por ordenador con un código de programa, que está configurado, cuando se ejecuta en una unidad de ordenador para activar al menos las siguientes etapas:

- extraer, capturar y recopilar datos de red sin procesar de al menos una función de red, como un componente de red, una herramienta de red, un interfaz de red y/o una aplicación de red,
- duplicar los datos de red sin procesar capturados,
- convertir los datos de red sin procesar capturados duplicados en un formato interpretable por el personal,
- almacenar los datos de red sin procesar convertidos en un almacenamiento de datos que admita procesamiento paralelo y escalado horizontal,
- poner a disposición los datos de red sin procesar almacenados a través de al menos un interfaz de programación de aplicaciones para un despliegue adicional en cuanto a la automatización de la red con respecto a la detección de fallos y el reacondicionamiento de la red de telecomunicaciones, y para el modelado de topología de la red de telecomunicaciones, y
- recuperar a través de al menos un interfaz de programación de aplicaciones al menos un subconjunto de los datos de red sin procesar disponibles, dependiendo el subconjunto del despliegue adicional, y
- buscar en los datos de red sin procesar recuperados datos indicativos y utilizables para la detección de fallos y/o el modelado de topología,
- analizar (131) los datos de red sin procesar recuperados con respecto a los parámetros del protocolo, e
- identificar (131) en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, al menos una causa raíz de problemas que perturban/afectan el estado de funcionamiento actual de la red de telecomunicaciones,
- indicar (133) la al menos una causa raíz identificada a un operador de la red de telecomunicaciones a través de un interfaz de usuario.

12. El sistema de acuerdo con la reivindicación 11, en el que la red de telecomunicaciones está mapeada lógicamente en una red en capas, comprendiendo la red en capas al menos una capa de función de red, una capa de conversión, una capa de almacenamiento y una capa de aplicación, estando las capas interrelacionadas a través de los interfaces de red respectivos, en el que el sistema comprende un medio interpretable por ordenador con un código de programa, que se configura, cuando se ejecuta en una unidad informática, para activar al menos las siguientes etapas:

- extraer, capturar y recopilar de la red sin procesar de la al menos una función de red que se ejecuta en la capa de función de red,
- duplicar los datos de red sin procesar capturados,
- convertir los datos de red sin procesar capturados duplicados en un formato interpretable por el personal dentro de la capa de conversión,
- almacenar los datos de red sin procesar convertidos en la capa de almacenamiento de datos que soporte procesamiento paralelo y escalado horizontal, y
- hacer que los datos de red sin procesar almacenados estén disponibles en la capa de aplicación a través de al menos un interfaz de programación de aplicaciones para un despliegue adicional en cuanto a automatización de red y modelado de topología de la red de telecomunicaciones, y
- recuperar a través de al menos un interfaz de programación de aplicaciones al menos un subconjunto de los datos de red sin procesar disponibles, dependiendo el subconjunto del despliegue adicional, y
- buscar en los datos de red sin procesar recuperados datos indicativos y utilizables para la detección de fallos y/o el modelado de topología,
- analizar (131) los datos de red sin procesar recuperados con respecto a los parámetros del protocolo, e
- identificar (131) en la red de telecomunicaciones, basándose en los datos de red sin procesar almacenados analizados, al menos una causa raíz de problemas que perturban/afectan el estado de funcionamiento actual de la red de telecomunicaciones,
- indicar (133) la al menos una causa raíz identificada a un operador de la red de telecomunicaciones a través de un interfaz de usuario.

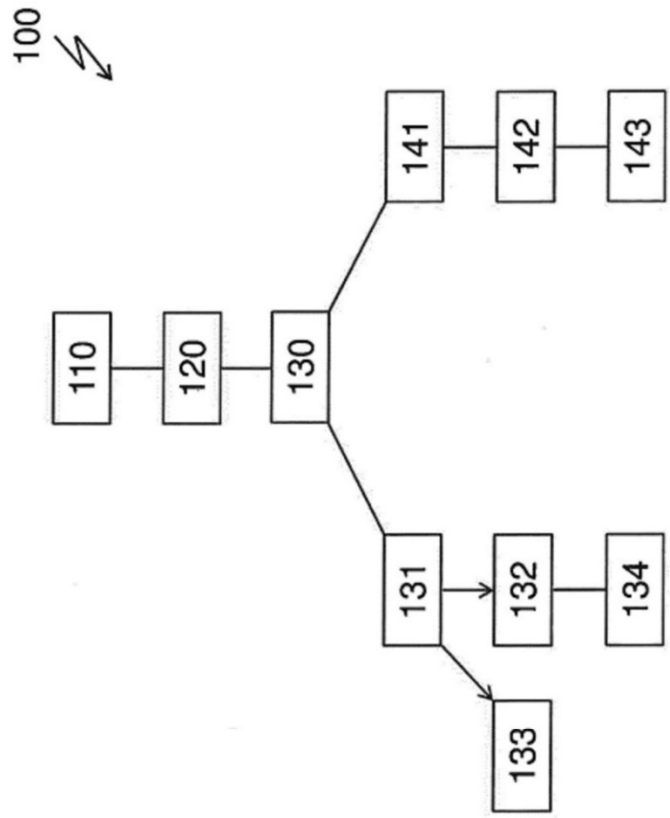

Fig. 1

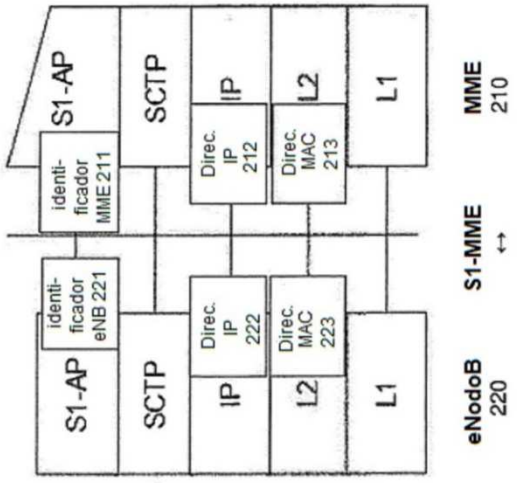
S1-AP
SCTP
IP
L2
L1
identi-ficador MME 211
Direc. IP 212
Direc. MAC 213
MME 210
S1-MME
identi-ficador eNB 221
Direc. IP 222
Direc. MAC 223
eNodoB 220

Fig. 2