(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 718 199**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 12/715 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **02.09.2015 PCT/EP2015/070057**

(87) Fecha y número de publicación internacional: **17.03.2016 WO16037917**

(96) Fecha de presentación y número de la solicitud europea: **02.09.2015 E 15756668 (8)**

(97) Fecha y número de publicación de la concesión europea: **27.02.2019 EP 3192226**

(54) Título: **Dispositivo y procedimiento para el control de una red de comunicación**

(30) Prioridad:

08.09.2014 DE 102014217944
06.05.2015 DE 102015107073

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.06.2019

(73) Titular/es:

RHEINMETALL DEFENCE ELECTRONICS GMBH (100.0%)
Brüggeweg 54
28309 Bremen, DE

(72) Inventor/es:

STEHMEIER, HENRICH

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Dispositivo y procedimiento para el control de una red de comunicación

La presente invención se refiere a un dispositivo para el control de una red de comunicación con una pluralidad de terminales para la comunicación de datos. La presente invención se refiere también a un router con tal dispositivo, un conmutador con tal dispositivo, un cortafuegos con tal dispositivo, así como una red de comunicación con tal dispositivo. La presente invención además a un procedimiento y un producto de programa informático para el control de una red de comunicación.

El campo técnico de la presente invención se refiere a la seguridad (seguridad IT) de redes de comunicación, por ejemplo, redes de comunicación de empresas, universidades, autoridades y otras organizaciones.

Las redes de comunicación de empresas y similares se encuentran cada vez más en la mira de los atacantes, en particular para expiarlas. Los escenarios de amenazas para las redes de comunicación se especializan cada vez más, están diseñados a menudo a largo plazo y utilizan técnicas de camuflaje altamente especializadas. Los atacantes buscan a menudo durante sus ataques a las redes de comunicación de empresas y similares específicamente puntos vulnerables en su estrategia de seguridad.

Las soluciones de seguridad convencionales, tales como cortafuegos, soluciones de IPS y de antivirus y puertas de enlace web (Web-Gateways), están diseñadas para detectar patrones de ataque conocidos mediante la utilización de medidas de seguridad dependientes de firmas. Sin embargo, las generaciones más actuales de ataques no están limitadas a patrones de ataque conocidos, sino que son dinámicas. Por ejemplo, se persiguen objetivos en varios vectores de ataque y fases, lo que aumenta drásticamente el potencial de amenaza para las redes de empresas.

Las configuraciones de red estáticas convencionales tienen la desventaja de ser un blanco más fácil del espionaje y de los ataques por parte de atacantes, tales como entidades no autorizadas.

Un control de una red de comunicación con un controlador SDN se describe en el documento ZHOU HAIFENG ET AL: “Evolving defense mechanism for future network security”, IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, tomo 53, número 4, con fecha 8 de abril de 2015 (2015-04-08), páginas 45 a 51, XP011577593, ISSN: 0163-6804, DOI: 10.1109/MCOM.2015.7081074. En este caso se utiliza una estrategia de cambio de configuración de red en dependencia de parámetros del sistema y del usuario.

Soluciones basadas en SDN para una protección de red defensiva contra objetivos en movimiento se describen en el documento KAMPANAKIS PANOS ET AL: “SDN-based solutions for moving target defense network protection”, PROCEEDING OF IEEE INTERNATIONAL SYMPOSIUM ON A WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS 2014, IEEE, con fecha 19 de junio de 2014 (2014-06-19), páginas 1 a 6, XP032656398, DOI: 10.1109/WOWMOM.2014.6918979.

Teniendo en cuenta estos antecedentes, un objetivo de la presente invención es proporcionar una red de comunicación más segura.

Según un primer aspecto se propone un dispositivo para el control de una red de comunicación con una pluralidad de terminales para la comunicación de datos. El dispositivo comprende una unidad de control que está diseñada para desacoplar un plano de datos y un plano de control de la comunicación de datos y modificar al menos una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, durante una sesión de comunicación mediante la utilización del plano de control desacoplado.

Dado que la unidad de control modifica, en particular de manera dinámica, la al menos una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, durante cada sesión de comunicación, un observador o atacante externo de la red de comunicación no puede expiar prácticamente la red de comunicación, porque la configuración y, por tanto, el aspecto de la red de comunicación resultan indeterminables e impredecibles para el observador externo. Adicional o alternativamente se pueden modificar también patrones de datos visibles de la red de comunicación. Esto aumenta la seguridad de la red de comunicación.

Ejemplos de la al menos una característica de la red de comunicación, modificables por la unidad de control, son el cambio de direcciones virtuales de terminales de la red de comunicación, el cambio de la configuración de la red de comunicación, el cambio del comportamiento de enrutamiento de la red de comunicación y el cambio de aplicaciones y/o sus asignaciones de puerto.

Por una sesión de comunicación o sesión se entiende una comunicación entre uno de los terminales de la red de comunicación con una unidad situada por fuera de la red de comunicación o dentro de la red de comunicación. La sesión de comunicación se puede basar también en protocolos sin estado, por ejemplo, HTTP (Hypertext Transfer Protocol, Protocolo de transferencia de hipertexto).

La unidad de control puede estar implementada mediante hardware y/o también software. En caso de una implementación mediante hardware, la unidad de control puede estar configurada como dispositivo o como parte de

un dispositivo, por ejemplo, como ordenador o como microprocesador o como router o conmutador. En caso de una implementación por software, la unidad de control puede estar configurada como producto de programa informático, como una función, como una rutina, como parte de un código de programa o como objeto ejecutable.

Una herramienta adecuada para la implementación de la unidad de control es el controlador SDN de código abierto OpenMUL (Open-Source SDN-Controller OpenMUL) (véase referencia [1]). El controlador OpenMUL pone a disposición una plataforma de control implementada en C y basada en SDN/OpenFlow. La unidad de control está diseñada aquí preferentemente para utilizar el protocolo OpenFlow (véase referencia [2]), así como la técnica Moving-Target-Defence (MTD) (véase referencia [3]). Mediante la utilización de Moving-Target-Defence, la unidad de control está diseñada en particular para modificar de manera dinámica la red de comunicación. El OpenFlow es un protocolo de comunicación que proporciona acceso a los componentes de hardware de un conmutador o un router que ejecutan el procesamiento de paquetes de red entrantes (el llamado plano de reenvío (Forwarding Plane)).

El propio dispositivo puede estar implementado por hardware y/o software. En el caso de una implementación por hardware del dispositivo, éste puede estar configurado, por ejemplo, como ordenador, como parte de un router, como parte de un conmutador o como parte de un cortafuegos. En el caso de una implementación por software, el dispositivo puede estar configurado como producto de programa informático, como una función, como una rutina, como parte de un código de programa o como objeto ejecutable,

La red de comunicación se puede identificar también como red o red de ordenador y es, por ejemplo, una red LAN (Local Area Network, red de área local) o una red WAN (Wide Area Network, red de área amplia).

El desacoplamiento del plano de datos y del plano de control de la comunicación de datos se puede realizar, por ejemplo, mediante redes definidas por software (Software-Defined-Networking) (véase referencias [4] y [5]).

Ejemplos de terminales de la red de comunicación son las calculadoras, los ordenadores, los routers, los conmutadores, los cortafuegos, los sistemas embebidos o similares.

La unidad de control está diseñada para modificar proactivamente la al menos una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, durante la sesión de comunicación mediante la utilización del plano de control desacoplado.

La unidad de control es adecuada entonces para modificar proactivamente la al menos una característica visible. Por tanto, se modifica la al menos una característica de la red de comunicación, incluso antes de producirse una amenaza o un daño en la red de comunicación. De este modo se puede proporcionar una seguridad proactiva en tiempo real para la red de comunicación.

Por modificación proactiva se entiende aquí en particular que se modifica la al menos una característica visible al finalizar cada flujo de datos. Por consiguiente, la presente unidad de control está diseñada, a diferencia de una modificación reactiva convencional, para modificar de manera proactiva o para modificar de manera proactiva y reactiva en una situación de amenaza identificada o un año detectado.

La unidad de control está diseñada en particular para modificar proactivamente la red de comunicación de tal modo que zonas de seguridad diferentes con niveles de seguridad diferentes y/o funciones de seguridad diferentes se pueden establecer dinámicamente en la red de comunicación. Por ejemplo, la unidad de control puede cambiar las zonas de seguridad establecidas en dependencia de escenarios de amenaza identificados. La unidad de control está diseñada también preferentemente para establecer una operación de día y una operación de noche en la red de comunicación, que tienen niveles de seguridad diferentes.

Según otra forma de realización, la unidad de control está diseñada para cambiar una dirección virtual al menos de un terminal de la pluralidad de terminales durante la sesión de comunicación mediante la utilización del plano de control desacoplado. Una dirección virtual es una dirección lógica que se puede convertir en una dirección física mediante una unidad lógica o una unidad de ordenador.

Según otra forma de realización, el dispositivo comprende un generador aleatorio para emitir un valor aleatorio. La unidad de control está diseñada aquí para cambiar la dirección virtual en dependencia del valor aleatorio emitido por el generador aleatorio.

Según otra forma de realización, la unidad de control está diseñada para modificar la configuración de la red de comunicación durante la sesión de comunicación mediante la utilización del plano de control desacoplado. Un cambio en la configuración de la red de comunicación comprende preferentemente un cambio de los niveles de seguridad establecidos o de las zonas de seguridad establecidas de la red de comunicación. Por tanto, el dispositivo puede reaccionar de manera diferente a escenarios de ataque diferentes mediante el cambio de la configuración de la red de comunicación.

Según otra forma de realización, la unidad de control está diseñada para modificar un comportamiento de enrutamiento de la red de comunicación durante la sesión de comunicación mediante la utilización del plano de

control desacoplado. Como resultado del cambio propuesto del comportamiento de enrutamiento de la red de comunicación, un atacante no puede sacar ninguna conclusión útil a partir de una grabación o registro del comportamiento de enrutamiento de la red de comunicación debido a la ausencia de una característica estática del comportamiento de enrutamiento.

Según otra forma de realización, la unidad de control está diseñada para modificar al menos una aplicación de la red de comunicación durante la sesión de comunicación mediante la utilización del plano de control desacoplado. Debido a los cambios de las aplicaciones de la red de comunicación, un atacante no puede obtener ninguna información útil sobre la red de comunicación.

Según otra forma de realización, la unidad de control está diseñada para modificar al menos una asignación de puerto de la al menos una aplicación durante la sesión de comunicación mediante la utilización del plano de control desacoplado. Debido a los cambios de la asignación de puerto de una aplicación de la red de comunicación, un atacante no puede obtener ninguna información útil sobre la red de comunicación

Según otra forma de realización, la unidad de control está diseñada para sustituir un primer algoritmo criptográfico, utilizado por la red de comunicación, por un segundo algoritmo criptográfico durante la sesión de comunicación.

La unidad de control puede seleccionar el segundo algoritmo criptográfico preferentemente a partir de una pluralidad de algoritmos criptográficos preparados.

Un atacante no puede obtener ventajosamente informaciones útiles sobre la red de comunicación, como en el caso de la utilización de un algoritmo criptográfico estático, debido a la sustitución de los algoritmos criptográficos.

Por un algoritmo criptográfico se entiende un algoritmo que calcula al menos un valor criptográfico, por ejemplo, mediante una función criptográfica. Los algoritmos criptográficos comprenden algoritmos de cifrado, por ejemplo, SSL (Secure Sockets Layer, capa de puertos seguros), así como firmas digitales. Los valores criptográficos pueden comprender claves criptográficas, por ejemplo, claves simétricas, y/o valores hash.

Según otra forma de realización, la unidad de control está diseñada para modificar un patrón de datos de la red de comunicación, en particular un perfil de datos útiles al menos de uno de los terminales.

Mediante la modificación de un patrón de datos o varios patrones de datos de la red de comunicación, la unidad de control permite simular un tráfico de datos para un atacante. El tráfico de datos simulado se puede identificar también como imitación de datos o imitación de comunicación. La unidad de control está diseñada también preferentemente para cambiar los terminales acoplados a la red de comunicación, es decir, terminales de red o participantes en la red, con el fin de modificar así los patrones de datos de la red de comunicación. Debido a la modificación de los patrones de datos, a un atacante le resulta claramente difícil ejecutar comparaciones satisfactorias de patrones binarios.

Según otra forma de realización, la sesión de comunicación comprende una pluralidad de transacciones de datos (data flows). En este caso, la unidad de control está diseñada para modificar la al menos una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, después de una cantidad parcial de la pluralidad de transacciones.

La cantidad parcial de transacciones, después de la que la unidad de control modifica la al menos una característica visible de la red de comunicación, se puede activar o especificar, por ejemplo, mediante un generador aleatorio.

Según otra forma de realización, la sesión de comunicación comprende una pluralidad de transacciones de datos, estando diseñada la unidad de control para modificar la al menos una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, después de cada transacción de la pluralidad de transacciones.

El cambio de la característica o de las características después de cada transacción permite aumentar más el grado de seguridad para la red de comunicación.

Según otra forma de realización, la unidad de control está diseñada para desacoplar el plano de control y el plano de datos de la comunicación de datos mediante la red definida por software. La red definida por software es una variante para construir dispositivos o terminales para redes de comunicación que separa dos componentes entre sí, específicamente datos y comandos, y los abstrae (véase al respecto las referencias [4] y [5]).

Según otra forma de realización, el dispositivo comprende un generador aleatorio acoplado a la unidad de control. El generador aleatorio está diseñado para activar de manera aleatoria o casi aleatoria la unidad de control con el fin de modificar la al menos una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, al menos una vez durante la sesión de comunicación, en particular varias veces durante la sesión de comunicación. El generador aleatorio o generador de números aleatorios genera una secuencia de valores aleatorios o números aleatorios. El generador aleatorio puede estar configurado como generador determinístico de números aleatorios o como un generador no determinístico de números aleatorios.

Según otra forma de realización, el dispositivo comprende una primera unidad de protección para detectar, aislar y combatir accesos de entidades no autorizadas a la red de comunicación. Según esta forma de realización, la primera unidad de protección es adecuada para detectar un ataque o un acceso de una entidad no autorizada para la red de comunicación, aislar el ataque detectado en la red de comunicación y tomar también medidas contra este ataque.

Según otra forma de realización, el dispositivo comprende una segunda unidad de protección para avisar y alertar a un sistema de evaluación acoplable al dispositivo. La segunda unidad de protección está diseñada ventajosamente para advertir y alertar a un sistema de evaluación acoplable al dispositivo, que puede ser operado, por ejemplo, por una entidad estatal.

Según otra forma de realización, el dispositivo comprende una tercera unidad de protección para restablecer al menos una función de red crítica.

En este caso, la tercera unidad de protección puede estar diseñada en particular para activar al menos una unidad redundante para ejecutar la función de red crítica después de detectarse el fallo de una función de red crítica con el fin de restablecer la función de red crítica. Por consiguiente, el presente dispositivo es adecuado ventajosamente para restablecer automáticamente funciones de red críticas.

Según otra forma de realización, el dispositivo comprende una unidad de análisis para proporcionar datos de análisis en caso de accesos de entidades no autorizadas a la red de comunicación.

Según otra forma de realización, el dispositivo comprende una unidad de evaluación de datos para determinar mediante la utilización de los datos de análisis proporcionados datos de estado que son adecuados en particular para indicar una situación de seguridad en la red de comunicación.

Según otra forma de realización, el dispositivo comprende una unidad de interfaz para transmitir los datos de estado a un sistema de evaluación acoplable al dispositivo. El sistema de evaluación puede estar acoplado al dispositivo, por ejemplo, también mediante Internet. La unidad de interfaz está diseñada para establecer una transmisión protegida criptográficamente entre el sistema de evaluación y el dispositivo. Por ejemplo, la unidad de interfaz puede establecer también un túnel de comunicación protegido entre el dispositivo y el sistema de evaluación.

Según otra forma de realización, la red de comunicación presenta una infraestructura que comprende capas que se superponen. La infraestructura tiene en particular las capas superpuestas siguientes: capa 1, capa 2, capa 3, capa 4, capa 5, capa 6, capa 7. La unidad de control está implementada aquí como una red de superposición virtual (red overlay) que superpone la capa 2 y la capa 3 de la infraestructura.

Según otra forma de realización, la red de superposición virtual está implementada mediante la utilización del protocolo Virtual-Extensible LAN. Por ejemplo, la red de superposición está implementada mediante VXLAN (Virtual Extensible LAN). VXLAN es un protocolo de encapsulación para dejar funcionar la red de superposición en una infraestructura de capa 3 existente (véase referencia [6]).

Según otra forma de realización, la unidad de control está integrada en un cortafuegos, en un conmutador o en un router de la red de comunicación.

Según otra forma de realización, la unidad de control está implementada mediante software.

Según otra forma de realización, el dispositivo soporta IPv4 (Protocolo de Internet versión 4; véase referencia [7]) e IPv6 (Protocolo de Internet versión 6; véase referencia [8]).

Según otra forma de realización, el dispositivo utiliza una combinación formada por un protocolo de seguridad y un protocolo de túnel. La utilización del protocolo de túnel permite aumentar más la seguridad de la comunicación de datos.

Un ejemplo de protocolo de seguridad es IPsec (véase referencia [9]). Un ejemplo de protocolo de túnel es L2TP (véase referencia [10]). Otro ejemplo de un protocolo de túnel adecuado es Open-VPN (véase referencia [11]).

La unidad respectiva, por ejemplo, la unidad de análisis o la unidad de protección, puede estar implementada por hardware y/o también por software. En el caso de una implementación por hardware, la unidad puede estar configurada como dispositivo o como parte de un dispositivo, por ejemplo, como ordenador o como procesador o como conmutador. En el caso de una implementación por software, la unidad puede estar configurada como producto de programa informático, como una función, como una rutina, como parte de un código de programa o como objeto ejecutable.

Según un segundo aspecto se propone un router para una red de comunicación que integra un dispositivo según el primer aspecto o según una de sus formas de realización. Por un router se entiende en particular un aparato de red que puede transmitir paquetes de red entre varias redes de comunicación. Un router se puede utilizar para la conexión a Internet, para el acoplamiento seguro de varias ubicaciones de una empresa o para el acoplamiento directo de varios segmentos de red locales, dado el caso, con la adaptación a protocolos de red diferentes.

Según un tercer aspecto se propone un conmutador para una red de comunicación que integra un dispositivo según el primer aspecto o según una de sus formas de realización. Por un conmutador se entiende un elemento de acoplamiento que puede conectar entre sí segmentos de red. Éste garantiza dentro de un segmento de red que los paquetes de datos lleguen a su destino. Un conmutador se puede identificar también como conmutador de red o distribuidor.

Según un cuarto aspecto se propone un cortafuegos para una red de comunicación que integra un dispositivo según el primer aspecto o según una de sus formas de realización. Por un cortafuegos se entiende un elemento de red que protege una red de comunicación, una parte de la red de comunicación o un ordenador individual de la red de comunicación contra accesos a red no deseados. Un cortafuegos puede representar un sistema de seguridad o puede ser parte de un sistema de seguridad.

Según un quinto aspecto se propone una red de comunicación que integra una pluralidad de terminales para la comunicación de datos y un dispositivo según el primer aspecto o según una de sus formas de realización.

Según un sexto aspecto se propone un procedimiento para el control de una red de comunicación con una pluralidad de terminales para la comunicación de datos. El procedimiento comprende un desacoplamiento de un plano de control y de un plano de datos de la comunicación de datos y una modificación al menos de una característica de la red de comunicación, que es visible desde el exterior de la red de comunicación, durante una sesión de comunicación mediante la utilización del plano de control desacoplado.

Según un séptimo aspecto se propone un producto de programa informático que provoca la ejecución del procedimiento según el sexto aspecto en una unidad controlada por programa.

Un producto de programa informático, por ejemplo, un medio de programa informático, se puede proporcionar o suministrar, por ejemplo, como medio de almacenamiento, por ejemplo, tarjeta de memoria, lápiz USB, CD-ROM, DVD, o también en forma de un fichero que se puede descargar de un servidor en una red. Esto se puede llevar a cabo, por ejemplo, en una red de comunicación inalámbrica mediante la transmisión de un fichero correspondiente con el producto de programa informático o el medio de programa informático.

Las formas de realización y las características descritas del dispositivo propuesto son válidas respectivamente para el procedimiento propuesto.

Otras implementaciones posibles de la invención comprenden también combinaciones no mencionadas explícitamente de características o formas de realización descritas antes o a continuación respecto a los ejemplos de realización. En este sentido, el técnico incluirá también aspectos individuales como mejoras o complementos de la forma básica respectiva de la invención.

La invención se explica detalladamente a continuación por medio de formas de realización preferidas con referencia a las figuras adjuntas. Muestran:

Fig. 1 un diagrama de bloques esquemático de un primer ejemplo de realización de un dispositivo para el control de una red de comunicación;

Fig. 2 un diagrama de bloques esquemático de un segundo ejemplo de realización de un dispositivo para el control de una red de comunicación;

Fig. 3 un diagrama de bloques esquemático de un tercer ejemplo de realización de un dispositivo para el control de una red de comunicación;

Fig. 4 un diagrama de bloques esquemático de una red de comunicación con un dispositivo según una de las figuras 1 a 3;

Fig. 5 un diagrama de bloques esquemático de una arquitectura SDN con plano de datos y plano de control desacoplados para la implementación de una unidad de control;

Fig. 6 un diagrama de bloques esquemático de un ejemplo de realización de un router con un dispositivo para el control de una red de comunicación según una de las figuras 1 a 3;

Fig. 7 un diagrama de bloques esquemático de un ejemplo de realización de un conmutador con un dispositivo para el control de una red de comunicación según una de las figuras 1 a 3;

Fig. 8 un diagrama de bloques esquemático de un ejemplo de realización de un cortafuegos con un dispositivo para el control de una red de comunicación según una de las figuras 1 a 3; y

Fig. 9 un diagrama de flujo esquemático de un ejemplo de realización de un procedimiento para el control de una red de comunicación.

Los elementos iguales o de igual funcionamiento están provistos de los mismos números de referencia en las figuras, si no se indica lo contrario.

En la figura 1 está representado un diagrama de bloques esquemático de un primer ejemplo de realización de un dispositivo 10 para el control de una red de comunicación 100. La red de comunicación 100 comprende una pluralidad de terminales 21 a 26 para la comunicación de datos. La pluralidad de terminales 21 a 26 puede comprender routers, conmutadores, cortafuegos, ordenadores, ordenadores personales, sistemas embebidos, instalaciones de control o similares. La red de comunicación 100 es, por ejemplo, una red LAN (Local Area Network) o una red WAN (Wide Area Network). El dispositivo 10 para el control de la red de comunicación 100 se puede identificar también como dispositivo de control 10.

El ejemplo de realización del dispositivo 10 de la figura 1 comprende una unidad de control 11, una unidad de análisis 12, una unidad DNS 13 (DNS: Domain Name Server, sistema de nombres de dominio) y una unidad de protección 18. La unidad de control 11, la unidad de análisis 12, la unidad DNS 13 y la unidad de protección 18 pueden estar acopladas o unidas de manera lógica o física. Por ejemplo, el dispositivo 10 puede estar configurado también como un ordenador que integra la unidad de control 11, la unidad de análisis 12, la unidad DNS 13 y la unidad de protección 18.

La unidad de control 11 del dispositivo 10 está diseñada para desacoplar un plano de datos L1 (véase figura 5) y un plano de control L2 (véase figura 5) de la comunicación de datos. El plano de datos L1 (Data Plane) se puede identificar también como capa de control o nivel de control. El plano de control L2 (Control Plane) se puede identificar también como capa de control o nivel de control.

La unidad de control 11 está diseñada también para modificar al menos una característica de la red de comunicación 100, que es visible desde el exterior 200 (figura 4) de la red de comunicación 100, mediante la utilización del plano de control desacoplado L2. Por el término desde el exterior de la red de comunicación 100 se entiende, por ejemplo, una unidad, por ejemplo, un ordenador, que está dispuesta en Internet 200 (figura 4) y no está autorizada y/o no está autentificada respecto a la red de comunicación 100.

Ejemplos de la al menos una característica de la red de comunicación 100, que puede ser modificada por la unidad de control 100, son los siguientes: cambio de direcciones virtuales de terminales 21 a 26 de la red de comunicación 100, cambio de la configuración de la red de comunicación 100, cambio del comportamiento de enrutamiento de la red de comunicación 100 y/o cambio de aplicaciones y/o de las asignaciones de puerto de las aplicaciones en la red de comunicación 100.

En particular, la unidad de control 11 está diseñada para modificar proactivamente la red de comunicación 100. La unidad de control 11 está diseñada en particular para modificar proactivamente la red de comunicación 100 de tal modo que se establecen zonas de seguridad diferentes con niveles de seguridad diferentes en la red de comunicación 100 y/o funciones de seguridad diferentes en la red de comunicación 100. En particular en dependencia de un escenario de amenaza identificado, la unidad de control 11 puede cambiar las zonas de seguridad establecidas y, por tanto, la configuración de la red de comunicación 100.

La unidad de control 11 puede estar configurada también para sustituir un primer algoritmo criptográfico, utilizado por la red de comunicación 100, por un segundo algoritmo criptográfico durante el funcionamiento de la red de comunicación 100.

Alternativa o adicionalmente, la unidad de control 11 puede estar diseñada para modificar un patrón de datos de la red de comunicación 100. Un ejemplo de tal patrón de datos de la red de comunicación 100 es un perfil de datos útiles al menos de uno de los terminales 21 a 26.

Una sesión de comunicación, descrita arriba, puede comprender una pluralidad de transacciones de datos (Data Flows). La unidad de control 11 puede estar diseñada aquí para modificar la al menos una característica de la red de comunicación 100, visible desde el exterior 200 de la red de comunicación 100, después de una cantidad parcial de la pluralidad de transacciones. La cantidad parcial de la pluralidad de transacciones puede ser también 1, de modo que la unidad de control 11 modifica la al menos una característica visible de la red de comunicación 100 después de cada transacción.

La unidad de análisis 12 del dispositivo 10 está diseñada preferentemente para proporcionar datos de análisis en caso de accesos de entidades no autorizadas a la red de comunicación 100. En la figura 3, explicada más adelante, se muestran detalles de este suministro de datos de análisis para un sistema de evaluación 300 acoplable al dispositivo 10.

La figura 2 muestra un diagrama de bloques esquemático de un segundo ejemplo de realización de un dispositivo 10 para el control de una red de comunicación 100. El segundo ejemplo de realización de la figura 2 comprende todas las características del primer ejemplo de realización de la figura 1. El dispositivo 10 de la figura 2 tiene también una unidad de evaluación de datos 14 y un generador aleatorio 19 para proporcionar un valor aleatorio ZW. La figura 2 muestra también que la unidad de protección 18 comprende una primera unidad de protección 15, una segunda unidad de protección 16, así como una tercera unidad de protección 17.

La unidad de evaluación de datos 14 está diseñada para determinar datos de estado mediante la utilización de los datos de análisis proporcionados por la unidad de análisis 12. Los datos de estado indican en particular una situación de seguridad de la red de comunicación 100.

Como se explica arriba, el generador de números aleatorios 19 proporciona un valor aleatorio ZW. La unidad de control 11 puede estar diseñada aquí para cambiar, por ejemplo, una dirección virtual de uno de los terminales 21 a 26 en dependencia del valor aleatorio ZW proporcionado por el generador aleatorio 19. El generador aleatorio 19 puede estar diseñado también para activar de manera aleatoria o casi aleatoria la unidad de control 11 con el fin de modificar la al menos una característica de la red de comunicación 100, que es visible desde el exterior 200 de la red de comunicación 100, al menos una vez durante la sesión de comunicación o también varias veces durante la sesión de comunicación.

Como se explica arriba, la unidad de protección 18 de la figura 2 comprende la primera unidad de protección 15, la segunda unidad de protección 16 y la tercera unidad de protección 17. La primera unidad de protección 15 está diseñada para detectar, aislar y combatir accesos de entidades no autorizadas a la red de comunicación 100. La segunda unidad de protección 16 está diseñada para avisar y alertar a un sistema de evaluación 300 acoplable al dispositivo 10. La tercera unidad de protección 17 está diseñada para restablecer al menos una función de red crítica de la red de comunicación 100.

En este sentido, la figura 3 muestra un tercer ejemplo de realización de un dispositivo 10 para el control de una red de comunicación 100. El tercer ejemplo de realización de la figura 3 comprende todas las características del segundo ejemplo de realización de la figura 2. El dispositivo 10 de la figura 3 comprende también una unidad de interfaz 20 que está diseñada para acoplar el dispositivo 10 a un sistema de evaluación 300. Por ejemplo, la unidad de interfaz 20 está acoplada a la unidad de análisis 12, la unidad DNS 13 y la unidad de evaluación de datos 14. La unidad de interfaz 20 puede estar acoplada también a otras unidades del dispositivo 10, por ejemplo, a la unidad de control 11 o al generador aleatorio 19 (no mostrado). Así, por ejemplo, el generador aleatorio 19 se puede inicializar mediante la unidad de interfaz 20.

En la figura 4 está representado un diagrama de bloques esquemático de una red de comunicación 100. La red de comunicación 100 comprende un dispositivo 10 configurado según uno de los ejemplos de realización de las figuras 1 a 3.

La red de comunicación 100 de la figura 4 tiene un número de terminales 21 a 23. El ejemplo de realización de la figura 4 muestra tres terminales 21 a 23, sin limitar la generalidad.

La red de comunicación 100 de la figura 4 comprende también un router 30, un conmutador 40, un primer cortafuegos 51, un segundo cortafuegos 52, una red LAN desmilitarizada, acoplada entre el primer cortafuegos 51 y el segundo cortafuegos 52, y una red LAN interna 62 que acopla la pluralidad de terminales 21 a 23 al segundo cortafuegos 52 (cortafuegos interno), así como al router 30, al conmutador 40 y al dispositivo 10.

La figura 4 muestra también que la red de comunicación 100 se puede acoplar a Internet 200. Las entidades no autorizadas, mencionadas arriba, que atacan potencialmente la red de comunicación 100, están dispuestas en particular en Internet 200 o conectadas a la misma.

La figura 5 muestra un diagrama de bloques esquemático de una arquitectura SDN con plano de datos L1 y plano de control L2 desacoplados para implementar un ejemplo de realización de la unidad de control 11.

La arquitectura de la figura 5 muestra que el plano de datos L1, el plano de control L2 y el plano de aplicación L3 están desacoplados uno del otro. Los planos o capas L1, L2, L3 están unidos entre sí por medio de la técnica de comunicación a través de APIs 101-104 (API: Application Programming Interface, interfaz de programación de aplicaciones).

La API 101 se puede identificar también como Southbound-API (API hacia el sur). Por ejemplo, la Southbound-API 101 se implementa mediante OpenFlow. Las APIs 102-104 se pueden identificar también como Northbound-APIs. (APIs hacia el norte).

En el plano de datos L1 están dispuestos aparatos de red físicos 21 a 25 y aparatos de red virtuales 26 a 28. El número y la distribución de los aparatos de red físicos 21 a 25 y los aparatos de red virtuales 26 a 28 en el plano de datos L1 se indican meramente a modo de ejemplo.

El plano de control L2 comprende un software de control SDN 70 con distintos servicios de red 81 a 83 para la implementación de la unidad de control 11.

El plano de aplicación L3 comprende varias aplicaciones 91 a 93. Las aplicaciones 91 a 93 se pueden identificar también como aplicaciones empresariales.

Como se explica arriba, el plano o capa inferior de la arquitectura SDN es el plano de datos L1 que comprende una pluralidad de aparatos de red 21 a 28. En el plano de control L2 no se establece ninguna diferencia entre aparatos

de red físicos y virtuales 21 a 28 o conmutadores. Por esta razón, los aparatos de red virtuales 26 a 28 forman parte también aquí del plano de datos L1. La comunicación entre el plano de datos L1 y el plano de control L2 mediante la interfaz Southbound 101 se representa mediante un protocolo Southbound. En este sentido es una premisa que los aparatos de red participantes 21 a 28 dominen el protocolo Southbound utilizado. En particular, los aparatos de red 21 a 28 deben soportar sólo un conjunto mínimo de comandos del protocolo Southbound. Para su implementación se puede utilizar el protocolo OpenFlow. Un objetivo del protocolo Southbound es la implementación de un conjunto de comandos básicos para manipular las tablas de flujo en los conmutadores con el fin de hacer transparente la complejidad y la heterogeneidad en el plano de datos L1.

En el plano de control L2 está dispuesto el software de control SDN 70. Éste se puede entender también como Middleware que abstrae los aparatos de red 21 a 28 del plano de datos L1 para aplicaciones SDN.

La figura 6 muestra un diagrama de bloques esquemático de un ejemplo de realización de un router 30 que integra un dispositivo 10 para el control de una red de comunicación 100. El dispositivo 10 está configurado, por ejemplo, según uno de los ejemplos de realización de las figuras 1 a 3.

La figura 7 muestra un diagrama de bloques esquemático de un ejemplo de realización de un conmutador 40 que integra un dispositivo 10 para el control de una red de comunicación 100. El dispositivo 10 está configurado, por ejemplo, según uno de los ejemplos de realización de las figuras 1 a 3.

La figura 8 muestra un diagrama de bloques esquemático de un ejemplo de realización de un cortafuegos 50 que integra un dispositivo 10 para el control de una red de comunicación 100. El dispositivo 10 está configurado, por ejemplo, según uno de los ejemplos de realización de las figuras 1 a 3.

La figura 9 muestra un diagrama de flujo esquemático de un ejemplo de realización de un procedimiento para el control de una red de comunicación 100. El procedimiento de la figura 9 comprende las etapas siguientes 901 y 902.

En la etapa 901 se desacoplan entre sí un plano de datos L1 y un plano de control L2 de la comunicación de datos. El resultado de la etapa 901 es un plano de control L2 desacoplado del plano de datos L1 y un plano de datos L1 desacoplado del plano de control L2.

En la etapa 902 se modifica una característica de la red de comunicación 100, que es visible desde el exterior de la red de comunicación 100, mediante la utilización del plano de control desacoplado L2.

Aunque la presente invención se ha explicado por medio de ejemplos de realización, la misma se puede modificar de múltiples maneras. Así, por ejemplo, es posible disponer también el dispositivo para el control de la red de comunicación en otra unidad mostrada en las figuras (por ejemplo, router o conmutador) de la red de comunicación. Es posible también disponer el dispositivo para el control de la red de comunicación por fuera de la red de comunicación. Asimismo, la herramienta OpenMUL para implementar la unidad de control del dispositivo para el control de la red de comunicación se indica meramente a modo de ejemplo. En este sentido se pueden utilizar también herramientas alternativas.

Lista de números de referencia

10	Dispositivo
11	Unidad de control
12	Unidad de análisis
13	Unidad DNS
14	Unidad de evaluación de datos
15	Primera unidad de protección
16	Segunda unidad de protección
17	Tercera unidad de protección
18	Dispositivo de protección
19	Generador aleatorio
20	Unidad de interfaz
21	Terminal
22	Terminal

23	Terminal
24	Terminal
25	Terminal
26	Terminal
27	Terminal
28	Terminal
30	Router
40	Conmutador
50	Cortafuegos
51	Cortafuegos
52	Cortafuegos
61	LAN
62	LAN
70	Software de control SDN
81-83	Servicio de red
91-93	Aplicación
100	Red de comunicación
101	API
102	API
103	API
104	API
200	Internet
300	Sistema de evaluación
L1	Plano de datos
L2	Plano de control
L3	Plano de aplicación
ZW	Valor aleatorio

REFERENCIAS

[1] http://www.openmul.org/openmul-controller.html

(disponible en la fecha de solicitud)

[2] Nick McKeown et al: OpenFlow: Enabling innovation in campus networks, ACM Communications Review, abril de 2008

[3] http://www.dhs.gov/science-and-technology/csd-mtd

(disponible en la fecha de solicitud)

[4] Software-Defined Networking: The New Norm for Networks, White Paper, Open Networking Foundation, 13 de abril de 2012

[5] Sean Michael Kerner: OpenFlow Inventor Martin Casado on SDN, VMware and Software Defined Networking Hype, Enterprise Networking Planet, 29 de abril 2013

[6] RFC7348: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Network over Layer 3 Networks

[7] RFC791 – Internet Protocol; Ipv4

[8] RFC3513 – Internet Protocol; IPv6

[9] RFC4301 - IPsec

[10] RFC2661 – L2TP

[11] Open-VPN: https://openvpn.net/

REIVINDICACIONES

1. Dispositivo (10) para el control de una red de comunicación (100) con una pluralidad de terminales (21 a 28) para la comunicación de datos con:

una unidad de control (11) que está diseñada para desacoplar un plano de datos (L1) y un plano de control (L2) de la comunicación de datos y modificar al menos proactivamente una característica de la red de comunicación (100), que es visible desde el exterior (200) de la red de comunicación (100), durante una sesión de comunicación mediante la utilización del plano de control desacoplado (L2),

estando diseñada la unidad de control (11) para cambiar una dirección virtual al menos de un terminal de la pluralidad de terminales (21 a 28) durante la sesión de comunicación mediante la utilización del plano de control desacoplado (L2),

presentando el dispositivo (10) un generador aleatorio (19) para emitir un valor aleatorio (ZW),

estando diseñada la unidad de control (11) para cambiar la dirección virtual en dependencia del valor aleatorio (ZW) emitido por el generador aleatorio (19).

2. Dispositivo de acuerdo con la reivindicación 1, **caracterizado por que** la unidad de control (11) está diseñada para modificar proactivamente la red de comunicación (100) de tal modo que zonas de seguridad diferentes con niveles de seguridad diferentes y/o funciones de seguridad diferentes se pueden establecer dinámicamente en la red de comunicación (100).

3. Dispositivo de acuerdo con una de las reivindicaciones 1 o 2, **caracterizado por que** la unidad de control (11) está diseñada para modificar la configuración de la red de comunicación (100) durante la sesión de comunicación mediante la utilización del plano de control desacoplado (L2).

4. Dispositivo de acuerdo con una de las reivindicaciones 1 a 3, **caracterizado por que** la unidad de control (11) está diseñada para modificar un comportamiento de enrutamiento de la red de comunicación (100) durante la sesión de comunicación mediante la utilización del plano de control desacoplado (L2).

5. Dispositivo de acuerdo con una de las reivindicaciones 1 a 4, **caracterizado por que** la unidad de control (11) está diseñada para modificar al menos una aplicación de la red de comunicación (100) y/o una asignación de puerto de la al menos una aplicación durante la sesión de comunicación mediante la utilización del plano de control desacoplado (L2).

6. Dispositivo de acuerdo con una de las reivindicaciones 1 a 5, **caracterizado por que** la unidad de control (11) está diseñada para sustituir un primer algoritmo criptográfico, utilizado por la red de comunicación (100), por un segundo algoritmo criptográfico durante la sesión de comunicación.

7. Dispositivo de acuerdo con una de las reivindicaciones 1 a 6, **caracterizado por que** la unidad de control (11) está diseñada para modificar un patrón de datos de la red de comunicación (100), en particular un perfil de datos útiles al menos de uno de los terminales (21 a 28).

8. Dispositivo de acuerdo con una de las reivindicaciones 1 a 7, **caracterizado por que** la sesión de comunicación comprende una pluralidad de transacciones de datos, estando diseñada la unidad de control (11) para modificar la al menos una característica de la red de comunicación (100), que es visible desde el exterior (200) de la red de comunicación (100), después de una cantidad parcial de la pluralidad de transacciones.

9. Dispositivo de acuerdo con una de las reivindicaciones 1 a 8, **caracterizado por que** la sesión de comunicación comprende una pluralidad de transacciones de datos, estando diseñada la unidad de control (11) para modificar la al menos una característica de la red de comunicación (100), que es visible desde el exterior (200) de la red de comunicación (100), después de cada transacción de la pluralidad de transacciones.

10. Dispositivo de acuerdo con una de las reivindicaciones 1 a 9, **caracterizado por que** la unidad de control (11) está diseñada para desacoplar el plano de datos (L1) y el plano de control (L2) de la comunicación de datos mediante red definida por software (Software-Defined-Networking).

11. Dispositivo de acuerdo con una de las reivindicaciones 1 a 10, **caracterizado por** un generador aleatorio (19), acoplado a la unidad de control (11), que está diseñado para activar de manera aleatoria la unidad de control (11) con el fin de modificar la al menos una característica de la red de comunicación (100), que es visible desde el exterior (200) de la red de comunicación (100), al menos una vez durante la sesión de comunicación, en particular varias veces durante la sesión de comunicación.

12. Dispositivo de acuerdo con una de las reivindicaciones 1 a 11, **caracterizado por** una primera unidad de protección (15) para detectar, aislar y combatir accesos de entidades no autorizadas a la red de comunicación (100).

13. Dispositivo de acuerdo con la reivindicación 12, **caracterizado por** una segunda unidad de protección (16) para advertir y alarmar a un sistema de evaluación (300) acoplable al dispositivo (10).

14. Dispositivo de acuerdo con la reivindicación 12 o 13, **caracterizado por** una tercera unidad de protección (17) para restablecer al menos una función de red crítica.

15. Dispositivo de acuerdo con una de las reivindicaciones 1 a 14, **caracterizado por** una unidad de análisis (12) para proporcionar datos de análisis en caso de accesos de entidades no autorizadas a la red de comunicación (100).

16. Dispositivo de acuerdo con la reivindicación 15, **caracterizado por** una unidad de evaluación de datos (14) para determinar mediante la utilización de los datos de análisis proporcionados datos de estado que son adecuados en particular para indicar una situación de seguridad en la red de comunicación (100).

17. Dispositivo de acuerdo con la reivindicación 15, **caracterizado por** una unidad de interfaz (20) para transmitir los datos de estado a un sistema de evaluación (300) acoplable al dispositivo (10).

18. Dispositivo de acuerdo con una de las reivindicaciones 1 a 17, **caracterizado por que** la red de comunicación (100) presenta una infraestructura que comprende capas que se superponen, estando implementada la unidad de control (11) como una red de superposición virtual que superpone una capa 2 y una capa 3 de la infraestructura.

19. Dispositivo de acuerdo con una de las reivindicaciones 1 a 18, **caracterizado por que** el dispositivo (10) utiliza una combinación formada por un protocolo de seguridad y un protocolo de túnel.

20. Router (30) para una red de comunicación (100) que integra un dispositivo (10) de acuerdo con una de las reivindicaciones 1 a 19.

21. Conmutador (40) para una red de comunicación (100) que integra un dispositivo (10) de acuerdo con una de las reivindicaciones 1 a 19.

22. Cortafuegos (50) para una red de comunicación (100) que integra un dispositivo (10) de acuerdo con una de las reivindicaciones 1 a 19.

23. Red de comunicación (100) con:

una pluralidad de terminales (21 a 28) para la comunicación de datos y

un dispositivo (10) para el control de la red de comunicación (100) de acuerdo con una de las reivindicaciones 1 a 19.

24. Procedimiento para el control de una red de comunicación (100) con una pluralidad de terminales (21 a 28) para la comunicación de datos, con las etapas:

desacoplamiento (901) de un plano de datos (L1) y de un plano de control (L2) de la comunicación de datos y

modificación proactiva (902) al menos de una característica de la red de comunicación (100), que es visible desde el exterior (200) de la red de comunicación (100), durante una sesión de comunicación mediante la utilización del plano de control desacoplado (L2),

cambiándose una dirección virtual al menos de un terminal de la pluralidad de terminales (21 a 28) durante la sesión de comunicación mediante la utilización del plano de control desacoplado (L2),

cambiándose la dirección virtual en dependencia de un valor aleatorio (ZW) emitido por un generador aleatorio (19).

25. Producto de programa informático que provoca la ejecución del procedimiento según la reivindicación 24 en una unidad controlada por programa.

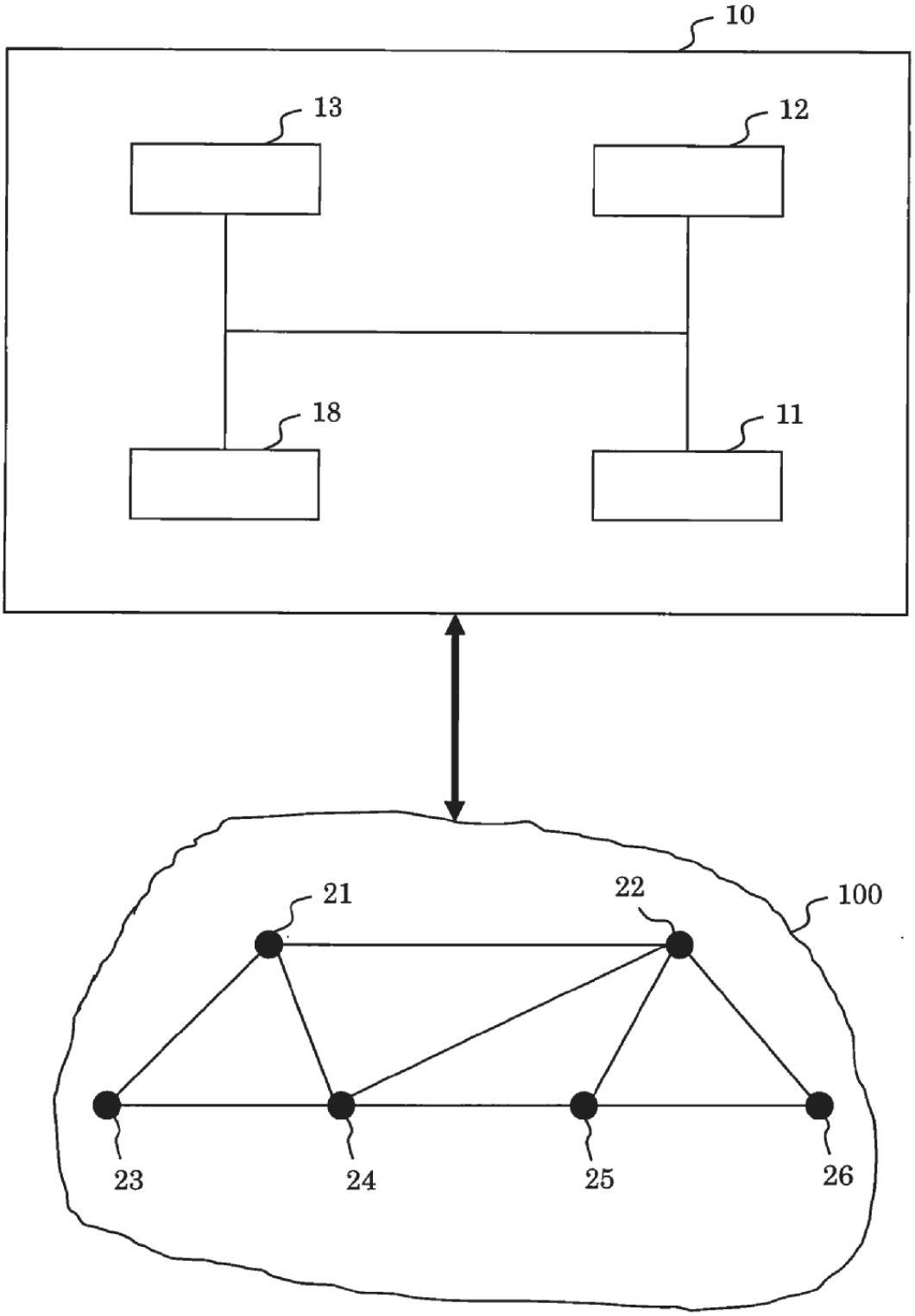

FIG. 1

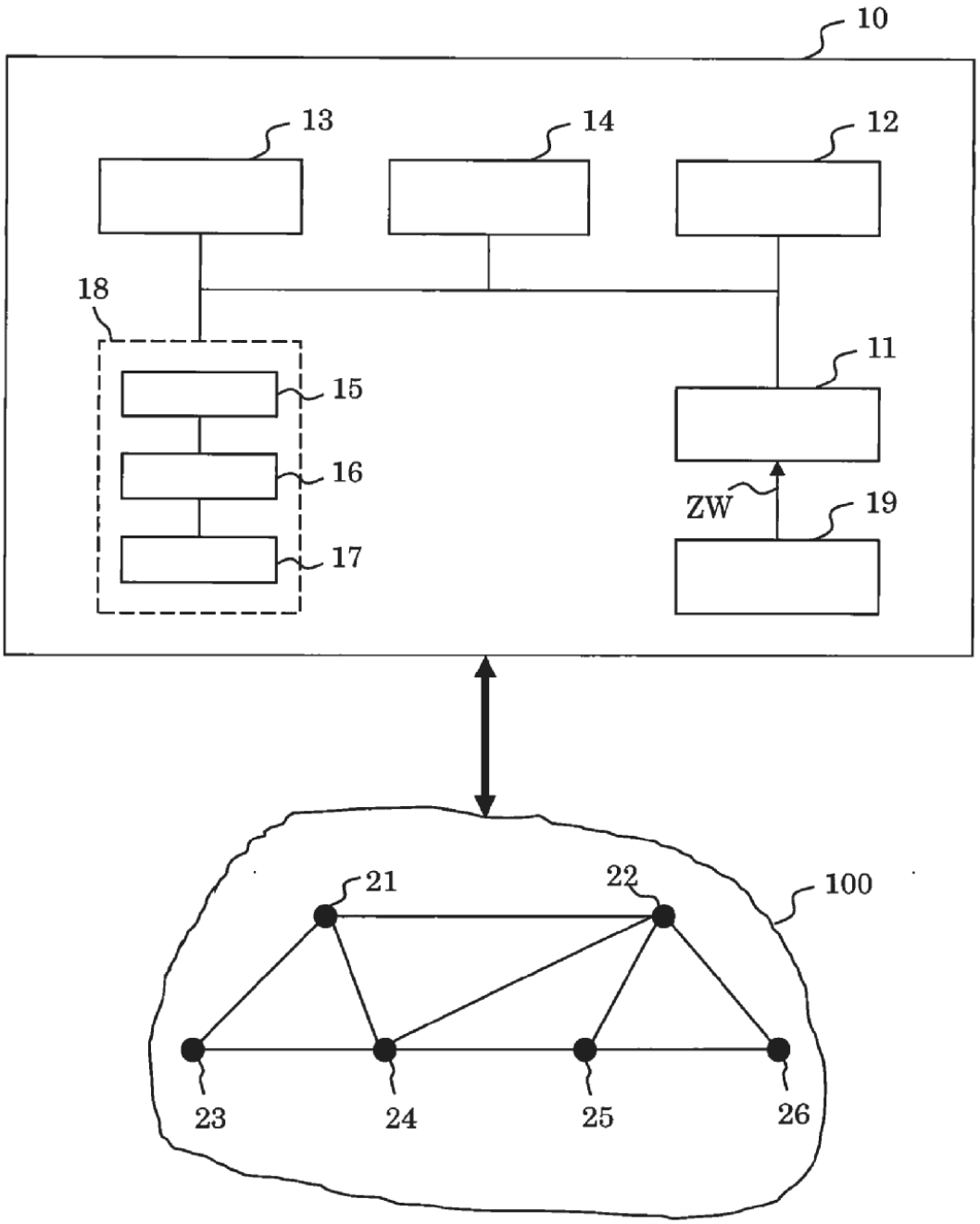

FIG. 2

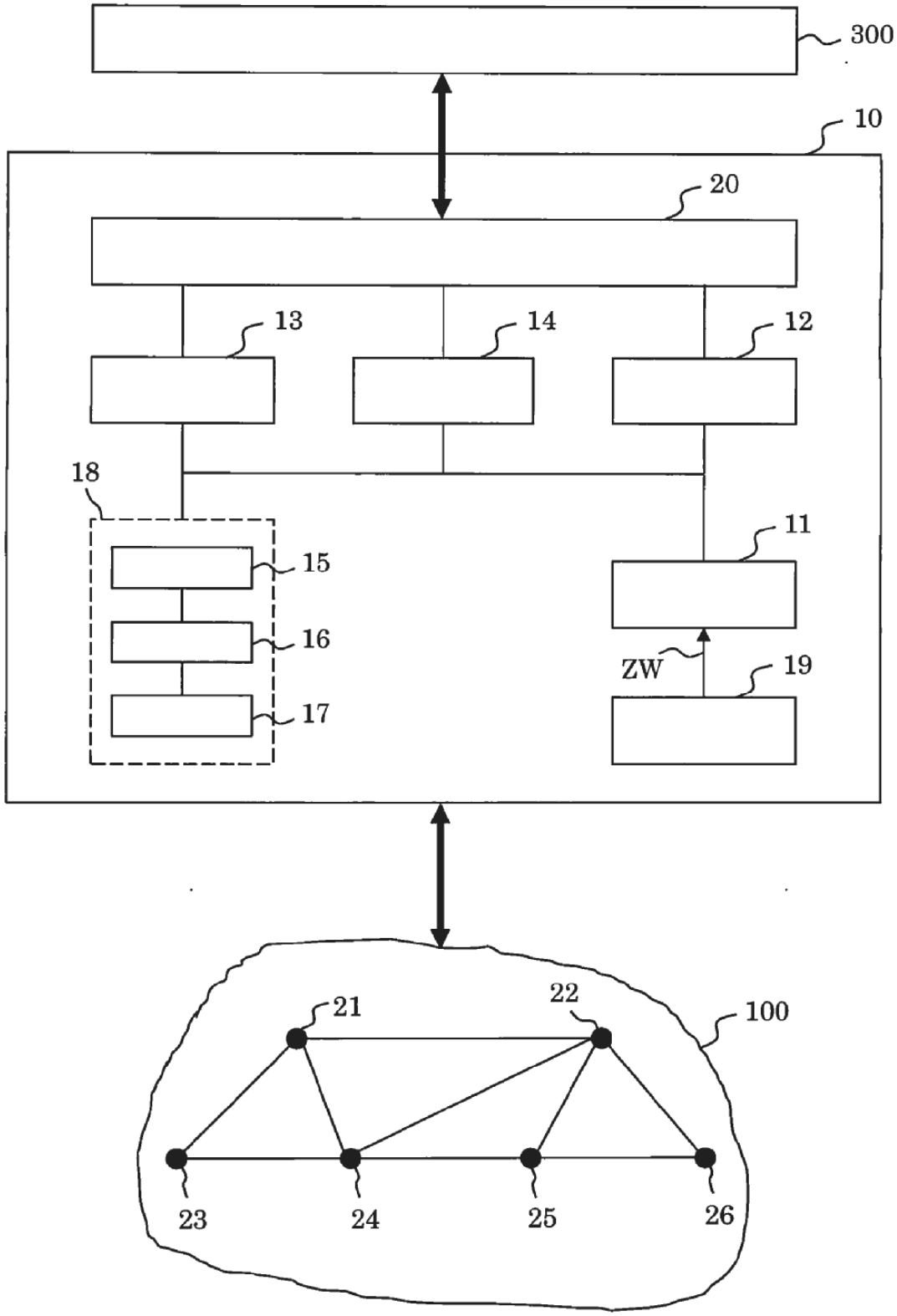

FIG. 3

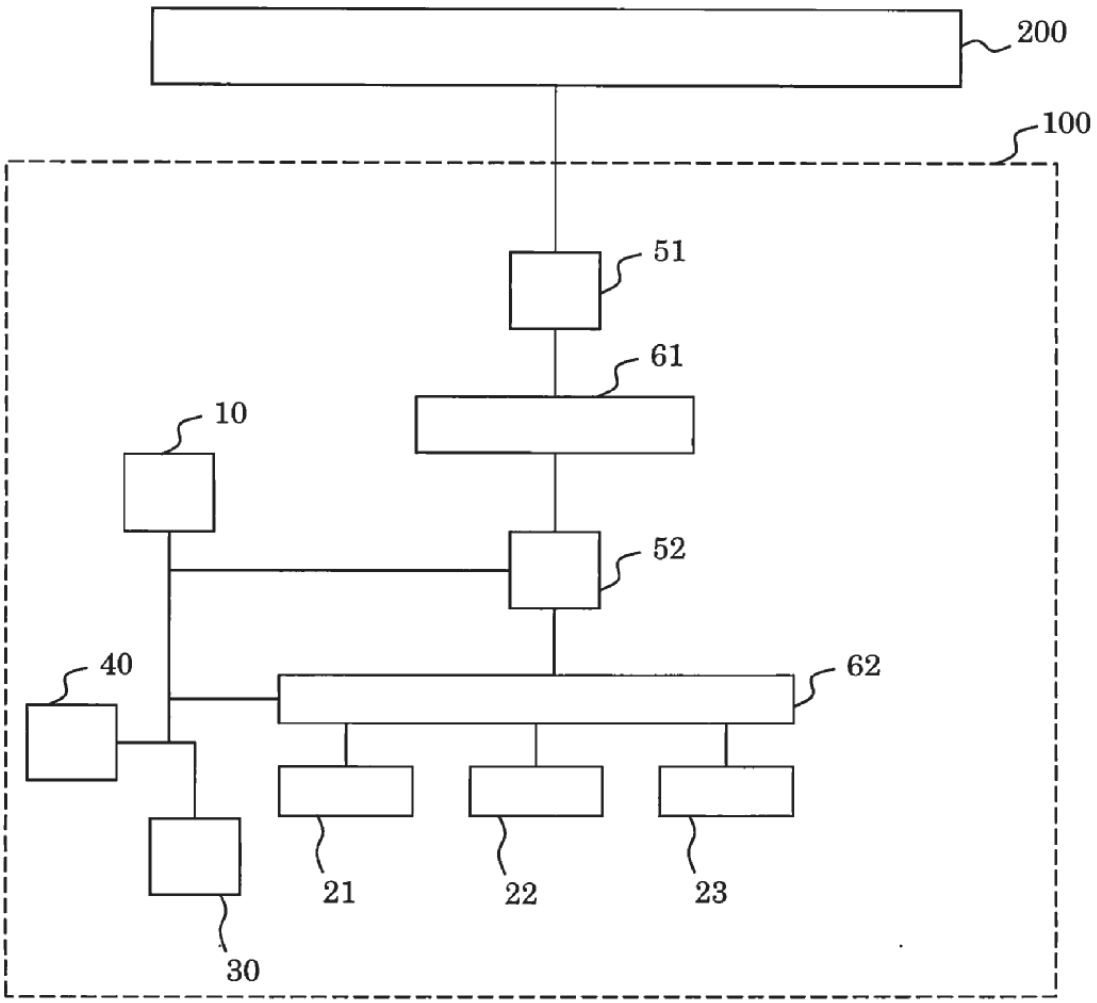

FIG. 4

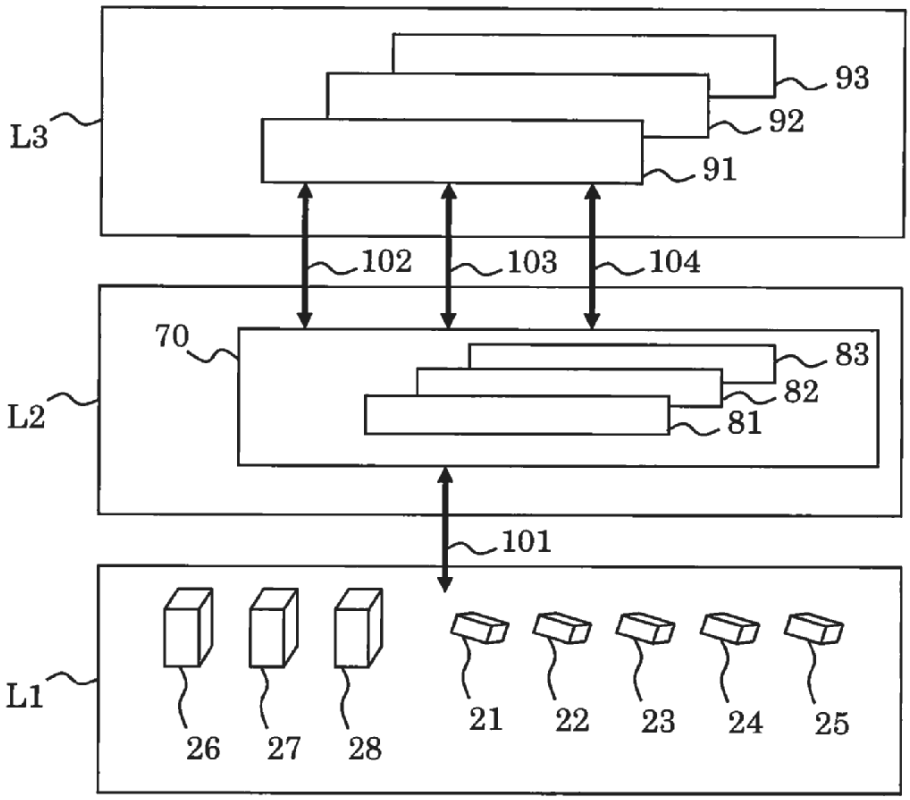

FIG. 5

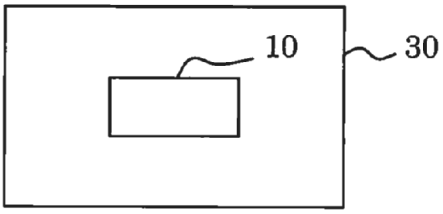

FIG. 6

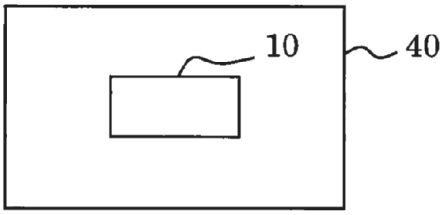

FIG. 7

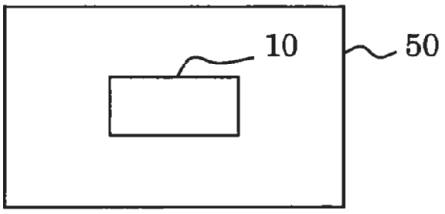

FIG. 8

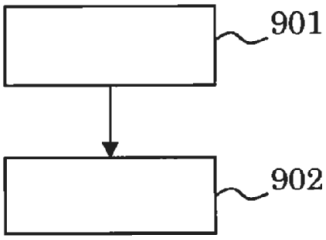

FIG. 9