

**DETECCIÓN DE UN ATAQUE DE DENEGACIÓN DE SERVICIO (DOS) EN
UN DISPOSITIVO ASCENDENTE EN BASE A LA SEÑALIZACIÓN DE LA
RED DE ACCESO POR RADIO (RAN)**

Campo técnico

5 La presente divulgación se refiere al ámbito de la detección de un ataque de denegación de servicio (DoS) y, en particular, a un nodo de red de radio que detecta un ataque DoS en un dispositivo ascendente en base a la señalización RAN.

Antecedentes

10 Los ataques de denegación de servicio distribuido (DDoS) están cada vez más extendidos. Un ataque DDoS se basa en que un atacante obtiene el control de una gran cantidad de dispositivos conectados a la Internet, formando de esta manera una botnet. La prevalencia de los dispositivos IoT aumenta constantemente. Los posibles problemas de seguridad y el creciente volumen de
15 dispositivos IoT los convierten en objetivos para que los atacantes creen botnets que puedan lanzar ataques DDoS hacia objetivos que residen en la Internet.

Hay varios tipos de ataques DDoS. Un ejemplo es el ataque volumétrico de inundación UDP. El protocolo UDP se utiliza normalmente en comunicaciones sensibles al tiempo, por ejemplo, tráfico de voz, video y juegos. Sin embargo, el
20 protocolo UDP se puede utilizar en un ataque volumétrico, llamado ataque de inundación UDP, ya que no es necesario establecer un canal de comunicación antes de transmitir un paquete UDP.

De manera similar a un ataque de inundación UDP, un ataque de inundación TCP SYN (mensaje de sincronización) da como resultado un alto volumen de tráfico pero con características diferentes.

Por lo tanto, existen varios tipos de ataques volumétricos, con altas tasas
5 de paquetes que intentan causar el agotamiento de los recursos de un servidor y/o enlace de red. El ataque de inundación UDP y los ataques TCP SYN son ataques de tipo DDoS en los que se envía una inundación de paquetes a un servidor objetivo con el objetivo de sobrecargar la capacidad del servidor para recibir, procesar y/o responder.

10 Sumario

Un objetivo es mejorar cómo se detectan los ataques DoS.

De acuerdo con un primer aspecto, se proporciona un procedimiento para la detección de un ataque de denegación de servicio, DoS, en un dispositivo ascendente, el procedimiento se realiza en un nodo de red de radio. El
15 procedimiento comprende: obtener una métrica en base a la señalización de red de acceso de radio, RAN, para la comunicación entre un equipo de usuario, UE y el nodo de red de radio; y determinar que hay un ataque DoS en curso en el dispositivo ascendente en base a la métrica, en la que el dispositivo ascendente se proporciona en dirección ascendente desde el nodo de red de radio.

20 La métrica se puede basar en un volumen de solicitudes de programación transmitidas desde el UE.

La determinación de que un ataque DoS está en curso puede incluir la determinación de que el volumen de solicitudes de programación es menor que un volumen umbral de solicitudes de programación.

5 La métrica se puede basar en informes de estado de búfer, BSR, desde el UE.

La determinación de que un ataque DoS está en curso puede comprender la determinación de que una estadística de frecuencia de los BSR indica una frecuencia mayor que una frecuencia de umbral.

10 La determinación de que un ataque DoS está en curso puede comprender la determinación de que los BSR indican un alto nivel de búfer a lo largo del tiempo.

La métrica se puede basar en un volumen de bloques de recursos físicos utilizados, PRB.

15 La determinación de que un ataque DoS está en curso puede comprender la determinación de que el volumen de los PRB es mayor que un volumen umbral de los PRB.

El procedimiento puede comprender además: señalar una alerta que indique que el ataque DoS está en curso.

20 La determinación de que un ataque DoS está en curso se puede configurar para detectar una inundación de paquetes de protocolo de datagramas de usuario, UDP.

La determinación de que un ataque DoS está en curso se puede configurar para detectar una inundación de mensajes de protocolo de control de transporte, TCP, de sincronización, SYN.

El ataque DoS puede implicar un ataque de plano de usuario.

5 De acuerdo con un segundo aspecto, se proporciona un nodo de red de radio para la detección de un ataque de denegación de servicio, DoS, en un dispositivo ascendente. El nodo de red de radio comprende: un procesador; y una memoria que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio: obtenga una métrica en base a
10 la señalización de la red de acceso de radio, RAN, para la comunicación entre un equipo de usuario, UE y el nodo de red de radio; y determine que hay un ataque DoS en curso en el dispositivo ascendente en base a la métrica, en la que el dispositivo ascendente se proporciona en dirección ascendente desde el nodo de red de radio.

15 La métrica se puede basar en un volumen de solicitudes de programación transmitidas desde el UE.

Las instrucciones para determinar que un ataque DoS está en curso pueden comprender instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio determine que el volumen de
20 solicitudes de programación es menor que un volumen umbral de solicitudes de programación.

La métrica se puede basar en informes de estado de búfer, BSR, desde el UE.

Las instrucciones para determinar que un ataque DoS está en curso pueden comprender instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio determine que una estadística de frecuencia de los BSR indica una frecuencia mayor que una frecuencia umbral.

Las instrucciones para determinar que un ataque DoS está en curso pueden comprender instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio determine que los BSR indican un alto nivel de búfer a lo largo del tiempo.

La métrica se puede basar en un volumen de bloques de recursos físicos utilizados, PRB.

Las instrucciones para determinar que un ataque DoS está en curso pueden comprender instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio determine que el volumen de los PRB es mayor que un volumen umbral de los PRB.

El nodo de red de radio puede comprender además instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio señale una alerta que indica que el ataque DoS está en curso.

Las instrucciones para determinar que un ataque DoS está en curso pueden comprender instrucciones que, cuando son ejecutadas por el

procesador, hacen que el nodo de red de radio detecte una inundación de paquetes de protocolo de datagramas de usuario, UDP.

Las instrucciones para determinar que un ataque DoS está en curso pueden comprender instrucciones que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio detecte una inundación de mensajes de protocolo de control de transporte, TCP, de sincronización, SYN.

El ataque DoS puede implicar un ataque de plano de usuario.

De acuerdo con un tercer aspecto, se proporciona un programa informático para la detección de un ataque de denegación de servicio, DoS, en un dispositivo ascendente. El programa informático comprende un código de programa informático que, cuando se ejecuta en un nodo de red de radio, hace que el nodo de red de radio: obtenga una métrica en base a la señalización de la red de acceso de radio, RAN, para la comunicación entre un equipo de usuario, UE y el nodo de red de radio; y determine que hay un ataque DoS en curso en el dispositivo ascendente en base a la métrica, en la que el dispositivo ascendente se proporciona en dirección ascendente desde el nodo de red de radio.

De acuerdo con un cuarto aspecto, se proporciona un producto de programa informático que comprende un programa informático de acuerdo con el tercer aspecto y un medio legible por ordenador que comprende una memoria no transitoria en la que se almacena el programa informático.

En general, todos los términos utilizados en las reivindicaciones se deben interpretar de acuerdo con su significado ordinario en el campo técnico, a menos que se defina explícitamente lo contrario en la presente memoria. Todas las referencias a “una/un/el elemento, aparato, componente, medio, etapa, etc.” se deben interpretar abiertamente como referidas al menos a una instancia del elemento, aparato, componente, medio, etapa, etc., a menos que se indique explícitamente lo contrario. Las etapas de cualquier procedimiento divulgado en la presente memoria no tienen que realizarse en el orden exacto divulgado, a menos que se indique explícitamente.

10 Breve descripción de los dibujos

Los aspectos y realizaciones se describen ahora, a modo de ejemplo, con referencia a los dibujos acompañantes, en los que:

La Fig. 1 es un diagrama esquemático que ilustra un entorno en el que se pueden aplicar las realizaciones presentadas en la presente memoria;

15 La Fig. 2 es un diagrama esquemático que ilustra una realización de una implementación distribuida del nodo de red de radio;

La Fig. 3 ilustra una pila de protocolos que comprende un conjunto de protocolos para la comunicación RAN entre el UE (equipo de usuario) y el nodo de red de radio;

20 Las Figs. 4A-B son diagramas de flujo que ilustran realizaciones de procedimientos para la detección de un ataque DoS en un dispositivo ascendente;

La Fig. 5 es un diagrama esquemático que ilustra los componentes del nodo de red de radio de la Fig. 1;

La Fig. 6 es un diagrama esquemático que muestra los módulos funcionales del nodo de red de radio de la Fig. 1 de acuerdo con una realización;

5 y

La Fig. 7 muestra un ejemplo de un producto de programa informático que comprende medios legibles por ordenador.

Descripción detallada

Los aspectos de la presente divulgación se describirán ahora con más
10 detalle a continuación con referencia a los dibujos acompañantes, en los que se muestran ciertas realizaciones de la invención. Sin embargo, estos aspectos se pueden incorporar de muchas formas diferentes y no se deben interpretar como limitantes; más bien, estas realizaciones se proporcionan a modo de ejemplo para que esta divulgación sea exhaustiva y completa, y para transmitir
15 completamente el alcance de todos los aspectos de la invención a los expertos en la técnica. Los números similares se refieren a elementos similares a lo largo de la descripción.

De acuerdo con las realizaciones presentadas en la presente memoria, se proporciona una forma de detectar ataques DoS volumétricos iniciados por un
20 UE comprometido (por ejemplo, dispositivos IoT o cualquier otro tipo de UE) conectado a la red de acceso de radio (RAN). La detección la realiza el nodo de red de radio que proporciona la RAN. Esta detección se consigue mediante el

análisis de métricas derivadas de la señalización RAN, relacionadas con el UE en cuestión. No se evalúa el contenido de los paquetes; la detección DoS opera sin necesidad de una inspección profunda de paquetes. Esta detección permite que el nodo de red de radio ya mitigue un ataque DoS, como se describe con
5 más detalle a continuación.

La Fig. 1 es un diagrama esquemático que ilustra un entorno en el que se pueden aplicar las realizaciones presentadas en la presente memoria. Una red de comunicación celular 8 comprende una red central 3 y uno o más nodos de red de radio 1 (también conocidos como estaciones base) que proporcionan una
10 RAN para uno o más UE 2.

El nodo de red de radio 1 puede ser la forma de estaciones base de radio que son gNode Bs, gNB o Nodo Bs evolucionado, también conocido como eNode Bs o eNB. Los nodos de red de radio también pueden tener la forma de Nodos Bs, BTS (Estaciones Transceptoras de Base) y/o BSS (Subsistemas de
15 Estaciones de Base), etc. El nodo de red de radio 1 proporciona conectividad de radio utilizando la RAN a través de una interfaz inalámbrica 4a-b a uno o más UE 2. El nodo de red de radio 1 se puede implementar en forma de un solo dispositivo de hardware o distribuir en varios dispositivos, como se ilustra en la Fig. 2 y se explica a continuación.

20 A través de la interfaz inalámbrica de la RAN, la comunicación de enlace descendente (DL) 4a se produce desde el nodo de red de radio 1 hasta el UE 2 y la comunicación de enlace ascendente (UL) 4b se produce desde el UE 2 hasta

el nodo de red de radio 1. La calidad de la interfaz de radio inalámbrica para cada UE 2 puede variar con el tiempo y dependiendo de la posición del UE 2, debido a efectos tales como el desvanecimiento, la propagación por trayectos múltiples, la interferencia, etc.

5 El término UE también se conoce como terminal de comunicación móvil, dispositivo de usuario, terminal móvil, terminal de usuario, agente de usuario, dispositivo inalámbrico, terminal inalámbrico, dispositivo de máquina a máquina, etc., y se puede implementar, por ejemplo, por lo que hoy se conoce comúnmente como un teléfono móvil, un teléfono inteligente, un dispositivo IoT
10 o un ordenador tipo tableta/ordenador portátil con conectividad inalámbrica.

La red de comunicación celular 8 puede, por ejemplo, cumplir con una o una combinación de 5G NR (radio nueva de quinta generación), LTE (Evolución a Largo Plazo), LTE-Advanced, 6G (sexta generación), W-CDMA (Múltiplex por División de Código de Banda Ancha) o cualquier otra red inalámbrica actual o
15 futura, siempre que se apliquen los principios descritos en la presente memoria.

El nodo de red de radio 1 está conectado a la red central 3 para la conectividad a las funciones centrales de la red y a una red de área extensa 9, tal como la Internet. Un servidor 5 también está conectado a la red. Tanto los datos del plano de usuario como los datos del plano de control se transmiten a
20 través de los enlaces UL y DL 4a/4b de la RAN.

Es posible que un atacante pueda obtener el control del UE 2 para orquestar un ataque de denegación de servicio (DoS), por ejemplo, dirigido

contra un nodo en la red central 3 y/o el servidor 5. Cuando se utilizan múltiples dispositivos, tales como el UE 2, en el mismo ataque, se denomina ataque DoS distribuido (DDoS). Si bien cada UE 2 puede formar parte de un ataque DDoS, en adelante se denomina ataque DoS.

5 Cuando un UE 2 se ha visto comprometido a efectos de DoS, dicho UE se denomina DoS UE en la presente memoria. Una forma de ataque DoS es una inundación UDP, en la que un atacante controla un DoS UE 2 para transmitir una gran cantidad de paquetes UDP a un dispositivo de destino. Otro tipo de ataque DoS es un ataque de inundación TCP SYN. Este ataque funciona de acuerdo
10 con el mismo principio que la inundación UDP, ya que el mensaje TCP SYN es un mensaje inicial de un establecimiento de conexión TCP y se puede transmitir a un servidor antes de que se establezca la conexión TCP y seguir cumpliendo con el protocolo TCP. Esto puede ser atractivo desde la perspectiva de un
15 atacante, ya que tanto un paquete UDP como un paquete TCP SYN se pueden enviar desde un UE comprometido, y estos paquetes se pueden repetir opcionalmente de forma arbitraria en el tiempo y la frecuencia. Tanto el ataque de inundación UDP como el ataque de inundación TCP SYN se denominan ataques volumétricos.

 De acuerdo con las realizaciones presentadas en la presente memoria, el
20 nodo de red de radio 1 detecta un ataque DoS contra un nodo ascendente (por ejemplo, un nodo de la red central 3 o el servidor 5), donde el ataque DoS se basa (al menos parcialmente) en el tráfico desde el UE 2. Un nodo ascendente

se debe interpretar como un nodo situado más centralmente desde el nodo de red de radio 1, es decir, en la dirección topológica distinta al UE y/o en la misma dirección topológica que la red central o la red de área amplia 9, vista desde el nodo de red de radio 1.

- 5 La Fig. 2 es un diagrama esquemático que ilustra una realización de una implementación distribuida del nodo de red de radio 1. El nodo de red de radio 1 está formado por un nodo de banda base 6 y un nodo de radio 7.

El nodo de red de radio 1 comprende un nodo de banda base 10 que es una unidad de procesamiento de banda base y uno o más nodos de radio
10 remotos 11. Cuando se aplica en una arquitectura O-RAN (RAN Abierta), el nodo de banda base puede ser un nodo O-DU (unidad distribuida de O-RAN) y el nodo de radio puede ser un nodo O-RU (unidad de radio de O-RAN). En la terminología 5G, por ejemplo, de acuerdo con una arquitectura C-RAN (Red de Acceso de Radio Centralizada/en la Nube), el nodo de banda base 10 puede ser
15 un gNB-CU y el nodo de radio 11 puede ser un gNB-DU.

El nodo de banda base 10 y el nodo de radio 11 pueden estar en diferentes ubicaciones. El nodo de banda base 10 está situado en dirección ascendente del nodo de radio 11, es decir, hacia la red central 3. En consecuencia, el nodo de radio 11 se puede situar en dirección descendente del nodo de banda base 10,
20 hacia el UE 2. Hay uno o más enlaces fronthaul 18 entre el nodo de banda base 10 y el nodo de radio 11. Los enlaces fronthaul 18 son enlaces de comunicación bidireccionales. Los enlaces fronthaul 18 se pueden implementar utilizando una

Interfaz de Radio Pública Común (CPRI) o eCPRI (CPRI evolucionada) y Ethernet. Se pueden emplear múltiples enlaces de fronthaul en otras topologías que las que se muestran en la Fig. 1. Los enlaces de fronthaul múltiples también se pueden denotar como una red de fronthaul. El nodo de banda base 10 y el

5 nodo de radio 11 pueden implementar subconjuntos de funcionalidad de la RAN para la comunicación por radio con el UE 2. Además, se pueden virtualizar algunas funcionalidades para la comunicación por radio, también conocidas como RAN en la nube.

La Fig. 3 ilustra una pila de protocolos 20 que comprende un conjunto de

10 protocolos 21, 22, 23, 24 de la comunicación RAN entre el UE 2 y el nodo de red de radio 1 de la Fig. 1. La pila de protocolos 20 se ilustra aquí para transferir un paquete IP 10 a través de la RAN. La pila de protocolos se compone de un protocolo de adaptación de datos de servicio (SDAP) 21, un protocolo de convergencia de datos de paquetes (PDCP) 22 y un control de enlace de radio

15 (RLC) 23. En el nivel más bajo, hay un protocolo de control de acceso a medios (MAC) 24.

Cada protocolo 21 - 24, toma una unidad de datos de servicio (SDU) 10, 11, 12, 13 de una capa de protocolo superior para formar la carga útil 11a, 12a, 13a, 14a. A continuación, el protocolo 21 – 24 agrega datos de control

20 específicos desde el protocolo, por ejemplo, los encabezados 11b, 12b, 13b, 14b, para producir una unidad de datos de protocolo (PDU) 11, 12, 13, 14 respectiva.

La PDU se proporciona a la siguiente capa inferior en la pila de protocolos 20, formando la SDU para esa capa.

La capa MAC 24 puede combinar múltiples SDU de la capa RLC 23 en una sola PDU 14 (que comprende las cargas útiles respectivas 14a, 14'a y los
5 encabezados 14b, 14b'). En otras palabras, un bloque de transporte de MAC PDU está formado por una o varias MAC PDU. Para SDAP y PDCP, existe una relación uno a uno entre PDU 11, 12 y el paquete IP 10.

Las Figs. 4A-B son diagramas de flujo que ilustran realizaciones de procedimientos para la detección de un ataque DoS en un dispositivo
10 ascendente, como la red central 3 o el servidor 5 de la Fig. 1. El procedimiento se realiza en un nodo de red de radio 1. En primer lugar, se describirán las realizaciones ilustradas por la Fig. 4A.

En una etapa de obtención de métricas 40, el nodo de red de radio 1 obtiene (al menos una) métrica en base a la señalización RAN para la
15 comunicación entre un UE y el nodo de red de radio 1. La señalización RAN comprende uno o más procedimientos de protocolo, cuya estructura y utilización se pueden definir en las especificaciones normalizadas pertinentes, por ejemplo, entre otras, del Proyecto de Asociación de 3ª Generación o del Grupo de Trabajo de Ingeniería de Internet.

20 La métrica se puede basar en un volumen de solicitudes de programación transmitidas desde el UE. Alternativamente o adicionalmente, la métrica se basa

en los informes de estado del búfer (BSR) del UE. Alternativamente o adicionalmente, la métrica se basa en un volumen de los PRB utilizados.

En una etapa de ataque DoS condicional 42, el nodo de red de radio 1 determina si hay un ataque DoS en curso hacia el dispositivo ascendente 3 en base a la métrica. El dispositivo ascendente es externo al nodo de red de radio 1 y se proporciona en dirección ascendente desde el nodo de red de radio 1.

Cuando la métrica contiene una indicación de un volumen de solicitudes de programación, el ataque DoS se puede determinar en base a que el volumen de solicitudes de programación sea menor a un volumen umbral de solicitudes de programación. El volumen de solicitudes de programación se puede definir, por ejemplo, como el número de solicitudes de programación por unidad de tiempo.

Una solicitud de programación es una solicitud de un UE al nodo de red de radio 1 para transmitir tráfico UL. Si el nodo de red de radio 1 concede la solicitud, programa el tráfico UL para el UE y envía un mensaje de concesión, indicando dónde está programado el tráfico UL para la transmisión de los UE. Si un intervalo de tiempo entre paquetes es corto, no es necesario enviar una nueva solicitud de programación a la red.

Por lo tanto, cuando un ataque DoS volumétrico está en curso y el búfer del DoS UE se llena de datos para la transmisión UL, lo que lleva a una alta tasa de envío de paquetes UL, el volumen de solicitudes de programación es significativamente menor que para el tráfico normal.

Los BSR son parte de un procedimiento de capa MAC que utiliza el UE para proporcionar información sobre la cantidad de datos disponibles para la transmisión en los búferes UL. Los BSR se envían al nodo de red de radio de servicio 1. Cuando la métrica se basa en los BSR del UE, el ataque DoS se
5 puede determinar en base a una estadística de frecuencia de los BSR, lo que indica una frecuencia mayor que una frecuencia de umbral. La frecuencia se puede definir como el número de BSR por unidad de tiempo, o utilizando un equivalente, tal como el tiempo medio entre transmisiones de BSR.

Cuando hay un ataque DoS volumétrico en el plano del usuario, los BSR
10 son más frecuentes debido a la transmisión constante del tráfico de ataque UL, en comparación con un escenario benigno con tráfico de menor velocidad.

Alternativamente o adicionalmente, se puede determinar un ataque DoS en base a los BSR que indican un alto nivel de búfer a lo largo del tiempo. Debido a los cortos intervalos entre las PDU durante un ataque y la posible
15 concatenación de PDCP PDU (en caso de LTE), el nivel de búfer mantendrá un valor alto durante un ataque DoS volumétrico.

Cuando la métrica se basa en un volumen de los PRB utilizados, el ataque DoS se puede determinar en base a que el volumen de los PRB sea mayor que un volumen umbral de los PRB.

20 El nodo de red de radio 1 se puede configurar para detectar cualquier ataque DoS volumétrico, tal como una inundación de paquetes UDP y/o una

inundación de mensajes TCP SYN. Por lo tanto, el ataque DoS que se detecta puede implicar un ataque de plano de usuario.

Cuando no se determina un ataque DoS, el procedimiento vuelve a la etapa de obtención de métricas 40. Cuando se determina un ataque DoS, este se puede utilizar interna o externamente, después de lo cual el procedimiento puede finalizar o volver a la etapa de obtención de métricas 40.

Mirando ahora a la Fig. 4B, solo se describirán las etapas nuevas o modificadas, en comparación con la Fig. 4A.

En una etapa de ataque de señal opcional 44, el nodo de red de radio 1, el nodo de red de radio 1 señala una alerta que indica que el ataque DoS está en curso.

Esta señalización se puede producir localmente dentro del nodo de red de radio 1. En este caso, el nodo de red de radio 1 puede actuar como el PEP (punto de aplicación de políticas), por ejemplo, al denegar (o restringir) los recursos de radio para el DoS UE. Por lo tanto, el DoS UE no tiene acceso por radio, lo que impide que el DoS UE envíe cualquier (o cantidad excesiva) de tráfico. Esto proporciona una respuesta rápida a un ataque detectado. Dado que las realizaciones presentadas en la presente memoria se implementan en el nodo de red de radio 1, este nodo tiene poder sobre la programación y permite que la respuesta y la mitigación del ataque ocurran rápidamente y con un efecto sustancial.

Alternativamente o adicionalmente, la señalización del ataque DoS se produce desde el nodo de red de radio 1 hasta la red central 3. En este caso, el nodo de red de radio 1 actúa como un punto de decisión de políticas (PDP), mientras que un nodo de red dentro de la red central actúa como el PEP. Por ejemplo, la función de gestión de acceso y movilidad (AMF) de la red central puede actuar como PEP. De esta manera, la AMF puede utilizar alertas, información de ataque, información de DoS UE, que se proporciona desde el nodo de red de radio 1, para actuar sobre ella y responder al DoS UE, por ejemplo, al cancelar o poner en cuarentena el DoS UE de la red.

Las métricas se pueden basar en el tráfico del plano de control, es decir, no en el tráfico del plano de usuario de la RAN, incluso si el tráfico del plano de control a menudo admite el tráfico del plano del usuario. El tráfico del plano de control puede ocurrir, por ejemplo, a través de la interfaz Uu proporcionada para un UE por el nodo de red de radio 1. Las realizaciones presentadas en la presente memoria no se basan en la inspección del contenido de los paquetes.

Ahora se describirán los resultados de una simulación para ilustrar cómo se puede detectar DoS. El DoS simulado es un ataque de inundación UDP, pero los mismos principios son aplicables para las inundaciones TCP SYN u otros ataques DoS volumétricos. En la simulación, el UE es una Raspberry Pi, que actúa como un DoS UE en forma de controlador IoT que normalmente se comunica con brazos robóticos.

El UE tiene un patrón de tráfico específico para el tráfico benigno. Este tráfico benigno tiene las siguientes características:

- Tráfico de protocolo TCP que envía paquetes a los brazos robóticos.
- Se envían paquetes de 160-320 bytes cada 10 ms.
- 5 • Se envían algunos paquetes de tamaño 1514 bytes cada 200-500 ms.

Adicionalmente, el UE se simula, en un escenario de tráfico mixto, para enviar ataques de inundación UDP, en ciertos períodos de tiempo. Por lo tanto, el tráfico malicioso se mezcla con el tráfico benigno a lo largo del tiempo. La simulación se configuró para ejecutarse durante 30 segundos, donde el período
10 de ataque se ejecuta durante 10 segundos en medio de los 30 segundos, con destino a una subred /24. Los resultados se comparan con la ejecución solo de tráfico benigno.

El tráfico benigno en el escenario de tráfico mixto es del mismo tipo que el tráfico benigno descrito anteriormente. El tráfico malicioso se dirigía a una
15 subred /24, donde había varios objetivos que respondían en el servicio de interés. La carga útil UDP se estableció en un tamaño de 512 bytes.

El número de SR cae significativamente (alrededor del 62 por ciento) durante el período de ataque. Adicionalmente, el número de PRB aumenta significativamente durante el período de ataque para admitir el aumento del
20 tráfico UL que requiere un mayor tráfico de plano de usuario y, por lo tanto, un mayor número de los PRB por unidad de tiempo.

Las realizaciones presentadas en la presente memoria no examinan ni analizan ningún paquete IP que se esté transportando en los protocolos de radio. En su lugar, se examinan y analizan las métricas derivadas del plano de control de la RAN. Esto puede permitir la detección de ataques DoS incluso cuando los
5 paquetes IP están ocultos u oscurecidos, tal como a través del cifrado, desde el nodo de red de radio 1.

Dado que el ataque DoS es detectado por el nodo de red de radio 1 que está topológicamente cerca del UE comprometido, el ataque DoS se puede detectar más rápido y abordar mejor. Más aún, el nodo de red de radio 1 puede
10 explotar métricas, tales como el volumen de SR, BSR y el uso de PRB, que no están disponibles en un contexto IP puro.

La detección por el nodo de red de radio 1 también permite que el nodo de red de radio 1 aplique una respuesta local y acciones de mitigación. Por ejemplo, el nodo de red de radio 1 puede denegar recursos de radio para los
15 DoS UE, lo que reduce los efectos en la RAN de un DoS UE, además de mitigar el ataque en el dispositivo de destino ascendente. Más aún, también se puede proteger la infraestructura de telecomunicaciones, por ejemplo, reduciendo o eliminando el tráfico DoS que de otro modo podría consumir ancho de banda de la red de retorno a la red central. También, las realizaciones presentadas en la
20 presente memoria resuelven problemas de escalabilidad en la red, por lo que se reduce la necesidad de soluciones de detección DoS adicionales.

La Fig. 5 es un diagrama esquemático que ilustra los componentes del nodo de red de radio 1 de la Fig. 1. Un procesador 60 se proporciona utilizando cualquier combinación de una o más de una unidad central de procesamiento (CPU), unidad de procesamiento gráfico (GPU), multiprocesador, unidad de procesamiento neuronal (NPU), microcontrolador, procesador de señal digital (DSP), etc., capaz de ejecutar instrucciones de software 67 almacenadas en una memoria 64, que por lo tanto puede ser un producto de programa informático. El procesador 60 se podría implementar alternativamente utilizando un circuito integrado específico de la aplicación (ASIC), una matriz de puertas programables en campo (FPGA), etc. El procesador 60 se puede configurar para ejecutar el procedimiento descrito con referencia a las Figs. 4A y 4B anteriores.

La memoria 64 puede ser cualquier combinación de memoria de acceso aleatorio (RAM) y/o memoria de solo lectura (ROM). La memoria 64 también comprende almacenamiento persistente no transitorio, que, por ejemplo, puede ser una sola o una combinación memoria magnética, memoria óptica, memoria de estado sólido o incluso memoria montada de forma remota.

También se proporciona una memoria de datos 66 para leer y/o almacenar datos durante la ejecución de instrucciones de software en el procesador 60. La memoria de datos 66 puede ser cualquier combinación de RAM y/o ROM.

El nodo de red de radio 1 comprende además una interfaz de E/S 62 para comunicarse con entidades externas y/o internas. Opcionalmente, la interfaz de E/S 62 también incluye una interfaz de usuario.

Un transceptor 61 comprende componentes analógicos y digitales adecuados para permitir la transmisión y recepción de señales con UE que utilizan una o más antenas 63.

Se omiten otros componentes del nodo de red de radio 1 para no
5 oscurecer los conceptos presentados en la presente memoria.

La Fig. 6 es un diagrama esquemático que muestra los módulos funcionales del nodo de red de radio 1 de la Fig. 1 de acuerdo con una realización. Los módulos se implementan utilizando instrucciones de software, tales como un programa informático que se ejecuta en el nodo de red de radio 1.
10 Alternativamente o adicionalmente, los módulos se implementan utilizando hardware, tal como uno o más de un ASIC (Circuito Integrado Específico de Aplicación), una FPGA (Matriz de Puertas Programables en Campo) o circuitos lógicos discretos. Los módulos corresponden a las etapas de los procedimientos ilustrados en las Figs. 4A y 4B.

15 Un obtenedor de métrica 70 corresponde a la etapa 40. Un determinante de ataque DoS 72 corresponde a la etapa 42. Un señalizador de ataque 74 corresponde a la etapa 44.

La Fig. 7 muestra un ejemplo de un producto de programa informático 90 que comprende medios legibles por ordenador. En este medio legible por
20 ordenador, un programa informático 91 se puede almacenar en una memoria no transitoria. El programa informático puede hacer que un procesador ejecute un procedimiento de acuerdo con las realizaciones descritas en la presente

memoria. En este ejemplo, el producto del programa informático tiene la forma de una memoria de estado sólido extraíble, por ejemplo, una unidad de Bus Serie Universal (USB). Como se explicó anteriormente, el producto del programa informático también podría estar incorporado en la memoria de un dispositivo, tal como el producto del programa informático 64 de la Fig. 5. Mientras que el programa informático 91 se muestra aquí esquemáticamente como una sección de la memoria de estado sólido extraíble, el programa informático se puede almacenar de cualquier manera que sea adecuada para el producto del programa informático, tal como otro tipo de memoria de estado sólido extraíble, o un disco óptico, tal como un CD (disco compacto), un DVD (disco versátil digital) o un disco Blu-Ray.

Los aspectos de la presente revelación se han descrito principalmente anteriormente con referencia a algunas realizaciones. Sin embargo, como aprecia fácilmente una persona experta en la técnica, otras realizaciones distintas de las divulgadas anteriormente son igualmente posibles dentro del alcance de la invención, tal como se define en las reivindicaciones de patente adjuntas. Por lo tanto, aunque se han divulgado varios aspectos y realizaciones en la presente memoria, otros aspectos y realizaciones serán evidentes para los expertos en la técnica. Los diversos aspectos y realizaciones divulgados en la presente memoria son para fines ilustrativos y no pretenden ser limitativos, con el verdadero alcance y espíritu indicado por las siguientes reivindicaciones.