

REIVINDICACIONES CAPÍTULO II

1. Un procedimiento para la detección de un ataque de denegación de servicio, DoS, en un dispositivo ascendente, realizándose el procedimiento en un nodo de red de radio (1) y comprendiendo el procedimiento:

- 5 obtener (40) una métrica sobre la base de la señalización de la red de acceso de radio, RAN, para la comunicación entre un equipo de usuario UE (2), y el nodo de red de radio (1);, en donde la métrica se basa en informes de estado de búfer, BSR, desde el UE y/o en donde la métrica se basa en un volumen de bloques de recursos físicos, PRB, utilizados; y
- 10 determinar (42) que un ataque DoS está en curso en el dispositivo ascendente (1) sobre la base de la métrica, en donde el dispositivo ascendente se proporciona en dirección ascendente desde el nodo de red de radio (1), en donde, en caso de que la métrica se base en los BSR, la determinación (42) de que un ataque DoS está en curso comprende la determinación de que una
- 15 estadística de la frecuencia de los BSR indica una frecuencia que es mayor que una frecuencia umbral.

2. El procedimiento de acuerdo con la reivindicación 1, en el que la métrica se basa en un volumen de solicitudes de programación transmitidas desde el UE.

- 20 3. El procedimiento de acuerdo con la reivindicación 2, en el que la determinación (42) de que un ataque DoS está en curso comprende la

determinación de que el volumen de solicitudes de programación es menor que un volumen umbral de solicitudes de programación.

4. El procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la determinación (42) de que un ataque DoS está en curso
5 comprende la determinación de que los BSR indican un alto nivel de búfer a lo largo del tiempo.

5. El procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la determinación (42) de que un ataque DoS está en curso comprende la determinación de que el volumen de los PRB es mayor que un
10 volumen umbral de los PRB.

6. El procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, que comprende además:

señalizar (44) una alerta que indica que el ataque DoS está en curso.

7. El procedimiento de acuerdo con una cualquiera de las reivindicaciones
15 anteriores, en el que la determinación (42) de que un ataque DoS está en curso está configurada para detectar una inundación de paquetes de protocolo de datagramas de usuario, UDP.

8. El procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que la determinación (42) de que un ataque DoS está en curso
20 está configurada para detectar una inundación de mensajes de protocolo de control de transporte, TCP, de sincronización, SYN.

9. El procedimiento de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que el ataque DoS implica un ataque de plano de usuario.

10. Un nodo de red de radio (1) para la detección de un ataque de denegación de servicio, DoS, en un dispositivo ascendente (3, 5),
5 comprendiendo el nodo de red de radio (1):

un procesador (60); y

una memoria (64) que almacena instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1):

10 obtenga una métrica sobre la base de la señalización de la red de acceso de radio, RAN, para la comunicación entre un equipo de usuario UE (2), y el nodo de red de radio (1), en donde la métrica se basa en informes de estado de búfer, BSR, desde el UE y/o en donde la métrica se basa en un volumen de bloques de recursos físicos, PRB, utilizados; y

15 determine que hay un ataque DoS en curso en el dispositivo ascendente (1) sobre la base de la métrica, en donde el dispositivo ascendente se proporciona en dirección ascendente desde el nodo de red de radio (1), en donde en caso de que la métrica se base en los BSR, las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1)
20 determine que una estadística de la frecuencia de los BSR indica una frecuencia que es mayor que una frecuencia umbral.

11. El procedimiento de acuerdo con la reivindicación 13, en el que la métrica se basa en un volumen de solicitudes de programación transmitidas desde el UE.

12. El nodo de red de radio (1) de acuerdo con la reivindicación 14, en el
5 que las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1) determine que el volumen de solicitudes de programación es menor que un volumen umbral de solicitudes de programación.

10 13. El nodo de red de radio (1) de acuerdo con una cualquiera de las reivindicaciones 10 a 12, en el que las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1) determine que los BSR indican un alto nivel de búfer a lo largo del tiempo.

15 14. El nodo de red de radio (1) de acuerdo con una cualquiera de las reivindicaciones 10 a 13, en el que las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1) determine que el volumen de los PRB es mayor que un volumen umbral de los PRB.

20 15. El nodo de red de radio (1) de acuerdo con una cualquiera de las reivindicaciones 10 a 14, que comprende además instrucciones (67) que, cuando

son ejecutadas por el procesador, hacen que el nodo de red de radio (1) señale una alerta que indica que el ataque DoS está en curso.

16. El nodo de red de radio (1) de acuerdo con una cualquiera de las reivindicaciones 10 a 15, en el que las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1) detecte una inundación de paquetes de protocolo de datagramas de usuario, UDP.

17. El nodo de red de radio (1) de acuerdo con una cualquiera de las reivindicaciones 10 a 16, en el que las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1) detecte una inundación de mensajes de protocolo de control de transporte, TCP, de sincronización, SYN.

18. El nodo de red de radio (1) de acuerdo con una cualquiera de las reivindicaciones 10 a 17, en el que el ataque DoS implica un ataque de plano de usuario.

19. Un programa informático (67, 91) para la detección de un ataque de denegación de servicio, DoS, en un dispositivo ascendente (3, 5), comprendiendo el programa informático el código de un programa informático que, cuando se ejecuta en un nodo de red de radio (1) hace que el nodo de red de radio (1):

obtenga una métrica sobre la base de la señalización de la red de acceso de radio, RAN, para la comunicación entre un equipo de usuario UE (2), y el nodo de red de radio (1), en donde la métrica se basa en informes de estado de búfer, BSR, desde el UE y/o en donde la métrica se basa en un volumen de bloques de recursos físicos, PRB, utilizados; y

determine que hay un ataque DoS en curso en el dispositivo ascendente (1) sobre la base de la métrica, en donde el dispositivo ascendente se proporciona en dirección ascendente desde el nodo de red de radio (1), en donde en caso de que la métrica se base en los BSR, las instrucciones para determinar que un ataque DoS está en curso comprenden instrucciones (67) que, cuando son ejecutadas por el procesador, hacen que el nodo de red de radio (1) determine que una estadística de la frecuencia de los BSR indica una frecuencia que es mayor que una frecuencia umbral.

20. Un producto de programa informático (64, 90) que comprende un programa informático de acuerdo con la reivindicación 19 y un medio legible por ordenador que comprende la memoria no transitoria en la que se almacena el programa informático.