



(51) International Patent Classification:

H04W 12/12 (2021.01) H04L 9/00 (2022.01)

(21) International Application Number:

PCT/SE2023/050073

(22) International Filing Date:

27 January 2023 (27.01.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; SE-164 83 Stockholm (SE).

(72) Inventors: **ABDELRAZEK, Loay**; Mörbýdalen 6, SE-182 52 Danderyd (SE). **KÖVÉR, János**; Alingsåsvägen 20. lgh 1201, SE-121 48 Johanneshov (SE). **ULLAH, Ikram**; G-1921, Quail Lane, King Abdullah, of University of Science & Technology, Thuwal, 13955 (SA).

(74) Agent: **EGRELIUS, Fredrik**; Ericsson AB, Patent Unit Kista, Torshamnsgatan 23, 164 80 Stockholm (SE).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM,

DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

- with international search report (Art. 21(3))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE

(54) Title: DETECTING A DENIAL-OF-SERVICE (DOS) ATTACK ON AN UPSTREAM DEVICE BASED ON RADIO ACCESS NETWORK (RAN) SIGNALLING

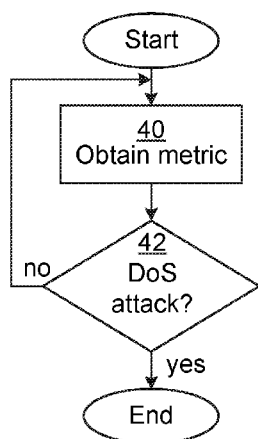


Fig. 4A

(57) Abstract: It is provided a method for detecting a denial-of-service, DoS, attack, on an upstream device, the method being performed in a radio network node. The method comprises: obtaining a metric based on radio access network, RAN, signalling for communication between a user equipment, UE, and the radio network node; and determining that a DoS attack is in progress on the upstream device based on the metric, wherein the upstream device is provided upstream from the radio network node.



DETECTING A DENIAL-OF-SERVICE (DOS) ATTACK ON AN UPSTREAM DEVICE BASED ON RADIO ACCESS NETWORK (RAN) SIGNALLING

TECHNICAL FIELD

[0001] The present disclosure relates to the field of detecting a denial-of-service (DoS) attack, and in particular to a radio network node detecting a DoS attack on an upstream device based on RAN signalling.

BACKGROUND

[0002] Distributed denial of service (DDoS) attacks are becoming more widespread. A DDoS attack is based on an attacker gaining control of a great number of devices connected to the Internet, thereby forming a botnet. IoT devices are constantly increasing in prevalence. The potential security issues and increasing volume of IoT devices make them targets for attackers to create botnets that can launch DDoS attacks towards targets that reside on the Internet.

[0003] There are several types of DDoS attacks. One example is the UDP flood volumetric attack. The UDP protocol is normally used in time-sensitive communications, for example voice, video, and gaming traffic. However, the UDP protocol can be used in a volumetric attack, called a UDP flood attack, since a communication channel does not need to be established prior to transmit a UDP packet.

[0004] Similarly to a UDP flood attack, a TCP SYN (synchronise message) flood attack results in a high traffic volume but with different characteristics.

[0005] Hence, there are several types of volumetric attacks, with high packet rates that attempt to cause exhaustion of resources of a server and/or network link. The UDP flood attack and TCP SYN attacks are DDoS type attacks in which a flood of packets are sent to a targeted server with the aim of overwhelming the ability of the server to receive, process and/or respond.

SUMMARY

[0006] One object is to improve how DoS attacks are detected.

[0007] According to a first aspect, it is provided a method for detecting a denial-of-service, DoS, attack, on an upstream device, the method being performed in a radio

network node. The method comprises: obtaining a metric based on radio access network, RAN, signalling for communication between a user equipment, UE, and the radio network node; and determining that a DoS attack is in progress on the upstream device based on the metric, wherein the upstream device is provided upstream from the radio network node.

[0008] The metric may be based on a volume of scheduling requests transmitted from the UE.

[0009] The determining that a DoS attack is in progress may comprise determining that the volume of scheduling requests is less than a threshold volume of scheduling requests.

[0010] The metric may be based on buffer status reports, BSRs, from the UE.

[0011] The determining that a DoS attack is in progress may comprise determining that a statistic of frequency of BSRs indicate a frequency that is greater than a threshold frequency.

[0012] The determining that a DoS attack is in progress may comprise determining that the BSRs indicate a high buffer level over time.

[0013] The metric may be based on a volume of used physical resource blocks, PRBs.

[0014] The determining that a DoS attack is in progress may comprise determining that the volume of PRBs is greater than a threshold volume of PRBs.

[0015] The method may further comprise: signalling an alert indicating that the DoS attack is in progress.

[0016] The determining that a DoS attack is in progress may be configured to detect a flood of user datagram protocol, UDP, packets.

[0017] The determining that a DoS attack is in progress may be configured to detect a flood of transport control protocol, TCP, synchronise, SYN, messages.

[0018] The DoS attack may involve a user plane attack.

[0019] According to a second aspect, it is provided a radio network node for detecting a denial-of-service, DoS, attack on an upstream device. The radio network node comprises: a processor; and a memory storing instructions that, when executed by the processor, cause the radio network node to: obtain a metric based on radio access network, RAN, signalling for communication between a user equipment, UE, and the radio network node; and determine that a DoS attack is in progress on the upstream device based on the metric, wherein the upstream device is provided upstream from the radio network node.

[0020] The metric may be based on a volume of scheduling requests transmitted from the UE.

[0021] The instructions to determine that a DoS attack is in progress may comprise instructions that, when executed by the processor, cause the radio network node to determining that the volume of scheduling requests is less than a threshold volume of scheduling requests.

[0022] The metric may be based on buffer status reports, BSRs, from the UE.

[0023] The instructions to determine that a DoS attack is in progress may comprise instructions that, when executed by the processor, cause the radio network node to determine that a statistic of frequency of BSRs indicate a frequency that is greater than a threshold frequency.

[0024] The instructions to determine that a DoS attack is in progress may comprise instructions that, when executed by the processor, cause the radio network node to determine that the BSRs indicate a high buffer level over time.

[0025] The metric may be based on a volume of used physical resource blocks, PRBs.

[0026] The instructions to determine that a DoS attack is in progress may comprise instructions that, when executed by the processor, cause the radio network node to determine that the volume of PRBs is greater than a threshold volume of PRBs.

[0027] The radio network node may further comprise instructions that, when executed by the processor, cause the radio network node to signal an alert indicating that the DoS attack is in progress.

[0028] The instructions to determine that a DoS attack is in progress may comprise instructions that, when executed by the processor, cause the radio network node to detect a flood of user datagram protocol, UDP, packets.

[0029] The instructions to determine that a DoS attack is in progress may comprise instructions that, when executed by the processor, cause the radio network node to detect a flood of transport control protocol, TCP, synchronise, SYN, messages.

[0030] The DoS attack may involve a user plane attack.

[0031] According to a third aspect, it is provided a computer program for detecting a denial-of-service, DoS, attack on an upstream device. The computer program comprises computer program code which, when executed on a radio network node causes the radio network node to: obtain a metric based on radio access network, RAN, signalling for communication between a user equipment, UE, and the radio network node; and determine that a DoS attack is in progress on the upstream device based on the metric, wherein the upstream device is provided upstream from the radio network node.

[0032] According to a fourth aspect, it is provided a computer program product comprising a computer program according to the third aspect and a computer readable means comprising non-transitory memory in which the computer program is stored.

[0033] Generally, all terms used in the claims are to be interpreted according to their ordinary meaning in the technical field, unless explicitly defined otherwise herein. All references to "a/an/the element, apparatus, component, means, step, etc." are to be interpreted openly as referring to at least one instance of the element, apparatus, component, means, step, etc., unless explicitly stated otherwise. The steps of any method disclosed herein do not have to be performed in the exact order disclosed, unless explicitly stated.

BRIEF DESCRIPTION OF THE DRAWINGS

[0034] Aspects and embodiments are now described, by way of example, with reference to the accompanying drawings, in which:

[0035] Fig 1 is a schematic diagram illustrating an environment in which embodiments presented herein can be applied;

[0036] Fig 2 is a schematic diagram illustrating an embodiment of a distributed implementation of the radio network node;

[0037] Fig 3 illustrates a protocol stack comprising a set of protocols for RAN communication between the UE (user equipment) and the radio network node;

[0038] Figs 4A-B are flow charts illustrating embodiments of methods for detecting a DoS attack on an upstream device;

[0039] Fig 5 is a schematic diagram illustrating components of the radio network node of Fig 1;

[0040] Fig 6 is a schematic diagram showing functional modules of the radio network node of Fig 1 according to one embodiment; and

[0041] Fig 7 shows one example of a computer program product comprising computer readable means.

DETAILED DESCRIPTION

[0042] The aspects of the present disclosure will now be described more fully hereinafter with reference to the accompanying drawings, in which certain embodiments of the invention are shown. These aspects may, however, be embodied in many different forms and should not be construed as limiting; rather, these embodiments are provided by way of example so that this disclosure will be thorough and complete, and to fully convey the scope of all aspects of invention to those skilled in the art. Like numbers refer to like elements throughout the description.

[0043] According to embodiments presented herein, it is provided a way to detect volumetric DoS attacks initiated by a compromised UE (e.g., IoT devices or any other type of UE) connected to the radio access network (RAN). The detection is performed by the radio network node that provides the RAN. This detection is achieved by analysing metrics derived from RAN signalling, related to the UE in question. The content of the packets is not evaluated; the DoS detection operates without the need for deep packet inspection. This detection enables a DoS attack to be mitigated already by the radio network node, as described in more detail below.

[0044] Fig 1 is a schematic diagram illustrating an environment in which embodiments presented herein can be applied. A cellular communication network 8 comprises a core network 3 and one or more radio network nodes 1 (also known as base stations) that provide a RAN for one or more UEs 2.

[0045] The radio network node 1 can be the form of radio base stations being gNode Bs, gNBs, or evolved Node Bs, also known as eNode Bs or eNBs. The radio network nodes could also be in the form of Node Bs, BTSs (Base Transceiver Stations) and/or BSSs (Base Station Subsystems), etc. The radio network node 1 provides radio connectivity using the RAN over a wireless interface 4a-b to one or more UEs 2. The radio network node 1 can be implemented in the form of a single hardware device or distributed over several devices, as illustrated in Fig 2 and explained below.

[0046] Over the wireless interface of the RAN, downlink (DL) communication 4a occurs from the radio network node 1 to the UE 2 and uplink (UL) communication 4b occurs from the UE 2 to the radio network node 1. The quality of the wireless radio interface to each UE 2 can vary over time and depending on the position of the UE 2, due to effects such as fading, multipath propagation, interference, etc.

[0047] The term UE is also known as mobile communication terminal, user device, mobile terminal, user terminal, user agent, wireless device, wireless terminal, machine-to-machine device etc., and can be implemented by, for example, what today are commonly known as a mobile phone, smartphone, IoT device, or a tablet/laptop with wireless connectivity.

[0048] The cellular communication network 8 may e.g. comply with any one or a combination of 5G NR (fifth generation new radio), LTE (Long Term Evolution), LTE-Advanced, 6G (sixth generation), W-CDMA (Wideband Code Division Multiplex), or any other current or future wireless network, as long as the principles described herein are applicable.

[0049] The radio network node 1 is connected to the core network 3 for connectivity to network central functions and a wide area network 9, such as the Internet. A server 5 is also connected to the network. Both user plane data and control plane data are transmitted over the UL and DL links 4a/4b of the RAN.

[0050] It is possible that an attacker can gain control over the UE 2 to orchestrate a denial of service (DoS) attack, e.g. targeted against a node in the core network 3 and/or the server 5. When multiple devices, such as the UE 2, are used in the same attack, it is called a distributed DoS (DDoS) attack. While each UE 2 may in this way form part of a DDoS attack, hereinafter it is referred to a DoS attack.

[0051] When a UE 2 has been compromised for DoS purposes, such a UE is denoted a DoS UE herein. One form of DoS attack is a UDP flood, in which an attacker controls a DoS UE 2 to transmits a large amount of UDP packets to a target device. Another type of DoS attack is a TCP SYN flood attack. This attack works on the same principle as the UDP flood, since the TCP SYN message is an initial message of a TCP connection establishment, and can be transmitted to a server prior to the TCP connection being established and still comply with the TCP protocol. This may be attractive from an attacker perspective since both a UDP packet and a TCP SYN packet can be sent from a compromised UE, and these packets can optionally be repeated arbitrarily in time and frequency. Both the UDP flood attack and the TCP SYN flood attack are called volumetric attacks.

[0052] According to embodiments presented herein, the radio network node 1 detects a DoS attack against an upstream node (e.g. a node of the core network 3 or the server 5), where the DoS attack is (at least partly) based on traffic from the UE 2. An upstream node is to be interpreted as a node that is located more centrally from the radio network node 1, i.e. in the other topological direction than the UE and/or in the same topological direction as the core network or wide area network 9, as seen from the radio network node 1.

[0053] Fig 2 is a schematic diagram illustrating an embodiment of a distributed implementation of the radio network node 1. The radio network node 1 is made up of a baseband node 6 and a radio node 7.

[0054] The radio network node 1 comprises a baseband node 10 being a baseband processing unit and one or more remote radio nodes 11. When applied in an O-RAN (Open RAN) architecture, the baseband node can be an O-DU (O-RAN distributed unit) node and the radio node can be an O-RU (O-RAN radio unit) node. In 5G terminology, e.g. according to a C-RAN (Centralised/Cloud Radio Access Network) architecture, the baseband node 10 can be a gNB-CU and the radio node 11 can be a gNB-DU.

[0055] The baseband node 10 and the radio node 11 can be in different locations. The baseband node 10 is located upstream from the radio node 11, i.e. towards the core network 3. Consequently, the radio node 11 can be located downstream from the baseband node 10, towards the UE 2. There are one or more fronthaul links 18 between the baseband node 10 and the radio node 11. The fronthaul links 18 are bidirectional communication links. The fronthaul links 18 can be implemented using a Common Public Radio Interface (CPRI) or eCPRI (evolved CPRI) and Ethernet. Multiple fronthaul links can be employed in other topologies than what is shown in Fig 1. Multiple fronthaul links can also be denoted a fronthaul network. The baseband node 10 and the radio node 11 can each implement subsets of functionality of the RAN for radio communication with the UE 2. Furthermore, some functionality for the radio communication can be virtualized, also known as cloud RAN.

[0056] Fig 3 illustrates a protocol stack 20 comprising a set of protocols 21, 22, 23, 24 of the RAN communication between the UE 2 and the radio network node 1 of Fig 1. The protocol stack 20 is here illustrated for transferring an IP packet 10 over the RAN. The protocol stack is made up of a service data adaptation protocol (SDAP) 21, a packet data convergence protocol (PDCP) 22, and a radio link control (RLC) 23. On the lowest level, there is a media access control (MAC) protocol 24.

[0057] Each protocol 21 - 24, takes a service data unit (SDU) 10, 11, 12, 13 from a higher protocol layer to form the payload 11a, 12a, 13a, 14a. The protocol 21 – 24 then adds protocol specific control data, e.g. headers 11b, 12b, 13b, 14b, to produce a respective protocol data unit (PDU) 11, 12, 13, 14. The PDU is provided to the next lower layer in the protocol stack 20, forming the SDU for that layer.

[0058] The MAC layer 24 can combine multiple SDUs from the RLC layer 23 in a single PDU 14 (comprising respective payloads 14a, 14'a and headers 14b, 14b'). In other words, a MAC PDU transport block is formed by one or several MAC PDUs. For SDAP and PDCP, there is a one-to-one relationship between PDU 11, 12 and IP packet 10.

[0059] Figs 4A-B are flow charts illustrating embodiments of methods for detecting a DoS attack on an upstream device, such as the core network 3 or the server 5 of Fig 1. The method is performed in a radio network node 1. First, embodiments illustrated by Fig 4A will be described.

[0060] In an *obtain metric* step 40, the radio network node 1 obtains (at least one) metric based on RAN signalling for communication between a UE and the radio network node 1. The RAN signalling comprises one or more protocol procedures, the structure and usage of which can be defined in relevant standard specifications from, for example but not limited to, 3rd Generation Partnership Project or Internet Engineering Task Force.

[0061] The metric can be based on a volume of scheduling requests transmitted from the UE. Alternatively or additionally, the metric is based on buffer status reports (BSRs), from the UE. Alternatively or additionally, the metric is based on a volume of used PRBs.

[0062] In a conditional *DoS attack* step 42, the radio network node 1 determines whether a DoS attack is in progress towards the upstream device 3 based on the metric. The upstream device is external to the radio network node 1 and is provided upstream from the radio network node 1.

[0063] When the metric contains an indication of a volume of scheduling requests, the DoS attack can be determined based on the volume of scheduling requests being less than a threshold volume of scheduling requests. The volume of scheduling requests can e.g. be defined as number of scheduling requests per unit of time.

[0064] A scheduling request is a request from a UE to the radio network node 1 for transmitting UL traffic. If the radio network node 1 grants the request, it schedules UL traffic for the UE and sends a grant message, indicating where the UL traffic is scheduled for the UEs transmission. If a time interval between packets is short, a new scheduling request does not need to be sent to the network.

[0065] Hence, when a volumetric DoS attack is in progress, and the buffer of the DoS UE is filled with data for UL transmission leading to a high rate of UL packets being sent, the volume of scheduling requests is significantly lower than for normal traffic.

[0066] BSRs are part of a MAC layer procedure which is used by the UE to provide information about the amount of data available for transmission in the UL buffers. The BSRs are sent to the serving radio network node 1. When the metric is based on BSRs from the UE, the DoS attack can be determined based on a statistic of frequency of

BSRs, indicating a frequency that is greater than a threshold frequency. Frequency can be defined as number of BSRs per unit of time, or using an equivalent, such as mean time between BSR transmissions.

[0067] When there is a volumetric DoS attack on the user plane, BSRs are more frequent due to the constant transmission of UL attack traffic, compared to a benign scenario with lower rate traffic.

[0068] Alternatively or additionally, a DoS attack can be determined based on the BSRs indicating a high buffer level over time. Due to short intervals between the PDUs during an attack, and possible concatenation of PDCP PDUs (in case of LTE), the buffer level will maintain a high value during a volumetric DoS attack.

[0069] When the metric is based on a volume of used PRBs, the DoS attack can be determined based on the volume of PRBs being greater than a threshold volume of PRBs.

[0070] The radio network node 1 can be configured to detect any volumetric DoS attack, such as a flood of UDP packets and/or a flood of TCP SYN messages. Hence, the DoS attack that is detected can involve a user plane attack.

[0071] When a DoS attack is not determined, the method returns to the obtain metrics step 40. When a DoS attack is determined, this can be used internally or externally, after which the method can end or return to the *obtain metric* step 40.

[0072] Looking now to Fig 4B, only new or modified steps, compared to Fig 4A, will be described.

[0073] In an optional *signal attack* step 44, the radio network node 1, the radio network node 1 signals an alert indicating that the DoS attack is in progress.

[0074] This signalling can occur locally within the radio network node 1. In this case, the radio network node 1 can act as the PEP (policy enforcement point), e.g. by denying (or restricting) radio resources for the DoS UE. Hence, the DoS UE has no radio access, which prevents the DoS UE from sending any (or excessive amount of) traffic. This provides a quick response to a detected attack. Since the embodiments presented herein are implemented in the radio network node 1, this node has power over scheduling and

enables response and mitigation of the attack to occur quickly and with substantial effect.

[0075] Alternatively or additionally, the signalling of the DoS Attack occurs from the radio network node 1 to the core network 3. In this case, the radio network node 1 acts as a policy decision point (PDP) while a network node within the core network acts as the PEP. For instance, the access and mobility management function (AMF) of the core network can act as the PEP. In this way, the AMF can use alerts, attack information, DoS UE information, that is provided from the radio network node 1, to act on it and respond to the DoS UE, by for example de-registering or quarantining the DoS UE from the network.

[0076] The metrics can be based on control plane traffic, i.e. not RAN user plane traffic, even if the control plane traffic often support user plane traffic. The control plane traffic can e.g. occur over the Uu interface provided for a UE by the radio network node 1. Embodiments presented herein do not rely on inspection of the content of the packets.

[0077] The results of a simulation to illustrate how DoS can be detected will now be described. The simulated DoS is a UDP flood attack, but the same principles are applicable for TCP SYN floods or other volumetric DoS attacks. In the simulation, the UE is a Raspberry Pi, acting as a DoS UE in the form of a IoT controller that normally communicates with robotic arms.

[0078] The UE has specific traffic pattern for benign traffic. This benign traffic has the following characteristics:

- TCP protocol traffic sending packets to the robotic arms.
- 160-320 bytes packets are sent every 10ms.
- A few packets of size 1514 bytes are sent every 200-500ms.

[0079] Additionally, the UE is simulated, in a mixed traffic scenario, to send UDP flood attacks, in certain periods of time. Hence, malicious traffic is mixed with the benign traffic over time. The simulation was configured to run for 30 seconds, where the

attack period is run for 10 seconds in the middle of the 30 seconds, targeting a /24 subnet. The results are compared to running only benign traffic.

[0080] The benign traffic in the mixed traffic scenario is of the same type as the benign traffic described above. The malicious traffic targeted a /24 subnet, where there were several targets responding on the service of interest. The UDP payload was set to a size of 512 bytes.

[0081] The number SRs drops significantly (about 62 per cent) during the attack period. Additionally, the number PRBs increase significantly during the attack period to support the increased UL traffic which requires increased user plane traffic, and thus a greater number of PRBs per unit of time.

[0082] Embodiments presented herein do not examine or analyse any IP packets that are being carried in the radio protocols. Instead, metrics derived from the RAN control plane are examined and analysed. This may allow for DoS attack detection even when IP packets are hidden or obscured, such as through encryption, from the radio network node 1.

[0083] Since the DoS attack is detected by the radio network node 1 that is topologically close to the compromised UE, the DoS attack can be detected faster and addressed better. Moreover, the radio network node 1 can exploit metrics, such as SR volume, BSRs and PRB usage, that are not available in a pure IP context.

[0084] Detection by the radio network node 1 also enables the radio network node 1 to apply a local response and mitigation actions. For instance, the radio network node 1 can deny radio resources for DoS UEs, which reduces effects on the RAN by a DoS UE, in addition to mitigating the attack on the upstream target device. Moreover, also telecommunication infrastructure can be protected, e.g. by reducing or eliminating DoS traffic that might otherwise consume bandwidth the backhaul network to the core network. Also, embodiments presented herein resolve scalability issues in the network, whereby the need for additional DoS detection solutions is reduced.

[0085] Fig 5 is a schematic diagram illustrating components of the radio network node 1 of Fig 1. A processor 60 is provided using any combination of one or more of a suitable central processing unit (CPU), graphics processing unit (GPU), multiprocessor,

neural processing unit (NPU), microcontroller, digital signal processor (DSP), etc., capable of executing software instructions 67 stored in a memory 64, which can thus be a computer program product. The processor 60 could alternatively be implemented using an application specific integrated circuit (ASIC), field programmable gate array (FPGA), etc. The processor 60 can be configured to execute the method described with reference to Figs 4A and 4B above.

[0086] The memory 64 can be any combination of random-access memory (RAM) and/or read-only memory (ROM). The memory 64 also comprises non-transitory persistent storage, which, for example, can be any single one or combination of magnetic memory, optical memory, solid-state memory or even remotely mounted memory.

[0087] A data memory 66 is also provided for reading and/or storing data during execution of software instructions in the processor 60. The data memory 66 can be any combination of RAM and/or ROM.

[0088] The radio network node 1 further comprises an I/O interface 62 for communicating with external and/or internal entities. Optionally, the I/O interface 62 also includes a user interface.

[0089] A transceiver 61 comprises suitable analogue and digital components to allow signal transmission and signal reception with UEs using one or more antennas 63.

[0090] Other components of the radio network node 1 are omitted in order not to obscure the concepts presented herein.

[0091] Fig 6 is a schematic diagram showing functional modules of the radio network node 1 of Fig 1 according to one embodiment. The modules are implemented using software instructions such as a computer program executing in the radio network node 1. Alternatively or additionally, the modules are implemented using hardware, such as any one or more of an ASIC (Application Specific Integrated Circuit), an FPGA (Field Programmable Gate Array), or discrete logical circuits. The modules correspond to the steps in the methods illustrated in Figs 4A and 4B.

[0092] A metric obtainer 70 corresponds to step 40. A DoS attack determiner 72 corresponds to step 42. An attack signaller 74 corresponds to step 44.

[0093] Fig 7 shows one example of a computer program product 90 comprising computer readable means. On this computer readable means, a computer program 91 can be stored in a non-transitory memory. The computer program can cause a processor to execute a method according to embodiments described herein. In this example, the computer program product is in the form of a removable solid-state memory, e.g. a Universal Serial Bus (USB) drive. As explained above, the computer program product could also be embodied in a memory of a device, such as the computer program product 64 of Fig 5. While the computer program 91 is here schematically shown as a section of the removable solid-state memory, the computer program can be stored in any way which is suitable for the computer program product, such as another type of removable solid-state memory, or an optical disc, such as a CD (compact disc), a DVD (digital versatile disc) or a Blu-Ray disc.

[0094] The aspects of the present disclosure have mainly been described above with reference to a few embodiments. However, as is readily appreciated by a person skilled in the art, other embodiments than the ones disclosed above are equally possible within the scope of the invention, as defined by the appended patent claims. Thus, while various aspects and embodiments have been disclosed herein, other aspects and embodiments will be apparent to those skilled in the art. The various aspects and embodiments disclosed herein are for purposes of illustration and are not intended to be limiting, with the true scope and spirit being indicated by the following claims.

CLAIMS

1. A method for detecting a denial-of-service, DoS, attack, on an upstream device, the method being performed in a radio network node (1), the method comprising:
 - obtaining (40) a metric based on radio access network, RAN, signalling for communication between a user equipment (2), UE, and the radio network node (1); and
 - determining (42) that a DoS attack is in progress on the upstream device (1) based on the metric, wherein the upstream device is provided upstream from the radio network node (1).
2. The method according to claim 1, wherein the metric is based on a volume of scheduling requests transmitted from the UE.
3. The method according to claim 2, wherein the determining (42) that a DoS attack is in progress comprises determining that the volume of scheduling requests is less than a threshold volume of scheduling requests.
4. The method according to any one of the preceding claims, wherein the metric is based on buffer status reports, BSRs, from the UE.
5. The method according to claim 4, wherein the determining (42) that a DoS attack is in progress comprises determining that a statistic of frequency of BSRs indicate a frequency that is greater than a threshold frequency.
6. The method according to claim 4 or 5, wherein the determining (42) that a DoS attack is in progress comprises determining that the BSRs indicate a high buffer level over time.
7. The method according to any one of the preceding claims, wherein the metric is based on a volume of used physical resource blocks, PRBs.
8. The method according to claim 7, wherein the determining (42) that a DoS attack is in progress comprises determining that the volume of PRBs is greater than a threshold volume of PRBs.
9. The method according to any one of the preceding claims, further comprising:
 - signalling (44) an alert indicating that the DoS attack is in progress.
10. The method according to any one of the preceding claims, wherein the determining (42) that a DoS attack is in progress is configured to detect a flood of user datagram protocol, UDP, packets.

11. The method according to any one of the preceding claims, wherein the determining (42) that a DoS attack is in progress is configured to detect a flood of transport control protocol, TCP, synchronise, SYN, messages.
12. The method according to any one of the preceding claims, wherein the DoS attack involves a user plane attack.
13. A radio network node (1) for detecting a denial-of-service, DoS, attack on an upstream device (3, 5), the radio network node (1) comprising:
 - a processor (60); and
 - a memory (64) storing instructions (67) that, when executed by the processor, cause the radio network node (1) to:
 - obtain a metric based on radio access network, RAN, signalling for communication between a user equipment (2), UE, and the radio network node (1); and
 - determine that a DoS attack is in progress on the upstream device (1) based on the metric, wherein the upstream device is provided upstream from the radio network node (1).
14. The method according to claim 13, wherein the metric is based on a volume of scheduling requests transmitted from the UE.
15. The radio network node (1) according to claim 14, wherein the instructions to determine that a DoS attack is in progress comprise instructions (67) that, when executed by the processor, cause the radio network node (1) to determining that the volume of scheduling requests is less than a threshold volume of scheduling requests.
16. The radio network node (1) according to any one of claims 13 to 15, wherein the metric is based on buffer status reports, BSRs, from the UE.
17. The radio network node (1) according to claim 16, wherein the instructions to determine that a DoS attack is in progress comprise instructions (67) that, when executed by the processor, cause the radio network node (1) to determine that a statistic of frequency of BSRs indicate a frequency that is greater than a threshold frequency.
18. The radio network node (1) according to claim 16 or 17, wherein the instructions to determine that a DoS attack is in progress comprise instructions (67) that, when executed by the processor, cause the radio network node (1) to determine that the BSRs indicate a high buffer level over time.

19. The radio network node (1) according to any one of claims 13 to 18, wherein the metric is based on a volume of used physical resource blocks, PRBs.
20. The radio network node (1) according to claim 19, wherein the instructions to determine that a DoS attack is in progress comprise instructions (67) that, when executed by the processor, cause the radio network node (1) to determine that the volume of PRBs is greater than a threshold volume of PRBs.
21. The radio network node (1) according to any one of claims 13 to 20, further comprising instructions (67) that, when executed by the processor, cause the radio network node (1) to signal an alert indicating that the DoS attack is in progress.
22. The radio network node (1) according to any one of claims 13 to 21, wherein the instructions to determine that a DoS attack is in progress comprise instructions (67) that, when executed by the processor, cause the radio network node (1) to detect a flood of user datagram protocol, UDP, packets.
23. The radio network node (1) according to any one of claims 13 to 22, wherein the instructions to determine that a DoS attack is in progress comprise instructions (67) that, when executed by the processor, cause the radio network node (1) to detect a flood of transport control protocol, TCP, synchronise, SYN, messages.
24. The radio network node (1) according to any one of claims 13 to 23, wherein the DoS attack involves a user plane attack.
25. A computer program (67, 91) for detecting a denial-of-service, DoS, attack on an upstream device (3, 5), the computer program comprising computer program code which, when executed on a radio network node (1) causes the radio network node (1) to:
 - obtain a metric based on radio access network, RAN, signalling for communication between a user equipment (2), UE, and the radio network node (1); and
 - determine that a DoS attack is in progress on the upstream device (1) based on the metric, wherein the upstream device is provided upstream from the radio network node (1).
26. A computer program product (64, 90) comprising a computer program according to claim 25 and a computer readable means comprising non-transitory memory in which the computer program is stored.

1/2

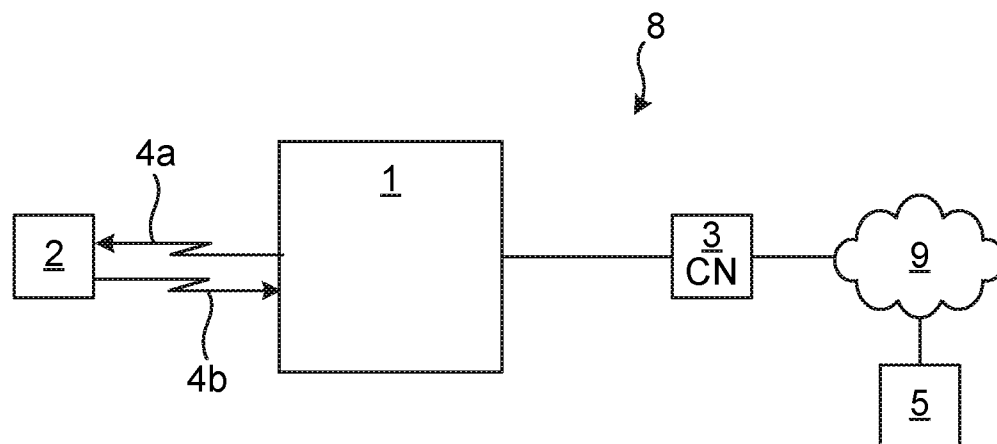


Fig. 1

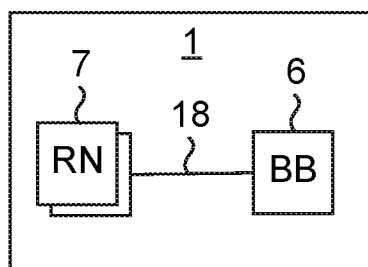


Fig. 2

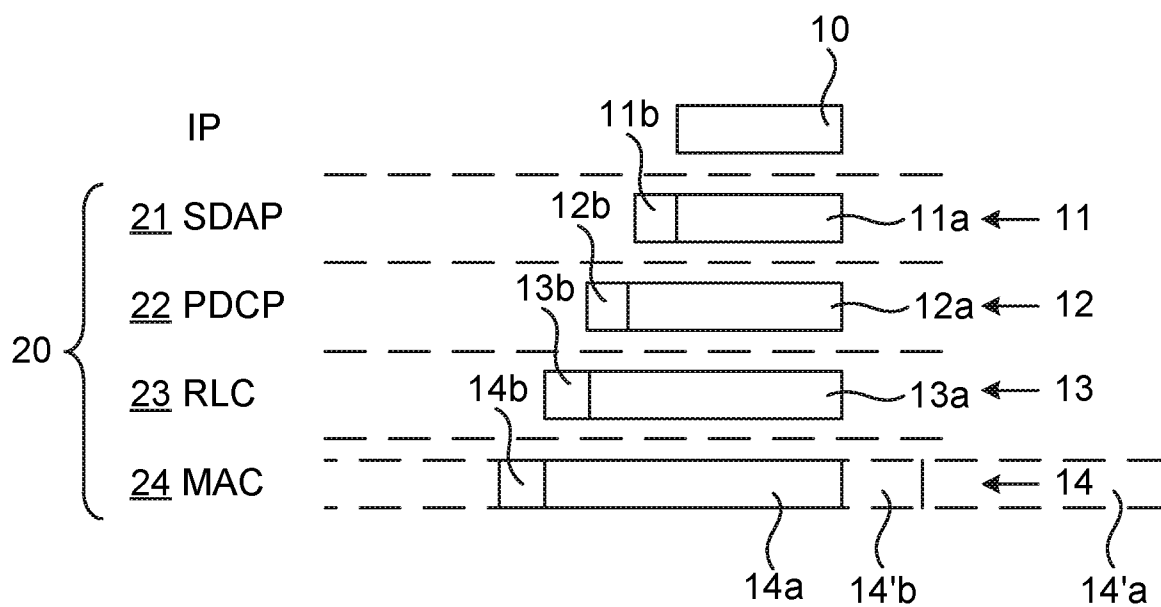


Fig. 3

2/2

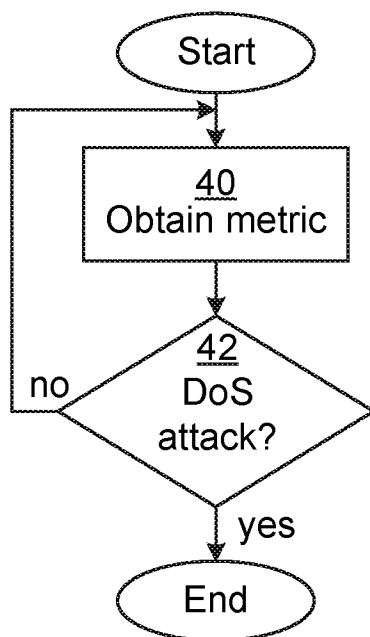


Fig. 4A

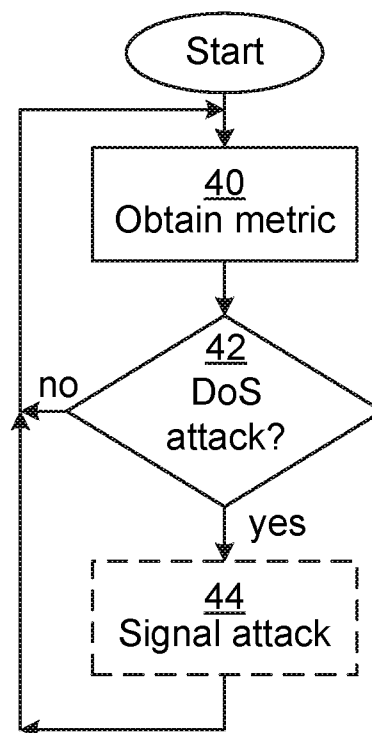


Fig. 4B

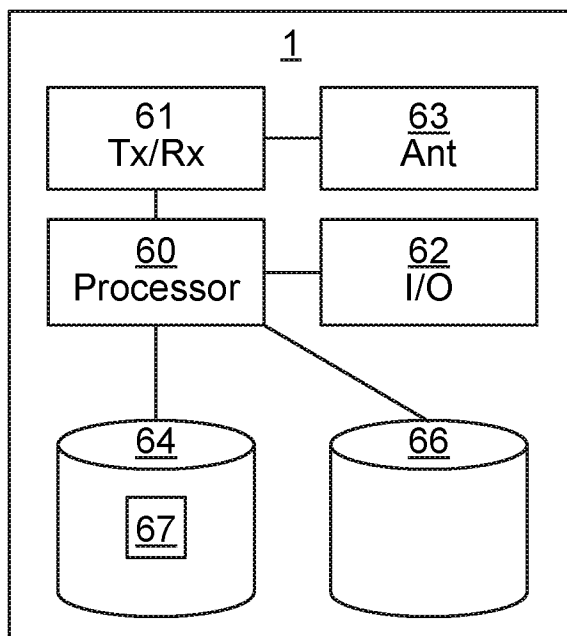


Fig. 5

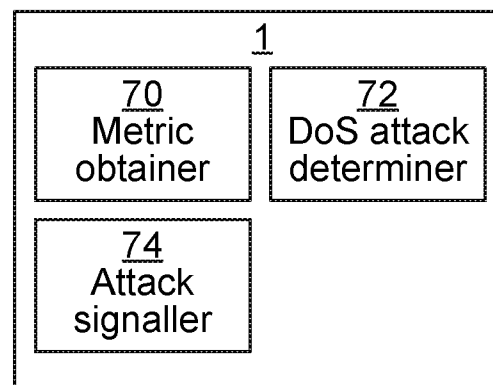


Fig. 6

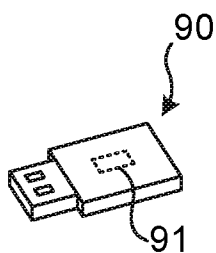


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2023/050073

A. CLASSIFICATION OF SUBJECT MATTER IPC: see extra sheet According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC: H04L, H04W		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched SE, DK, FI, NO classes as above		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2022218521 A1 (ERICSSON TELEFON AB L M), 20 October 2022 (2022-10-20); abstract; page 6, line 9 - page 7, line 6; page 8, line 16 - page 8, line 26; page 10, line 34 - page 10, line 36; page 11, line 1 - page 11, line 24; claims 1,9,10 --	1-26
A	US 9119075 B2 (KUSUMOTO YUICHI), 25 August 2015 (2015-08-25); abstract --	1-26
A	EP 3110103 A1 (VERISIGN INC), 28 December 2016 (2016-12-28); abstract -- -----	1-26
☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "D" document cited by the applicant in the international application "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family	
Date of the actual completion of the international search 21-08-2023	Date of mailing of the international search report 22-08-2023	
Name and mailing address of the ISA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Authorized officer Ralf Boström Telephone No. + 46 8 782 28 00	

Continuation of: second sheet

International Patent Classification (IPC)

H04W 12/12 (2021.01)

H04L 9/00 (2022.01)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/SE2023/050073

WO	2022218521 A1	20/10/2022	NONE		
US	9119075 B2	25/08/2015	BR	112013023339 A2	13/12/2016
			CN	103348719 B	07/12/2016
			EP	2688329 B1	01/05/2019
			JP	5668839 B2	12/02/2015
			JP	WO2012124207 A1	17/07/2014
			KR	20140003598 A	09/01/2014
			KR	101563413 B1	26/10/2015
			US	20130303120 A1	14/11/2013
			WO	2012124207 A1	20/09/2012
EP	3110103 A1	28/12/2016	US	20160381048 A1	29/12/2016
			US	9912678 B2	06/03/2018
			US	20180198808 A1	12/07/2018
			US	10193911 B2	29/01/2019