



(51) International Patent Classification:
H04W 12/122 (2021.01) H04L 9/40 (2022.01)

(21) International Application Number:
PCT/KR2022/002235

(22) International Filing Date:
15 February 2022 (15.02.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
202141006536 16 February 2021 (16.02.2021) IN
202141006536 24 January 2022 (24.01.2022) IN

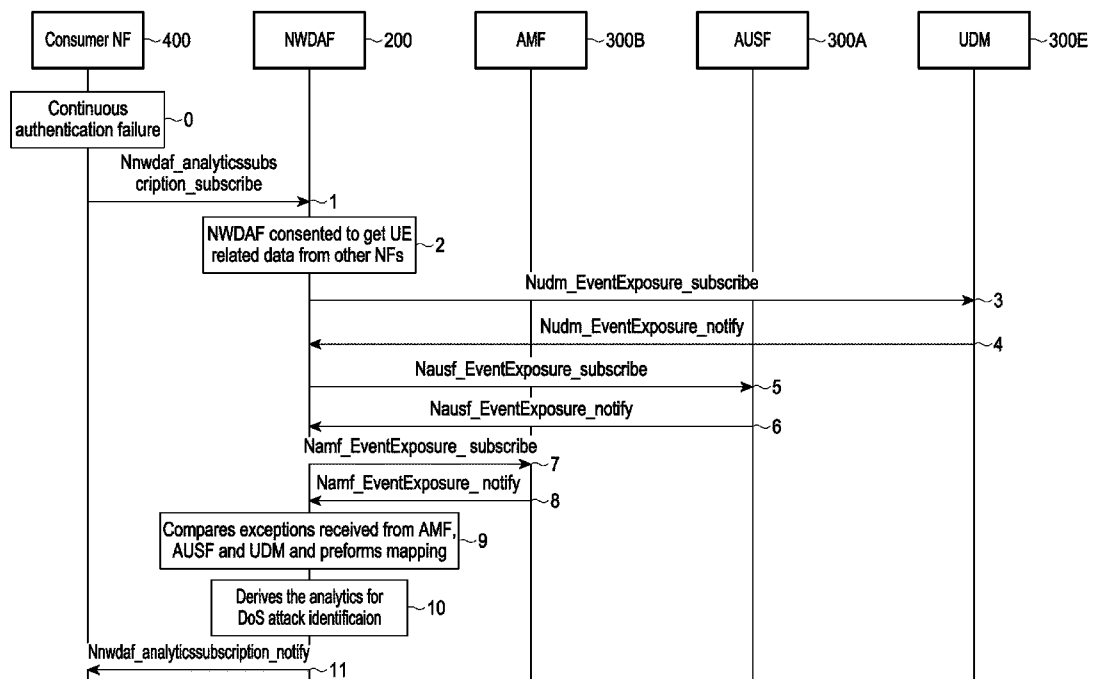
(71) Applicant: SAMSUNG ELECTRONICS CO., LTD.
[KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si,
Gyeonggi-do 16677 (KR).

(72) Inventors: SASI, Nivedya Parambath; #2870, Phoenix Building, Bagmane Constellation Business Park, Outer Ring Road, Doddanekundi Circle, Marathahalli Post, Bangalore 560037 (IN). RAJENDRAN, Rohini; #2870, Phoenix Building, Bagmane Constellation Business Park, Outer Ring Road, Doddanekundi Circle, Marathahalli Post, Bangalore 560037 (IN). RAJADURAI, Rajavelsamy; #2870, Phoenix Building, Bagmane Constellation Business Park, Outer Ring Road, Doddanekundi Circle, Marathahalli Post, Bangalore 560037 (IN).

(74) Agent: LEE, Keon-Joo et al.; Mihwa Bldg., 16 Daehak-ro 9-gil, Chongro-gu, Seoul 03079 (KR).

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JM, JO, JP, KE, KG, KH,

(54) Title: METHOD AND SYSTEM FOR DETECTING CYBER-ATTACKS USING NETWORK ANALYTICS



(57) Abstract: The disclosure relates to a 5G or 6G communication system for supporting a higher data transmission rate. A method of detecting cyber-attacks using network analytics in a UE is provided. The method includes receiving a request for sharing analytics information associated with UE from a consumer NF, requesting analytics information associated with UE and causing cyber-attack to at least one 5GC network entity, receiving analytics information associated with UE and causing the cyber-attack from at least one 5GC network entity, comparing an expected behavior of UE with an actual behavior based on analytics information provided by at least one 5GC network entity, deriving analytics associated with cyber-attack based on analytics information and comparison, and sending analytics associated with UE to consumer NF.



KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA,
MD, ME, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))*

Description

Title of Invention: METHOD AND SYSTEM FOR DETECTING CYBER-ATTACKS USING NETWORK ANALYTICS

Technical Field

- [1] The disclosure relates to wireless communication systems. More particularly, the disclosure relates to a method and a system for detecting cyber-attacks using network analytics.

Background Art

- [2] 5G mobile communication technologies define broad frequency bands such that high transmission rates and new services are possible, and can be implemented not only in "Sub 6GHz" bands such as 3.5GHz, but also in "Above 6GHz" bands referred to as mmWave including 28GHz and 39GHz. In addition, it has been considered to implement 6G mobile communication technologies (referred to as Beyond 5G systems) in terahertz bands (for example, 95GHz to 3THz bands) in order to accomplish transmission rates fifty times faster than 5G mobile communication technologies and ultra-low latencies one-tenth of 5G mobile communication technologies.
- [3] At the beginning of the development of 5G mobile communication technologies, in order to support services and to satisfy performance requirements in connection with enhanced Mobile BroadBand (eMBB), Ultra Reliable Low Latency Communications (URLLC), and massive Machine-Type Communications (mMTC), there has been ongoing standardization regarding beamforming and massive MIMO for mitigating radio-wave path loss and increasing radio-wave transmission distances in mmWave, supporting numerologies (for example, operating multiple subcarrier spacings) for efficiently utilizing mmWave resources and dynamic operation of slot formats, initial access technologies for supporting multi-beam transmission and broadbands, definition and operation of BWP (BandWidth Part), new channel coding methods such as a LDPC (Low Density Parity Check) code for large amount of data transmission and a polar code for highly reliable transmission of control information, L2 pre-processing, and network slicing for providing a dedicated network specialized to a specific service.
- [4] Currently, there are ongoing discussions regarding improvement and performance enhancement of initial 5G mobile communication technologies in view of services to be supported by 5G mobile communication technologies, and there has been physical layer standardization regarding technologies such as V2X (Vehicle-to-everything) for aiding driving determination by autonomous vehicles based on information regarding positions and states of vehicles transmitted by the vehicles and for enhancing user convenience, NR-U (New Radio Unlicensed) aimed at system operations conforming to

various regulation-related requirements in unlicensed bands, NR UE Power Saving, Non-Terrestrial Network (NTN) which is UE-satellite direct communication for providing coverage in an area in which communication with terrestrial networks is unavailable, and positioning.

- [5] Moreover, there has been ongoing standardization in air interface architecture/protocol regarding technologies such as Industrial Internet of Things (IIoT) for supporting new services through interworking and convergence with other industries, IAB (Integrated Access and Backhaul) for providing a node for network service area expansion by supporting a wireless backhaul link and an access link in an integrated manner, mobility enhancement including conditional handover and DAPS (Dual Active Protocol Stack) handover, and two-step random access for simplifying random access procedures (2-step RACH for NR). There also has been ongoing standardization in system architecture/service regarding a 5G baseline architecture (for example, service based architecture or service based interface) for combining Network Functions Virtualization (NFV) and Software-Defined Networking (SDN) technologies, and Mobile Edge Computing (MEC) for receiving services based on UE positions.
- [6] As 5G mobile communication systems are commercialized, connected devices that have been exponentially increasing will be connected to communication networks, and it is accordingly expected that enhanced functions and performances of 5G mobile communication systems and integrated operations of connected devices will be necessary. To this end, new research is scheduled in connection with eXtended Reality (XR) for efficiently supporting AR (Augmented Reality), VR (Virtual Reality), MR (Mixed Reality) and the like, 5G performance improvement and complexity reduction by utilizing Artificial Intelligence (AI) and Machine Learning (ML), AI service support, metaverse service support, and drone communication.
- [7] Furthermore, such development of 5G mobile communication systems will serve as a basis for developing not only new waveforms for providing coverage in terahertz bands of 6G mobile communication technologies, multi-antenna transmission technologies such as Full Dimensional MIMO (FD-MIMO), array antennas and large-scale antennas, metamaterial-based lenses and antennas for improving coverage of terahertz band signals, high-dimensional space multiplexing technology using OAM (Orbital Angular Momentum), and RIS (Reconfigurable Intelligent Surface), but also full-duplex technology for increasing frequency efficiency of 6G mobile communication technologies and improving system networks, AI-based communication technology for implementing system optimization by utilizing satellites and AI (Artificial Intelligence) from the design stage and internalizing end-to-end AI support functions, and next-generation distributed computing technology for implementing services at levels of complexity exceeding the limit of UE operation capability by utilizing ultra-

high-performance communication and computing resources.

- [8] In general, a network data analytics function (NWDAF) is part of architecture specified in TS 23.501 (FIG. 1A) and uses mechanisms and interfaces specified for a 5th generation core (5GC) network in TS 23.501 and operations, administration and maintenance (OAM) services.

Disclosure of Invention

Solution to Problem

- [9] FIG. 1A is an architecture for Nnwdaf_EventSubscription Service according to the related art.
- [10] Referring to FIG. 1A, the NWDAF interacts with different entities in the 5GC network for different purposes, such as data collection based on subscription to events provided by an authentication management function (AMF), a session management function (SMF), a policy control function (PCF), a unified data management (UDM), an application function (AF) and the OAM, retrieval of information from data repositories (e.g., user data repository (UDR) via the UDM for subscriber-related information), retrieval of information (e.g., from a network repository functions (NRFs) for network function (NF)-related information) and on demand provision of analytics to consumers.
- [11] FIG. 1B is an architecture for data collection from any 5th generation core network function (5GC NF) according to the related art. FIG. 1C is an architecture for network data analytics exposure according to the related art.
- [12] Referring to FIGS. 1B and 1C, a Nnf (A) interface is defined for NWDAFs to request subscription to data delivery for a particular context, to cancel subscription to data delivery and to request a specific report of data for a particular context with any NF.
- [13] A Nnwdaf interface is defined for 5GC NFs, to request subscription to network analytics delivery for a particular context, to cancel subscription to network analytics delivery and to request a specific report of network analytics for a particular context.
- [14] The NWDAF provides analytics information to the 5GC NFs, and the OAM as defined in clause 7 of TS 23.288. The analytics information are either statistical information of the past events, or predictive information. Different NWDAF instances may be present in the 5GC network, with possible specializations per type of analytics. The capabilities of a NWDAF instance are described in the NWDAF profile stored in the NRF.
- [15] According to use case 5 of TR 23.700-91, cyber-attacks can be efficiently detected by monitoring events and data packets in a user equipment (UE) and in the 5GC network with the support of the NWDAF and machine-learning algorithms. The UE and NWDAF collaborate with each other to detect the attacks that may occur in a UE,

a radio access network (RAN) or the 5GC network. Relevant parameters are to be collected from UEs for deriving the analytics in order to detect the cyber-attack. The cyber-attacks may be a denial of service (DoS) attack, a man in the middle (MitM) attack or an impersonation.

- [16] Based on the derived analytics using collected data from the UE, the NWDAF can provide the attack detection alerts to the OAM and the 5GC NFs that have subscribed to them so that they could take proper action.
- [17] There are two types DoS attacks as follows: DoS attack on the UE: which attempts to hinder the UE's access to the 5GC network, and DoS attack on the 5GC network, which attempts to hinder the 5GC networks ability to provide services to the subscribed UEs. The DoS can be mounted by a number of methods, including but are not limited to, manipulation of chosen fields in a master information blocks (MIB)/system information blocks (SIBs), an arbitrary bit flipping of signed MIB/SIBs, a replay of signed MIB/SIBs, a broadcast MIB/SIBs with invalid signatures, and a manipulation of a timing information in the UE or a gNodeB (gNBs). Since the MIB/SIBs are digitally signed, a DoS based on manipulation of chosen fields in MIB/SIBs (e.g., a barred cell) will be detected and prevented.
- [18] The MitM can be performed in various ways, such as, with a false base station acting as a relay node towards the legitimate gNB and a genuine UE connects with a fake gNB or in a different attack scenario where the UE can be malicious and the false base station is connected to a malicious UE either in the same or a different public land mobile network (PLMN).
- [19] FIG. 1D illustrates expected user equipment (UE) behavior parameters per exception identifier (ID) according to the related art.
- [20] Referring to FIG. 1D, according to table 6.7.5.1-1 of TS 23.288, a mapping between each exception ID and UE behavior parameters are as illustrated. When the NWDAF detects the UEs which deviate from the expected UE behavior, for example unexpected UE location, abnormal traffic pattern, wrong destination addresses or the like, the NWDAF notifies the result of the analytics to the consumer as specified in clause 6.7.5.3.
- [21] According to TS 23.502, when subscribing to event reporting, the NF consumer(s) provide: one or multiple event ID(s), event filter information, event reporting information. The event ID identifies a type of event being subscribed to (e.g., PDU session release, UE mobility out of an area of interest, or the like). The event filter information provides event parameter types and event parameter value(s) to be matched against, in order to meet the condition for notifying the subscribed event ID e.g., the event parameter type could be "Area of interest" and the event parameter value list could be a list of TAs. The Event Filter depends on the event ID. The event filter in-

formation is provided per event ID(s) being subscribed to: within a subscription different event ID(s) may be associated with different event filter information. The event reporting information described in the Table 4.15.1-1 below. Within a subscription all event ID(s) are associated with a unique event reporting information.

[22] A target of event reporting may indicate a specific UE or PDU session, a group of UE(s) or any UE (i.e., all UEs), within a subscription all event ID (s) are associated with the same target of event reporting (possibly corresponding to multiple UE or multiple PDU Sessions). A notification target address (+ Notification Correlation ID) allowing the event receiving NF to correlate notifications received from the event provider with this subscription. A subscription is associated with a unique notification target address (+ Notification Correlation ID). In the case where the NF consumer subscribes to the NF producer on behalf of other NF, the NF consumer includes the notification target address (+Notification Correlation ID) of other NF for the Event ID which is to be notified to other NF directly, and the notification target address (+Notification Correlation ID) of itself for the subscription change related event notification. Each notification target address (+ Notification Correlation ID) is associated with related (set of) Event ID(s).

[23] An expiry time represents the time up to which the subscription is desired to be kept as active. The NF service consumer may suggest an expiry time and provide to the NF service producer. Based on the operator's policy, the NF service producer decides whether the subscription can be expired. If the subscription can be expired, the NF service producer determines the expiry time and provide it in the response to the NF service consumer. If the event subscription is about to expire based on the received expiry time and the NF service consumer wants to keep receiving notifications, the NF service consumer update the subscription with the NF service producer in order to extend the expiry time. Once the expiry time associated with the subscription is reached, the subscription becomes invalid at the NF service producer. If the NF service consumer wants to keep receiving notifications, it creates a new subscription with the NF service producer.

[24] Thus, it is desired to address the above mentioned disadvantages or other shortcomings or at least provide a useful alternative.

[25] The above information is presented as background information only to assist with an understanding of the disclosure. No determination has been made, and no assertion is made, as to whether any of the above might be applicable as prior art with regard to the disclosure.

[26] Aspects of the disclosure are to address at least the above-mentioned problems and/or disadvantages and to provide at least the advantages described below. Accordingly, an aspect of the disclosure is to provide a method and a system for detecting cyber-attack

using network analytics.

[27] Another aspect of the disclosure is to provide methods to obtain user equipment (UE) related data (i.e., different parameters) for the deriving the network analytics for denial of service (DoS) attack and a man in the middle (MitM) attack.

[28] Another aspect of the disclosure is to provide the corresponding mitigation techniques based on the derived analytics provided by the network data analytics function (NWDAF).

[29] Additional aspects will be set forth in part in the description which follows and, in part, will be apparent from the description, or may be learned by practice of the presented embodiments.

[30] In accordance with an aspect of the disclosure, a method and system for detection of cyber-attacks (e.g., a DoS attack, a MitM attack, or the like) using network analytics is provided. The method includes different mechanisms to obtain UE related data (i.e., different parameters) for the analytics derivation by the NWDAF and the corresponding mitigation techniques based on the derived analytics.

[31] Other aspects, advantages, and salient features of the disclosure will become apparent to those skilled in the art from the following detailed description, which, taken in conjunction with the annexed drawings, discloses various embodiments of the disclosure.

Brief Description of Drawings

[32] The above and other aspects, features, and advantages of certain embodiments of the disclosure will be more apparent from the following description taken in conjunction with the accompanying drawings, in which:

[33] FIG. 1A is an architecture for Nnwdafe_EventSubscription Service according to the related art;

[34] FIG. 1B is an architecture for data collection from any 5th generation core network function (5GC NF) according to the related art;

[35] FIG. 1C is an architecture for network data analytics exposure according to the related art;

[36] FIG. 1D illustrates expected user equipment (UE) behavior parameters per exception identifier (ID) according to the related art;

[37] FIG. 2 is schematic diagram illustrating a UE communicating with a network data analytics function (NWDAF) through a plurality of network entities for detecting cyber-attacks using network analytics according to an embodiment of the disclosure;

[38] FIG. 3 is a signaling diagram illustrating NWDAF checks abnormality in authentication failure denial of service (DoS) attack (DoS attack) according to an embodiment of the disclosure;

[39] FIG. 4 is a signaling diagram illustrating NWDAF checking for abnormality in reg-

illustration failure a man in the middle (MitM) attack (MitM attack), according to an embodiment of the disclosure;

[40] FIG. 5 is a signaling diagram illustrating an authentication management function (AMF) and a session management function (SMF) providing inputs to NWDAF for deriving analytics for DoS detection according to an embodiment of the disclosure;

[41] FIG. 6 is a signaling diagram illustrating operations, administration, and maintenance (OAM) providing inputs to NWDAF for DoS identification according to an embodiment of the disclosure; and

[42] FIG. 7 is a signaling diagram illustrating OAM providing collected radio access network (RAN) inputs to NWDAF for MitM attack analytic derivation according to an embodiment of the disclosure.

[43] FIG. 8 is a view illustrating an internal structure of a network data analytics function (NWDAF) according to an embodiment of the disclosure.

[44] FIG. 9 is a view illustrating an internal structure of a consumer NF according to an embodiment of the disclosure.

[45] The same reference numerals are used to represent the same elements throughout the drawings.

Mode for the Invention

[46] The following description with reference to the accompanying drawings is provided to assist in a comprehensive understanding of various embodiments of the disclosure as defined by the claims and their equivalents. It includes various specific details to assist in that understanding but these are to be regarded as merely exemplary. Accordingly, those of ordinary skill in the art will recognize that various changes and modifications of the various embodiments described herein can be made without departing from the scope and spirit of the disclosure. In addition, descriptions of well-known functions and constructions may be omitted for clarity and conciseness.

[47] The terms and words used in the following description and claims are not limited to the bibliographical meanings, but, are merely used by the inventor to enable a clear and consistent understanding of the disclosure. Accordingly, it should be apparent to those skilled in the art that the following description of various embodiments of the disclosure is provided for illustration purpose only and not for the purpose of limiting the disclosure as defined by the appended claims and their equivalents.

[48] It is to be understood that the singular forms "a," "an," and "the" include plural referents unless the context clearly dictates otherwise. Thus, for example, reference to "a component surface" includes reference to one or more of such surfaces.

[49] The various embodiments of the disclosure described herein are not necessarily mutually exclusive, as some embodiments may be combined with one or more other

embodiments to form new embodiments. The term "or" as used herein, refers to a non-exclusive or, unless otherwise indicated. The examples used herein are intended merely to facilitate an understanding of ways in which the embodiments herein may be practiced and to further enable those skilled in the art to practice the embodiments herein. Accordingly, the examples should not be construed as limiting the scope of the embodiments herein.

[50] As is traditional in the field, embodiments may be described and illustrated in terms of blocks which carry out a described function or functions. These blocks, which may be referred to herein as managers, units, modules, hardware components or the like, are physically implemented by analog and/or digital circuits, such as logic gates, integrated circuits, microprocessors, microcontrollers, memory circuits, passive electronic components, active electronic components, optical components, hardwired circuits and the like, and may optionally be driven by firmware. The circuits may, for example, be embodied in one or more semiconductor chips, or on substrate supports, such as printed circuit boards, and the like. The circuits constituting a block may be implemented by dedicated hardware, or by a processor (e.g., one or more programmed microprocessors and associated circuitry), or by a combination of dedicated hardware to perform some functions of the block and a processor to perform other functions of the block. Each block of the embodiments may be physically separated into two or more interacting and discrete blocks without departing from the scope of the disclosure. Likewise, the blocks of the embodiments may be physically combined into more complex blocks without departing from the scope of the disclosure.

[51] Accordingly, the embodiments of the disclosure herein provide a method and a system for detection of cyber-attacks (e.g., a DoS attack, a MitM attack, or the like) using network analytics. The proposed method includes different mechanisms to obtain UE related data (i.e., different parameters) for the analytics derivation by the NWDAF and the corresponding mitigation techniques based on the derived analytics.

[52] Referring now to the drawings and more particularly to FIGS. 2 through 7, where similar reference characters denote corresponding features consistently throughout the figures, there are shown preferred embodiments of the disclosure.

[53] FIG. 2 is schematic diagram illustrating a wireless network system comprising a UE communicating with a NWDAF through a plurality of network entities and a consumer NF for detecting cyber-attacks using network analytics according to an embodiment of the disclosure.

[54] Referring to FIG. 2, a UE (100) is in a 5GC network (wireless network) (1000) and detects the cyber-attack using a NWDAF (200) and a plurality of network entities (300). In an embodiment of the disclosure, the UE (100) interacts with a consumer NF (400), wherein the consumer NF (400) is an entity from the plurality of network

entities (300).

- [55] The plurality of network entities are, for example, but not limited to an AUSF (300A), an AMF (300B), a SMF (300C), a PCF (300D), a UDM (300E), an AF (300F), and an OAM (300G).
- [56] Examples of the UE (100) include, but are not limited to a smartphone, a tablet computer, a personal digital assistance (PDA), an Internet of things (IoT) device, a wearable device, or the like.
- [57] In an embodiment of the disclosure, the UE (100) includes a memory (110), a processor (120), and a communicator (130).
- [58] In an embodiment of the disclosure, the memory (110) is configured to store information associated with the cyber-attack. The memory (110) stores instructions to be executed by the processor (120). The memory (110) may include non-volatile storage elements. Examples of such non-volatile storage elements may include magnetic hard disks, optical discs, floppy disks, flash memories, or forms of electrically programmable memories (EPROM) or electrically erasable and programmable (EEPROM) memories. In addition, the memory (110) may, in some examples, be considered a non-transitory storage medium. The term "non-transitory" may indicate that the storage medium is not embodied in a carrier wave or a propagated signal. However, the term "non-transitory" should not be interpreted that the memory (110) is non-movable. In some examples, the memory (110) may be configured to store larger amounts of information than the memory. In certain examples, a non-transitory storage medium may store data that can, over time, change (e.g., in a random access memory (RAM) or cache). The memory (110) maybe an internal storage unit or it may be an external storage unit of the UE (100), a cloud storage, or any other type of external storage.
- [59] The processor (120) communicates with the memory (110), and the communicator (130). The processor (120) is configured to execute instructions stored in the memory (110) and to perform various processes. The processor (120) may include one or a plurality of processors, maybe a general-purpose processor, such as a central processing unit (CPU), an application processor (AP), or the like, a graphics-only processing unit, such as a graphics processing unit (GPU), a visual processing unit (VPU), and/or an artificial intelligence (AI) dedicated processor, such as a neural processing unit (NPU).
- [60] The communicator (130) is configured for communicating internally between internal hardware components and with external devices (e.g., an AAnF server, UDM, a server, or the like) via one or more networks (e.g., radio technology). The communicator (130) includes an electronic circuit specific to a standard that enables wired or wireless communication.

- [61] In an embodiment of the disclosure, each of the NWDAF (200), the consumer NF (400), and the plurality of network entities may include a memory, a processor, and a communicator, respectively.
- [62] In an embodiment of the disclosure, the consumer NF (400) detects a continuous failure of a non-access-stratum (NAS) procedure of the UE (100) with the wireless 5GC network. Further, the consumer NF (400) determines a possibility of the cyber-attack on the UE (100) based on the detected continuous failure of the NAS procedure.
- [63] In an embodiment of the disclosure, the NAS procedure is one of an authentication procedure of the UE (100), a registration procedure of the UE (100), a service request procedure, a packet data unit (PDU) session establishment procedure for the UE (100), and a UE configuration update procedure.
- [64] Further, based on the possibility, the consumer NF (400) sends a request to the NWDAF (200) for sharing analytics information associated with the UE (100). Further, the NWDAF (200) request the analytics information associated with the UE (100) to a network entity from the plurality of network entities (300).
- [65] After receiving the request, the network entity from the plurality of network entities (300) sends an event report to the NWDAF (200) as the analytics information of the UE (100).
- [66] The NWDAF (200) then compares an expected behavior of the UE (100) with an actual behavior based on the analytics information provided by the network entity from the plurality of network entities (300). Based on the comparison, the NWDAF (200) derives analytic information about the cyber-attack on the UE (100) and sends to the consumer NF (400).
- [67] Thus, the cyber-attack on the UE (100) is detected using the above explained procedure.
- [68] FIG. 3 is a signaling diagram illustrating checking an abnormality in an authentication failure (DoS attack) of a UE by a NWDAF according to an embodiment of the disclosure.
- [69] Referring to FIG. 3, in an embodiment of the disclosure, upon request of the consumer NF (400), the NWDAF (200) collects and analyzes a behavioral information of the UE (100) and/or expected behavioral parameters of the UE (100) from the plurality of network entities (300) depending on an exception IDs.
- [70] 3GPP TR 23.700-91 has identified the use case of the NWDAF (200) detecting cyber-attacks by monitoring events and data packets in the UE (100) and the 5GC network. To achieve cyber-attacks detection, the NWDAF (200) collaborates with the UE (100) and any other NFs to collect related data as inputs, afterwards providing alerts of anomaly events as outputs to OAM and other NFs which have subscribed to them so that they could take proper actions.

- [71] Suspicion of DoS attack: 5G communication has high performance requirements for system capacity and data rate, improved capacity and higher data rate may lead to much higher processing capability cost for network entities, which may make some network entities (e.g., RAN, core network entities) to suffer from DoS attack. The NWDAF (200) may also enable the detection of DoS attacks. The DoS attacks are possible on radio access network (RAN) nodes, AF and the network entities like AMF, SMF, UDM, or the like.
- [72] Suspicion of MitM attack: MitM attacks or fraudulent relay nodes may modify or change the messages between the UE (100) and the RAN, resulting in failures of higher layer protocols, such as NAS or the primary authentication. The NWDAF (200) may detect the MitM attacks.
- [73] The UE (100) and the NWDAF (200) collaborate with each other to detect the cyber-attacks that may occur in the UE (100), the RAN or the 5GC network. The relevant parameters to be collected from the UE (100) are to be provided. Therefore, it needs to be clear that what all parameters helps in performing cyber-attack detection which are collected from the UE (100) and/or from the 5GC network and / or from the OAM. Attack detection alerts could be provided to OAM and the NFs that have subscribed to them so that they could take proper action.
- [74] The proposed solution discloses that the NWDAF (200) can collect information from different NFs in order to provide the relevant information to the requesting or subscribed consumer NF (400) for the network analytics.
- [75] Since the DoS attack or the MitM attack may also lead to dropped or changed packets between the UE (100) and a legitimate gNB, the abnormal and/or illegal failure indication, various categories of failure cause and timeouts with respect to the NAS messages are relevant for the analytics. Further information from the UDM and AUSF about the authentication status and the registration status in the network and the performance management from OAM can give additional information as explained below.
- [76] An authentication failure: the NWDAF (200) checks the reason for continuous authentication failure (DoS attack): in an embodiment of the disclosure, the NWDAF (200) checks for the continuous authentication failure, by comparing the exception parameters received from UDM, AUSF and the AMF.
- [77] Failure Scenarios during:
- [78] Case 1: Initial registration: during failure case (initial registration), the AMF is not aware of the failed SUPI. Only the SUCI information is available to AMF i.e., AMF performs the identity requests and obtains the SUCI.
- [79] Case 2: the UE is in connected mode and Authentication failure occurs. If a UE is in connected mode and authentication failure occurs, then re-authentication procedure can be initiated from the UE side. In such cases, AMF can map on which N1 interface the

authentication has failed for that particular UE and AMF checks on the SUPI corresponding to the SUCI. AMF can report the failed SUPI information to the NWDAF in order to perform the analytics for DoS attack.

[80] The subscription identifier de-concealing function (SIDF) service offered by the UDM in the home network of the subscriber responsible for de-concealing the SUPI from the SUCI. If the SUCI is concealed to a valid ID in the network, the UDM can provide the details of the failed SUPI, if there is an authentication failure.

[81] In an embodiment of the disclosure, in addition to MitM and DoS attack, the NWDAF should categorize the genuine authentication failure and send error cause. i.e., "error" due to radio conditions (e.g., a radio link failure-DRNS internal failure, congestion, lost radio interface synchronization due to bas radio condition, loss of UL synchronization.

[82] Inputs from UDM, AUSF and AMF to NWDAF is provided in Table 1.

[83] [Table 1]

Information	Description
UE ID	SUPI (UE ID in which the exception occurred)
> DNN	DNN for the PDU Session that SMF collects Data
> S-NSSAI	S-NSSAI for the PDU Session that SMF collects Data
> Start time of data collection	Start time of data collection
> End time of data collection	End time of data collection
>> Timestamp	A time stamp when AMF receives NAS message from UE
>> Timestamp	A time stamp when AMF sends NAS message to UE
>>> Provided backoff timer	A value of backoff timer provided to UE
>>>AUSF ID	AUSF which involved in authentication procedure
>>>AMF ID	AMF in which mobility and tracking information that NWDAF collects data
>>> TAI	Tracking Area selected by the UE
>>>CAG ID	(Optional) UE selected CAG Cell
>>>PCI	PCI in which the exception occurred
>>>Downlink Frequency	Frequency range at which the exception occurred
>>> Exception ID	Suspicion of Dos Attack
>>>Exception Category	Authentication failure
> SM NAS request from UE (1max) (if applicable)	Information on SM NAS messages that SMF receives from UE for PDU Session
>>> Type of SM NAS request (if applicable)	A type of SM NAS message transmitted by UE (e.g., PDU session establishment request, PDU session modification request, or the like)
>>>RAN UE ID	Uniquely identify the UE over NG interface
>>>VPLMN ID	UE selected serving network ID

[84] In an embodiment of the disclosure, the UDM, AUSF and AMF includes at least one of the parameters (in the table) as the input for analytics derivation.

[85] Output from NWDAF to Consumer NF is provided in Table 2.

[86] [Table 2]

Information	Description
> DNN (NOTE)	DNN that DoS is applied
> S-NSSAI (NOTE)	S-NSSAI that DoS is applied
> List of UEs classified based on experience level of DoS	One or more than one of the following lists (SUPI is used to identify UE)
>> Exception ID	Suspicion of Dos Attack
>>Exception category	Indication for Authentication failure
>> Analytics ID	To indicate when the analytics are derived and based on what event ID

[87] Services provided by NWDAF:

[88] Service operation name: Nudm_EventExposure_Subscribe.

[89] Description: The NWDAF requests the UDM to provide the inputs for analytics derivation. Input, Required: Event ID, Event filter, Any UE or SUPI, internal group identifier.

[90] Input, Optional: None. Output, Required: Event report (AUSF ID, AMF ID, SUPI), Exception category.

[91] Output, Optional: None.

[92] Service operation name: Nausf_EventExposure_Subscribe.

[93] Description: The NWDAF requests the AUSF to provide the inputs for analytics derivation. Input, Required: Event ID, Event filter, Any UE or SUPI, internal group identifier.

[94] Input, Optional: None. Output, Required: Event report (AUSF ID, AMF ID, SUPI), Exception category.

[95] Output, Optional: None.

[96] Service operation name: Namf_EventExposure_Subscribe.

[97] Description: The NWDAF requests the AMF to provide the inputs for analytics derivation. Input, Required: Event ID, Event filter, Any UE or SUPI, internal group identifier.

[98] Input, Optional: None.

[99] Output, Required: Event report (AMF ID, AUSF ID, RI, SUCI, TAI, CAG (closed access group cells) ID), Exception category. Output, Optional: CAG ID.

[100] The operations of the sequence diagram in FIG. 3 is as explained below.

[101] Operation 0: At operation 0, continuous authentication failure of the UE (100) is

detected.

- [102] Operation 1: The consumer NF (400) (e.g., SMF, PCF, AMF, or the like) requests to/ subscribes to the NWDAF (200) using *Nnwdaf_AnalyticsSubscription_Subscribe/nwdaf_AnalyticsInfo_Request (Analytics ID set to "DoS attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information)*, for obtaining analytics information on "DoS attack Identification".
- [103] In an embodiment of the disclosure, the derived Analytics are provided by NWDAF (200) if the consumer NF (400) wants to take the analytics information into account when applying the DoS detection and /or DoS mitigation.
- [104] In another embodiment of the disclosure, the consumer NF (400) may subscribe to/ request signaling failure notification/response from the NWDAF (200) for a group of UEs, any UE or a specific UE. The Analytics ID indicates the NWDAF (200) to identify misused or hijacked UEs through signaling failure analytic.
- [105] Operation 2: The NWDAF (200) is consented to get the UE (100) related data from the other network functions.
- [106] Operation 3: The NWDAF (200) sends a subscription request to the UDM (300E) using *Nudm_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI)* asking the analytics information.
- [107] Operation 4: The UDM (300E) sends the event reports to the NWDAF (200) over *Nudm_EventExposure_Notify* based on requirements contained in the subscription request received from the NWDAF (200). The event report shared by the UDM (300E) includes at least one of the following parameters, a UE characteristics (e.g., a UE ID, an internal group Identifier, a list of authorized UEs under TA requested, or the like) and all other parameters defined in TS 23.502 clause 4.15.1. The event reports additionally include the AUSF ID and SUPI, in which the continuous authentication failure occurs. Along with the event report, the UDM (300E) provides the exception category = "Authentication failure" to the NWDAF (200) based on the analysis.
- [108] Operation 5: NWDAF (200) to AUSF 300A: *Nausf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI)*. The NWDAF (200) sends a subscription requests to the related AUSF (s) if it has not subscribed to such data.
- [109] Operation 6: The AUSF (300A) sends event reports to the NWDAF (200) over *Nausf_EventExposure_Notify* based on the report requirements contained in the subscription request received from the NWDAF (200).
- [110] If requested by the NWDAF (200) via Event Filter(s), the AMF (300B) checks whether the UE's (100) behavior matches an expected UE behavioral information. In an embodiment of the disclosure, the AUSF (300A) sends the event reports to the NWDAF (200) only when it detects that the UE's (100) behavior is deviated from the

expected UE behavior.

- [111] In an embodiment of the disclosure, the expected UE behavior is offered to the AUSF (300A) as a part of the authentication procedure. The event report includes at least one of the following parameters. The UE characteristics (e.g., a UE ID, an internal group Identifier, a list of authorized UEs under TA requested, or the like) and all other parameters defined in TS 23.502 clause 4.15.1. Along with the event report AUSF provides the exception category = "*Authentication failure*" to the NWDAF (200) based on the analysis.
- [112] In an embodiment of the disclosure, the AUSF (300A) provides the AMF ID with a trust to the NWDAF (200).
- [113] In another embodiment of the disclosure, the UDM (300E) provides the trusted AMF ID to the NWDAF (200).
- [114] Operation 7: NWDAF (200) to AMF (300B): *Namf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI)*.
- [115] The NWDAF (200) sends a subscription requests to the related AMF (300B) (s) if it has not subscribed to such data.
- [116] Operation 8: The AMF (300B) sends he event reports to the NWDAF (200) over *Nausf_EventExposure_Notify* based on a report requirements contained in the subscription request received from the NWDAF (200).
- [117] In an embodiment of the disclosure, if the NWDAF (200) request the event report via event Filter(s), then the AMF (300B) checks whether the UE's (100) behavior matches its expected UE behavioral information. In this case, the AMF (300B) sends the event reports to the NWDAF (200) only when it detects that the UE's (100) behavior deviated from its expected UE behavior.
- [118] In an embodiment of the disclosure, the expected UE behavior is offered to the AMF (300B) as a part of access and mobility data subscription.
- [119] The event report includes at least one of the following parameters: UE characteristics (e.g., a UE ID, an internal group Identifier, a list of authorized UEs under TA requested, or the like) and all other parameters defined in TS 23.502 clause 4.15.1.
- [120] In another embodiment of the disclosure, the AMF (300B) further provides the parameters, such as SUCI, a tracking area identity (TAI), a CAG ID (if applicable), a physical cell Id (PCI), a downlink (DL) frequency,an AMF ID, an AUSF ID, RI and other possible parameters, or like.
- [121] In an embodiment of the disclosure, the AMF (300B) obtains the PCI and DL frequency from the RAN and send it to the NWDAF (200) for further analytic derivation.
- [122] Operations 9-10: Upon receiving the notify message from the UDM (300E), the AUSF (300A) and the AMF (300B), the NWDAF (200) compares the exception pa-

- rameters received from the UDM (300E), the AUSF (300A) and the AMF (300B).
- [123] In an embodiment of the disclosure, data analytics may be performed on TAI, AMF ID, PCI, CAG ID based on the received data.
- [124] (Optional) In an embodiment of the disclosure, the NWDAF (200) verifies the credibility of the AMF (300B) or other NFs with the UDM (300E).
- [125] The NWDAF (200) analyses in a particular AMF ID, the total number of failures occurs and for a particular TAI, the number of failures occurred (i.e., miss operations and/or miss implementation of the network. NWDAF also map the received SUCI from AMF with the SUPI received from the AUSF/UDM and analyze whether the issue is with the UE or with the AMF.
- [126] In an embodiment of the disclosure, the AMF (300B) collects the TAI and CAG ID from the genuine gNB and also the AMF (300B) collects the UE (100) provided TAI and CAG ID and send it to NWDAF for analysis.
- [127] In another embodiment of the disclosure, the NWDAF (200) compares both the TAI and CAG ID received from AMF for the requested UE (i.e., genuine gNB broadcasted TAI and TAI in AMF report for UE's abnormality). If the TAI does not match, NWDAF performs the analytics (i.e., identification of DoS attack at the UE).
- [128] In another embodiment of the disclosure, the NWDAF (200) requests the OAM (300G) to provide UE mobility related and RAN specific information to perform the analytics for DoS attack.
- [129] Operation 11: The NWDAF (200) provides the analytics for DoS attack Identification to the consumer NF through *NnwdaF_AnalyticsSubscription_Notify*. The message includes Internal group Identifier or SUPI, DNN, S-NSSAI, Analytics ID, Exception category, Exception indication, Exception ID. The consumer NF (400) starts a DoS Mitigation after receiving the derived analytics from the NWDAF (200). The Exception ID, Exception category as defined as follows: Exception ID = "*Suspicion of Dos attack*" Exception category: "*Authentication failure*"
- [130] In an embodiment of the disclosure, the dispersion analytics is considered as one of the use cases for DOS attack detection.
- [131] The AMF (300B) and the SMF (300C) can provide either per UE transaction or optionally if subscription with periodic notification is requested an amount of UE transactions exchanged at the location. Dispersion analytics results can be used to predict the signaling storm for an Area of Interest (AOI) by the NWDAF (200) and the output result (e.g., signaling overload and failed transactions) can be used to detect the presence of DoS attack at the network.
- [132] In another embodiment of the disclosure, the NWDAF (200) detects those UEs that deviates from the expected UE behavior i.e., based on the unexpected transaction dispersion amount.

- [133] In another embodiment of the disclosure, the information about the TAIs provides the area in which the dispersion/attack occurs.
- [134] Possible mitigation and/or corrective actions:
- [135] In an embodiment of the disclosure, if the issue is with the AMF (300B), the AUSF (300A), the gNB, particular TAI or CAG ID or PCI, then the NWDAF (200) provides remarks to the network (for example, OAM server) to act on it.
- [136] In another embodiment of the disclosure, if the NWDAF (200) identifies the back off timer takes more time for certain UE (e.g., back off timer will be more for the UE with denial of access than the genuine UE) which provides the denial of access, then NWDAF marks it as a malicious UE.

[137] [Table 3]

Information	Description
UE ID	SUPI (UE ID in which the exception occurred)
> DNN	DNN for the PDU Session that SMF collects Data
> S-NSSAI	S-NSSAI for the PDU Session that SMF collects Data
> Start time of data collection	Start time of data collection
> End time of data collection	End time of data collection
>> Timestamp	A time stamp when AMF receives NAS message from UE
>> Timestamp	A time stamp when AMF sends NAS message to UE
>> Provided backoff timer	A value of backoff timer provided to UE
>> AUSF ID	AUSF which involved in authentication procedure
>> AMF ID	AMF in which mobility and tracking information that NWDAF collects data
>> TAI	Tracking Area selected by the UE
>> CAG ID	(Optional) UE selected CAG Cell
>> PCI	PCI in which the exception occurred
>> Downlink Frequency	Frequency range at which the exception occurred
>> Exception ID	Suspicion of MitM Attack
>> Exception Category	Registration failure
> SM NAS request from UE (1max) (if applicable)	Information on SM NAS messages that SMF receives from UE for PDU Session
>> Type of SM NAS request (if applicable)	A type of SM NAS message transmitted by UE (e.g., PDU session establishment request, PDU session modification request, or the like)
>> VPLMN ID	UE selected serving network ID
>> RAN UE ID	Uniquely identify the UE over NG interface

[138] Inputs provided by the AMF (300B) and an NG-RAN (500) to the NWDAF (200) for

the MitM analytics is provided in Table 3. The AMF (300B) and the NG-RAN (500) include at least one of the parameters (in the table) as the input for analytics derivation.

[139] Output from the NWDAF (200) to consumer NF (400) is provided in Table 4.

[140] [Table 4]

Information	Description
> DNN (NOTE)	DNN that MitM is applied
> S-NSSAI (NOTE)	S-NSSAI that MitM is applied
> List of UEs classified based on experience level of DoS	One or more than one of the following lists (SUPI is used to identify UE)
>> Exception ID	Suspicion of MitM Attack
>>Exception category	Indication for Registration failure
>> Analytics ID	To indicate when the analytics are derived and based on what event ID

[141] In an embodiment of the disclosure, in addition to MitM and DoS attack, the NWDAF (200) categorize the genuine authentication failure with error cause i.e., an "error" due to radio conditions (e.g., a radio link failure-DRNS internal failure, congestion, lost radio interface synchronization due to bas radio condition, loss of UL synchronization, or the like).

[142] FIG. 4 is a signaling diagram illustrating NWDAF checking for abnormality in registration failure (MitM attack) according to an embodiment of the disclosure.

[143] Referring to FIG. 4, the operations include the following:

[144] Operation 0: The consumer NF (400) (e.g., AMF) observes the continuous registration failure.

[145] Operation 1: The consumer NF (400) (e.g., SMF, PCF, AMF, or the like) requests to/ subscribes to the NWDAF (200) using *Nnwdafl_AnalyticsSubscription_Subscribe/nwdafl_AnalyticsInfo_Request* (*Analytics ID set to "MitM attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information*) for obtaining analytics information on the "MitM attack Identification".

[146] Derived Analytics are provided by the NWDAF (200) if the consumer NF (400) wants to take the analytics information into account when applying the MitM mitigation and /or MitM identification.

[147] The consumer NF (400) may subscribe to/request signaling failure notification/ response from NWDAF for a group of UEs, any UE or a specific UE. The Analytics

- ID indicates the NWDAF (200) to identify misused or hijacked UEs through signaling failure analytic.
- [148] Operation 2: NWDAF (200) to AMF (300B): *Namf_EventExposure_Subscribe* (*Event ID(s)*, *Event Filter(s)*, *Internal-Group-Identifier*, *any UE or SUPI*). The NWDAF (200) sends subscription requests to the related AMF (s) if it has not subscribed to such data.
- [149] Operation 3: A Genuine gNB broadcast its TAI (i.e., TAI1).
- [150] Operation 4: the AMF (300B) collects the TAI and CAG ID broadcasted by the genuine gNB. The AMF (300B) also collects the PCI, Downlink frequency, RAN UE NGAP ID, or the like, from the genuine gNB. Similarly, the AMF (300B) collects the information (TAI, CAG ID) provides by the UE (100) during registration request.
- [151] Operation 5: The AMF (300B) sends the event reports to the NWDAF (200) over *Namf_EventExposure_Notify* based on the report requirements contained in the subscription request received from the NWDAF (200).
- [152] The event report includes at least one of the following parameters: UE characteristics (e.g., a UE ID, an internal group Identifier, a list of authorized UEs under TA requested, or the like) and all other parameters defined in TS 23.502 clause 4.15.1.
- [153] In another embodiment of the disclosure, the AMF (300B) further provides the parameters, such as SUCI, tracking area identity (TAI), CAG ID (if applicable), PCI, downlink frequency (DL frequency), AMF ID, AUSF ID, RI and other possible parameters, or the like.
- [154] In an embodiment of the disclosure, the AMF (300B) obtains the PCI and DL frequency from the NG-RAN (500) and send it to the NWDAF (200) for further analytic derivation.
- [155] In an embodiment of the disclosure, if the TAI provided by the UE (100) in the registration request (for e.g., TA3) is different from the tracking area broadcasted by the genuine gNB (i.e., TA1), AMF (300B) rejects the registration request.
- [156] In an embodiment of the disclosure, an expected UE behavior is offered to the AMF (300B) as a part of Access and Mobility Subscription Data. If the actual UE (100) behavior varies from the expected UE behavior, then he AMF (300B) provides the exception indication with exception ID to the NWDAF (200). The event report includes at least one of the following parameters: UE characteristics (e.g., a UE ID, an internal group Identifier, a list of authorized UEs under TA requested, or the like) and all other parameters defined in TS 23.502 clause 4.15.1.
- [157] Along with the event report, the AMF (300B) also includes TAI (in which the registration failure occurs), CAG ID (UE selected CAG ID), PCI, RAN UE NGAP ID, downlink frequency, the exception indication and exception category for the abnormal UE and/ or UE(s) based on the latest observation or analysis. Exception category

- includes which type of failure cases has been occurred or observed and exception indication defines the reason for failure. Exception category: Registration failure, Exception indication: Mismatch in TAI values received from UE and broadcasted by genuine gNB.
- [158] Operation 6: The NWDAF (200) compares the AMF (300B) provided information and identifies the mismatch in inputs received from the genuine gNB and from the UE (100).
- [159] Operation 7: Based on the analysis or observation (If there is a miss match), the NWDAF (200) derives the analytics for man in the middle attack and reason for registration failure.
- [160] In an embodiment of the disclosure, data analytics may be performed on TAI, AMF ID, PCI, CAG ID based on the received data.
- [161] Operation 8: The NWDAF (200) provides the analytics for MitM attack identification to the consumer NF through *Nnwdafl_AnalyticsSubscription_Notify*. The message includes an internal group identifier or SUPI, DNN, S-NSSAI, analytics ID, exception category, exception indication, and an exception ID. The consumer NF starts DoS Mitigation after receiving the derived analytics from the NWDAF. The exception ID, exception category, exception indication as defined as follows: exception ID = "Suspicion of MitM attack" Exception category: "Registration failure" Exception indication: "Mismatch in TAI values received from UE and broadcasted by genuine gNB"
- [162] Possible mitigation and/or corrective actions: in an embodiment of the disclosure, if the registration failure occurs due to unexpected UE location (TA or cells which the UE stays), then the PCF may extend the Service Area Restrictions with current UE location. The AMF (300B) may extend the mobility restriction with current UE location.
- [163] In another embodiment of the disclosure depending on the exception ID, the NWDAF may in addition perform data collection from OAM as specified in clause 6.2.3.2. of TS 23.288. Based on that OAM indicates the mitigation needs to be taken for each failure case.
- [164] In another embodiment of the disclosure, the OAM (300G) collects the RAN specific information from the NG-RAN (500) and provides to the NWDAF (200) as an input to derive analytics for MitM attacks and DoS attacks.
- [165] The SMF (300C) and the AMF (300B) provides exception (for registration failure) to the NWDAF (200) for the UE(s) performing DoS.
- [166] Malicious UEs can hijack the communication between legitimate UE and the 5G core network. Based on the results, malicious UEs acts as legitimate UEs and try to access the 5GC network and request for service. With this, it is preventing legitimate UEs

getting the service from core network.

- [167] In such cases, in an embodiment of the disclosure, when a request from malicious UE occurs, the AMF (300B) should reject the registration request and whenever the NWDAF (200) requests for subscribed events, the AMF (300B) provides the exception indication with reason for registration failure.
- [168] In another embodiment of the disclosure, the NWDAF (200) is subscribed to the SMF (300C) for DoS attack identification analytics. Whenever a malicious UE sends unexpected PDU session update request or PDU session establishment request, the SMF (300C) should identify the unexpected requests. Once there is request for subscribed events from the NWDAF (200), the SMF (300C) provides the exception indication for the respective event IDs by including the reason for service failure.
- [169] In an embodiment of the disclosure, if the issue is with the AMF (300B), the AUSF (300A), the gNB, particular TAI or CAG ID or PCI, then the NWDAF (200) provides remarks to the network (for example, an OAM server) to act on it.
- [170] In another embodiment of the disclosure, if the NWDAF (200) identifies the back off timer takes more time for certain UE (e.g., back off timer will be more for the UE with denial of access than the genuine UE) which provides the denial of access, then NWDAF (200) marks it as a malicious UE.

[171] [Table 5]

Information	Description
UE ID	SUPI
> DNN	DNN for the PDU Session that SMF collects Data
> S-NSSAI	S-NSSAI for the PDU Session that SMF collects Data
> Start time of data collection	Start time of data collection
> End time of data collection	End time of data collection
>> Timestamp	A time stamp when SMF receives SM NAS message from UE
>> Type of SM NAS message from network	A type of SM NAS message with backoff timer provided to UE (e.g., PDU session establishment reject, PDU session modification reject, PDU session release command, or the like)
>> Timestamp	A time stamp when SMF sends SM NAS message to UE
>> Provided backoff timer	A value of backoff timer provided to UE
> SM NAS request from UE (1max)	Information on SM NAS messages that SMF receives from UE for PDU Session
>> Type of SM NAS request	A type of SM NAS message transmitted by UE (e.g., PDU session establishment request, PDU session modification request, or the like)
>> Exception ID	Suspicion of Dos Attack
>>Exception Indication	Indication for SMF service failure
>>RAN UE ID	Uniquely identify the UE over NG interface
>>VPLMN ID	UE selected serving network ID

[172] Inputs provided by the SMF (300C) to the NWDAF (200) for DoS analytics is provided in Table 5. The SMF (300C) includes at least one of the parameters (in the table) as the input for analytics derivation.

[173] [Table 6]

Information	Description
UE ID	SUPI (UE ID in which the exception occurred)
> DNN	DNN for the PDU Session that SMF collects Data
> S-NSSAI	S-NSSAI for the PDU Session that SMF collects Data
> Start time of data collection	Start time of data collection
> End time of data collection	End time of data collection
>> Timestamp	A time stamp when AMF receives NAS message from UE
>> Timestamp	A time stamp when AMF sends NAS message to UE
>> Provided backoff timer	A value of backoff timer provided to UE
>>AMF ID	AMF in which mobility and tracking information that NWDAF collects data
>>CAG ID	(Optional) UE selected CAG Cell
>>PCI	PCI in which the exception occurred
>>Downlink Frequency	Frequency range at which the exception occurred
>> Exception ID	Suspicion of Dos Attack
>>Exception Category	Registration failure

[174] Inputs provided by the AMF (300B) to the NWDAF (200) for DoS analytics is provided in Table 6. The AMF (300B) includes at least one of the parameters (in the table) as the input for analytics derivation.

[175] [Table 7]

Information	Description
> DNN (NOTE)	DNN that DoS is applied
> S-NSSAI (NOTE)	S-NSSAI that DoS is applied
> List of UEs classified based on experience level of DoS	One or more than one of the following lists (SUPI is used to identify UE)
>> Exception ID	Suspicion of Dos Attack
>>>Exception Indication	Indication for service failure
>>> Analytics ID	To indicate when the analytics are derived and based on what event ID

[176] Table 7 includes output provided by the NWDAF (200) to the consumer NF (400) after the analytics.

[177] In an embodiment of the disclosure, in addition to MitM and DoS attack, the NWDAF (200) categorize the genuine authentication failure, i.e., an "error" due to radio conditions (e.g., a radio link failure-DRNS internal failure, a congestion, a lost radio interface synchronization due to bas radio condition, loss of UL synchronization, or the like.

[178] FIG. 5 is a signaling diagram illustrating AMF and SMF providing inputs to NWDAF for deriving analytics for DoS detection according to an embodiment of the disclosure.

[179] Referring to FIG. 5, the operations include the following:

[180] Operation 1: The consumer NF (400) (e.g., SMF, PCF, AMF, or the like) requests to/ subscribes to the NWDAF (200) using *Nnwdafl_AnalyticsSubscription_Subscribe/nwdafl_AnalyticsInfo_Request (Analytics ID set to "DoS attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information)* for obtaining analytics information on "DoS attack Identification". The derived Analytics are provided by the NWDAF (200) if the consumer NF (400) wants to take the analytics information into account when applying the DoS mitigation and /or DoS identification.

[181] The consumer NF (400) may subscribe to/request signaling failure notification/ response from the NWDAF (200) for a group of UEs, any UE or a specific UE. The Analytics ID indicates the NWDAF to identify misused or hijacked UEs through signaling failure analytic.

[182] Operation 2: NWDAF (200) to SMF (300C): *Nsmf_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI)*. The NWDAF (200) sends subscription requests to the related SMF(s) if it has not subscribed to such data.

- [183] Operation 3: The SMF (300C) identifies the event subscribed by the NWDAF (200) (i.e., DoS Attack Identification). The SMF (300C) analyses the abnormalities in UE or any UE(s).
- [184] Operation 4: The SMF (300C) sends event reports to the NWDAF (200) over *Nsmf_EventExposure_Notify* based on the report requirements contained in the subscription request received from the NWDAF (200). The event report includes at least one of the following parameters. UE characteristics (e.g., a UE ID, an internal group identifier, a list of UEs under TA requested for SMF service, or the like), DNN, S-NSSAI, start time of data collection, end time of data collection, SM NAS request from UE, type of SM NAS message from UE (PDU session establishment request, PDU session modification request), time stamp at which SMF receives and sends SM NAS message, provided back off timer, type of SM NAS message from network (PDU session establishment reject, PDU session modification reject, PDU session release command). The SMF includes the exception indication for the abnormal UE and/ or UE(s) based on the latest observation or analysis.
- [185] The expected UE (100) behavior is offered to the SMF (300C) and/ or the AMF (300B) as a part of session management subscription data and access and mobility subscription data, respectively. If the actual UE behavior varies from the expected UE behavior, then the SMF (300C) provides the exception indication to the NWDAF (200). The SMF (300C) also includes the expected UE behavior in the report. Exception indication defines the reason for SMF service failure, e.g., reject in unexpected PDU session modification request and/or unexpected PDU session establishment request.
- [186] Operation 5: NWDAF (200) to AMF (300B): *Namf_EventExposure_Subscribe* (*Event ID(s)*, *Event Filter(s)*, *Internal-Group-Identifier*, *any UE or SUPI*). The NWDAF (200) sends subscription requests to the related AMF(s) (300B) if it has not subscribed to such data.
- [187] Operation 6: The AMF (300B) identifies the event subscribed by NWDAF (200) (i.e., DoS Attack Identification). The AMF (300B) also analyses the abnormalities in the UE (100) or any UE(s).
- [188] Operation 7: The AMF (300B) sends the event reports to the NWDAF (200) over *Namf_EventExposure_notify* based on the report requirements contained in the subscription request received from the NWDAF (200). The event report includes at least one of the following parameters. The UE characteristics (e.g., a UE ID, an internal group Identifier, a list of UEs under TA for this particular AMF), DNN, S-NSSAI, start time of data collection, end time of data collection, AMF ID, PCI, CAG ID, TAI, Downlink frequency, Exception ID, Exception Indication.
- [189] In an embodiment of the disclosure, the AMF (300B) collects the parameters (e.g.,

PCI and DL frequency) from the RAN and send to the NWDAF (200) for deriving analytics.

- [190] In an embodiment of the disclosure, the AMF (300B) includes the exception indication for the abnormal UE and/ or UE(s) based on the latest observation or analysis.
- [191] In an embodiment of the disclosure, the expected UE behavior is offered to the SMF (300C) and/ or the AMF (300B) as a part of session management subscription data and access and mobility subscription data, respectively. When the AMF (300B) detects frequent mobility re-registration of one or more UEs, the AMF (300B) checks the UE characteristics and compare the actual UE behavior with the expected UE behavior. Based on that AMF (300B) provides the exception indication to the NWDAF (200). The AMF (300B) also includes the expected UE behavior in the event report. The exception indication defines the reason for AMF service failure, such as unexpected UE ID, NAS message timeouts, NAS message integrity protection failure or registration failure, or the like.
- [192] Operations 8a-8b: With the data obtained in operation 4 and/or operation 7, the NWDAF (200) compares the expected UE behavior and the actual UE behavior. Based on that, the NWDAF (200) derives requested analytics. In an embodiment of the disclosure, data analytics may be performed on TAI, AMF ID, PCI, CAG ID based on the received data.
- [193] Operation 9: The NWDAF (200) provides the analytics for DoS attack identification to the consumer NF (400) through *Nnwdaf_AnalyticsSubscription_Notify*. The message includes Internal group Identifier or SUPI, DNN, S-NSSAI, Analytics ID, Exception indication, Exception ID. The consumer NF (400) starts DoS Mitigation after receiving the derived analytics from the NWDAF (200).
- [194] Possible mitigation and/or corrective actions: In an embodiment of the disclosure, the AMF (300B) should reject the registration request for the suspected UE and similarly the SMF (300C) should reject the PDU session establishment for the suspected UE.
- [195] In an embodiment of the disclosure, if there is an unexpected wakeup, the AMF (300B) applies MM back off timer to the UE (100).
- [196] In an embodiment of the disclosure, if the issue is with the AMF (300B), the AUSF (300A), gNB, particular TAI or CAG ID or PCI, then the NWDAF (200) provides remarks to the network (for example, OAM server) to act on it.
- [197] In another embodiment of the disclosure, if the NWDAF (200) identifies the back off timer takes more time for certain UE (e.g., a back off timer will be more for the UE with denial of access than the genuine UE) which provides the denial of access, then NWDAF marks it as a malicious UE.
- [198] FIG. 6 is a signaling diagram illustrating OAM providing inputs to NWDAF for DoS identification according to an embodiment of the disclosure.

- [199] Referring to FIG. 6, performance measurements provided by OAM (300G) will be used by the NWDAF (200) to determine congestion levels. Performance measurements are related to information transfer over the user plane and/or the control plane (e.g., a UE throughput, a DRB setup management, an RRC connection number, a PDU session management, and a radio resource utilization as defined in TS 28.552).
- [200] In an embodiment of the disclosure, in addition to MitM and DoS attack, the NWDAF (200) should categorize the genuine authentication failure, i.e., an "error" due to radio conditions (e.g., a radio link failure-DRNS internal failure, a congestion, a lost radio interface synchronization due to bas radio condition, a loss of UL synchronization, or the like).
- [201] Referring to FIG. 6, the operations are as follows:
- [202] Operation 1: The consumer NF (400) (e.g., SMF, PCF, AMF, or the like) requests to/ subscribes to the NWDAF (200) using *Nnwdaf_AnalyticsSubscription_Subscribe/nwdaf_AnalyticsInfo_Request (Analytics ID set to "DoS attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information)* for obtaining analytics information on "DoS attack Identification". The derived Analytics are provided by the NWDAF (200) if the consumer NF (400) wants to take the analytics information into account when applying the DoS mitigation and /or DoS identification.
- [203] The consumer NF (400) may subscribe to/request signaling failure notification/ response from the NWDAF (200) for a group of UEs, any UE or a specific UE. The Analytics ID indicates the NWDAF (200) to identify misused or hijacked UEs through signaling failure analytic.
- [204] Operation 2: NWDAF (200) to OAM (300G): *Noam_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI)*.
- [205] The NWDAF (200) sends subscription requests to the related OAM(s) (300G) if it has not subscribed to such data.
- [206] Operation 3a: The OAM (300G) identifies the type of event is subscribed by the NWDAF (200) (i.e., DoS Attack Identification).
- [207] Operation 3b. The OAM (300G) collects the abnormalities in the UE mobility and communication information, congestion on the AMF (300B) and the SMF (300C), performance measurement on RAN (performance measurements are related to information transfer over the user plane and/or the control plane (e.g., a UE throughput, DRB setup management, RRC Connection Number, PDU session management, and radio resource utilization as defined in TS 28.552). OAM analyses the abnormalities in a UE or any UE(s) as per the event Id and event filter information.
- [208] Operation 4: The OAM (300G) sends the event report over *Noam_EventExposure_Notify* to the NWDAF (200). The event report includes at least

one of the following parameters:

- [209] UE characteristics (e.g., a UE ID, an internal group identifier, a list of UEs under TA), TAI, CAG ID, AMF ID, SMF ID, start time of data collection, end time of data collection, , PCI, Downlink frequency, RAN UE ID, VPLMN ID, C-RNTI, SM NAS request from a UE, a type of SM NAS message from a UE, or the like.
- [210] In an embodiment of the disclosure, the event report also includes, NAS message timeouts, NAS message integrity protection failure or registration failure, or the like.
- [211] Expected UE behavior is offered to the OAM (300G). The OAM (300G) checks the UE characteristics and compare the actual UE behavior with the expected UE behavior. The OAM (300G) also include the expected UE behavior in the report.
- [212] Operation 5: With the data obtained in operation 4, the NWDAF (200) compares the expected UE behavior and the actual UE behavior. Based on that the NWDAF (200) derives requested analytics.
- [213] In an embodiment of the disclosure, data analytics may be performed on TAI, AMF ID, PCI, CAG ID based on the received data.
- [214] Operation 6: The NWDAF (200) provides the analytics for DoS attack identification to the consumer NF (400) through *Nnwdaf_AnalyticsSubscription_Notify*. The message includes Internal group Identifier or SUPI, DNN, S-NSSAI, Analytics ID, Exception ID. The consumer NF starts DoS Mitigation after receiving the derived analytics from the NWDAF.
- [215] In an embodiment of the disclosure, if the unexpected radio link failures are per UE location bases, the AMF may allow the use of coverage enhancement (CE) in the affected location. In addition, the Operator may improve the coverage conditions in the affected location.
- [216] If the unexpected radio link failures are per UE bases, then the AMF (300B) and/or the AF (300F) may allow the use of CE for the affected UE (100).
- [217] Possible mitigation and/or corrective actions: The NWDAF (400) can conditionally indicate the exception ID to the OAM (300G). Based on the received exception ID. The OAM (300G) can indicate the AMF (300B) to reject the registration request causing the congestion. The OAM (300G) can indicate the SMF (300C) to reject the PDU session establishment request. The OAM (300G) can indicate the PCF to update the packet filter in the PCC Rules that triggers the SMF (300C) to update the related QoS flow and configures the UPF.
- [218] In an embodiment of the disclosure, if the issue is with the AMF (300B), AUSF (300A), gNB, particular TAI or CAG ID or PCI, then NWDAF provides remarks to the network (for example, OAM server) to act on it.
- [219] In another embodiment of the disclosure, if the NWDAF (200) identifies the back off timer takes more time for certain UE (e.g., a back off timer will be more for the UE

with denial of access than the genuine UE) which provides the denial of access, then the NWDAF (200) marks it as a malicious UE.

- [220] FIG. 7 is a signaling diagram illustrating OAM providing collected RAN inputs to NWDAF for MitM attack analytic derivation according to an embodiment of the disclosure.
- [221] Referring to FIG. 7, in an embodiment of the disclosure, in addition to MitM and DoS attack, the NWDAF (200) should categorize the genuine authentication failure and send error cause. i.e., an "error" due to radio conditions (e.g., a radio link failure-DRNS internal failure, a congestion, a lost radio interface synchronization due to bas radio condition, a loss of UL synchronization, or the like).
- [222] Referring to FIG. 7, the operations are as follows:
- [223] Operation 1: The consumer NF (400) (e.g., SMF, PCF, AMF, or the like) requests to/ subscribes to the NWDAF (200) using *Nnwdafl_AnalyticsSubscription_Subscribe/nwdafl_AnalyticsInfo_Request (Analytics ID set to "MitM attack identification", Target of Analytics Reporting = Internal-Group-Identifier, any UE or SUPI, Analytics Filter Information)* for obtaining analytics information on "MitM attack Identification". Derived Analytics are provided by the NWDAF (200) if the consumer NF (400) wants to take the analytics information into account when applying the MitM mitigation and / or MitM identification.
- [224] The consumer NF (400) may subscribe to/request signaling failure notification/ response from the NWDAF (200) for a group of UEs, any UE or a specific UE. The Analytics ID indicates the NWDAF to identify misused or hijacked UEs through signaling failure analytic.
- [225] Operation 2: NWDAF (200) to the OAM (300G): *Noam_EventExposure_Subscribe (Event ID(s), Event Filter(s), Internal-Group-Identifier, any UE or SUPI)*.
- [226] The NWDAF (200) sends subscription requests to the related OAM(s) if it has not subscribed to such data.
- [227] Operation 3a: The OAM (300G) identifies the type of event is subscribed by the NWDAF (200) (i.e., MitM Attack Identification). The OAM (300G) also performs the RAN selection for data collection.
- [228] Operation 3b. The OAM (300G) performs the data collection from the RAN in which the UE (100) is connected. The OAM (300G) collects the performance measurement on RAN (Performance Measurements are related to information transfer over the user plane and/or the control plane (e.g., a UE throughput, DRB setup management, RRC connection number, PDU session management, and radio resource utilization as defined in TS 28.552). OAM analyses the abnormalities in UE or any UE(s) as per the event Id and event filter information.
- [229] Operation 4: The OAM (300G) sends the event report over

Noam_EventExposure_Notify to the NWDAF (200). The event report includes at least one of the following parameters: UE characteristics (e.g., a UE ID, an internal group identifier, a list of UEs under TA), TAI, CAG ID, C-RNTI, downlink frequency, PCI, RAN UE ID, VPLMN ID, start time of data collection, end time of data collection, the manipulation of chosen fields in MIB/SIBs, arbitrary bit flipping of signed MIB/SIBs, replay of signed MIB/SIBs, broadcast MIB/SIBs with invalid signatures and also by manipulation of timing information in a UE or gNBs, an SM NAS request from a UE, a type of SM NAS message from a UE, or the like.

[230] The expected UE behavior is offered to the OAM (300G). The OAM (300G) checks the UE characteristics and compare the actual UE behavior with the expected UE behavior. Based on that OAM provides the exception indication to the NWDAF (200). The OAM (300G) also include the expected UE behavior in the report.

[231] Operation 5: With the data obtained in operation 4, the NWDAF (200) compares the expected UE behavior and the actual UE behavior. Based on that the NWDAF (200) derives requested analytics.

[232] In an embodiment of the disclosure, data analytics may be performed on TAI, AMF ID, PCI, CAG ID based on the received data.

[233] Operation 6: The NWDAF (200) provides the analytics for MitM attack Identification to the consumer NF through *Nnwdaf_AnalyticsSubscription_Notify*. The message includes internal group Identifier or SUPI, DNN, S-NSSAI, Analytics ID, Exception indication, Exception ID. The consumer NF (400) starts MitM Mitigation after receiving the derived analytics from the NWDAF (200).

[234] In an embodiment of the disclosure, if the unexpected radio link failures are per UE location bases, the AMF (300B) may allow the use of coverage enhancement (CE) in the affected location. In addition, the Operator may improve the coverage conditions in the affected location.

[235] If the unexpected radio link failures are per UE bases, then the AMF (300B) and/or the AF (300F) may allow the use of CE for the affected UE the Dos attack on the network side AMF (300B) provides the exception of SMF performing DoS: In this alternative it is assumed that the AMF (300B) is the consumer NF (400). The DoS attack on SMF (300C) makes the SMF (300C) unavailable for the subscribed users and in such cases, there may be continuous SMF service failure (e.g., an unexpected PDU session reject, an unexpected PDU session release or PDU session update, or the like.

[236] In another embodiment of the disclosure, the SMF (300C) service gets failed due to DNN based congestion or S-NSSAI based congestion at the SMF (300C) by malicious or hijacked UEs. Therefore, in such scenarios after receiving event subscription request from the NWDAF (200), the AMF (300B) needs to identify the reason for SMF (300C) service failure and based on that AMF (300B) requests the analytics from the NWDAF

(200).

- [237] The OAM (300G) provides the exception of RAN performing DoS: In this alternative it is assumed that the OAM (300G) is the consumer NF (400). The DoS attack on RAN makes the RAN unavailable for the subscribed users.
- [238] Performance measurements are related to information transfer over the user plane and/or the control plane (e.g., a UE throughput, DRB setup management, RRC connection number, PDU session management, and radio resource utilization as defined in TS 28.552). The NWDAF may obtain measurements by invoking management services that are defined in TS 28.532 and TS 28.550. Therefore, in such cases the OAM (300G) identifies the exception in RAN performance and the OAM (300G) requests for analytics from the NWDAF (200).
- [239] The OAM (300G) provides the exception of AMF (300B) performing DoS: The AMF (300B) rejects the continuous registration request from UEs, whose SUPI belongs to different region or unexpected GUTI, (i.e., not under the TA of this particular AMF). DoS Attack on the AMF (300B) makes the AMF (300B) unavailable for the subscribed user. Therefore, in such scenarios after receiving event subscription request from the NWDAF (200), the OAM (300G) needs to identify the reason for AMF (300B) service failure and /or continuous registration request failure and based on that the OAM (300G) requests for analytic from the NWDAF (200).
- [240] In another embodiment of the disclosure, even after the primary authentication is successful, the AMF (300B) reports a registration failure to UDM (300E). In such cases the UDM (300E) should be able to provide the exception indication on the AMF (300B) to the NWDAF (200) to derive the analytics.
- [241] Possible mitigation and/or corrective actions: In case of DoS attack in V-AMF, the AMF re-allocation is recommended so that it will span a new AMF, by retaining the old context with a new IP.
- [242] The OAM (300G) can indicate the AMF (300B) to inform the UE (100) to select a new cell or to re-allocate the AMF (300B) to serve the UE (100) based on its location update.
- [243] In an embodiment of the disclosure, the NAS procedure being one of: authentication procedure, registration procedure, service request procedure, PDU session establishment procedure, UE configuration update procedure.
- [244] In another embodiment of the disclosure, the recovery mechanism being at least one of: release of resources reserved for the UE (100) in the network, indicating the UE (100) to move out of the current cell or tracking area or serving PLMN, indicating the UE (100) to update the configuration (using PARLOS or onboarding procedure), indicating to the UE (100) an appropriate backoff timer value, or the like.
- [245] In an embodiment of the disclosure, the consumer NF (400) requests the NWDAF

(200) for sharing analytics information associated with the UE (100). The consumer NF (400) identifies an anomalous activity and based on the observation, the consumer NF (400) requests the NWDAF (200) to perform the analytics and identifies that the abnormality is due to which cyber-attack.

[246] FIG. 8 is a view illustrating an internal structure of a network data analytics function (NWDAF) according to an embodiment of the disclosure.

[247] Referring to FIG. 8, according to an embodiment of the disclosure, a NWDAF (800) may include at least one controller (e.g., at least one processor) (810) and a transceiver (820) including a receiver and a transmitter. The location management device may include a memory (not shown). The transceiver (820) and the memory may be connected to the at least one controller (810) to be operated under the control of the at least one controller (810).

[248] The at least one controller (810) may control a series of steps to perform the operation of the NWDAF described in connection with the embodiments. The transceiver (820) may transmit and receive signals to/from the consumer NF (900) and any other devices.

[249] FIG. 9 is a view illustrating an internal structure of a consumer NF according to an embodiment of the disclosure.

[250] Referring to FIG. 9, according to an embodiment of the disclosure, a consumer NF (900) may include at least one controller (e.g., at least one processor) (910) and a transceiver (920) including a receiver and a transmitter. The location management device may include a memory (not shown). The transceiver (920) and the memory may be connected to the at least one controller (910) to be operated under the control of the at least one controller (910).

[251] The at least one controller (910) may control a series of steps to perform the operation of the consumer NF described in connection with the embodiments. The transceiver (920) may transmit and receive signals to/from the NWDAF (800) and any other devices.

[252] In an embodiment of the disclosure, a method performed by network data analytics function (NWDAF), the method comprising: receiving a request for sharing analytics information associated with a user equipment (UE) from a consumer network function (NF); requesting the analytics information associated with the UE to at least one 5th generation core (5GC) network entity; receiving the analytics information associated with the UE from the at least one 5GC network entity; comparing an expected behavior of the UE with an actual behavior based on the analytics information provided by the at least one 5GC network entity; deriving analytics associated with a cyber-attack based on the analytics information and a result of the comparing of the expected behavior of the UE; and sending the analytics associated with the cyber-attack on the

UE to the consumer NF.

- [253] In addition, the method comprises receiving, by the consumer NF, requested analytics information associated with the UE from the NWDAF; and indicating, by the consumer NF, a recovery mechanism for the cyber-attack based on the analytical information received, to the UE.
- [254] In addition, wherein the recovery mechanism comprises at least one of: a release of resources reserved for the UE in a 5th generation core network; an indication the UE to move out of one of a current cell, a tracking area and a serving public land mobile network (PLMN); an indication to the UE to update a UE configuration; or an indication to the UE for an appropriate backoff timer value.
- [255] In addition, wherein the cyber-attack includes one of a denial-of-service (DoS) attack, a man in the middle (MitM) attack, or an impersonation.
- [256] In addition, wherein the receiving, by the NWDAF, of the request for sharing analytics information associated with the UE comprises: detecting, by the consumer NF, a continuous failure of a non-access-stratum (NAS) procedure of the UE with a 5G network; determining, by the consumer NF, a possibility of the cyber-attack on the UE based on the detected continuous failure of the NAS procedure; and sending, by the consumer NF, a request for sharing analytics information associated with the UE to the NWDAF.
- [257] In addition, wherein the NAS procedure includes one of an authentication procedure, a registration procedure, a service request procedure, a packet data unit (PDU) session establishment procedure, or a UE configuration update procedure.
- [258] In addition, wherein the requesting, by the NWDAF, of the analytics information associated with the UE to at least one 5GC network entity comprises: sending, by the NWDAF, a request to a unified data management (UDM), an authentication server function (AUSF) and an access and mobility management function (AMF) for sharing information associated with a DoS attack, wherein the request comprises an event identity (ID), an event filter, and an internal-group-Identifier.
- [259] In addition, wherein the requesting, by the NWDAF, of the analytics information associated with the UE to the at least one 5GC network entity comprises: sending, by the NWDAF, a request to an Access and mobility management function (AMF) for sharing information associated with a man in the middle (MitM) attack, wherein the request comprises an event Identity (ID), an event filter, and an internal-group-identifier.
- [260] In addition, wherein the receiving, by the NWDAF, of the analytics information associated with the cyber-attack from the at least one 5GC network entity comprises: receiving, by the NWDAF, an event report comprising an AUSF ID, a subscription permanent identifier (SUPI) for the UE which is under a DoS attack, a back-off timer

and an exception category associated with a UE performing the DoS attack, from the UDM; receiving, by the NWDAF, the event report comprising an authentication management function (AMF) ID and a SUPI ID for the UE which is under the DoS attack, a backoff timer and an exception category associated with a UE performing the DoS attack, from the AUSF; receiving, by the NWDAF, a mapping comprising an indication on which N1 interface a NAS authentication has failed for the corresponding UE from the AMF; checking, by the AMF, a failed SUPI corresponding to a subscription concealed identifier (SUCI) of the corresponding UE; and receiving, by the NWDAF, an event report comprising a SUCI, a tracking area identity (TAI), a closed access group identifier (CAG ID), a physical cell ID (PCI), a downlink (DL) frequency, a backoff timer and an exception category associated with the UE performing the DoS attack, from the AMF.

- [261] In addition, wherein the sending, by the NWDAF, of the analytics information associated with the cyber-attack during an analysis to the consumer NF comprises: sending, by the NWDAF, an exception ID indicating a suspicion of the DoS attack, an exception category of failure, a UE characteristics, a SUPI list, and a list of UEs classified based on experience level of the DoS attack to the consumer NF; and performing, by the consumer NF, a release of a resource associated with the UE based on the analytic results provides by the NWDAF.
- [262] In addition, wherein the receiving, by the NWDAF, of the analytics information associated with the cyber-attack from the at least one 5GC network entity comprises: checking, by an AMF, a TAI broadcasted by a genuine gNB and provided by the UE during a registration request of the UE; receiving, by the NWDAF, an event report which includes a SUCI, TAI, CAG ID, PCI, RAN UE ID, backoff timer and an exception category associated with the UE performing MitM attack, from the AMF; comparing, by the NWDAF, the actual UE behavior and the expected UE behavior provided by the AMF; and receiving, by the NWDAF, the event report associated with the MitM attack from an operations, administration and maintenance (OAM).
- [263] In addition, wherein the sending, by the NWDAF, of the analytics information associated with the cyber-attack during an analysis to the consumer NF comprises: sending, by the NWDAF, an exception ID corresponding to a suspicion of an MitM attack, an exception category, a UE characteristics, a SUPI list, and a list of UEs classified based on experience level of the MitM attack to the consumer NF; and performing, by the consumer NF, a release of resource with the UE based on the analytics information provides by the NWDAF.
- [264] In an embodiment of the disclosure, A wireless network system for detecting cyber-attacks using network analytics in a user equipment (UE), the wireless network system comprising: the UE; at least one 5th generation core (5GC) network entity; a consumer

network function (NF); and a network data analytics function (NWDAF) configured to: receive a request for sharing analytics information associated with the UE from the NF, request the analytics information associated with the UE and causing the cyber-attack to at the least one 5GC network entity, receive the analytics information associated with the UE from the at least one 5GC network entity, compare an expected behavior of the UE with an actual behavior based on the analytics information provided by the at least one 5GC network entity, derive analytics associated with the cyber-attack based on the analytics information and a result of the comparing of the expected behavior of the UE, and send the analytics associated with the UE to the consumer NF.

[265] While the disclosure has been shown and described with reference to various embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the spirit and scope of the disclosure as defined by the appended claims and their equivalents.

Claims

- [Claim 1] A method performed by network data analytics function (NWDAF) in a wireless communication system, the method comprising:
receiving a request for sharing analytics information associated with a user equipment (UE) from a consumer network function (NF);
requesting the analytics information associated with the UE to at least one 5th generation core (5GC) network entity;
receiving the analytics information associated with the UE from the at least one 5GC network entity;
comparing an expected behavior of the UE with an actual behavior based on the analytics information provided by the at least one 5GC network entity;
deriving analytics associated with a cyber-attack based on the analytics information and a result of the comparing of the expected behavior of the UE; and
sending the analytics associated with the cyber-attack on the UE to the consumer NF.
- [Claim 2] The method of claim 1, wherein the cyber-attack includes one of a denial-of-service (DoS) attack, a man in the middle (MitM) attack, or an impersonation.
- [Claim 3] The method of claim 1, wherein requesting the analytics information associated with the UE to at least one 5GC network entity comprises:
sending a request to a unified data management (UDM), an authentication server function (AUSF) and an access and mobility management function (AMF) for sharing information associated with a DoS attack, wherein the request comprises an event identity (ID), an event filter, and an internal-group-identifier.
- [Claim 4] The method of claim 1, wherein requesting the analytics information associated with the UE to the at least one 5GC network entity comprises:
sending a request to an access and mobility management function (AMF) for sharing information associated with a man in the middle (MitM) attack, wherein the request comprises an event identity (ID), an event filter, and an internal-group-identifier.
- [Claim 5] The method of claim 3, wherein receiving the analytics information associated with the cyber-attack from the at least one 5GC network entity comprises:

receiving an event report comprising an AUSF ID, a subscription permanent identifier (SUPI) for the UE which is under a DoS attack, a back-off timer and an exception category associated with a UE performing the DoS attack, from the UDM;

receiving the event report comprising an authentication management function (AMF) ID and a SUPI ID for the UE which is under the DoS attack, a backoff timer and an exception category associated with a UE performing the DoS attack, from the AUSF;

receiving a mapping comprising an indication on which N1 interface a NAS authentication has failed for the corresponding UE from the AMF;

receiving an event report comprising a subscription concealed identifier (SUCI), a tracking area identity (TAI), a closed access group identifier (CAG ID), a physical cell ID (PCI), a downlink (DL) frequency, a backoff timer and an exception category associated with the UE performing the DoS attack, from the AMF,

wherein a SUPI corresponding to a SUCI of the corresponding UE is checked by the AMF.

[Claim 6]

The method of claim 5, wherein sending the analytics information associated with the cyber-attack during an analysis to the consumer NF comprises:

sending an exception ID indicating a suspicion of the DoS attack, an exception category of failure, a UE characteristics, a SUPI list, and a list of UEs classified based on experience level of the DoS attack to the consumer NF wherein the release of the resource associated with the UE is performed by the consumer NF based on the analytic results provides by the NWDAF.

[Claim 7]

The method of claim 1, wherein receiving the analytics information associated with the cyber-attack from the at least one 5GC network entity comprises:

receiving an event report which includes a SUCI, TAI, CAG ID, PCI, RAN UE ID, backoff timer and an exception category associated with the UE performing MitM attack, from an AMF;

comparing the actual UE behavior and the expected UE behavior provided by the AMF; and

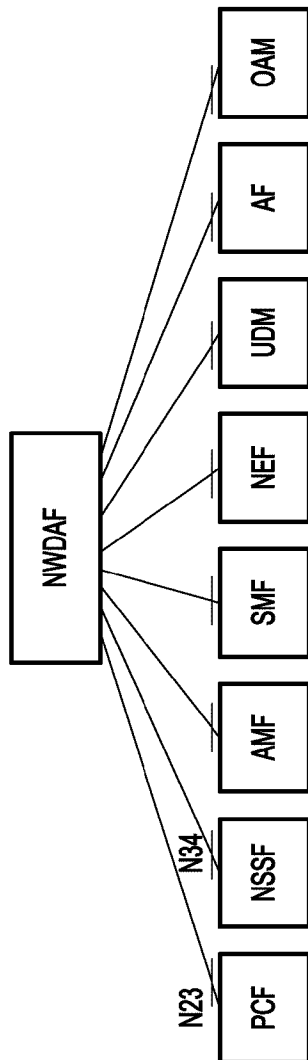
receiving the event report associated with the MitM attack from an operations, administration and maintenance (OAM),

wherein a TAI broadcasted by a genuine gNB and provided by the UE

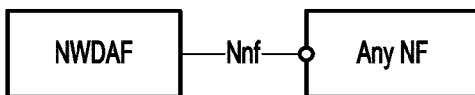
- is checked by the AMF during a registration request of the UE.
- [Claim 8] The method of claim 1, wherein sending the analytics information associated with the cyber-attack during an analysis to the consumer NF comprises:
sending an exception ID corresponding to a suspicion of an MitM attack, an exception category, a UE characteristics, a SUPI list, and a list of UEs classified based on experience level of the MitM attack to the consumer NF
wherein a release of resource with the UE is performed by the consumer NF based on the analytics information provides by the NWDAF.
- [Claim 9] A method performed by a consumer network function (NF) in a wireless communication, the method comprising:
transmitting a request for sharing analytics information associated with a user equipment (UE) to a network data analytics function (NWDAF);
and
receiving analytics associated with a cyber-attack on the UE from the NWDAF.
- [Claim 10] The method of claim 9, further comprising:
receiving analytics information associated with the UE from the NWDAF; and
indicating, to the UE, a recovery mechanism for the cyber-attack based on the analytical information received.
- [Claim 11] The method of claim 10, wherein the recovery mechanism comprises at least one of:
a release of resources reserved for the UE in a 5th generation core network;
an indication the UE to move out of one of a current cell, a tracking area and a serving public land mobile network (PLMN);
an indication to the UE to update a UE configuration; or
an indication to the UE for an appropriate backoff timer value.
- [Claim 12] The method of claim 9, further comprising:
detecting a continuous failure of a non-access-stratum (NAS) procedure of the UE with a 5G network;
determining a possibility of the cyber-attack on the UE based on the detected continuous failure of the NAS procedure; and
sending, to the NWDAF, a request for sharing analytics information associated with the UE.

- [Claim 13] The method of claim 12, wherein the NAS procedure includes one of an authentication procedure, a registration procedure, a service request procedure, a packet data unit (PDU) session establishment procedure, or a UE configuration update procedure.
- [Claim 14] A network data analytics function (NWDAF) in a wireless communication system, the NWDAF comprising:
transceiver; and
at least one processor coupled to the transceiver, wherein the at least one processor is configured to operate one of methods according to claims 1 to 8.
- [Claim 15] A consumer network function (NF) in a wireless communication system, the consumer NF comprising:
transceiver; and
at least one processor coupled to the transceiver r, wherein the at least one processor is configured to operate one of methods according to claims 9 to 13.

[Fig. 1A]



[Fig. 1B]



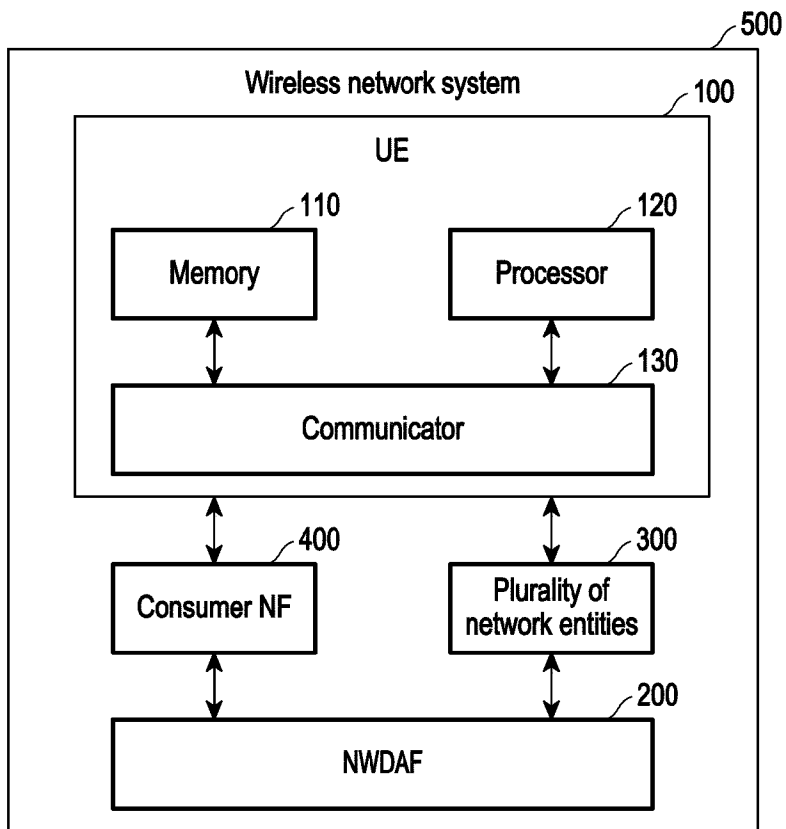
[Fig. 1C]



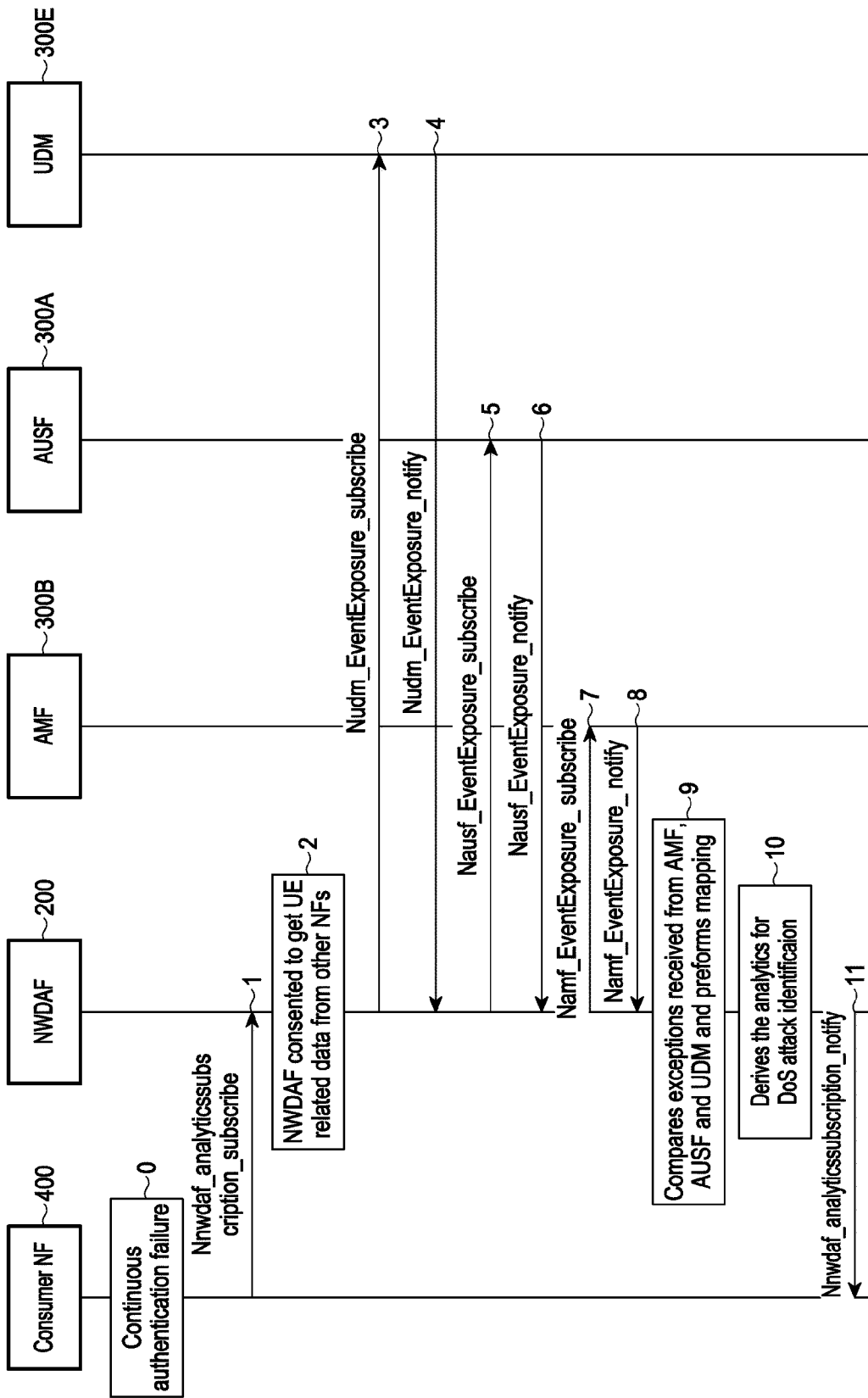
[Fig. 1D]

Exception ID	UE behaviour parameters to provide	NF for data collection
Unexpected UE location	Expected UE moving trajectory Stationary indication	AMF
Unexpected long-live/large rate flows	Periodic time Scheduled communication time Communication duration time	SMF
Unexpected wakeup	Periodic time Communication duration time Scheduled communication time	SMF
Suspicion of DDoS attack	Periodic time Communication duration time Scheduled communication time Scheduled communication type Traffic profile	SMF
Too frequent service access	Periodic time	SMF
Unexpected radio link failures	Expected UE moving trajectory	AMF
Ping-ponging across neighbouring cells	Expected UE moving trajectory Stationary indication	AMF

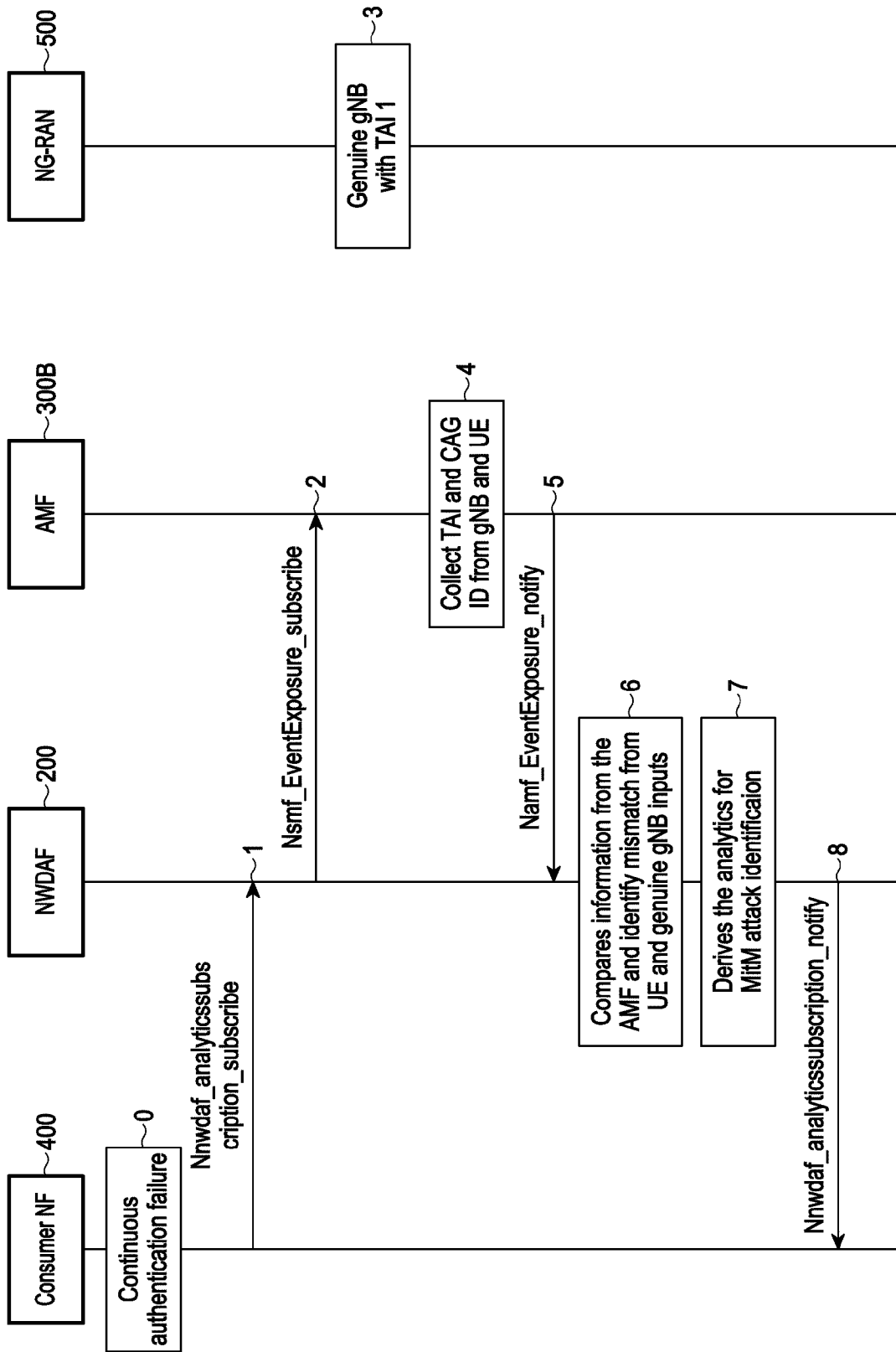
[Fig. 2]



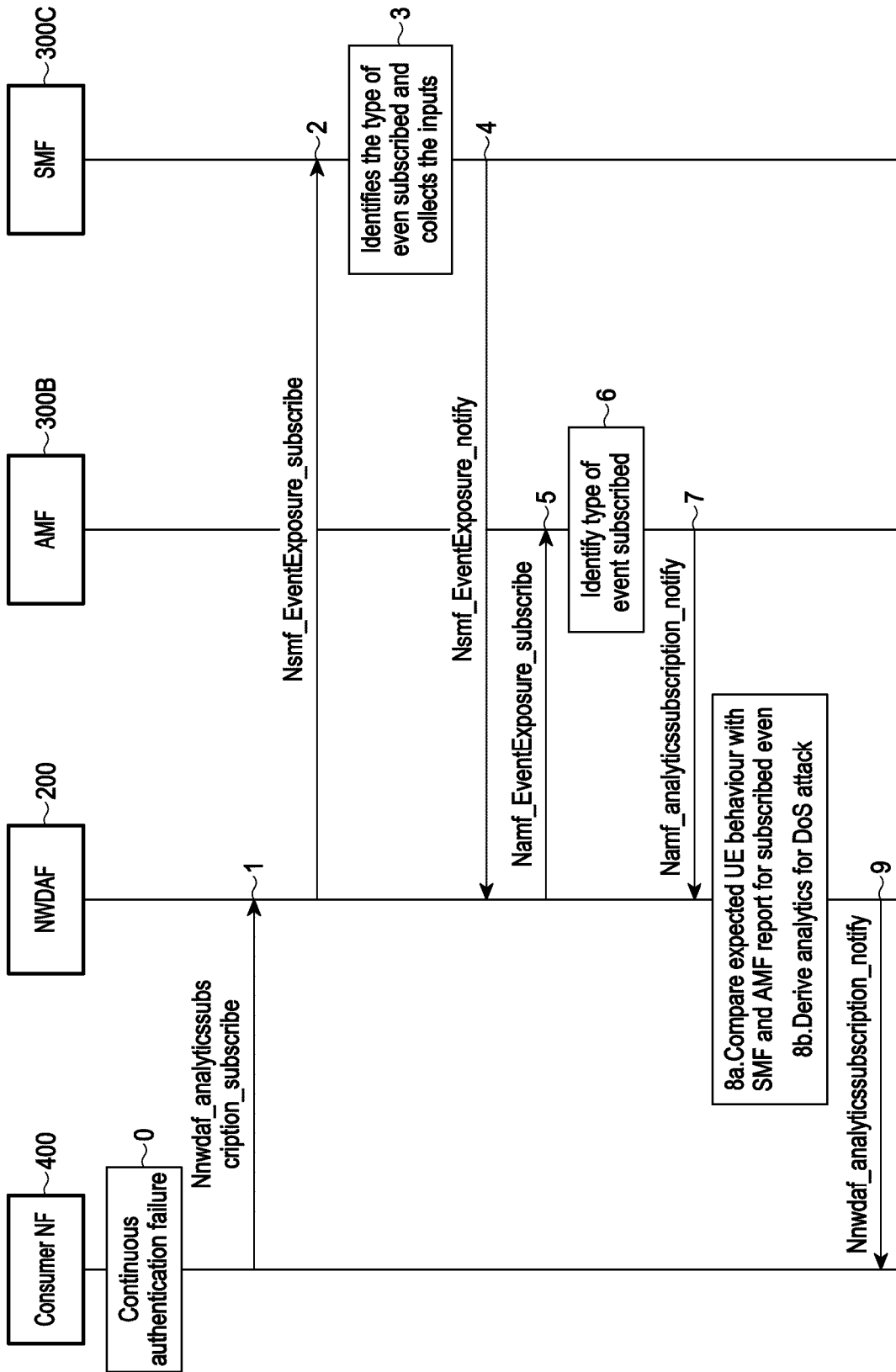
[Fig. 3]



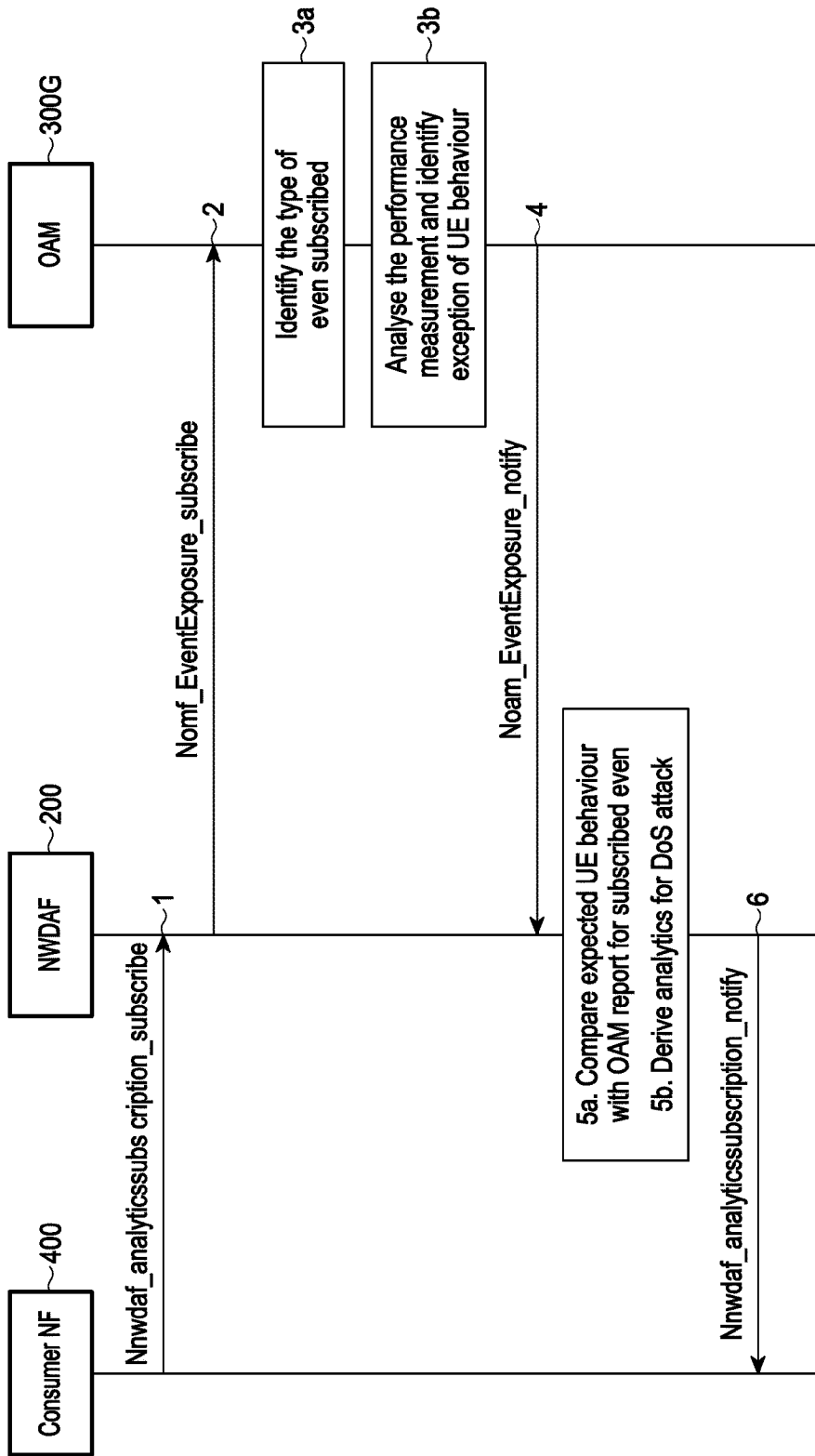
[Fig. 4]



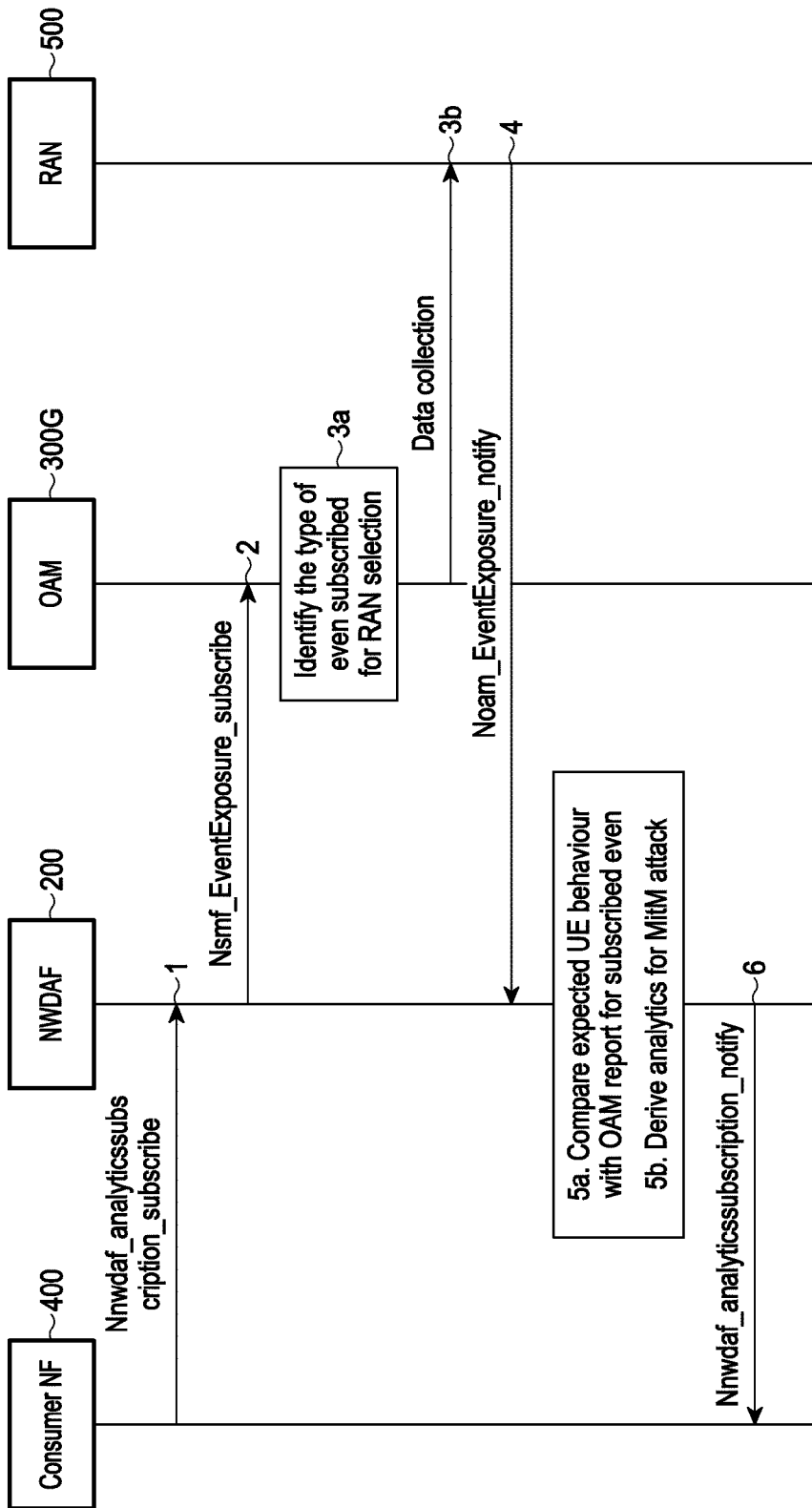
[Fig. 5]



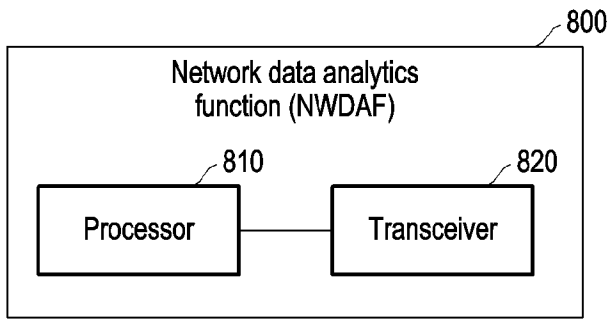
[Fig. 6]



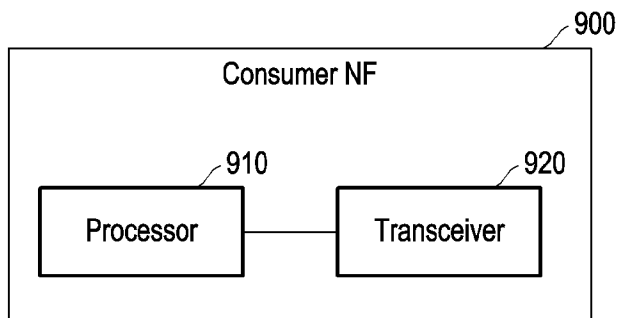
[Fig. 7]



[Fig. 8]



[Fig. 9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2022/002235

A. CLASSIFICATION OF SUBJECT MATTER H04W 12/122(2021.01)i; H04L 9/40(2022.01)i		
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) H04W 12/122(2021.01); H04W 24/08(2009.01)		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean utility models and applications for utility models Japanese utility models and applications for utility models		
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKOMPASS(KIPO internal) & Keywords: NWDAF (network data analytics function), cyber-attack, consumer NF, share, analytics, compare, recovery		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	LENOVO et al., 'Analytics for MitM Attack Detection', S3-210419, 3GPP TSG-SA3 Meeting #102e, e-meeting, 11 January 2021 section 6.Y.2.4	1-4,9,14-15 5-8,10-13
X	LENOVO et al., 'KI#16, Sol#31, Additional clarifications', S2-2009388, 3GPP TSG-SA WG2 Meeting #142e, e-meeting, 23 November 2020 section 6.31.4	9,15
X	SPIRENT COMM. et al., 'KI #9, Solution Completion and Procedures: Dispersion Analytic Output Provided by NWDAF', S2-2008055, 3GPP SA WG2 Meeting #141E, Online, 26 October 2020 section 6.30.4	9,15
X	ERICSSON et al., 'KI#10, sol#68 - Update to remove errors', S2-2009375, SA WG2 Meeting #142E, e-meeting, 22 November 2020 section 6.68.4	9,15
A	US 2020-0252813 A1 (CONVIDA WIRELESS, LLC) 06 August 2020 (2020-08-06) paragraphs [0367]-[0377]; and figure 22	1-15
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> 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 12 May 2022		Date of mailing of the international search report 12 May 2022
Name and mailing address of the ISA/KR Korean Intellectual Property Office 189 Cheongsa-ro, Seo-gu, Daejeon 35208, Republic of Korea Facsimile No. +82-42-481-8578		Authorized officer YANG, Jeong Rok Telephone No. +82-42-481-5709

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2022/002235

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2020-0252813	A1	06 August 2020	CN	111095970	A	01 May 2020
				EP	3659359	A1	03 June 2020
				JP	2020-530703	A	22 October 2020
				KR	10-2020-0035146	A	01 April 2020
				US	11051192	B2	29 June 2021
				US	2021-0282038	A1	09 September 2021
				WO	2019-032968	A1	14 February 2019
