US 20250267069A1

(19) **United States**

(12) **Patent Application Publication**

SUNG et al.

(10) **Pub. No.: US 2025/0267069 A1**

(43) **Pub. Date: Aug. 21, 2025**

(54) **METHOD OF MANAGING ABNORMAL NETWORK BEHAVIOR AND DEVICE FOR PERFORMING THE SAME**

(71) Applicant: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE**, Daejeon (KR)

(72) Inventors: **Jihoon SUNG**, Daejeon (KR); **Myung Ki SHIN**, Seoul (KR)

(73) Assignee: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE**, Daejeon (KR)

(21) Appl. No.: **18/965,027**

(22) Filed: **Dec. 2, 2024**

(30) **Foreign Application Priority Data**

Feb. 16, 2024	(KR)	10-2024-0022916
Aug. 30, 2024	(KR)	10-2024-0118083
Oct. 23, 2024	(KR)	10-2024-0146031
Nov. 19, 2024	(KR)	10-2024-0165164

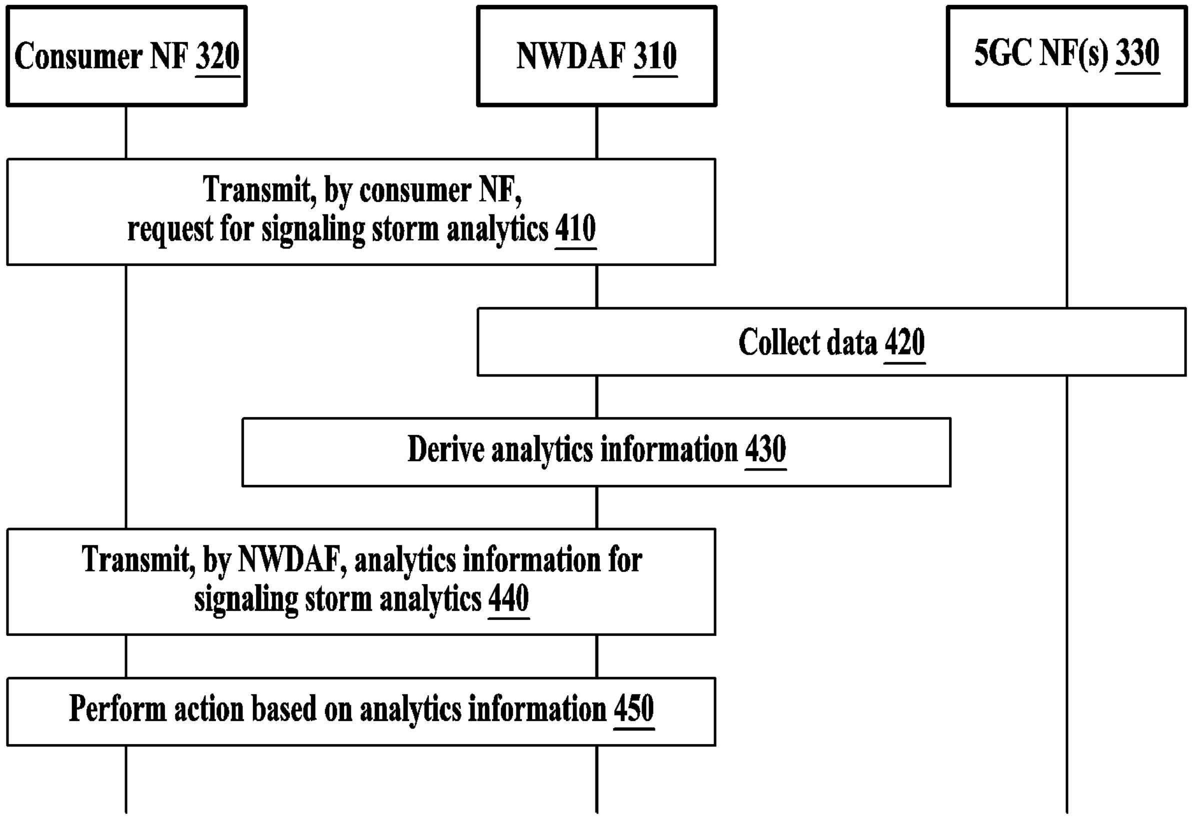
Publication Classification

(51) **Int. Cl.**
H04L 41/14 (2022.01)

(52) **U.S. Cl.**
CPC ***H04L 41/14*** (2013.01)

(57) **ABSTRACT**

Disclosed are an abnormal network behavior management method and a device for performing the same. A method of managing an abnormal network behavior includes receiving a request for analytics of a signaling storm from a consumer network function (NF), collecting data for the analytics of the signaling storm from a fifth-generation core (5GC) NF, generating analytics information about the signaling storm based on the collected data, and transmitting the analytics information to the consumer NF, wherein the request includes analytic filter information including an instance identification (ID) of a target NF that analytics of the signaling storm is to be provided for.


Consumer NF 320
NWDAF 310
5GC NF(s) 330
Transmit, by consumer NF, request for signaling storm analytics 410
Collect data 420
Derive analytics information 430
Transmit, by NWDAF, analytics information for signaling storm analytics 440
Perform action based on analytics information 450

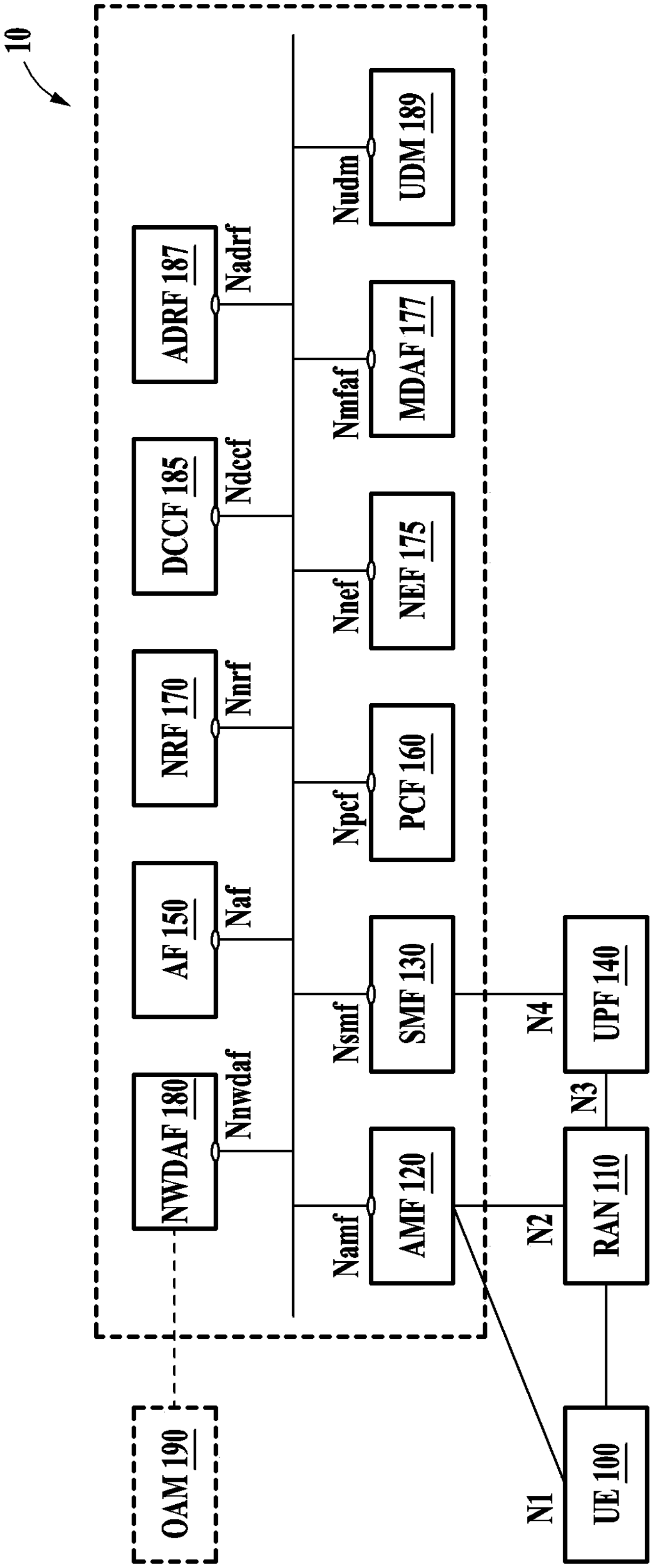

10
NWDAF 180
Nnwdaf
AF 150
Naf
NRF 170
Nnrf
DCCF 185
Ndccf
ADRF 187
Nadrf
Namf
AMF 120
Nsmf
SMF 130
Npcf
PCF 160
Nnef
NEF 175
Nmfaf
MDAF 177
Nudm
UDM 189
OAM 190
N1
UE 100
N2
RAN 110
N3
N4
UPF 140

FIG. 1

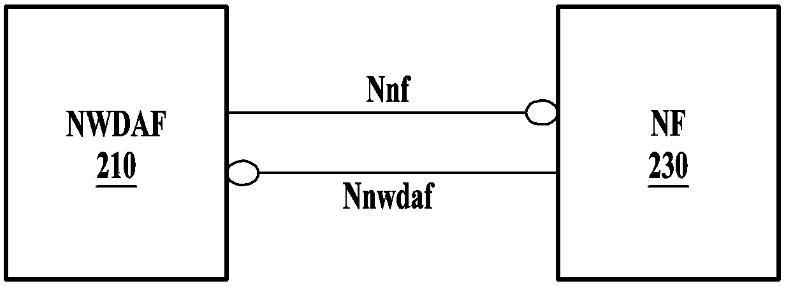

NWDAF
210
Nnf
Nnwdaf
NF
230

FIG. 2

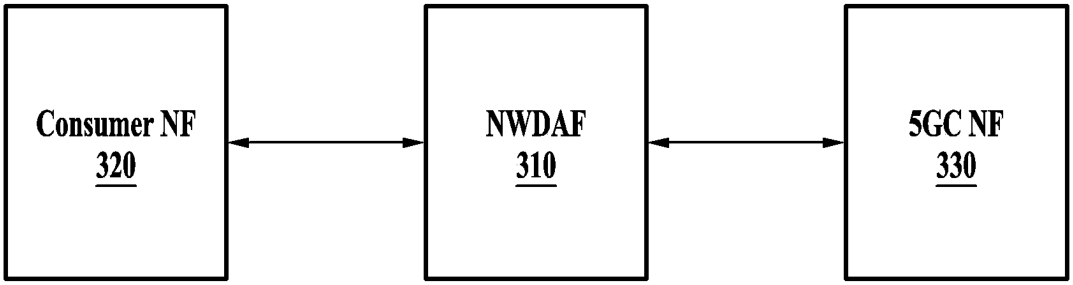

Consumer NF
320
NWDAF
310
5GC NF
330

FIG. 3

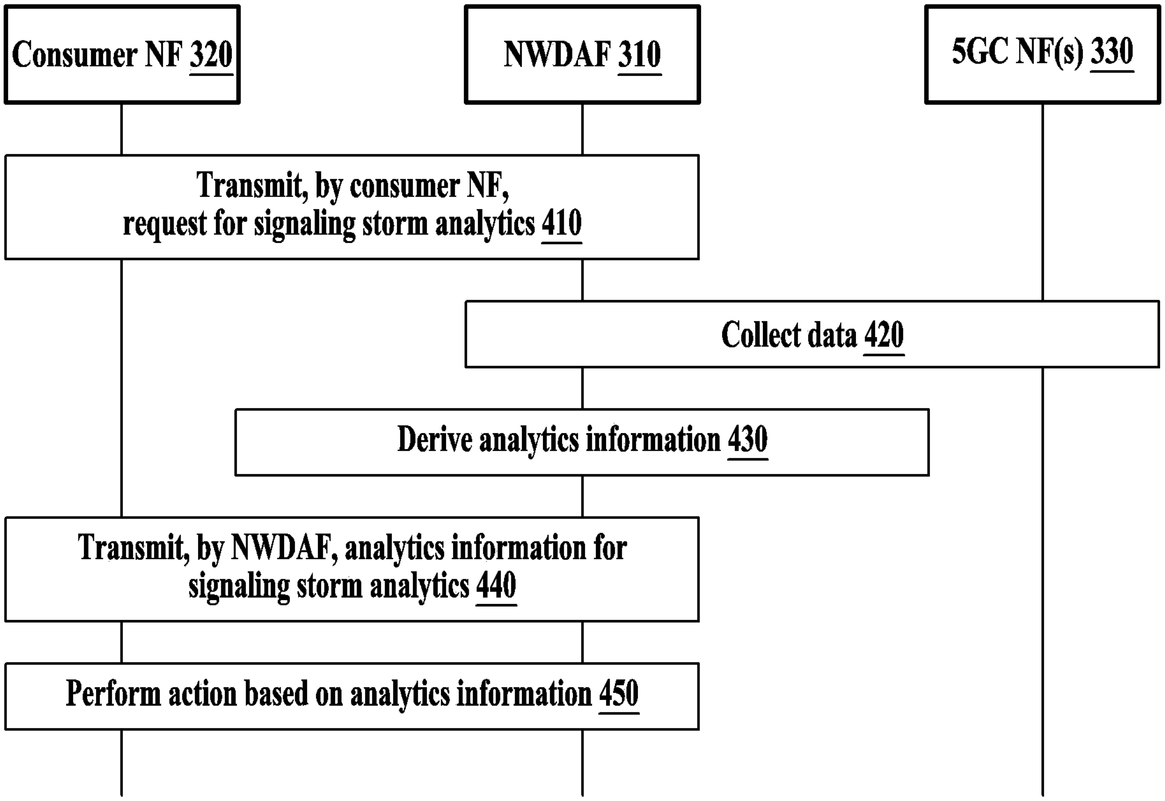

Consumer NF 320
NWDAF 310
5GC NF(s) 330
Transmit, by consumer NF, request for signaling storm analytics 410
Collect data 420
Derive analytics information 430
Transmit, by NWDAF, analytics information for signaling storm analytics 440
Perform action based on analytics information 450

FIG. 4

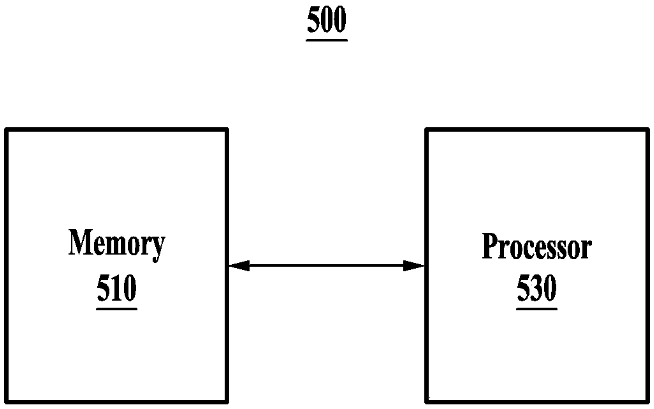

500
Memory 510
Processor 530

FIG. 5

METHOD OF MANAGING ABNORMAL NETWORK BEHAVIOR AND DEVICE FOR PERFORMING THE SAME

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of Korean Patent Application No. 10-2024-0022916 filed on Feb. 16, 2024, Korean Patent Application No. 10-2024-0118083 filed on Aug. 30, 2024, Korean Patent Application No. 10-2024-0146031 filed on Oct. 23, 2024, and Korean Patent Application No. 10-2024-0165164 filed on Nov. 19, 2024, in the Korean Intellectual Property Office, the entire disclosures of which are incorporated herein by reference for all purposes.

BACKGROUND

1. Field of the Invention

[0002] One or more embodiments relate to a method of managing an abnormal network behavior and a device for performing the same.

2. Description of the Related Art

[0003] A fifth-generation (5G) mobile communication system defined an NWDAF, which is a network function that analyzes and provides data collected from 5G networks.

[0004] For automation and optimization of the 5G mobile communication system, NWDAF collects raw data of each network function and application function, converts the raw data into big data, and processes the big data to provide network analytics information.

[0005] Sixth generation (6G) aims to encompass Internet of Things (IoT) devices in a massive mobile communication system. The 5G/6G system needs to manage IoT devices that are much more than the number of existing terminals and thus, requires congestion control management technology.

[0006] The above description is information the inventor (s) acquired during the course of conceiving the present disclosure, or already possessed at the time, and is not necessarily art publicly known before the present application was filed.

SUMMARY

[0007] To encompass massive devices in a mobile communication system, an improved dynamic congestion control to analyze and predict communication patterns of terminals is required.

[0008] An embodiment may provide congestion control technology for considering a communication pattern and guaranteeing transmission for massive IoT devices in a mobile communication system.

[0009] An embodiment may provide technology for managing an abnormal network behavior.

[0010] However, the technical goals are not limited to those described above, and other technical goals may be present.

[0011] According to an aspect, there is provided a method of managing an abnormal network behavior, the method including receiving a request for analytics of a signaling storm being an abnormal network behavior from a consumer network function (NF), collecting data for the analytics of the signaling storm from a fifth-generation core (5GC) NF, generating analytics information about the signaling storm based on the collected data, and transmitting the analytics information to the consumer NF, wherein the request may include analytic filter information including an instance identification (ID) of a target NF that analytics of the signaling storm is to be provided for.

[0012] The request may include analytics reporting information including a signaling number threshold and a user equipment (UE) number threshold, and the signaling number threshold may indicate the number of signalings received within a time period.

[0013] The data may include UE-related context data, and the UE-related context data may include information regarding a number of session reports received from a user plane function (UPF), and the number of session reports received from the UPF may be a number of session reports received from the UPF triggered by a downlink (DL) packet if a PDU session is in a 5G CM (connection management)-idle state.

[0014] The data may include NF context data, the NF context data may include NF load status information, and the NF load status information may indicate a current load of an NF and an NF service.

[0015] The data may include NF feature data; and the NF feature data may include load information of a connected UPF.

[0016] The data may include application function (AF) data indicating application activation time information, and the AF data may include information regarding an application ID, user activation time information, a number of UEs, an active time, an inactive time, and a UE ID type.

[0017] According to an aspect, there is provided a server device for managing an abnormal network behavior, the server device including a processor, and a memory electrically connected to the processor and configured to store instructions executable by the processor, wherein the instructions, when executed by the processor, may cause the server device to perform a plurality of operations, the plurality of operations including receiving a request for analytics of a signaling storm being an abnormal network behavior from a consumer NF, collecting data for the analytics of the signaling storm from a 5GC NF, generating analytics information about the signaling storm based on the collected data, and transmitting the analytics information to the consumer NF, wherein the request may include analytic filter information including an instance ID of a target NF that analytics of the signaling storm is to be provided for.

[0018] The request may include analytics reporting information including a signaling number threshold and a UE number threshold, and the signaling number threshold may indicate the number of signalings received within a time period.

[0019] The data may include UE-related context data, and the UE-related context data may include information regarding a number of session reports received from a UPF, and the number of session reports received from the UPF may be a number of session reports received from the UPF triggered by a DL packet if a PDU session is in a 5G CM (connection management)-idle state.

[0020] The data may include NF context data, the NF context data may include NF load status information, and the NF load status information may indicate a current load of an NF and an NF service.

[0021] The data may include NF feature data; and the NF feature data may include load information of a connected UPF.

[0022] The data may include AF data indicating application activation time information, and the AF data may include information regarding an application ID, user activation time information, a number of UEs, an active time, an inactive time, and a UE ID type.

[0023] Additional aspects of embodiments 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 disclosure.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] These and/or other aspects, features, and advantages of the invention will become apparent and more readily appreciated from the following description of embodiments, taken in conjunction with the accompanying drawings of which:

[0025] FIG. **1** illustrates a network system according to an embodiment;

[0026] FIG. **2** is a diagram illustrating network data analytics according to an embodiment;

[0027] FIG. **3** is a diagram illustrating an abnormal network behavior analytics process according to an embodiment;

[0028] FIG. **4** is a flowchart illustrating a method of controlling an abnormal network behavior according to an embodiment; and

[0029] FIG. **5** is a schematic block diagram of a device for performing an NWDAF according to an embodiment.

DETAILED DESCRIPTION

[0030] The following structural or functional description is provided as an example only and various alterations and modifications may be made to the embodiments. Here, the embodiments are not construed as limited to the disclosure and should be understood to include all changes, equivalents, and replacements within the idea and the technical scope of the disclosure.

[0031] Although terms of "first," "second," and the like are used to explain various components, the components are not limited to such terms. These terms are used only to distinguish one component from another component. For example, a first component may be referred to as a second component, or similarly, the second component may be referred to as the first component within the scope of the present disclosure.

[0032] When it is mentioned that one component is "connected" or "accessed" to another component, it may be understood that the one component is directly connected or accessed to another component or that still other component is interposed between the two components.

[0033] The singular forms "a", "an", and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. As used herein, "A or B," "at least one of A and B," "at least one of A or B," "A, B or C," "at least one of A, B and C," and "at least one of A, B, or C," each of which may include any one of the items listed together in the corresponding one of the phrases, or all possible combinations thereof. It will be further understood that the terms "comprises/comprising" and/or "includes/including" when used herein, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components and/or groups thereof.

[0034] Unless otherwise defined, all terms used herein including technical or scientific terms have the same meaning as commonly understood by one of ordinary skill in the art to which examples belong. It will be further understood that terms, such as those defined in commonly-used dictionaries, should be interpreted as having a meaning that is consistent with their meaning in the context of the relevant art and will not be interpreted in an idealized or overly formal sense unless expressly so defined herein.

[0035] As used in connection with the present disclosure, the term "module" may include a unit implemented in hardware, software, or firmware, and may interchangeably be used with other terms, for example, "logic," "logic block," "part," or "circuitry". A module may be a single integral component, or a minimum unit or part thereof, adapted to perform one or more functions. For example, according to an embodiment, the module may be implemented in a form of an application-specific integrated circuit (ASIC).

[0036] The term "unit" or the like used herein may refer to a software or hardware component, such as a field-programmable gate array (FPGA) or an application-specific integrated circuit (ASIC), and the "unit" performs predefined functions. However, the term "unit" is not limited to software or hardware. A "unit" may be configured to be in an addressable storage medium or configured to operate one or more processors. Accordingly, the "unit" may include, for example, components, such as software components, object-oriented software components, class components, and task components, processes, functions, attributes, procedures, sub-routines, segments of program code, drivers, firmware, microcode, circuitry, data, databases, data structures, tables, arrays, and variables. The functionalities provided in the components and "units" may be combined into fewer components and "units" or may be further separated into additional components and "units." Furthermore, the components and "units" may be implemented to operate on one or more central processing units (CPUs) within a device or a security multimedia card. In addition, "unit" may include one or more processors.

[0037] Hereinafter, embodiments will be described in detail with reference to the accompanying drawings. When describing the embodiments with reference to the accompanying drawings, like reference numerals refer to like components, and any repeated description related thereto will be omitted.

[0038] Terms used herein to identify a connection node, to indicate network entities, to indicate messages, to indicate an interface among network entities, to indicate various pieces of identification information are examples for ease of description. Thus, terms are not limited to terms described later in this disclosure and other terms referring to a subject having the equivalent technical meaning may be used.

[0039] Herein, for ease of description, of the currently existing communication standards, terms and names defined by long-term evolution (LTE) and new radio (NR) standards, which are the latest standards defined by the third-generation partnership project (3GPP) association, are used. However, embodiments described hereinafter are not limited to the terms and names and a system in compliance with other standards may be applicable in the same manner.

[0040] FIG. **1** illustrates a network system according to an embodiment.

[0041] Referring to FIG. **1**, according to an embodiment, a network system **10** (e.g., a fifth-generation (5G) network system, a sixth-generation (6G) network system, or a 5G/6G network system) may include a plurality of entities **100** to **190**. A user equipment (UE) (or a user terminal) **100** may access a 5D core network through a radio access network (RAN) **110**. The RAN **110** may be a base station that provides a wireless communication function to the UE **100**. An operation, administration, and maintenance (OAM) **190** may be a system for managing terminals and networks.

[0042] The unit performed by each function provided by the network system **10** may be defined as a network function (NF). The NF may include an access and mobility management function (AMF) **120**, a session management function (SMF) **130**, a user plane function (UPF) **140**, an application function (AF) **150**, a policy control function (PCF) **160**, a network repository function (NRF) **170**, a network exposure function (NEF) **175**, a management data analytics function (MDAF) **177**, a network data analytics function (NWDAF) **180**, a data collection coordination function (DCCF) **185**, an analytics data repository function (ADRF) **187**, and a unified data management (UDM) **189**. The AMF **120** may manage network access and mobility of a terminal, the SMF **130** may perform a session-related function, the UPF **140** may manage transfer of user data, and the AF **150** may perform a role to communication with a fifth-generation core (5GC) to provide an application service. The PCF **160** may manage a policy, and the NRF **170** may manage a function to store state information of NFs and process a request for finding an NF that other NFs can access.

[0043] The NWDAF **180** may analyze data collected from a network (e.g., a 5G network) and provide analytics results to support network automation. The NWDAF **180** may collect/store/analyze information from a network. The NWDAF **180** may collect information from the OAM **190**, an NF forming the network (e.g., the AMF **120**, the SMF **130**, the UPF **140**, the PCF **160**, the NRF **170**, the NEF **175**, the MDAF **177**, the DCCF **185**, the ADRF **187**, and/or the UDM **189**), a UE, or the AF **150**. The NWDAF **180** may provide the analytics results to an unspecified NF (e.g., the AMF **120**, the SMF **130**, the UPF **140**, the PCF **160**, the NRF **170**, the NEF **175**, the MDAF **177**, the DCCF **185**, the ADRF **187**, and/or the UDM **189**), the OAM **190**, the UE, or the AF **150**. The analytics results may be used independently by each NF (e.g., the AMF **120**, the SMF **130**, the UPF **140**, the PCF **160**, the NRF **170**, the NEF **175**, the MDAF **177**, the DCCF **185**, the ADRF **187**, and/or the UDM **189**), the OAM **190**, the UE, or the AF **150**.

[0044] FIG. **2** is a diagram illustrating network data analytics according to an embodiment. An NWDAF **210** (e.g., the NWDAF **180** of FIG. **1**) may provide NWDAF services to an NF **230**. The NWDAF services may include services such as analytics information subscription (Nnwdaf_AnalyticsSubscription), analytics information request (Nnwdaf_AnalyticsInfo), data management (Nnwdaf_DataManagement), machine learning (ML) model provisioning (Nnwdaf_MLModelProvision), ML model information request (Nnwdaf_MLModelInfo), ML model monitor (Nnwdaf_MLModelMonitor), ML model training (Nnwdaf_MLModelTraining), ML model training information request (Nnwdaf_MLModelTrainingInfo), roaming user analytics (Nnwdaf_RoamingAnalytics), and roaming data management (Nnwdaf_RoamingData). The NWDAF services provided by the NWDAF **210** may be as in Table 1.

TABLE 1

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnwdaf_AnalyticsSubscription	Subscribe	Subscribe/Notify	PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF
	Unsubscribe		PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF
	Notify		PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF, MFAF
	Transfer	Request/Response	NWDAF
Nnwdaf_AnalyticsInfo	Request	Request/Response	PCF, NSSF, AMF, SMF, NEF, AF, OAM, CEF, NWDAF, DCCF
	ContextTransfer	Request/Response	NWDAF
Nnwdaf_DataManagement	Subscribe	Subscribe/Notify	NWDAF, DCCF
	Notify		NWDAF, DCCF, MFAF, ADRF
	Fetch	Request/Response	NWDAF, DCCF, MFAF, ADRF
Nnwdaf_MLModelProvision	Subscribe	Subscribe/Notify	NWDAF
	Unsubscribe		NWDAF
	Notify		NWDAF
Nnwdaf_MLModelInfo	Request	Request/Response	NWDAF
Nnwdaf_MLModelMonitor	Subscribe	Subscribe/Notify	NWDAF
	Unsubscribe		NWDAF
	Notify		NWDAF
	Register	Request/Response	NWDAF
	Request		NWDAF
Nnwdaf_MLModelTraining	Subscribe	Subscribe/Notify	NWDAF
	Unsubscribe		NWDAF
	Notify		NWDAF

TABLE 1-continued

Service Name	Service Operations	Operation Semantics	Example Consumer(s)
Nnwdaf__MLModelTrainingInfo	Request	Request/Response	NWDAF
Nnwdaf__RoamingAnalytics	Subscribe	Subscribe/Notify	H-NWDAF, V-NWDAF
	Unsubscribe		H-NWDAF, V-NWDAF
	Notify		H-NWDAF, V-NWDAF
	Request	Request/Response	H-NWDAF, V-NWDAF
Nnwdaf__RoamingData	Subscribe	Subscribe/Notify	H-NWDAF, V-NWDAF
	Unsubscribe		H-NWDAF, V-NWDAF
	Notify		H-NWDAF, V-NWDAF

NOTE 1:
How OAM consumes Nnwdaf services and which Analytics information is relevant is defined in TS 28.550 [7] Annex H and out of the scope of this TS.
NOTE 2:
How CEF consumes Nnwdaf services and which Analytics information is relevant is defined in TS 28.201 [21] and out of the scope of this TS.)
NOTE 3:
The Nnwdaf__MLModelProvision service and the Nnwdaf__MLModelInfo service are provided by an NWDAF containing MTLF and consumed by an NWDAF containing AnLF.

[0045] The NWDAF **210** may perform analytics in response to a request from the NF **230**, and provide analytics information (e.g., analytics results) to the NF **230**. The NWDAF **210** may provide the analytics information according to the services described in Table 1, as in Table 2.

TABLE 2

Analytics Information	Request Description	Response Description
Slice Load level information	Analytics ID: load level information	Load level provided as number of UE registrations and number of PDU sessions for a Network Slice and Network Slice instances as well as resource utilization for Network Slice instances.
Observed Service experience information	Analytics ID: Service Experience	Observed Service experience statistics or predictions may be provided for a Network Slice or an Application. They may be derived from an individual UE, a group of UEs or any UE. For slice service experience, they may be derived from an application, a set of Applications or all Applications on the Network Slice.
NF Load information	Analytics ID: NF load information	Load statistics or predictions information for specific NF(s).
Network Performance information	Analytics ID: Network Performance	Statistics or predictions on the load in an Area of Interest; in addition, statistics or predictions on the number of UEs that are located in that Area of Interest.
UE mobility information	Analytics ID: UE Mobility	Statistics or predictions on UE mobility. When visited AOI(s) is included in the Analytics Filter information, only statistics on UE mobility can be provided.
UE Communication information	Analytics ID: UE Communication	Statistics or predictions on UE communication.
Expected UE behavioral parameters	Analytics ID: UE Mobility and/or UE Communication	Analytics on UE Mobility and/or UE Communication.
UE Abnormal behavior information	Analytics ID: Abnormal behavior	List of observed or expected exceptions, with Exception ID, Exception Level and other information, depending on the observed or expected exceptions.
E2E data volume transfer time	Analytics ID: E2E data volume transfer time	Analytics on E2E data volume transfer time.
User Data Congestion information	Analytics ID: User Data Congestion	Statistics or predictions on the user data congestion for transfer over the user plane, for transfer over the control plane, or for both.
QoS Sustainability	Analytics ID: QoS Sustainability	For statistics, the information on the location and the time for the QoS change and the threshold(s) that were crossed; or, for predictions, the information on the location and the time when a potential QoS change may occur and what threshold(s) may be crossed.

TABLE 2-continued

Analytics Information	Request Description	Response Description
Session Management Congestion Control Experience	Analytics ID: Session Management Congestion Control Experience	Statistics on session management congestion control experience for specific DNN and/or S-NSSAI.
Redundant Transmission Experience	Analytics ID: Redundant Transmission Experience	Statistics or predictions aimed at supporting redundant transmission decisions for URLLC services.
WLAN performance	Analytics ID: WLAN performance	Statistics or predictions on WLAN performance of UE.
Dispersion	Analytics ID: UE Dispersion	Statistics or predictions that identify the location (i.e. areas of interest) or network slice(s) where a UE, or a group of UEs disperse their data volume, or disperse mobility or session management transactions or both.
DN Performance	Analytics ID: DN Performance	Statistics or predictions on user plane performance for a specific Edge Computing application.
PFD Determination	Analytics ID: PFD Determination	Statistics on PFD information for a known application identifier(s).
Movement Behavior	Analytics ID: Movement Behavior	Statistics or predictions on movement behavior for an applicable area
Signaling Storm	Analytics ID: Signaling storm	Statistics or predictions on controlling signaling storm for network abnormal behavior mitigation or prevention.

[0046] For example, the NWDAF **210** may analyze “signaling storm” in response to a request from the NF **230** (e.g., analytics regarding Analytics ID=“signaling storm”), and provide the NF **230** with statistics or predictions regarding control of the signaling storm to mitigate or prevent a network abnormal behavior as analytics information.

[0047] Hereinafter, among the services of Table 1, the analytics information subscription service (Nnwdaf_AnalyticsSubscription service) and the analytics information request service (Nnwdaf_AnalyticsInfo service) are described in detail.

[0048] The NWDAF **210** (e.g., the NWDAF **180** of FIG. **1**) may provide the analytics information subscription service (Nnwdaf_AnalyticsSubscription service) to the NF **230**. The analytics information subscription service may enable subscription and unsubscription of network data analytics information (or network data analytics results) generated by the NWDAF **210**. The analytics information subscription service may receive network analytics information (or network analytics results) periodically according to the need of a network function of the NF **230** subscribing to the service or receive analytics information (or analytics results) if a predetermined condition is satisfied. The analytics information subscription service may be provided through three operations of subscription, unsubscription, and notification.

[0049] The subscription operation (Nnwdaf_Anlaytics-Subscription_Subscribe operation) may include a required input and/or an optional input. The required input may include single network slice selection assistance information (S-NSSAI), an event identifier or analytics ID (or analytics information ID), a notification target address, and event reporting information. The optional input may include information additionally required to process the analytics information. For example, the optional input may include an event filter or an analytics filter (or an analytics information filter). Of course, the embodiments are not limited to the above examples.

[0050] In the unsubscription operation (Nnwdaf_AnlayticsSubscription_Unsubscribe operation), the NF **230** may transmit the subscription identifier information to the NWDAF **180**, and the NWDAF **210** may transmit, as output, a message informing that unsubscription has been confirmed, to the NF **230** that requested unsubscription.

[0051] In the notification operation (Nnwdaf_Anlaytics-Subscription_Notify operation), the NWDAF **210** may notify the NF **230** successfully subscribing to the analytics information subscription service of designated network data analytics information (or network data analytics results) periodically or when a predetermined condition is satisfied. The notification operation may include an event identifier or analytics ID (or analytics information ID), and a notification target address.

[0052] The NWDAF **210** may provide the analytics information request service (Nnwdaf_AnalyticsInfo service) to the NF **230**. The analytics information request service, unlike the analytics information subscription service, may be a service for the NF **230** to request analytics regarding predetermined information and receive result values immediately when the request is completed. The operation of the analytics information request service may include a request and a response. The NF **230** requesting analytics information may transmit an analytics information request message (e.g., Nnwdaf_AnalyticsInfo_Request service operation) to the NWDAF **180**.

[0053] The NWDAF **210** may transmit the analytics information to each NF **230** requesting the analytics information. The analytics information may be used to optimize the performance of an operation (or a network function) performed by each NF **230** (e.g., congestion control, Quality of Service (QOS) management, traffic control, mobility management, load dispersion, or terminal power control).

[0054] The NF **230** (e.g., the UE **100**, the RAN **110**, the AMF **120**, the SMF **130**, the UPF **140**, the AF **150**, the PCF **160**, the NRF **170**, the NEF **175**, the MDAF **177**, the DCCF **185**, the ADRF **187**, and/or the OAM **190** of FIG. **1**) may become a consumer NF requesting analytics results from the NWDAF **210**. Each NF **230** may become a service consumer NF of the network data analytics service. The NWDAF **210**

may collect data from each NF **230** and analyze the data to generate the analytics information requested by the consumer NF. The NWDAF **210** may transmit the analytics information to the consumer NF transmitting the analytics request. Accordingly, the NWDAF **210** may become a provider NF of the analytics results requested by the consumer NF. The NWDAF **210** may become a service provider NF that provides the analytics information requested by the service consumer NF.

[0055] The NWDAF **210** may include one or more of an analytics logical function (AnLF) and a model training logical function (MTLF). The NWDAF **210** may include either the MTLF or the AnLF or may support both.

[0056] An NWDAF (e.g., the NWDAF **210**) including the AnLF may perform inference and derive analytics information (e.g., derive statistics and/or predictions according to an analytics consumer request). The NWDAF including the AnLF may expose an analytics service for network data (e.g., Nnwdaf_AnalyticsSubscription or Nnwdaf_AnalyticsInfo).

[0057] An NWDAF (e.g., the NWDAF **210**) including the MTLF may train an ML model, and expose a new training service (e.g., provide the initial version that is not trained or a trained model).

[0058] FIG. **3** is a diagram illustrating an abnormal network behavior analytics process according to an embodiment.

[0059] An NWDAF **310** (e.g., the NWDAF **180** of FIG. **1** or the NWDAF **210** of FIG. **2**) may support analytics for mitigation and prevention of a network abnormal behavior (e.g., a signaling storm). The NWDAF **310** may support signaling storm analytics. In signaling storm analytics, the NWDAF **310** may provide analytics information (e.g., statistics and/or predictions) regarding an expected normal level of signaling and deviations (e.g., significant deviations) indicating a signaling storm. The NWDAF **310** may identify whether the signaling storm is due to signaling from an NF or signaling (e.g., massive signaling) from a UE based on requested analytics ID.

[0060] A consumer NF **320** (e.g., the NF **230** of FIG. **2**) may transmit a request for signaling storm analytics. The consumer NF **320** may include one or more of the UE **100**, the RAN **110**, the AMF **120**, the SMF **130**, the UPF **140**, the AF **150**, the PCF **160**, the NRF **170**, the NEF **175**, the MDAF **177**, the DCCF **185**, the ADRF **187**, and/or the OAM **190** of FIG. **1**.

[0061] The consumer NF **320** may trigger the signaling storm analytics based on a trigger condition. That is, the consumer NF **320** may transmit a request for signaling storm analytics to the NWDAF **310**. For example, the consumer NF **320** may subscribe to NF load analytics from the NWDAF **310**, and trigger the signaling storm analytics based on the output (or analytics information) of the NF load analytics (e.g., CPU usage of 80% or more). In addition, the consumer NF **320** may subscribe to "abnormal behavior" analytics from the NWDAF **310**, and trigger the signaling storm analytics based on output of the abnormal behavior analytics (e.g., suspicion of DDOS attack). Further, the consumer NF **320** may subscribe to "dispersion (or dispersion analytics)" analytics from the NWDAF **310**, and trigger the signaling storm analytics according to the results of the dispersion analytics (e.g., when the transaction dispersion exceeds an expected transaction dispersion configurable threshold).

[0062] The NWDAF **310** may receive a request for signaling storm analytics from the consumer NF **320** (e.g., the NF **230** of FIG. **2**). The request for signaling storm analytics may be analytics information subscription (Nnwdaf_AnalyticsSubscription) or analytics information request (Nnwdaf_AnalyticsInfo). The consumer NF **320** may include the following parameters in the analytics information subscription (Nnwdaf_AnalyticsSubscription) or the analytics information request (Nnwdaf_AnalyticsInfo):

[0063] (1) Analytics ID="signaling storm";

[0064] (2) Target of Analytics Reporting: a list of NFs or one or more UE group IDs (e.g., only if reporting of a signaling storm caused by UEs is desired);

[0065] (3) Target Incident ID(s) (e.g., a signaling storm caused by UEs, a signaling storm caused by an NF, or both);

[0066] (4) Analytics Filter Information:

[0067] i) NF ID list: instance IDs or NF set IDs of target NF that signaling storm analytics is to be provided for;

[0068] ii) Area of Interest (AOI) and/or S-NSSAI which restricts the scope of signaling storm analytic to a specific area and/or slice;

[0069] (5) Expected Report Time: indicates the time limit by which analytics results need to be received (e.g., 10 seconds, 5 minutes, etc.);

[0070] (6) Analytics target period indicates the time period over which the statistics or predictions are requested;

[0071] (7) Optionally, preferred level of accuracy of the analytics;

[0072] (8) Analytics Reporting Information:

[0073] i) Reporting threshold and filter:

[0074] Signaling number threshold: indicates the number of the received signalings within the time period.

[0075] ii) UE number threshold: indicates a threshold of the number of UEs of which the number of one type of request messages meets the frequency of UE requests threshold. For example, if the number of UEs that initiate registration requests exceeds the threshold (e.g., 10 times per hour) and the number of such UEs (i.e., the number of UEs that initiate registration requests) exceeds "100" (e.g., the threshold is preset to "100"), the NWDAF may provide the analytics.

[0076] The NWDAF **310** may collect data for signaling storm analytics from a 5GC NF **330**. The 5GC NF **330** may include one or more of the UE **100**, the RAN **110**, the AMF **120**, the SMF **130**, the UPF **140**, the AF **150**, the PCF **160**, the NRF **170**, the NEF **175**, the MDAF **177**, the DCCF **185**, the ADRF **187**, and/or the OAM **190** of FIG. **1**.

[0077] For example, the NWDAF **310** may collect one or more of UE-related context data (e.g., signaling feature data), NF context, NF feature data, AF data (e.g., application activation time information), OAM data, and/or MDAF data. In addition, the NWDAF may collect UE behavioral information per UE group.

[0078] The collection of UE-related context data may be as in Table 3. The UE-related context data may include information (e.g., parameters) listed in Table 3.

TABLE 3

Information	Source	Description
UE ID		Identifies a single UE
Signaling feature data		NF procedures containing signaling exchange information related to a particular UE or session from the Connection, Registration, Mobility and Session Managements procedures. (NOTE 1)
>Request type and number from UE/RAN (0 . . . max)	AMF	Type and number of requests for N1 or N2 interface and number of requests, such as received Initial Registration Request, Mobility and Periodic Registration Request, Service Request, etc.
>>Time duration from receiving request from UE/RAN to response to UE/RAN	AMF	Time duration between the request from UE/RAN and response to UE/RAN.
>>Number of successful responses of UE/RAN	AMF	Number of successful responses associated to their initial requests, such as Registration Response, etc.
>>Number of failed responses of UE/RAN	AMF	Number of failed responses associated to their initial requests, such as Registration Reject, Service Reject, etc.
>>Reason of failed responses of UE/RAN	AMF	Reasons of failed responses associated to their initial requests, e.g. reject, no-response, etc.
>>A posterior Type of requests of UE/RAN (0 . . . max)	AMF	A posterior Request types triggered from UE/RAN, for NF Service request, or request to UE/RAN.
>Request type and number from NF (0 . . . max)	NF, SCP	Request type received from NF, e.g. Namf_N1N2Trans, Namf_comm, etc., as well as the number of requests received from NF, e.g. Namf_N1N2Trans, Namf_comm, etc.
>>Time duration from receiving request from NF to response to NF	NF, SCP	Time duration between the request from NF and response to NF.
>>Number of successful responses of NF	NF, SCP	Number of successful responses associated to their initial requests.
>>Number of failed responses of NF	NF, SCP	Number of failed responses associated to their initial requests.
>>Reason of failed responses of NF	NF, SCP	Reasons of failed responses associated to their initial requests, e.g. reject, no-response, etc.
>>Number of redundant signaling of NF	NF, SCP	Number of received redundant signaling. The redundant signaling means the signaling which is transmitted in multiple times.
>>A posterior Type of requests of NF (0 . . . max)	NF, SCP	A posterior Request types triggered from NF, for NF Service request.
>Public Warning information	AMF	Public Warning information as defined in the TS 23.041[X], such as WRITE-REPLACE WARNING REQUEST, etc.
>Frequent Mobility Registration Update	AMF	The number of Mobility Registration Updates N within a period M may be an indication for abnormal ping-pong behavior, where N and M are operator's configurable parameters.
>Number of receiving Session Report from UPFs	SMF	Number of receive Session Report from UPF triggered by DL packet in case of PDU Session is in 5G CM(connection management)-idle state.
UE Context in NF		
>state transition information(State transition information)	AMF, SMF	UE related state transition information such as transition type, frequency of CM state changes etc. State transition identifier): "Access Type change to 3GPP access"; "Access Type change to non-3GPP access"; "RM state change to RM-DEREGISTERED"; "RM state change to RM-REGISTERED"; "CM state change to CM-IDLE"; "CM state change to CM-CONNECTED"; "Handover"; or "Mobility Registration Update". "Frequent Mobility Registration Update"(table 6.7.2.2-1) Or, PDU Session related state transition information such as transition type, frequency SM state changes, etc. State transition identifier: "PDU Session Establishment"; "PDU Session Release"; "Communication failure"; or "PLMN change".

TABLE 3-continued

Information	Source	Description
		It can be reported for a group of UEs (e.g., the number of total transitions or percentage of the group UEs who have transitions).
>timer information	AMF, SMF	Timer information which has been set for the UE (e.g., timer type, duration.)

(NOTE 1):

NWDAF can optionally provide transaction dispersion analytic information for MM and SM transactions.

NOTE 2:

MM in NOTE 1 can be obtained from Namf_EventExposure service:

Total number of Mobility Management transactions:

The Total number of Mobility Management transactions is used to collect the number of MM transactions of a SUPI or Internal Group ID, for example Dispersion Analytics as specified in TS 23.288 [50]. The Total number of transactions is incremented when the NAS signalling transactions from Authentication, Registration, De-Registration, Service Request and UE Configuration Update procedures is completed. Only the periodic reporting mode applies.

NOTE 3:

SM in NOTE 1 can be obtained from Nsmf_EventExposure Service:

Total number of Session Management transactions

The total number of Session Management transaction is used to collect the number of SM transactions of a SUPI or Internal Group ID, for example Dispersion Analytics as specified in TS 23.288 [50]. The transaction count is incremented when the NAS transactions from PDU Session Establishment, PDU Session Authentication, PDU Session Modification and PDU Session Release procedures is concluded. Only the periodic reporting mode applies.

[0079] The collection of NF context data may be as in Table 4. The NF context data may include information (e.g., parameters) listed in Table 4.

TABLE 4

Information	Source	Description
NF ID		NF instance ID
>NF profile	NRF	NF Profile information such as allowed NF information for the NF and NF Service(s).
>NF load status information	NRF, OAM	Load information indicates the current load of the NF and NF Service(s), e.g. CPU, memory, and/or percentage of load information.
>Capacity and priority information of NFs and NF Services	NRF, OAM, SCP	Capacity and priority information of the registered NF and NF Service(s).
>NF heart-beat related information	NF	NF heart-beat related information such as responding time, Number of retransmissions, heart-beat intervals.

[0080] The collection of NF feature data may be as in Table 5. The NF feature data may include information (e.g., parameters) listed in Table 5.

TABLE 5

Information	Source	Description
NF ID		NF instance ID
>Usage information of UE IP address resources	SMF	Usage information of UE IP address resources (dynamic and static, V4, V6, etc.) for CP or UP allocation, such as number, usage, number of UE IPs, which prohibit allocation during certain time interval, etc. This parameter is valid for SMF only.
>Load information of connected UPFs	SMF	Load information of connected UPFs such as using PFCP Load Control Information. This parameter is valid for SMF only.
SCP Signaling statistics	SCP	The number of different types of signaling received and sent by SCP during a target time period, etc. This parameter is valid for SCP only.

[0081] The collection of AF data may be as in Table 6. The AF data may be application activation time information, and includes information (e.g., parameters) listed in Table 6.

TABLE 6

Information	Source	Description
Application ID	AF	Identifies the application providing this information.
User activation time information (1 . . . max)	AF	Information of activation time for the users (e.g. IoT users) per application.
>Number of UEs	AF	The total number of UEs
>Active Time	AF	The time stamp of the users per application switch to active, or the start and end time of the users activity per application.
>Inactive Time	AF	The time stamp of the users per application switch to inactive, or the start and end time of the users inactivity per application, if applicable.
>UE ID type	AF	Identifies a group of UEs, e.g. external group ID, or a list of UE IDs.

[0082] The collection of OAM data may be as in Table 7. The NWDAF may collect data from an OAM (e.g., the OAM **190** of FIG. **1**). The OAM data may include information (e.g., parameters) listed in Table 7.

TABLE 7

Information	Source	Description
NRF ID		NRF instance ID
Number of NF service registration requests	OAM	Number of registration request received at the NRF
>Number of successful NF service registrations	OAM	Number of successful registrations
>Number of failed NF service registrations due to encoding error of NF profile	OAM	Number of failed registrations
>Number of failed NF service registrations due to NRF internal error	OAM	Number of failed registrations
>Received time	OAM	Time stamp that the related request is received at the NRF.
Number of NF service update requests	OAM	Number of update request received at the NRF
>Number of successful NF service updates	OAM	Number of successful updates
>Number of failed NF service updates due to encoding error of NF profile	OAM	Number of failed updates
>Number of failed NF service updates due to NRF internal error	OAM	Number of failed updates
>Received time	OAM	Time stamp that the related request is received at the NRF.
Number of NF discovery requests	OAM	Number of discovery request received at the NRF
>Number of successful NF discoveries	OAM	Number of successful discovery attempts
>Number of failed NF service discoveries due to unauthorized NF Service consumer	OAM	Number of failed discovery attempts
>Number of failed NF discoveries due to input errors	OAM	Number of failed discovery attempts
>Number of failed NF discoveries due to NRF internal error	OAM	Number of failed discovery attempts
>Received time	OAM	Time stamp that the related request is received at the NRF.

[0083] The collection of MDAF data may be as in Table 8. The NWDAF may collect data from an MDAF (e.g., the MDAF **177** of FIG. **1**) (e.g., MDAS/MDAF) of control plane congestion analytics. The MDAF data may include information (e.g., parameters) listed in Table 8.

TABLE 8

Information	Source	Description
affectedObject	MDAF	Indication of 5GC NFs where congestion issues occurred or potentially may occur.

TABLE 8-continued

Information	Source	Description
cPCongestionIssueID	MDAF	This field holds the ID of the control plane congestion issue which is reported.

[0084] The NWDAF **310** may generate analytics information about the signaling storm based on the collected data, and provide the analytics information (e.g., signaling storm statistics and/or signaling storm predictions) to the consumer NF **320**.

[0085] An example of output of the analytics information from the NWDAF **310** may be signaling storm statistics. The signaling storm statistics may be as in Table 9.

TABLE 9

Information	Description
Report (1 . . . max)	List of observed signaling storm statistics.
>Target NF ID	A list of impacted NFs of signaling storm detected by NWDAF.
>Cause of the signaling storm	The potential cause of NF Abnormality (i.e. massive signaling from UE or NF abnormal signaling).
>Source UE/NF	Group of the UE(s) identified as slice ID or internal group ID or NF(s) identified as NF list which cause the signaling storm.
>(OPTIONAL) signaling information	The statistics of signaling information.
>>Received Signaling Analytics	Information of signaling received by the target NF(s).
>>>Total number of received signaling	Indicates the statistics on the number of signaling messages received by the target NF(s) in the time slot.
>>>Growth rate of received signaling	Difference between the number of signaling messages received by the NF in the time slot and the number of signaling messages received by the target NF(s) in the previous time slot.
>>>Signaling analytics of UE	Indicates the statistics on the number of signaling messages received from UEs within the time slot. NOTE 1
>(OPTIONAL) Timer List	The list of timer information per source UE(s). NOTE 1
>>Type of timer	The type of timer which has been set.
>>Timer duration	The timer duration that has be selected for the source UE(s).

NOTE 1:
Only available when Cause of signaling storm is massive signaling from UEs, and there exists Source UE(s).

[0086] Another example of output of the analytics information from the NWDAF **310** may be signaling storm predictions. The signaling storm predictions may be as in Table 10.

TABLE 10

Information	Description
(Report (1 . . . max)	List of predicted signaling storm analytics.
>Target NF ID	A list of impacted NFs signaling storm predicted by NWDAF.
>Cause of the signaling storm	The potential cause of NF Abnormality (i.e. massive signaling from UE or NF abnormal signaling).
>Source UE/NF	Group of the UE(s) identified as slice ID or internal group ID or NF(s) identified as NF list which cause the signaling storm.
>(OPTIONAL) signaling information	The predicted of signaling information.
>>Reference Point	The information of the reference point impacted.
>>Service Operation(s)	The information of the service operation(s) impacted.
>>Received Signaling Analytics	Information of signaling received by the target NF(s).
>>>Received number of signaling	Received number of signaling of the specific signaling type.
>>>Growth rate of received signaling	Difference between the number of signaling messages received by the NF in the time slot and the number of signaling messages received by the target NF(s) in the previous time slot.
>>>Signaling analytics of UE	Indicates the statistics on the number of signaling messages received from UEs within the time slot. NOTE 1
>(OPTIONAL) Timer List	The list of timer information per Source UE(s). NOTE 1
>>Type of timer	The type of timer.
>>Timer duration	The timer duration that commonly is selected for the Source UE(s).
>Priority	Priority (relative to other NFs of the same type) of candidate NFs as defined in the TS 29.510 [18].
>Capacity	Candidate NF capacity information, expressed as a weight relative to other NF instances of the same type as defined in the TS 29.510 [18].
>Confidence	Confidence of this prediction.

NOTE 1:
Only available when Cause of signaling storm is massive signaling from UEs, and there exists Source UE(s).

[0087] Still another example of output of the analytics information from the NWDAF **310** may include the signaling storm statistics and the signaling storm predictions described above.

[0088] The consumer NF **320** may perform an action (e.g., an operation for mitigation and/or prevention) based on the analytics information (e.g., the signaling storm statistics and/or the signaling storm predictions). The operation for mitigation and/or prevention may be based on the policy/configuration of an operator and NF implementation. Table 11 shows examples of causes of the signaling storm and corresponding actions.

TABLE 11

Cause of the signaling storm	Actions of NFs
Massive signaling from UE	AMF sets MM NAS related timer (e.g. back-off, T3512) with suggested time range for a selected set of UEs.
Massive signaling from UE	SMF sets SM NAS related timer (e.g. back-off) with suggested time range for a selected set of Sessions.
Massive signaling from UE	AMF/SMF sets suggested N1/N2 interface related ingress/egress threshold, or AMF triggers RAN to initiate overload control for a selected set of UEs in specific slice or priority as defined in clause 8.7.7 of TS 38.413 [8] to start overload control.) The AMF may assign an abnormal slice to the UEs and initiate overload control for the specific slice.
NF abnormal signaling	NRF configures the local policy to prevent the source NF with abnormal signaling from being discovered or discovering others.
NF abnormal signaling	Source NF configures to (re)select other NFs instead of NF with abnormal signaling and may unsubscribes the NF with abnormal signaling.
NF abnormal signaling	Source NF configures to deprioritize the NFs/Services with abnormal signaling from being selected.
NF abnormal signaling	Source NF triggers UE Reregistration and/or Session Reestablishments to avoid NF with abnormal signaling.
NF abnormal signaling	SCP blocks or throttles messages originating from an NF/service with abnormal signaling.
NF abnormal signaling	SCP redirects requests towards an NF service producer with abnormal signaling towards another service producer.
NF abnormal signaling	SCP notifies communication peers of an NF with abnormal signaling about abnormal condition, e.g. high load.

[0089] FIG. **4** is a flowchart illustrating a method of controlling an abnormal network behavior according to an embodiment.

[0090] FIG. **4** shows the procedure for supporting mitigation and/or prevention of an abnormal network behavior (e.g., a network signaling storm). The NWDAF **310** may provide analytics information about a signaling storm, thereby supporting mitigation and/or prevention of a signaling storm.

[0091] In operation **410**, the consumer NF **320** (e.g., an MDAF/MDAS) may transmit a request for signaling storm analytics to the NWDAF **310**. The request for signaling storm analytics may include analytics information subscription (Nnwdaf_AnalyticsSubscription) or analytics information request (Nnwdaf_AnalyticsInfo). For example, the consumer NF **320** may subscribe to or transmit a request to analytics information for signaling storm analytics (e.g., statistics and/or predictions for a signaling storm) using an Nnwdaf_AnalyticsSubscription_Subscribe or Nnwdaf_AnalyticsInfo_Request service operation. The analytics information may be NWDAF assistance information.

[0092] The request for signaling storm analytics may include thresholds such as a confidence level and/or accuracy of detection. In addition, the request for signaling storm analytics may include, as analytic filters, an indication of the use case for a signaling storm (e.g. a signaling storm due to UE mobility).

[0093] Analytics ID may be set to "signaling storm analytics". The target for analytics reporting may be set to be any NF or any UE. The analytic filters may be provided as described with reference to FIG. **3**.

[0094] The consumer NF **320** may request a combination of one or more of statistics, predictions, mitigation, and prevention for a given analytics target period.

[0095] The consumer NF **320** may subscribe to "NF load analytics" from the NWDAF **310**, and trigger the signaling storm analytics based on output (or analytics information) of the NF load analytics (e.g., CPU usage of 80% or more). In addition, the consumer NF **320** may subscribe to "abnormal behavior" analytics from the NWDAF **310**, and trigger the signaling storm analytics based on output of the abnormal behavior analytics (e.g., suspicion of DDOS attack). Further, the consumer NF **320** may subscribe to "dispersion (or dispersion analytics)" analytics from the NWDAF **310**, and trigger the signaling storm analytics according to the results of the dispersion analytics (e.g., when the transaction dispersion exceeds an expected transaction dispersion configurable threshold).

[0096] In operation **420**, the NWDAF **310** may collect data (or input data) for signaling storm analytics from the 5GC NF **330**. For example, to collect data for signaling storm analytics, the NWDAF **310** may retrieve the data from the 5GC NF **330** using Nnf_EventExposure_Subscribe.

[0097] The data may include one or more of UE-related context data (e.g., signaling feature data), NF context, NF feature data, AF data (e.g., application activation time information), OAM data, MDAF data, and/or UE behavioral information (e.g., UE behavioral information per UE group).

[0098] The NWDAF may optionally request additional data aligned with an analysis target identified in operation **410**.

[0099] In operation **430**, the NWDAF **310** may derive analytics information for signaling storm analytics based on the request (e.g., the request for signaling storm analytics) from the consumer NF **320** and the collected data. The NWDAF **310** may collect additional data from other NFs including MDAF/MDAS/NWDAF. If the use case of a signaling storm is provided in response to the request for signaling storm analytics in operation **410**, the NWDAF **310** may collect the data from the 5GC NF **330** based on the use case of a signaling storm.

[0100] In operation **440**, the NWDAF may invoke Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response or a response to the consumer NF for the output data analytics. The NWDAF **310** may transmit the analytics information for signaling storm analytics to the consumer NF **320**. To output the analytics information, the NWDAF **310** may invoke the Nnwdaf_AnalyticsSubscription_Notify or Nnwdaf_AnalyticsInfo_Request response or the response to the consumer NF **320**.

[0101] In operation **450**, the consumer NF **320** may perform an action based on the analytics information. Upon receiving the detection and/or prediction and/or mitigation, the consumer NF **320** may perform an action according to the description of Table 11.

[0102] FIG. **5** is a schematic block diagram of a device for performing an NWDAF according to an embodiment.

[0103] Referring to FIG. **5**, according to an embodiment, a device **500** for performing an NWDAF (e.g., a server device) may be substantially the same as the NWDAF (e.g., the NWDAF **180** of FIG. **1**, the NWDAF **210** of FIG. **2**, or the NWDAF **310** of FIG. **3**) described with reference to FIGS. **1** to **4**. The device **500** may include a memory **510**, and a processor **530**.

[0104] The memory **510** may store instructions (e.g., a program) executable by the processor **530**. For example, the instructions may include instructions for executing the operation of the processor **530** and/or the operation of each component of the processor **530**.

[0105] The memory **510** may be implemented as a volatile memory device or a non-volatile memory device. The volatile memory device may be implemented as a dynamic random-access memory (DRAM), a static random-access memory (SRAM), a thyristor RAM (T-RAM), a zero capacitor RAM (Z-RAM), or a twin transistor RAM (TTRAM). The non-volatile memory device may be implemented as an electrically erasable programmable read-only memory (EEPROM), a flash memory, a magnetic RAM (MRAM), a spin-transfer torque (STT)-MRAM, a conductive bridging RAM (CBRAM), a ferroelectric RAM (FeRAM), a phase change RAM (PRAM), a resistive RAM (RRAM), a nanotube RRAM, a polymer RAM (PoRAM), a nano floating gate Memory (NFGM), a holographic memory, a molecular electronic memory device), and/or an insulator resistance change memory.

[0106] The processor **530** may execute computer-readable code (e.g., software) stored in the memory **510** and instructions triggered by the processor **530**. The processor **530** may be a hardware-implemented data processing device having a circuit that is physically structured to execute desired operations. The desired operations may include, for example, code or instructions included in a program. The hardware-implemented data processing device may include, for example, a microprocessor, a central processing unit (CPU), a processor core, a multi-core processor, a multiprocessor, an application-specific integrated circuit (ASIC), and a field-programmable gate array (FPGA).

[0107] The operation performed by the processor **530** may be substantially the same as the operation of the NWDAF (e.g., the NWDAF **180** of FIG. **1**, the NWDAF **210** of FIG. **2**, or the NWDAF **310** of FIG. **3**) described with reference to FIGS. **1** to **4**. Accordingly, a further description thereof will be omitted.

[0108] The components described in the embodiments may be implemented by hardware components including, for example, at least one digital signal processor (DSP), a processor, a controller, an application-specific integrated circuit (ASIC), a programmable logic element, such as a field programmable gate array (FPGA), other electronic devices, or combinations thereof. At least some of the functions or the processes described in the embodiments may be implemented by software, and the software may be recorded on a recording medium. The components, the functions, and the processes described in the embodiments may be implemented by a combination of hardware and software.

[0109] The embodiments described herein may be implemented using hardware components, software components, or a combination thereof. A processing device may be implemented using one or more general-purpose or special purpose computers, such as, for example, a processor, a controller and an arithmetic logic unit, a digital signal processor, a microcomputer, a field programmable array, a programmable logic unit, a microprocessor or any other device capable of responding to and executing instructions in a defined manner. The processing device may run an operating system (OS) and one or more software applications that run on the OS. The processing device also may access, store, manipulate, process, and create data in response to execution of the software. For purpose of simplicity, the description of a processing device is used as singular; however, one skilled in the art will appreciate that a processing device may include multiple processing elements and multiple types of processing elements. For example, a processing device may include multiple processors or a processor and a controller. In addition, different processing configurations are possible, such as parallel processors.

[0110] The software may include a computer program, a piece of code, an instruction, or some combination thereof, to independently or collectively instruct or configure the processing device to operate as desired. Software and data may be embodied permanently or temporarily in any type of machine, component, physical or virtual equipment, computer storage medium or device, or in a propagated signal wave capable of providing instructions or data to or being interpreted by the processing device. The software also may be distributed over network coupled computer systems so that the software is stored and executed in a distributed fashion. The software and data may be stored by one or more non-transitory computer readable recording mediums.

[0111] The method according to the above-described embodiments may be recorded in non-transitory computer-readable media including program instructions to implement various operations which may be performed by a computer. The media may also include, alone or in combination with the program instructions, data files, data structures, and the like. The program instructions recorded on the media may be those specially designed and constructed for the purposes of the embodiments, or they may be of the well-known kind and available to those having skill in the computer software arts. Examples of non-transitory computer-readable media include magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD ROM discs and DVDs; magneto-optical media such as optical discs; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory (ROM), random access memory (RAM), flash memory, and the like. The media may be transfer media such as optical lines, metal lines, or waveguides including a carrier wave for transmitting a signal designating the program command and the data construction. Examples of program instructions include both machine code, such as code produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

[0112] The described hardware devices may be configured to act as one or more software modules in order to perform the operations of the above-described embodiments, or vice versa.

[0113] A number of embodiments have been described above. Nevertheless, it should be understood that various modifications may be made to these embodiments. For example, suitable results may be achieved if the described techniques are performed in a different order, and/or if components in a described system, architecture, device, or circuit are combined in a different manner, and/or replaced or supplemented by other components or their equivalents.

[0114] Therefore, other implementations, other embodiments, and equivalents to the claims are also within the scope of the following claims.

What is claimed is:

1. A method of managing an abnormal network behavior, the method comprising:

receiving a request for analytics of a signaling storm being an abnormal network behavior from a consumer network function (NF);

collecting data for the analytics of the signaling storm from a fifth-generation core (5GC) NF;

generating analytics information about the signaling storm based on the collected data; and

transmitting the analytics information to the consumer NF,

wherein the request comprises analytic filter information comprising an instance identification (ID) of a target NF that analytics of the signaling storm is to be provided for.

2. The method of claim **1**, wherein

the request comprises analytics reporting information comprising a signaling number threshold and a user equipment (UE) number threshold, and

the signaling number threshold indicates the number of signalings received within a time period.

3. The method of claim **1**, wherein

the data comprises UE-related context data, and

the UE-related context data comprises information regarding a number of session reports received from a user plane function (UPF), and

the number of session reports received from the UPF is a number of session reports received from the UPF triggered by a downlink (DL) packet if a PDU session is in a 5G CM (connection management)-idle state.

4. The method of claim **1**, wherein

the data comprises NF context data,

the NF context data comprises NF load status information, and

the NF load status information indicates a current load of an NF and an NF service.

5. The method of claim **1**, wherein

the data comprises NF feature data; and

the NF feature data comprises load information of a connected UPF.

6. The method of claim **1**, wherein

the data comprises application function (AF) data indicating application activation time information, and

the AF data comprises information regarding:

an application ID;

user activation time information;

a number of UEs;

an active time;

an inactive time; and

a UE ID type.

7. A server device for managing an abnormal network behavior, the server device comprising:

a processor; and

a memory electrically connected to the processor and configured to store instructions executable by the processor,

wherein the instructions, when executed by the processor, cause the server device to perform a plurality of operations, the plurality of operations comprising:

receiving a request for analytics of a signaling storm being an abnormal network behavior from a consumer network function (NF);

collecting data for the analytics of the signaling storm from a fifth-generation core (5GC) NF;

generating analytics information about the signaling storm based on the collected data; and

transmitting the analytics information to the consumer NF,

wherein the request comprises analytic filter information comprising an instance identification (ID) of a target NF that analytics of the signaling storm is to be provided for.

8. The server device of claim **7**, wherein

the request comprises analytics reporting information comprising a signaling number threshold and a user equipment (UE) number threshold, and

the signaling number threshold indicates the number of signalings received within a time period.

9. The server device of claim **7**, wherein

the data comprises UE-related context data, and

the UE-related context data comprises information regarding a number of session reports received from a user plane function (UPF), and

the number of session reports received from the UPF is a number of session reports received from the UPF triggered by a downlink (DL) packet if a PDU session is in a 5G CM (connection management)-idle state.

10. The server device of claim **7**, wherein

the data comprises NF context data,

the NF context data comprises NF load status information, and

the NF load status information indicates a current load of an NF and an NF service.

11. The server device of claim **7**, wherein

the data comprises NF feature data; and

the NF feature data comprises load information of a connected UPF.

12. The server device of claim **7**, wherein

the data comprises application function (AF) data indicating application activation time information, and

the AF data comprises information regarding:

an application ID;

user activation time information;

a number of UEs;

an active time;

an inactive time; and

a UE ID type.

* * * * *