**SA WG2 Meeting #S2-162 S2-2405021**

**15 April – 19 April, 2024, Changsha, China (revision of S2-2404511, S2-2402750)**

**Source: SK Telecom, China Mobile, Dish Network, ETRI, KDDI, KPN N.V., Lenovo, LG Uplus, Rakuten Mobile, Samsung, TOYOTA MOTOR CORPORATION, vivo, OPPO**

**Title: KI#4, New Solution: NWDAF-assisted Network Abnormal Behaviour Mitigation and Prevention**

**Document for: Approval**

**Agenda Item: 19.15**

**Work Item / Release: FS\_AIML\_CN /Rel-19**

*Abstract of the contribution: This contribution proposes a new solution for FS\_AIML\_CN KI#4*.

# 1. Discussion

Since Release 15, 5G Core (5GC) has introduced many new features along with an increasing number of network functions based on Service-based Architecture (SBA). With the increasing number of interconnections among various network functions and the Core network being central to 5G System (5GS), making a robust and resilient Core is more complicated and challenging. This is because 5GC needs to perform correctly and accurately all the time, including handling of abnormal network functions that could cause unintended malicious traffic. It should be able to prevent against (un)expected scenarios such as signal storm period and related misbehaving network functions.

Furthermore, with a stateless architecture and during the signal storm period, 5GC needs to be able to efficiently process and perform their functionalities without impacting on transaction, latency and throughput. This new solution is an NWDAF-assisted network abnormal behaviour mitigation and prevention. To make the Core more robust and resilient, e.g., against (un)expected abnormal / signal storm. The clause 5.2.4 of TR 23.700-84 (the key issue description of KI#4: NWDAF enhancements to support network abnormal behaviours (i.e. signalling storm) mitigation and prevention) contains as below,

“

This Key issue aims to provide solutions for prediction, detection, prevention, and mitigation of network abnormal behaviours, i.e. signalling storm, with the assistance of NWDAF. In particular, the following aspects will be addressed:

- Identify scenarios that can result in a signalling storm situation

- Whether and how existing analytics or new analytics can be used to assist detection and prediction of signalling storm, including aspects of input /output data that needs to be collected/provided by the NWDAF.

What NF(s) will be consumer of such analytics and whether and how they can use them.

- Whether and how signalling storm can be prevented or mitigated based on the inputs provided by NWDAF.

NOTE 1: In terms of data access right, privacy and security improvement, cooperation with SA3 is needed.

NOTE 2: The study of this key issue will consider the study/work done by SA WG5 and CT WG4 in this regard already and collaborate with SA WG5/CT WG4 regarding the handling of abnormal network behaviours.

”

This contribution proposes a new solution for FS\_AIML\_CN KI#4.

# 2. Text Proposal

It is proposed to agree the following solution into TR 23.700-84.

**\*\*\* Start of the change \*\*\***

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues and Use Cases

|  |  |  |
| --- | --- | --- |
|  | Key Issues | Use cases (optional) |
| Solutions | <Key Issue #1> | <Key Issue #2> | <Key Issue #4> | <use case #3> | 6 |
| #1 |  |  |  |  |  |
| #2 |  |  |  |  |  |
| X |  |  | X | X | x |

**\*\*\* Next change (all new text) \*\*\***

## 6.X Solution #X: NWDAF-assisted Network Abnormal Behaviour Mitigation and Prevention

### 6.X.1 Description

This solution resolves KI#4 for NWDAF enhancements to support network abnormal behaviours (i.e. signalling storm) mitigation and prevention. In terms of scenarios, there are cases where it is difficult to troubleshoot and or understand whether the NFs themselves are behaving correctly or not. Often, they may not know that their features/functions are behaving (un)expectedly, probably from cases such as signalling storm, and complexities in NF signalling exchange procedures. This can occur despite the irregularity of number of UEs or types of UE devices.

Hence, NFs need to be robust and resilient to ensure that the UE signalling exchange information are validated(detected, predicted, mitigated and prevented) through the AI/ML NWDAF-assistance. In such cases, NFs need to be able to extract/transfer their signalling exchange information and context information to NWDAF to be guided, e.g., mitigation and prevention for any potential (un)expected behaviours. In this, signalling storm mitigation and prevention in general should not be limited to counting a certain number of message-types from certain specific NFs. The solution is to include Input data such as:

* an individual and/or groups of NF’s sudden increase/decrease (bursts) of TPS (Transaction per second) and/or CPS (Connection per second) from various NF interfaces (e.g., SBIs and non-SBIs)
* an individual and/or groups of NF’s information involved in procedure of a UE or a session such as Connection, Registration, Mobility and Session Managements procedure
* an individual and/or groups of NF’s information contains information about UE or session context enabling the NWDAF to determine the cause of a signalling storm

Furthermore, all of the potential scenarios can be observed and measured over a certain duration to include start and end time, number of successful/failed attempts of various UE and NF service requests.

### 6.x.2 Procedures

#### 6.X.1.1 General

The NWDAF can provide information on network abnormal behaviours (i.e. signalling storm) as follows.



**Figure 6.x.1.1-1: Procedure for NWDAF-assisted Network Abnormal Behaviour Mitigation and Prevention**

1. The consumer NF or e.g., MDAF/MDAS subscribes to or sends a request to NWDAF assistance information for the Abnormal NF signalling storm using either Nnwdaf\_AnalyticsSubscription\_Subscribe or Nnwdaf\_AnalyticsInfo\_Request service operation. The request additionally includes thresholds such as confidence level and accuracy of detection. The request may also include as analytic filters an indication of the use case for signalling storm (e.g. signalling storm due to UE mobility).
2. The NWDAF retrieves Input data from NFs, using Nnf\_EventExposure\_Subscribe, such as signalling exchange information and context information to derive the required analytics as depicted in clause 6.X.1.2.
3. The NWDAF derives the required analytics based on the consumer NF request. The NWDAF can collect additional Input data from different NFs, e.g., including from MDAF/MDAS. The NWDAF collects input data from NFs taking into account the use case of signalling storm if provided in step 1.
4. The NWDAF invokes Nnwdaf\_AnalyticsSubscription\_Notify or Nnwdaf\_AnalyticsInfo\_Request response or response to the consumer NF for the Output data analytics as depicted in clause 6.X.1.3.
5. The consumer upon receiving the detection, prediction and mitigation shall execute based on the output as depicted in clause 6.X.1.4.

NOTE: A care needs to be taken with regards to load when requesting data collection to avoid signalling storm caused by the NWDAF-assisted Network Abnormal Behaviour Mitigation and Prevention procedure.

#### 6.X.1.2 Input Data

NFs can extract various information when acting as a consumer or producer. It is assumed to consider Input Data from a Producer NF perspective. The NWDAF collects signalling storm information as listed in Table 6.x.1.2-1 to 6.x.1.2-3.

Table 6.x.1.2-1: input data collected by NWDAF for AMF

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| NF ID | AMF | NF instance ID of the service producer or consumer |
| Signalling exchange information | AMF | NF procedures containing signalling exchange information related to a particular UE or session from the Connection, Registration, Mobility and Session Managements procedures. |
| > Type of requests from UE/RAN | AMF | Request type for N1 or N2 interface, such as received Initial Registration Request, Mobility and Periodic Registration Request, Service Request, etc. |
| > Number of requests from UE/RAN | AMF | Number of requests for N1 or N2 interface, such 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 |
| > Number of failed responses of UE/RAN | AMF | Number of failed responses associated to their initial requests |
| > Reason of failed responses of UE/RAN | AMF | Reasons of failed responses associated to their initial requests |
| > 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 |
| > > A posterior Type of responses of UE/RAN (0..max) | AMF | A posterior Response types triggered from UE/RAN, for NF Service response, or response to UE/RAN |
| > Type of requests from NF | AMF | Request type received from NF, e.g., Namf\_N1N2Trans, Namf\_comm, etc. |
| > Number of requests from NF | AMF | Number of requests received from NF, e.g., Namf\_N1N2Trans, Namf\_comm, etc. |
| > Time duration from receiving request from NF to response to NF | AMF | Time duration between the request from NF and response to NF. |
| > Number of successful responses of NF | AMF | Number of successful responses associated to their initial requests  |
| > Number of failed responses of NF | AMF | Number of failed responses associated to their initial requests |
| > Reason of failed responses of NF | AMF | Reasons of failed responses associated to their initial requests |
| > A posterior Type of requests of NF (0..max) | AMF | A posterior Request types triggered from NF, for NF Service request |
| > > A posterior Type of responses of NF (0..max) | AMF | A posterior Response types triggered from NF, for NF Service response |
| > Public Warning information | AMF/OAM | Public Warning information such as WRITE-REPLACE WARNING REQUEST, etc. |
| > Number of UE AM Policy Updates | AMF | Number of policy requests from PCF such as URSP, Restriction Area, etc. |
|  |  |  |
| NF Context information | AMF | NF context information related to a particular UE/Session context |
| > State transition information | AMF | 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". |
| > timer information | AMF/OAM | UE related timer information such as timer type, duration, etc. |
|  |  |  |
|  |  |  |

Table 6.x.1.2-2: input data collected by NWDAF for SMF

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| NF ID | SMF | NF instance ID of the service producer or consumer |
| Signalling exchange information | SMF | NF procedures containing signalling exchange information related to a particular UE or session from the Connection, Registration, Mobility and Session Managements procedures. |
| > Type of requests from NF | SMF | Request type received such as PDU Session Establishment, Modification, Release Request, etc. |
| > Number of requests from NF | SMF | Number of requests received such as PDU Session Establishment, Modification, Release Request, etc. |
| > Time duration from receiving request from NF to response to NF | SMF | Time duration between the request from NF and response to NF. |
| > Number of successful responses of NF | SMF | Number of successful responses associated to their initial requests  |
| > Number of failed responses of NF | SMF | Number of failed responses associated to their initial requests |
| > Reason of failed responses of NF | SMF | Reasons of failed responses associated to their initial requests |
| > A posterior Type of requests of NF (0..max) | SMF | A posterior Request types triggered from NF, for NF Service request. |
| > A posterior Type of responses of NF (0..max) | SMF | A posterior Response types triggered from NF, for NF Service response. |
| > Number of requests for UE SM Policy Update | SMF | Number of requests from PCF to update UE SM Policy per PDU Session, such as QoS, PCC Rules, etc. |
|  |  |  |
|  |  |  |
|  |  |  |
| > Load information of connected UPFs | SMF/OAM | Load information of connected UPFs such as using PFCP Load Control Information. |
| > 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 5GCM-idle state |
|  |  |  |
|  |  |  |
| NF Context information |  | NF context information related to UE/Session context |
| > Usage information of UE IP address resources | SMF/OAM | 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. |
| > State transition information | SMF | 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". |
| > timer information | SMF/OAM | PDU Session related timer information such as timer type, duration, etc.an individual and/or groups of NF’s information contains  |
|  |  |  |
|  |  |  |

Table 6.x.1.2-3: input data collected by NWDAF for NRF/SCP

|  |  |  |
| --- | --- | --- |
| Information | Source | Description |
| NF ID | NRF | NF instance ID of the service producer or consumer |
| Signalling exchange information | NRF/SCP | NF procedures containing signalling exchange information related between NF and NRF procedures. NRF/SCP can be used within deployment Model-C/D scope of indirect communication with/without delegated discovery. |
| > Type of requests from NRF | NRF | Request type received such as NF registration and discovery, etc.  |
| > Number of requests from NF | NRF | Number of NF requests received such as NF registration and discovery, etc. |
| > Time duration from receiving request from NRF to response to NF | NRF | Time duration between the request from NRF and response to NF. |
| > NF profile | NRF/OAM | NF Profile information such as allowed NF information per NF and NF Service |
| > NF load information of registered NFs and NF Services | NRF/OAM | Load information indicates the current load of NFs and NF Services, e.g., CPU, memory, and/or percentage of load information. |
| > Capability and priority information of NFs and Services | NRF/OAM | Capability and priority information of registered NFs and NF Services |
| > NF heart-beat related information | NRF/OAM | NF heart-beat related information such as responding time, Number of retransmissions, heart-beat intervals, etc |
|  |  |  |
| > Success and failure trend | NRF/OAM | Number Requests/response related trend such as within a certain time interval, ratio, cause/error code etc. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Editor’s Note: It is FFS which parameters in tables above are per UE, and which ones are per NF, and whether and how the ones per NF are retrieved from OAM.

#### 6.X.1.3 Output Analytics

The output analytics of signalling storm detection of NWDAF is defined in Table 6.X.1.3-1.

Table 6.X.1.3-1: signalling storm detection

|  |  |
| --- | --- |
| Information | Description |
| Report (1..max) | List of observed signalling storm |
|  > Target NF ID | The target of signalling storm detected by NWDAF |
|  > Abnormality ID | The potential cause of NF Abnormality (e.g. massive UE/frequent access, NF abnormal signalling, etc.) |
|  > Source SUPI/NF list | SUPI(s) of the UE(s) or NF(s) which cause the signalling storm |

The output analytics of signalling storm prediction of NWDAF is defined in Table 6.X.1.3-2.

Table 6.X.1.3-2: signalling storm predictions

|  |  |
| --- | --- |
| Information | Description |
| Report (1..max) | List of observed signalling storm |
|  > Target NF ID | The target of signalling storm predicted by NWDAF |
|  > Abnormality ID | The potential cause of NF Abnormality (e.g. massive UE/frequent access, NF abnormal signalling, etc.) |
|  > Source SUPI/NF list | SUPI(s) of the UE(s) or NF(s) which cause the signalling storm |
|  > Confidence | Confidence of this prediction |

#### 6.X.1.4 Mitigation or Prevention

The following existing mechanism can be used to mitigate and prevent the signaling storm.

Table 6.X.1.4-1: Example mechanisms to mitigate and prevent the signalling storm

|  |  |
| --- | --- |
| Abnormality ID | Actions of NFs |
| Massive UE access | AMF sets MM NAS related timer (e.g., back-off, T3512) with suggested time range for a selected set of UEs |
| Massive UE access | SMF sets SM NAS related timer (e.g., back-off) with suggested time range for a selected set of Sessions |
| Massive UE access | PCF sets AM/SM policy control for a selected set of UEs/Sessions |
| Massive UE access | 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 [yy] to start overload control. |
| NF abnormal signalling | NRF/SCP configures the local policy to prevent the source NF from being discovered or discovering others.Source NF configures to reselect other target NFs and unsubscribes the existing abnormal NF. |
| NF abnormal signalling | NRF/SCP configures the local policy to prevent the source NF from being discovered or discovering others or deprioritize the source NFs/Services from being select less. |
| NF abnormal signalling | Source NF configures to reselect other target NFs and unsubscribes the existing abnormal NF or triggers UE Reregistration and/or Session Reestablishments, and reselects to other target NFs |

NOTE : Detailed mechanisms to mitigate and prevent the signalling storm will consider operator policy.

Editor’s Note: Table 6.X.1.4-1 lists are to be updated further based on discussions.

Editor’s Note: NWDAF may leverage MDAF/MDAS for deriving the output data, and which parameters in the tables above shall be mandated and which ones to be optional is for FFS.

### 6.X.3 Impacts on services, entities and interfaces

NWDAF:

- Supports providing subscriptions and/or requests for Abnormal NF signalling storm Analytics.

- Supports deriving statistics and/or predictions of based on Analytics consumer subscriptions and/or requests.

Consumer NF:

- Supports subscribing or requesting Abnormal NF signalling storm Analytics from NWDAF using Nnwdaf\_AnalyticsSubscription\_Subscribe or Nnwdaf\_AnalyticsInfo\_Request service.

- Supports executing the mitigation and prevention actions based on the analytics data from NWDAF.

Source NF:

- Supports providing additional data exposure for Abnormal NF signalling storm Analytics using Nnf\_EventExposure Service.

**\*\*\* Next change \*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G system, Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[5] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[6] 3GPP TR 38.843: "Study on Artificial Intelligence (AI)/Machine Learning (ML) for NR air interface".

[7] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS)".

[yy] 3GPP TS 38.413: "NG Application Protocol (NGAP)".

**\*\*\* End of the change \*\*\***