**3GPP TSG-WG SA2 Meeting #164 *S2-2408246***

**Maastricht, Aug 19 – 23, 2024 (merger of S2-2408246 and S2-2408140)**

**Source: Nokia**

**Title: Resolving open issues in solution#11**

**Document for: Approval**

**Agenda Item: 19.14.1**

**Work Item / Release: FS\_AmbientIoT / Rel-19**

*Abstract: a new solution to support information transfer from the Ambient IoT devices to the network*

# 1. Introduction/Discussion

This contribution is prepared to resolve all the open issues left for solution#11.

# 2. Text Proposal

It is proposed to approve the following changes in TR 23.700-13 v0.4.0.

*FIRST CHANGE*

## 6.11 Solution #11: 5GC support for AF to communicate with AIoT devices

### 6.11.1 Description

This solution address aspects of key issue #3 on Support of Ambient IoT Services.

This solution enables the AF to communicate with the target AIoT devices for DO-DTT and DT traffic types via 5GC, dedicated for only Topology 2.

This solution considers scenarios in which an application service provider has prior information about intermediate nodes (abbreviated as I-node) expected to be located in specific places (e.g. intermediate nodes being used only in particular warehouses). Additionally, scenarios where the provider knows candidate locations for the target AIoT devices (e.g. the AIoT devices attached to goods are expected to be in particular warehouses or retail markets) are also considered.

The assumption and high-level procedures of this solution are as follows:

- The AIoT device ID is defined by the external application and provided by the AF to the 5GC when requesting the AIoT-related services. The uniqueness of the AIoT device ID per application is assumed to be guaranteed by the application itself, such as by adhering to standards like EPC (Electronic Product Code) and utilizing EPCglobal allocation, which manages a global registry for unique prefixes among different companies.

- AIoT devices are not registered with the 5GC.

- AIoT devices do not have NAS layer.

- Application layer security between AIoT devices and AS is assumed.

- AIoT Devices are provisioned with AIoT Device ID and associated security materials.

- A UE, additionally capable of directly communicating with the AIoT devices, is acting as the intermediate node.

- A UE acting as an intermediate node is registered with 5GC using the existing mechanism, with some enhancements to indicate its capability of acting as an intermediate node, and is authorized as an intermediate node (UE) during the registration procedure.

- The AF possesses information about the candidate location(s) of the target AIoT devices or about the preferred intermediate node (i.e. external UE ID) and provides them when requesting the AIoT related services to 5GC.

- If the AF is in the 3rd party domain, the AF can communicate with the 5GC via NEF that can be combined with the AIoT NF.

- When information about the preferred intermediate node is provided while it is not operational, or when the location(s) of the target AIoT devices are given, the 5GC selects the intermediate node based on the network information. The process of selecting such an intermediate node is not within the scope of this solution. This means that this solution supports both static and dynamic binding with the intermediate node.

- How to support security between each entity (e.g. between AIoT device and I-node, and AIoT device and CN) involved in the procedures (e.g. relying on application security or providing network security based on the information provided by the application) is assumed to be addressed by SA WG3.

- The Uu interface between the intermediate node and the gNB is assumed to be used, while possibly a new protocol stack, defined by RAN, is assumed to be used between the AIoT device and the intermediate node.

- For DO-DTT traffic (e.g. response from the AIoT device to the network), it can be sent over the NAS of the intermediate node.

Figure 6.11.1-1 shows the 5GS enhancement to support AIoT Device.



Figure 6.11.1-1 5GS enhancement to support AIoT Devices for Topology 2

### 6.11.2 Procedures

#### 6.11.2.1 Communication with AIoT devices

The procedure for communicating with AIoT devices based on AF request is depicted in figure 6.11.2.1-1.



Figure 6.11.2.1-1: Information Flow for AIoT data retrieval

To facilitate communication between an external AF with AIoT devices for data retrieval, this solution proposes certain measures to be taken:

0. It is assumed that the AF requesting 5GC to communicate with specific AIoT devices possesses their AIoT device IDs, either defined by the device manufacturer or the AF itself, along with candidate locations of the AIoT devices or information (e.g. external ID) of the intermediate node covering the target AIoT devices.

1. The intermediate node is a UE with the capability to directly communicate with the AIoT devices. The intermediate UE performs the registration procedure as specified in clause 4.2.2.2 of TS 23.502 [5] with the following enhancement:

- The UE indicates AIoT support in the MM capability.

- The subscription data of the UE is also enhanced to indicate whether the UE is allowed to perform the AIoT operation.

- The Registration Accept message also indicates whether the UE has been authorized to perform the AIoT operation. Validity information may also be included for the AIoT operation. Validity information can be time validity information (defined by start and end times) to indicate when the UE is allowed to perform the AIoT operation or location validity information (defined by TAI or cell ID) to indicate where the UE is allowed to performed the AIoT operation.

2. The AF sends a request to 5GC to communicate with the target AIoT devices for either DT or DO-DTT traffic type. The AF's request includes following parameters: the target AIoT device IDs defined by the external application and installed in the AIoT devices, the candidate locations of the target AIoT devices or the external ID (i.e. external UE ID) of the intermediate node that can directly communicate with the target AIoT devices, "command" information (e.g. read/write), optionally specific target data to be read by the AF.

3. Upon receiving the AF request, the NEF authorizes the AF request based on SLA.

4. The NEF translates the external ID (e.g. GPSI) of the intermediate node, if provided, to the SUPI via UDM and verifies whether the UE possessing the translated SUPIs is authorized to function as intermediate node through UDM. The NEF translates the location, if provided by the AF, into 3GPP based location information (Tracking areas TA(s), cell ID(s), etc). The NEF identifies the serving AMF(s) via UDM by utilizing the SUPI of the intermediate node, if applicable, or by considering the candidate locations of the AIoT devices. The NEF selects AIoTF that can be a standalone NF or collocated with the NEF. If multiple locations are provided, the overall procedures can be performed for each location.

5. An AIOT service request message is sent to the AIoTF, including the following parameters: AIoT session ID, the target AIoT devices, candidate locations or the SUPI of the intermediate node, Serving AMF(s) as derived in step 4, "command" information (e.g. read/write), optional Requested target data.

6. The AIoTF may select the intermediate node based on the information provided in step 5 to communicate with the target AIoT devices. The detailed procedures for selecting the intermediate node are described in clause 6.11.2.2. The selected UEs can be configured with information necessary for AIoT services, using the UE configuration update procedure.

7. The AIoTF requests the serving AMF to initiate the communication, which includes AIoT session ID, the target AIoT device IDs, candidate locations or SUPI of the selected intermediate node, "command" information (e.g. read/write) and optional Requested target data.

8. The AMF identifies the serving gNB by utilizing the SUPI of the intermediate node, if applicable, or by considering the candidate locations (i.e. a list of TAIs and cell IDs) of the AIoT devices. The AMF then requests the gNB to send a AIoT service request, which contains the target AIoT device IDs, candidate locations or UE NGAP ID of the selected intermediate node, "command" information (e.g. read/write), and optional Requested target data, to the selected I-node. The paging request message, if the selected I-node is in CM-IDLE state, or N2-AP Downlink NAS Transport message, if the selected I-node is in CM-CONNECTED state, can be used with some extensions to convey the AMF request, for example

9. The gNB requests the selected intermediate node to communicate with the AIoT data, providing the target AIoT device IDs, "command" information (e.g. read/write), and the Requested target data (if applicable). RRC paging message can be used by the gNB to send the request to the intermediate node if the selected I-node is in CM-IDLE or RRC-INACTIVE states. Alternatively, a dedicated RRC message can be used if the selected I-node is in RRC-CONNECTED state, for example. When RRC paging is used, the gNB may restrict the paging area only to the identified cells for optimization, if available.

10. The selected intermediate node sends out a request which includes the target AIoT device IDs and the Requested target data (if applicable).

NOTE: The radio resources required for communicating with AIoT devices are to be defined by RAN WGs.

11. The AIoT devices check whether their device IDs match any of the target AIoT device IDs included in the received request. If there's no match, the AIoT devices do not react.

12. If there's a match, the AIoT devices check the presence of Requested target data within the request as well as "command" information to check whether DT or DO-DTT traffic type is requested. In case of DO-DTT type requested, if the Requested target data is absent, the AIoT devices send a response message incorporating only their device IDs. If the Requested target data is present, the AIoT devices send a response message including their device IDs and only the data requested to the intermediate node.

13. The intermediate node receives the response message from the AIoT devices. If the AIoT device ID within the received message corresponds to any of the target AIoT device IDs obtained in step 10, the intermediate node assesses which AIoT devices, from the list of expected AIoT devices, have provided a response. The intermediate node may aggregate the response messages from the AIoT devices according to the configuration information if it was provided by the CN in advance. The intermediate node then forwards this information, encompassing AIoT device data (if applicable) and the AIoT device ID(s) over NAS signalling to the AF via gNB, AMF, AIoTF and NEF. The AMF or AIoTF may aggregate response messages from some or all of the targeted AIoT devices during the forwarding procedures to AF.

#### 6.11.2.2 Selection of intermediate nodes

The selection of the intermediate node can be performed based on the geographical location of the target AIoT devices or the identity of the intermediate node from AF. The procedure for selection of intermediate nodes based on geographical location is depicted in figure 6.11.2.2-1.



Figure 6.11.2.2-1: Information Flow for selecting I-node based on location of target devices from AF

1-4. Step 2 to 5 in clause 6.11.2.1 are performed.

5. The AIOTF collects necessary information from relevant NFs, for I-node selection, based on the requested location info.

a. The AIOTF first discovers the UEs present in the requested location and may also retrieve the UE related information from AMF, including connection status and reachability.

b. The AIOTF may retrieve information related to the UEs discovered in step 5a from UDM. This information enables checking, for example, whether the UEs are registered, authenticated, authorized to act as I-nodes. Additionally, the information from UDM can include the Expected UE behaviour, as described in clause 4.15.6.3 of TS 23.502 [5], that can be used to check the battery indication, stationary indication among other parameters.

c. The AIOTF may retrieve information related to the UEs discovered in step 5a from NWDAF. This information enables checking, for example, if the discovered UEs are not too much loaded to serve the devices, function well without anomalies, or will not move out of the coverage for a significant period based on the UE related analytics as specified in clause 6.7 of TS 23.288 [13].

6. The AIOTF, based on the information collected in step 5, selects a list(s) of potential I-nodes. The number of I-nodes selected can be based on factors such as the number of device IDs. If there are many available candidate I-nodes, the AIoTF may prioritize I-nodes in CM-CONNECTED state to optimize signalling. For I-nodes in CM-IDLE or RRC-Inactive states, the AIoTF may further refine the selection, for example, by checking if the last visited cell matches the location specified in step 4.

7. In case no I-nodes could be selected at step 6, AIOTF sends AIOT Response with the failure reason to the AF, and the subsequent steps are skipped.

8. The AIoTF requests the serving AMF to initiate the communication with the AIoT devices, which includes the target AIoT device IDs, and the selected I-node IDs.

9. The AMF forwards the AIOT read request to gNB along with the target AIOT device IDs and the selected I-node IDs.

10. The gNB performs additional validation to assess if the received I-nodes are optimal for serving the AIoT devices, considering its local conditions such as response time, etc. Subsequently, the gNB makes the final selection on the best I-node. It is also possible that the gNB does not select any of the requested I-nodes if local conditions are not satisfied.

11. The gNB may respond to the AIOTF via AMF with the final list of selected I-nodes. In case the gNB does not selection any I-node, the response may indicate there is no available UE.

As an alternative to 6.11.2.2-1, the following procedure as depicted in figure 6.11.2.2-2 can be supported.



1. UE Registration

The User Equipment (UE) registers with the 5G network. This involves the UE connecting to the gNodeB (gNB) and the network's core. The registration process ensures that the UE is authenticated and authorized for AIoT services.

2. AIoT Request

A request is initiated for an AIoT (Ambient IoT) service, such as inventory management. This request includes details such as the estimated location of the target AIoT devices and the target AIoT device IDs that need to be managed or interacted with. If the target AIoT device IDs are missing, it can be considered that the AF wants to inventory all the available AIoT devices within the interested location.

3. Location Info Conversion to Cell ID

The location information provided in the AIoT request is converted into a Cell ID managed within 3GPP. The Cell ID is a unique identifier for the cell (coverage area) that the base station (gNB) is serving.

4. 5GC AIoT request initiation

The network initiates an AIoT service request process to inventory the target AIoT devices and to locate the available UE readers within the specified cell. This request includes an AIoT service indicator that can be used by the UEs to decide whether to react or not.

5. Broadcast the AIoT request within the Cell

The discovery information is broadcast within the cell. This broadcast includes an AIoT indicator and the target AIoT device IDs.

NOTE 1: How a BS broadcasts the AIoT request (e.g., using MBS or SIBs) is assumed to be addressed by RAN WGs.

NOTE 2: It is assumed that the BS sending the broadcast message is installed indoors, so the cell coverage is presumed to be equivalent to the AIoT service area6. UE decision

 All UEs in the specified cell receive the broadcast message as in step 5, but only UEs that are capable of AIoT communication will react to the AIoT indicator broadcast in Step 5 and perform the following steps. This ensures that only relevant devices participate in the AIoT communication process

7. AIoT Communication

Communication is performed between the UE reader(s) and the AIoT devices. This step involves the actual data exchange, such as sending commands to the AIoT devices and receiving their responses.

8. Response per UE

The network collects responses from each UE involved in the AIoT communication. These responses include the UE ID, AIoT device ID, and optionally any relevant AIoT data that was exchanged.

9. AIoT Response

The AIoT response is consolidated and sent back to the AF. This response includes the AIoT device ID and the data collected from the AIoT devices, if any.

10. UE Info Check with NWDAF/UDM

Optionally, the UE information is checked against the Network Data Analytics Function (NWDAF) and/or User Data Management (UDM) systems. This step can provide additional information about the UE readers, allowing the 5GC to determine which UE to use as the reader for the AIoT devices when there are duplications. For instance, if two UEs are delivering data from the same AIoT device, the 5GC can decide to use only one of them by taking the additional information into consideration. If one of the UEs is expected to leave in 5 minutes, it would be safer to choose the other one as the reader for further communication

11. Determine Responsible UE(s)

The network determines which UEs are responsible for specific AIoT devices, especially in cases where multiple UEs may have interacted with the same device. This decision can be made based on the operator policy and/or the additional information retrieved in step 10, if available. A binding table is created in the AIoTF to map these relationships.

12. Additional AIoT Request

Another AIoT request can be initiated for the same target AIoT devices. This step might be part of an iterative process to refine the inventory and interaction with AIoT devices.

13. Look Up the Binding Table

The core network (e.g., AIoTF) looks up the binding table created in Step 11 to find the UEs that are responsible for the specific AIoT devices. This ensures that requests are directed to the appropriate UEs. If the target AIoT devices are missing, the network can broadcast the request to all the UEs within the location.

14. Direct Request to Reader UEs

Requests can be sent directly to the UEs identified as readers for the AIoT devices in the binding table. This step ensures efficient and accurate communication with the AIoT devices.

When communication with some of the target AIoT devices through the UE reader selected from the binding table fails, it may indicate that the target AIoT devices are out of coverage or broken. In this case, the network can remove the binding information from the table and perform steps 5 to 10 to maintain the latest binding status.

The procedure for selecting intermediate nodes when I-node ID is provided in the AF request is depicted in figure 6.11.2.2-3.



Figure 6.11.2.2-3: Information Flow for selection of I-nodes based on list of I-nodes from AF

1-4. Step 2 to 5 in clause 6.11.2.1 are performed.

5. The AIOTF collects necessary network information related to the requested UEs from relevant NFs.

a. The AIOTF may retrieve information related to the requested UE from UDM. This information enables checking, for example, whether the UEs are registered, authenticated, authorized to act as I-nodes. Additionally, the information from UDM can include the Expected UE behaviour, as described in clause 4.15.6.3 of TS 23.502 [5], that can be used to check the battery indication, stationary indication among other parameters.

b. The AIOTF may retrieve information related to the requested UE from NWDAF. This information enables checking, for example, if the discovered UEs are not too much loaded to serve the devices, function well without anomalies, or will not move out of the coverage for a significant period based on the UE related analytics as specified in clause 6.7 of TS 23.288 [13].

c. The AIOTF may retrieve information related to the requested UE from AMF, including its location, connection status and reachability.

6. The AIOTF, based on the information collected in step 5, validates whether the requested UE ID provided in the AF request can serve as an intermediate node.

7. If the requested UE is not operational and other "I-nodes allowed" flag was not set in the AF request, AIOTF sends AIOT Response with the failure reason to the AF, and the subsequent steps are skipped.

8. If the validation of the requested I-node fails and the 'other I-nodes allowed' flag was set in the AF request, the AIOTF may select a different list of UEs for the requested operation than the UE requested by the AF. This can be achieved by performing the step 5 in the figure 6.11.2.2-1 with the location set to the location information of the requested UE retrieved from AMF in step 5c.

9. The AIoTF requests the serving AMF to initiate the communication with the AIoT devices, which includes the target AIoT device IDs, and the selected I-node IDs.

10. The AMF forwards the AIOT read request to gNB along with the target AIOT device IDs and the selected I-node IDs.

11. The gNB performs additional validation to assess if the received I-nodes are optimal for serving the AIoT devices, considering its local conditions such as response time, received signal strength, etc. Subsequently, the gNB makes the final selection on the best I-node. It is also possible that the gNB does not select any of the requested I-nodes if local conditions are not satisfied.

12. The gNB may respond to the AIOTF via AMF with the final list of selected I-nodes.

### 6.11.3 Impacts on services, entities and interfaces

Impacts on existing entities:

**NEF:**

- Supports exposing a new API to AF for AIoT services.

**UDM:**

- Supports validating if a UE is authorized to act as an I-node.

**AMF:**

- Supports forwarding the AIOTF requests to gNB.

**gNB:**

- Supports handling new AIoT related services.

- Supports making the final selection of the I-node.

**UE (I-node):**

- Supports indicating its capability to support AIoT services during UE registration.

- Supports communicating with AIoT devices.

**New NF:**

- AIOTF:

- This can be a standalone NF or combined with NEF.

- Supports necessary network information for specific UEs or specific location from multiple NFs (e.g. AMF, UDM, NWDAF).

- Supports selecting or validating I-nodes.

- Supports forwarding the AF requests to AMF.

*END OF CHANGES*