July 18, 2019

SUPPORTING DYNAMIC NETWORK SLICING AND POLICY CREATION FOR END DEVICES IN PRIVATE 5G NETWORKS

Rajesh I. V

Ram Mohan R

Prashanth Patil

Prathap B

Palanivel Murugan M

SUPPORTING DYNAMIC NETWORK SLICING AND POLICY CREATION FOR END DEVICES IN PRIVATE 5G NETWORKS

AUTHORS:
Rajesh I V
Ram Mohan R
Prashanth Patil
Prathap B
Palanivel Murugan M

ABSTRACT

Described herein are techniques for handling dynamic slicing requirements of User Equipment (UE) by performing remote activation (e.g., Over-the-Air Provisioning (OTAP)) of the logical profiles captured in the embedded Subscriber Identity Module (eSIM) which are created for the different slicing needs in private 5G networks. Also described are techniques for installing policies based on the Manufacturer Usage Description (MUD) Uniform Resource Locator (URL) in a private 5G network and efficiently retaining it during a 5G outage.

DETAILED DESCRIPTION

Private 5G networks promise to support major use cases (e.g., enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC), massive Machine Type Communications (mMTC), etc.) for Industry 4.0 and Industrial Internet of Things (IIOT). With private 5G networks, the industrial verticals can own the private spectrum and manage the 5G system in a customized manner. This diverse set of services may be offered through network slices using Network Function Virtualization (NFV). Usually the profile stored in the Subscriber Identity Module (SIM) contain the operator's access information, subscription details, and third party SIM based applications. In a typical 5G network, service providers allocate the required resources for the subscribed network slices as per the Service Level Agreement (SLA) when the subscriber registers to the network.

With private 5G, the same underlying 5G architecture will be used and the owners can customize it as required. A first problem is that switchover in a dynamic environment for User Equipments (UEs) that need different network slices based on the operational

context or time schedules, is not possible today. The subscription is always fixed for the underlying device for the given Service Provider (SP). Though some SPs provide the network slice for a shorter duration for Business to Business to Consumer (B2B2C) requirements, this does not address the change in network slicing requirements. The latest Network Data Analytics Function (NWDAF) proposes slice handling based on load information, but that is not an adequate solution for operational context change.

For example, in a hospital, when equipment is used in an operation theater or the Intensive Care Unit (ICU), the generated data needs to be processed with certain slices, sometimes specific to the patient. When the equipment is moved to a different location of the hospital (e.g., a laboratory or service center), it may generate some data that does not need all network slices. In another example, in a manufacturing unit when the machineries are used in production, operational data may be created which needs certain slices to complete the process. When the machine is in an idle state (e.g., cooling or off production time) it may still generate health and service related information which does not require all network slices. There is no explicit mechanism described for handling dynamic change of slicing requirements as detailed above. This problem is applicable in private 5G networks which is mainly targeted to support various type of machineries.

A second problem is that smart IOT devices should be authorized to have only intended communications in the network. Internet Engineering Task Force (IETF) Request for Comments (RFC) 8520 discusses creating policies based on the Manufacturer Usage Description (MUD) files advertised by the manufacturers of IOT devices. This works well in Wi-Fi® Local Area Network (LAN), but there is no explicit mechanism for supporting this in private 5G networks.

For example, when the enterprise is based on a private 5G network (e.g., a manufacturing unit), and if there is any failure in the 5G components for small cells (for example), there is a need to switch over to alternate network to continue the operations. Switching to another SP is a difficult solution for IOT devices due to security challenges, for example. The recommended approach is to fall back to Wi-Fi. There can be a small time lag in switching the network and installing the required policies in private 5G networks.

Techniques are described herein to address the aforementioned problems for private 5G networks. With respect to the first problem, an enterprise that uses a private 5G network has the flexibility to leverage profile based activation on the eSIM of the end devices based on operational context. This approach provides more flexibility in the private 5G network.

IOT devices (UEs) have begun using eSIM (also known as Embedded Universal Integrated Circuit Card (eUICC), which is capable of storing multiple profiles and supporting Over-the-Air Provisioning (OTAP) and remote provisioning. Usually the profile contains the operator's access information, subscription details, and third-party SIM-based applications.

The enterprise private 5G network administrator identifies the slicing requirements of the equipment for various operational contexts and creates unique profiles for the combination of slices. The raw profiles and subscription information related to the UE are stored in a Unified Data Repository (UDM) which can be used by the appropriate Network Functions (NFs) including Network Slice Selection Functions (NSSFs).

5G is a Service Based Architecture (SBA) by which modular customizable NFs can be created. Using this approach, the Rule Engine (RE) may be created as a custom NF. The administrator may add rules specifying the supported profiles for each of the equipment, and when to change the profile for an equipment based on time schedule or identification of certain operational conditions. Optionally, there may be rules in the RE which require the RE to be subscribed to the NWDAF so that it is notified by the NWDAF of certain operational conditions which require changes in network slicing for certain equipment.

Using the profile activator, the administrator may add all the profiles on the eSIM of the UE and provision the current profile (e.g., via OTAP). The RE may trigger the network profile activator when there is a change requirement determined for network slicing for the underlying equipment. The RE may share the information or the required profile to be activated on the UE(s) and the same may be activated remotely. The switchover of the profile indicates the operational mode change of the UE for which required slices are dynamically applied by the private 5G.

The AMF retrieves the slices that are allowed by the user subscription based on the selected profile (the UDM stores the information) and interacts with the NSSF to select the appropriate network slice instance.

Figure 1 below illustrates a private 5G network configured to handle varying network slice requirements.

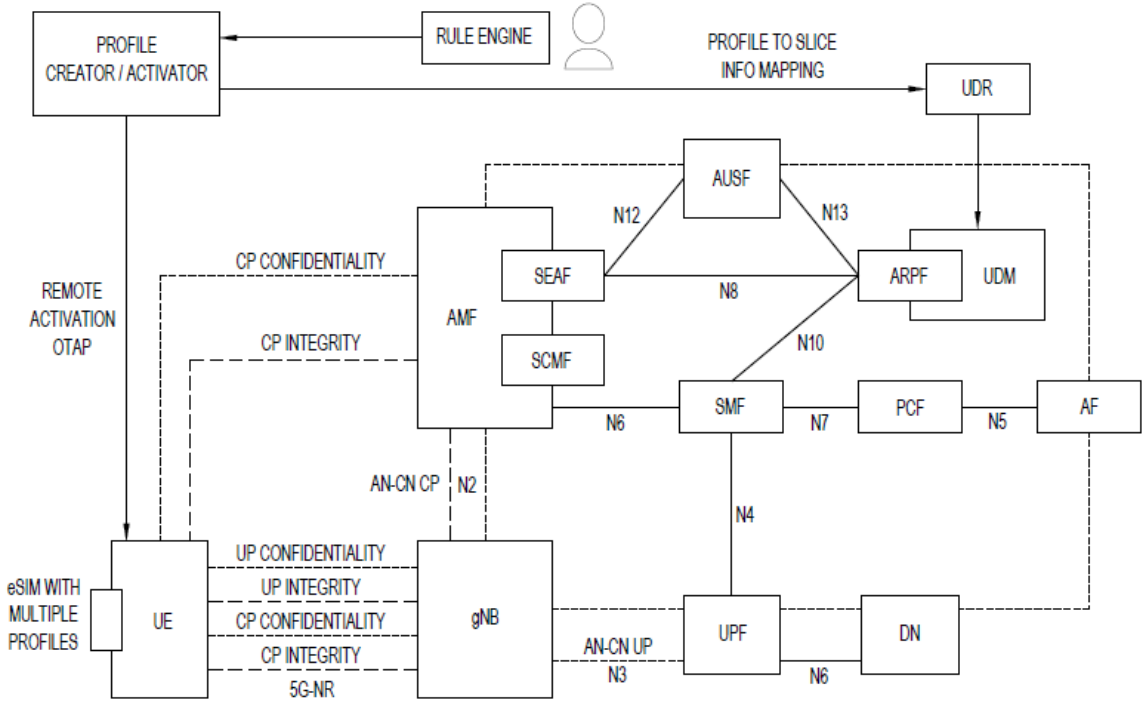

Figure 1

With respect to the second problem, smart IOT devices should be authorized to have only intended communications in the network. IETF RFC 8520 discusses creating policies based on the MUD files advertised by the manufacturers of IOT devices. Described herein is an approach for using the MUD controller to institute a policy for UE communication in private 5G networks. The UE may obtain the Internet Protocol version 4 (IPv4) address and/or its configuration parameters at or after the initial access signaling (i.e., Nsmf_PDUSession_CreateSMContext) to the private 5G network.

The Session Management Function (SMF) acts as a Dynamic Host Configuration Protocol (DHCP) server and performs the DHCP operation to issue the required configuration to the UE, or it acts as a relaying DHCP client towards the external DHCP server. If the SMF takes on a DHCP server role, then using the SBA approach, the MUD controller may be created as a NF (MUD Controller Function (MCF)) which is made discoverable through the NF Repository Function (NRF). The NRF maintains a record of available NF instances and their supported services. It allows other NF instances to subscribe and be notified of registrations from NF instances of a given type. The MCF may

subscribe to the SMF and be notified accordingly when the SMF handles DHCP processing. The notification contains essential information for further processing by the MCF.

Alternatively, the enterprise may establish a DHCP server that processes the DHCP request from the SMF on behalf of the UE. The DHCP server interacts with the MUD controller and passes the MUD Uniform Resource Locator (URL) obtained from the UE as part of the DHCP request. In either approach, the MUD controller downloads the MUD file from the manufacturer location and processes the content, creates Access Control Lists (ACLs), and applies them to the network device MUD.

The enterprise may maintain the Wi-Fi network as a backup for the private 5G network or at least to address critical devices or emergency services in the event of a private 5G service outage such as small cell failure. As the private 5G and Wi-Fi systems are both managed by the same enterprise, there may be a common DHCP server managed through IP Address Management (IPAM) used by both the SMF and the same Wi-Fi system. When there is a network outage in 5G, UEs may fall back to Wi-Fi. This triggers the DHCP process. In this case, the MUD controller processing should be avoided as it can take some time to establish the policy. The IPAM may ensure the same IP addresses are assigned to the UEs so that the established policies are still intact.

Figure 2 below illustrates a private 5G network configured to handle one or more policy requirements for the equipment.

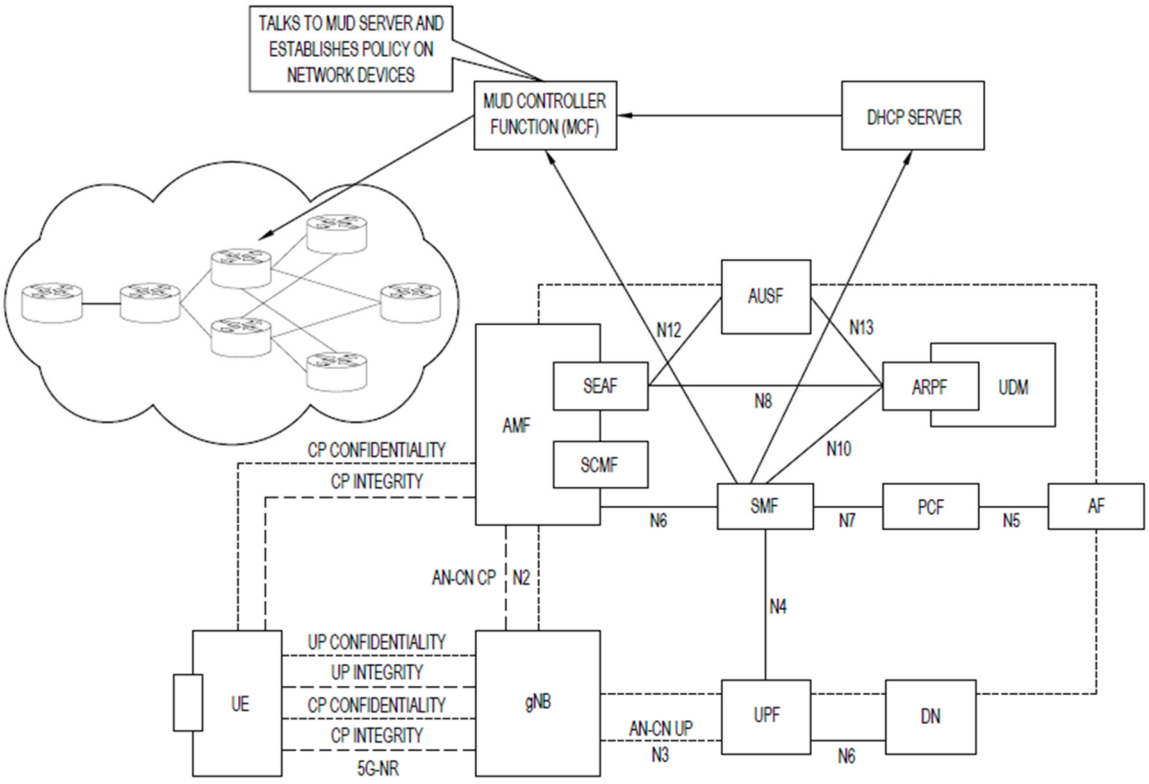

Figure 2

In summary, described herein are techniques for handling dynamic slicing requirements of UE by performing remote activation (e.g., OTAP) of the logical profiles captured in the eSIM which are created for the different slicing needs in private 5G networks. Also described are techniques for installing policies based on the MUD URL in a private 5G network and efficiently retaining it during a 5G outage.