5G Non-Public-Networks (NPN) Roaming Architecture

Marius Corici, Pousali Chakraborty, Thomas Magedanz
Fraunhofer FOKUS Institute, Berlin, Germany
{marius-iulian.corici, pousali.chakraborty, thomas.magedanz}@fokus.fraunhofer.de

Andre S. Gomes, Luis Cordeiro
OneSource, Coimbra, Portugal
{gomes, cordeiro}@onesource.pt

Kashif Mahmood
Telenor Research, Fornebu, Norway
kashif.mahmood@telenor.com

***Abstract*—With the increasing deployment of 5G Non-public Networks, the telco environment is becoming massively multi-administrated with a wide range of full networks deployed close and covering only the use case area. To benefit the most of this, a roaming solution must be set in place enabling devices to safely communicate using visited infrastructures either with local service or with the ones from the home networks. As a first step in this direction, this article proposes a new architecture for Non-public Networks roaming, stemming from the 3GPP 5G macro-operator roaming and adapted to the specifics of the communication for geographically-distant, small networks interconnected by third party unreliable backhauls. Furthermore, the architecture is exemplified, and its potential is evaluated as further extensions to the Fraunhofer FOKUS Open5GCore, showing that it outperforms today's roaming solution in terms of flexibility and privacy of deployment, backhaul usage and reduced network administration.**

***Index Terms*—5G; Non-Public-Networks; Roaming**

I. Introduction

With the current massive adoption of 5G network technologies, the network environment is transforming from an environment dominated by a set of large scale network operators, administrating country wide networks and offering ubiquitous services to millions of devices towards a massive multi-administrated environment. 5G enables the deployment of small-size Non-public Networks (NPNs), located at the use case premise and locally administrated, which connect only a reduced number of devices and provide a customized service for the specific use case needs [1]. Because of this capability a large number of deployments are foreseen for diverse use case types from mobile broadband services in education institutions and offices, to industrial environments and multimedia production, up to nomadic and mobile networks within construction sites, emergency situations and public transport.

One of the initial key success factors for the adoption of the macro-operator communication environment was roaming. While connected to a visited network, deployed by a different operator, a user can access the home network services as well as local services in the visited network. This feature enabled the wide spanning of GSM and LTE technology across the globe, where devices can be worldwide used rather transparently with a single subscription. Roaming is enabled through a specific set of peering functionalities deployed within both the visited and home networks, enabling the exchange of information to authenticate, authorize, account and charge the subscriber for the specific services.

However, the roaming mechanisms provided by 3GPP are not suitable for deployment for a very large number of dynamically growing NPNs each with their own reliability support and own administration policies. In order to adopt a roaming solution, would be the handling of the communication across third party provided backhaul with increased unreliability levels and high variations in capacity and delay. Also to maintain the privacy of communication, visiting subscriber data traffic should be isolated from the local services.

A similar and rather reduced in functional scope solution was deployed for local WiFi networks. The Eduroam network is over twenty thousand locations in Europe alone [2] and provides WiFi access mainly in educational institutions. Similar to the 3GPP roaming mechanisms, Eduroam provides a very good architectural perspective to handle the multi-administrated network environment with dynamic backhaul connectivity, but missing features, such as bi-directional authentication and authorization, as well as shared network between local and visiting users and home routed services.

To be able to respond to all the NPN communication requirements, we propose an extended roaming architecture with additional key functionalities, handling the flexibility and privacy of deployment, backhaul usage and reduced network administration. Specifically, these requirements were gathered by the discussion with Eduroam local network administrators. The proposed functionality is further described as extensions of the Fraunhofer FOKUS Open5GCore [3] software toolkit.

The rest of this paper is organized as follows. Sec. II introduces the 5G and Eduroam roaming mechanisms. Sec. III underlines the specific requirements to be reached by a new roaming solution while Sec. IV describes the new proposed high level architecture and functionality. Sec. V presents the design of our functional extensions as part of the Open5GCore and Sec. VI concludes and suggests directions for future work.

978-1-6654-2434-9/21/$31.00 ©2021 IEEE

II. Roaming Architectures

A. Eduroam

The architecture for eduroam roaming [4] is based on a federation, which by itself relies on trust among independent administrated networks to achieve authentication and authorization. There are two direct trust relations, i.e., user and Identity Provider (IdP) or IdP and Service Provider (SP), and one indirect trust relation (user and SP, though IdP). This trust is achieved through mutual authentication between users and IdPs, and by a RADIUS hierarchy between IdPs and SPs.

The authentication and authorization process starts with the usage of a common Service Set Identifier (SSID) for the wireless network of an SP, offering seamless connection regardless of the user location. To make sure that only authorized users connect to this network, IEEE 802.1X is used. The user, or its supplicant, sends the access request to an authenticator (e.g., Wi-Fi Access Point) at the SP, which will proxy the request through the RADIUS hierarchy until it reaches the authentication server of the user's home organization (IdP). This authentication request uses the Extensible Authentication Protocol (EAP) with two objectives: using an EAP method that ensures integrity and security of user credentials transport to the home organization and allowing the user to negotiate the method directly with its home organization. So, an EAP secure tunnel (most commonly with Transport Layer Security (TLS)) is established between users and IdPs, and RADIUS only transparently proxies the requests from one location to another. This proxying is based on the outer identity in the EAP message sent in clear text and must be a valid user identifier with a realm, i.e., something@realm or just @realm. This realm is the domain name of the institution the IdP belongs to, and the first part is an anonymous identity so not to reveal information about the user, connecting to the network.

In-between the SP and IdP, the trust fabric of the federation is a proxy hierarchy of RADIUS servers similar to the one of Domain Name System (DNS), which agree on shared secrets between hierarchy levels and thus trust each other. Each access request, as well as access responses moving through the inverse path, are thus routed through a chain in the hierarchy. Fig. 1, shows an example of such roaming procedure.

This federation, based on a RADIUS hierarchy, however, possesses several limitations that may affect the experience of the users. First, the authentication is not bi-directional. An user does not really know what eduroam network is being used to provide access, as the trust is indirectly provided by a trust relation between the IdP and the SP. Second, the user data path is connected to the visited network and, if any services are available for usage, these will be the services of the visited network. This creates an issue in terms of security for the visited network, which typically only wants local users to access their services. Also as a worse experience for users in roaming as they get disconnected from services at their home organization unless they use a Virtual Private Network (VPN). Finally, there is no signaling of error conditions in the RADIUS protocol, and the IEEE 802.1X standard also

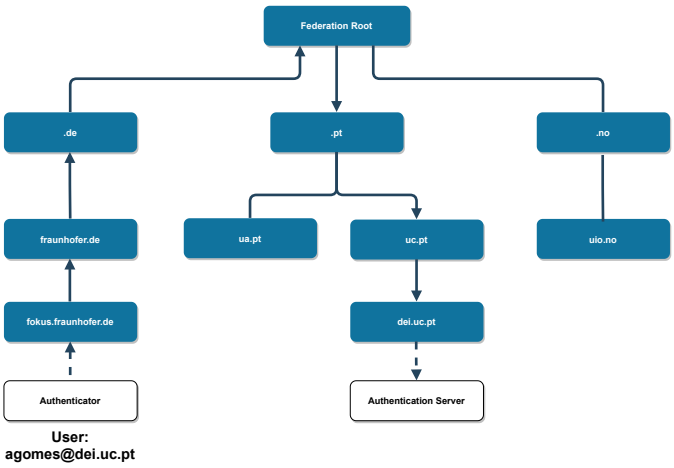

Fig. 1. eduroam RADIUS Hierarchy

does not allow conveying of extended failure reasons to the end user's device. This means that issues such as backhaul interruptions are not known to the user, and no notifications are sent to the user when the backhaul connection is broken. That may become a real problem when unreliable and shared backhaul links are used as of today, as users will not be able to connect and no alternative will be found automatically.

B. 5G Roaming Architecture

For being able to connect devices using the 5G and other access networks, 3GPP has specified a comprehensive standard core network architecture. It consists of User Equipment (UE) representing the device of the subscriber, which connects to the 5G Access Network (AN), that uses the 5G Core Network to provide the connectivity services. The core network is composed of different network functions [5]. The Access and Mobility Management Function (AMF) is responsible for connection and mobility management functionality. The Session Management Function (SMF) handles the Packet Data Unit (PDU) session related functionalities. Authentication Server Function (AUSF) works as the authenticator for the UE while the Unified Data Management (UDM) stores the subscription profile. One or more User Plane Functions (UPFs)s take care of data plane functionalities within the 5G system. Network Repository Function (NRF) in the 5G Core (5GC) network enables the discovery and the selection of Network Function (NF) instances and their supported services.

Two types of roaming approaches are supported in the 5G architecture [6].

1) **Local-Breakout** The authentication of the user residing in the visited network is handled by the home network. The addressing is performed by the visited network and the data traffic is offloaded from the visited network to the data network directly.
2) **Home-Routed** The authentication and addressing for the visited subscribers are managed by the home network. Additionally, the data traffic is routed via the home network to the data network.

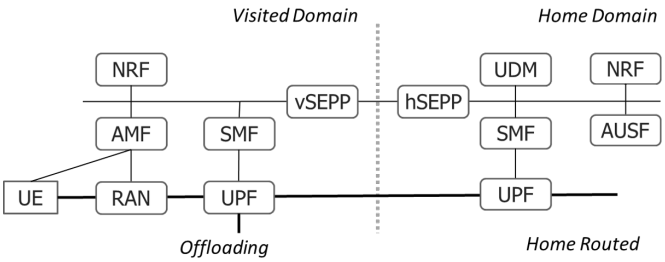

Fig. 2. 5G Roaming Architecture Example

For the communication between the visited and the home domain, 3GPP has defined another component: Security Edge Protection Proxy (SEPP). SEPP works as a service relay between the domains providing security and privacy for each of the domains as also for the interconnection [7].

Additional to these components, 3GPP defined the Service Communication Proxy (SCP) as a control plane routing agent. It has the capability to perform load balancing and overload handling within the network and can be deployed at network level, shared-slice level and slice-specific level [5].

The roaming architecture of 5G is tributary to the current interconnections between large scale operators. It relies on the availability of a peering context between the two operators and a service layer agreement, which is negotiated previously to any interconnection. Because of this, a rather large set of operations have to be executed in a non-automatic fashion. The operations include the discovery of the visited domains (introduced statically in the SEPP forwarding tables), the selection of the visited network (done by the UE using the network code when no same country code network could be found), the authentication and the authorization of communication between the networks (trust is achieved through contractual means), and the guarantee of the availability of the backhaul for the communication between the two networks [8]. None of these features could be assumed for small size NPNs. Instead they would have to be handled within an extension of the given architecture, as described in the following sections.

III. Requirements

As illustrated in the previous section, a comprehensive NPN roaming architecture has to respond to additional requirements compared to the current 5G network architecture. This includes as minimal the following:

1) **Adding new NPNs** - Easy and dynamic addition of new networks which can provide visited networks and visiting subscribers.
2) **Network Discovery and Selection** - The UEs should receive from the home domain an indication of the NPNs which could be located in the immediate vicinity and selected as visited domains. As these represent potential networks not actual available networks, an extended list may be added to cover potential subscriber movement.
3) **Visited Network Privacy** - Ensuring the security of the visited network from unauthorized accesses and the protection of the local services, from potential attacks from the visiting subscribers through data traffic isolation.
4) **Secure authentication of the visited and home networks** - Establishment of a "discovery and selection of the home domain" and of a "bi-directional authentication and authorization through a trust authority between the visited and home networks".
5) **Accounting** - Accounting and lawful interception in both visited and home domain to assure the understanding and back tracing of subscriber data traffic.
6) **Inter-domain exchange security and privacy** - Establishment of a secure end-to-end interconnection between the visited and the home domain.
7) **Communication over the backhaul** - Dynamic handling of unreliable intern-domain backhaul to reliably exchange control plane message and data plane traffic.

IV. NPN Roaming Architecture

To be able to address the additional requirements, we propose to add the following functionalities to the end-to-end 5G network as illustrated in Fig. 3.

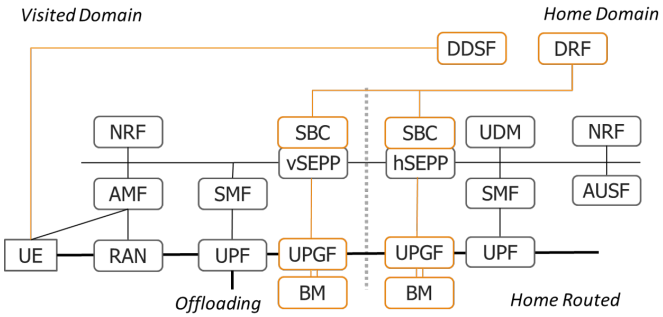

Fig. 3. Extended Inter-NPN Roaming Architecture

Domain Discovery and Selection Function (DDSF) - This function provides to the UE indications on the possible visited domain networks which may be selected in the location of the subscriber. The information exchange is highly similar to the one of the 4G Access Network Disovery and Selection Function (ANDSF). Different from the ANDSF, the information provided should include an ordered list of NPNs described by the country code and the network code. To be able to use this list, the UEs have to be able to support the national roaming feature, which it is theoretically possible even today, however is not activated due to policy reasons.

Bandwidth Management (BM) - To interconnect networks pertaining to geographically distant networks connected through unreliable backhauls, the system should include an additional NF which is able to determine dynamically available network connections between the local and remote domains and to notify on specific events. This includes the availability of different backhauls as well as their quality characteristics in terms of capacity, delay and packet loss. This functionality is highly similar to the functionality provided by Software Defined Wide Area Networks (SD-WAN). An SD-WAN solution

can be used as basis, further extended with the interaction, with the data and the control plane of the packet core.

User Plane Gateway Function (UPGF) - The UPGF represents an extended UPF able to execute operations related to secure connectivity from home to the remote domain complementing the BM functionality with additional data flow level firewall and gating. Such functionality should be present in any network deployment in order to protect the network albeit not depicted in 3GPP architectures.

Session Border Control (SBC) - The SBC represents a new NF added to the control plane, proxying all the messages from one domain to the other, similar to the 5G SCP component. The SBC is in charge of interconnecting with SBCs of other NPNs through a specific discovery, selection and secure authentication procedure as described in the following.

Domain Repository Function (DRF) - An additional logical NF added to the end-to-end architecture, enabling the discovery of the home domains for subscribers attempting to connect to the local network with non-local identities. The DRF is similar to the discovery of home domains in the Eduroam architecture. However, in order to not change the authenticaiton and authorization procedures, the domain discovery will be executed as an intermediary step in the registration of the subscriber.

In case of local breakout, the roaming scenario will follow the below steps:

1) When a user device is located in the coverage range of a potential visited NPN, it initiates registration procedures by establishing a radio connection with the local RAN and sending the registration request to the local AMF.
2) The local AMF will determine that the claimed identity, provided by the subscriber, is pertaining to the local domain or an external one. In case of external, the AMF will forward the request to the local SBC component.
3) The SBC will check if a connection already available with the home domain of the UE and if it will use that connection. If not, the SBC will query the DRF for the connectivity points of the home domain of the device.
4) The DRF will respond with the IP address where the home domain is expecting an SD-WAN connection to be established as well as with the IP address within the connection where the home SBC can be found.
5) The local SBC will forward this information to the BM to establish a secure connection with the home domain.
6) When the connectivity with the home domain is completed, the local SBC triggers to establish on its own a connectivity with the home SBC, enabling an end-to-end control plane across the backhaul.
7) If any of the previous steps before the interconnection between SBCs fails, then the UE will be notified that there is no possibility to connect using the visited domain i.e. registration fails. If the connectivity between SBCs is realized, then the registration procedure [9] will continue similar to the roaming situation.

If there is a need for home routed sessions, these will be established in the same way as the home routed services through adding the UPGFs in both the visited and home domain to the end-to-end data path. Additional to the roaming, through the BM, the UPGFs receive additional information on the momentary capacity of the backhaul, having the possibility to adapt the communication to the available resources.

Whenever there are no more visiting subscribers from a home domain, both the SBC and the BM will terminate their connections. The binding between two NPNs is maintained only when there are visiting subscribers and not in other cases.

Not all these functionalities are required for all the specific deployments. The end-to-end system could function without some of these functions, however, with a reduced set of features. For example, if there is no home routed data traffic, there is no need to deploy the UPGF in neither the home or the visited domains and the role of the BM is drastically reduced. The local AMF has to be aware that the control plane messages for visiting subscribers has to be forwarded to the SBC and the SMF should be configured to forward the complete home routed data traffic through the UPGF, which is a typical behaviour for a system. Both of these are configurations of the system and do not require modification to already deployed functions. This make the proposed architecture rather easy to be added to existing deployments.

V. Open5GCore Functional Extension

The Fraunhofer FOKUS Open5GCore toolkit is a practical implementation of the 3GPP 5G core network developed in C programming language for Linux OS. At the current moment, the Open5GCore Rel. 6 includes the essential functionality needed to deploy an NPN network, including the functionality for authentication and authorization, connectivity management, session management and mobility. The different NFs are implemented separately, as expected from the 3GPP standards following the specifications. Because of this, the Open5GCore has been deployed in a large set of environments where it interoperated with various base stations and devices as part of the end-to-end system. As such, we expect that through its vendor independent and standard allignment nature, Open5GCore provides a significant basis for prototype developments within the core networks. Additional to the NFs, the Open5GCore includes a UE and a gNB simulation for functional testing of network features. The platform also has a benchmarking tool enabling the easy configuration of different workloads and the acquisition of comprehensive monitored data on the status of the system enabling capacity and reliability testing.

For the backhaul management several extensions to the Wiregard are proposed. Wiregard was selected as basis of the implementation due to its large flexibility in terms of piggybacking information. Indeed, this feature was used to be able to piggyback path performance statistics, enabling an extensive data path selection in case multiple backhauls are available. Wiregard was extended with a control plane to establish dynamically different connections and to exchange the data path reports with external functions. With this, a bi-directional domain authentication and security association is created dynamically, upon the request from the Open5GCore

control plane. Furthermore, Wiregard gives the possibility to connect to multiple remote servers to be able to interact with multiple home domains for the visited subscribers. This solution outperforms the current roaming path establishments in terms of dynamic establishments and termination as well as in granular control of the available capacity across unreliable backhauls, making it ideal for inter-NPN connectivity.

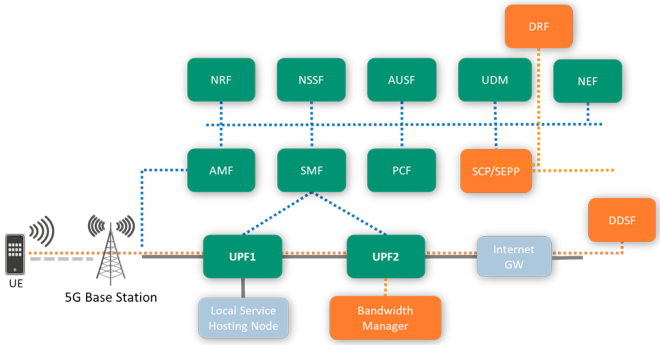

Fig. 4. Open5GCore Architecture

Furthermore, the Open5GCore was extended with an Internet Gateway (IGW) function through which the inter-domain data traffic is transmitted. The IGW provides the means for firewalling and gating of the specific domain by using specific linux tools such as iptables and traffic control - TC, and protect the domain from the other domains using the local policies.

Open5GCore is extended with the NF, DDSF to provide information about the available visited domain networks. UE queries the DDSF to find out available access networks while in visited network coverage area. DDSF provides lists of PLMNs to the UE for each of the network domain. The UE then selects one PLMN from the list and try to connect to the access network. If the connection is refused by the network then it tries with another PLMN from the list. Once the connection is accepted, the authentication of the UE is initiated by the local AMF following the concept of proposed authentication architecture in case of roaming.

To be able to complete the proposed architecture, an integrated SBC component is implemented including the functionality of SEPP [10] in terms of securing the control plane connectivity and SCP for proxying all the specific data traffic from the domain. SEPP is filtering the traffic coming from interconnected NPNs ensuring anti spoofing. Typically, the SCP is using the NRF information in order to determine where to transmit the messages for intra-domain connectivity. For the inter-domain connectivity, the information has to be received from the DRF. As not to over-complicate the architecture, for the DRF, the current NRF functionality is used, adding the specific configurations. Ultimately, for NF selection, the SBC is using two NRFs: one for the finding of NFs within the same domain and one for the external NFs. With this, functionality which is already available in the core network, is re-used and minimally modified to address the needs of this new interconnection, drastically reducing the implementation, testing and interoperability time. As a single component is communicating with external entities, the administrative footprint of supporting additional visiting subscribers is minimal.

VI. Conclusions and Further Work

NPN networks are gaining popularity in the local network deployments due to their specific 5G reliability and security. However, current deployed solutions are lacking native support for roaming. Immediate workarounds, using the carrier grade networks roaming, have significant drawbacks mainly due to the inflexibility in the deployments, lack of automation and potential instability brought by unreliable backhauls. To fill this gap, we have proposed a set of additional NFs combining the 3GPP 5G and the local network WiFi roaming paradigms so that to use the 5G functionality in a Eduroam like manner. This has paved the way for a comprehensive architecture acting as a blue-print for further developments. For the scope of this paper, we have focused on the general overview of the different new NFs implemented into the Open5GCore and concluded that it is providing the expected practical functionality. Further work is considering the evaluation of each of this architecture components separately as well as within an integrated system. Also, performance optimizations though advanced algorithms were beyond the scope of this paper and will be addressed in the future. In this regard, it may be worthwhile to consider comprehensive bandwidth management mechanisms and its dynamic interactions with the control and data plane.

Acknowledgment

This work was supported in part by the European Commission under the 5G-PPP project FUDGE-5G (H2020-ICT-42-2020 call, grant number 957242). The views expressed in this contribution are those of the authors and do not necessarily represent the project.

References

[1] 5GACIA, "5G Non-Public Networks for Industrial Scenarios," https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/WP_5G_NPN_2019_01.pdf, Jul 2019.

[2] "Eduroam Supporting Services," https://monitor.eduroam.org/, Mar 2021.

[3] F. FOKUS, "Open5GCore – The Next Mobile Core Net- work Testbed Platform," www.open5gcore.org (last visited on 25.03.2021).

[4] K. Wierenga, S. Winter, and T. Wolniewicz, "The eduroam Architecture for Network Roaming," Internet Requests for Comments, RFC Editor, RFC 7593, September 2015. [Online]. Available: https://tools.ietf.org/html/rfc7593

[5] 3GPP, "System architecture for the 5G System (5GS) ," https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.07.00_60/ts_123501v160700p.pdf, Jan 2021.

[6] R. Pathak, "Roaming in 5G Network," https://www.netmanias.com/en/post/blog/14592/5g/roaming-in-5g-network, Feb 2020.

[7] 3GPP, "Public Land Mobile Network (PLMN) Interconnection," https://www.etsi.org/deliver/etsi_ts/129500_129599/129573/16.05.00_60/ts_129573v160500p.pdf, Jan 2021.

[8] GSMA, "5G Roaming Guidelines," https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v2.0.pdf, May 2020.

[9] 3GPP, "Procedures for the 5G System (5GS) ," https://www.etsi.org/deliver/etsi_ts/123500_123599/123502/16.07.01_60/ts_123502v160701p.pdf, Jan 2021.

[10] "5G Roaming with SEPP (Security Edge Protection Proxy)," https://blog.3g4g.co.uk/2020/06/5g-roaming-with-sepp-security-edge.html, Jun 2020.