5G-SSAAC: Slice-specific Authentication and Access Control in 5G

Shanay Behrad
Orange Labs
Caen, France
shanay.behrad@orange.com

Emmanuel Bertin
Orange Labs
Caen, France
emmanuel.bertin@orange.com

Séphane Tuffin
Orange Labs
Lannion, France
stephane.tuffin@orange.com

Noel Crespi
Telecom SudParis, CNRS UMR 5157,
Institut Mines-Telecom
France
noel.crespi@it-sudparis.eu

***Abstract*—The fifth generation of mobile cellular networks (5G) is designed to support a set of new requirements and use cases, including connectivity for the IoT (Internet of Things). Due to the industry and the user's expectation of having connectivity embedded into IoT devices, the "wholesale wireless connectivity" concept is gaining more and more attention. According to this concept, connectivity providers sell connectivity to 3rd parties, which in turn provide it to their own devices. However, this concept brings also new architecture and security requirements that are not fully addressed by the state of the art. Taking advantage of the flexibility provided by virtualization technologies (including network slicing), we propose in this paper a new 5G-SSAAC (5G Slice Specific Authentication and Access Control) mechanism that delegates authentication and access control of the devices to the 3rd parties providing these devices, thereby decreasing the load of the connectivity provider's CN (core network), while increasing flexibility and modularity of the whole 5G network.**

Keywords—Loose Coupling, AAC, RAN, Network Slicing, 5G

I. INTRODUCTION

Virtualization technologies are being progressively incorporated into cellular network architectures, as a mean to offer cost-effective and flexible infrastructures and to provide services in a dynamic manner [1]. While classically, the design of cellular networks strongly distinguishes between access network (with functions related to radio technologies, e.g. radio resource management) and CN (with functions related to access control, routing, etc.), virtualization technologies make these borders more blurred. They are for example enabling MEC (Mobile Edge Computing) architectures that provide the ability to execute network functions in data centers that are in the proximity of the users [2, 3]. Therefore, CN functions may be executed in a proximity data center and vice versa.

Virtualization technologies are also enabling a greater openness of 5G network to 3rd parties (i.e., any business actor that is not the network operator), with the concept of network slicing. Each network slice addresses a specific set of quality of service parameters (throughput, latency, etc.) and could be dedicated to a 3rd party according to its requirements [4, 5]. Although network slices can be designed by enabling or disabling certain network functions (according to 3rd parties' requirements), the functions of the 5G RAN (radio access network) and the interfaces between the RAN and the CN are common for all network slices. Some network functions, like authentication and user access control, are done outside the network slices; these are the same for all of the network slices despite the different specifications of these slices [6, 7]. This means that, in 5G, the AAC (authentication and access control) of the users is done before the slice selection phase. However, despite the introduction of such virtualization techniques, cellular network architectures should still be considered as monolithic: the different parts of the network remain strongly coupled and dependent on each other. The network slicing concept is adding here flexibility, but still remains in the same architectural logic as the physical networks, with tightly coupled network components; there is no customization at the network level of the provided services [8].

This paper is intended as an initial step to introduce a more loosely coupled design into the whole 5G network architecture. We propose here a new approach to open network functions to 3rd parties, through a new kind of interface between the access network and 3rd parties' network slices. Our aim is notably to maximize the decoupling between them and increase the flexibility of the network to address various use-cases. In 5G-SSAAC (5G Slice Specific Authentication and Access Control) we focus on the AAC aspects of this decoupling process. We define three network functions in a 5G RAN to delegate the AAC of devices to the 3rd parties providing these devices. This allows 3rd parties to choose their own AAC method according to their security needs. In other words, the AAC is done inside the 3rd party's slice and not outside of it. It means that SIM-based AAC mechanisms might only be used wherever they are needed (e.g., for Mobile BroadBand access, not for IoT applications with constrained devices). From the 5G network operator's perspective, this possibility to delegate users' AAC to 3rd parties is an interesting tool for enabling wholesale wireless connectivity. In addition, this would prevent the network from managing the subscriptions of a huge amount of IoT devices from different 3rd party organizations.

The rest of the paper is organized as follows. In section II we introduce some motivating use cases and derive the related requirements, which are compared to the state of the art in section III. We then detail our 5G-SSAAC proposal in section IV. Section V is dedicated to evaluating the impact of the proposed 5G-SSAAC architecture on RAN through a testbed based on the OAI (Open Air Interface) open-source product. Finally, we provide some concluding remarks in section VI.

978-1-5386-9376-6/19/$31.00 ©2019 European Union

II. 5G SLICE- SPECIFIC AUTHENTICATION AND ACCESS CONTROL: USE CASES AND REQUIREMENTS

Three typical use cases are described below for deriving the requirements to address on the end users' side, on the 3rd party organizations' side, and for the 5G network operators.

A. Motivating Use Cases

1) Alice buys a device with cellular connectivity to stay connected everywhere (e.g., a connected vehicle). She wants to have wireless connectivity embedded inside her device. That means she does not want to have an additional subscription with a wireless carrier and the need to set up an accounting plan with that carrier.

2) Alice lives in a smart home with a smart light system, a smart energy usage control system, a smart entertainment system, and a smart lock system. The IoT devices of these systems are connected to the outside world through a 5G network. The importance of security leakage is not the same for all these systems (malicious access to the smart lock system is more dangerous that malicious access to the entertainment system) [9]. On the other hand, most of her devices are constrained devices with low energy and processing power and they are not able to support strong security algorithms [1].

3) Alice works as factory manager at Acme corporation. She wants to better automate the production of her factory. Alice subscribes to a 5G network slice, so her factory robots can access this slice through 5G connectivity. Acme only trusts itself to provide security policies, accounting and configurations data for its factory robots [10]. So Alice wants to manage the identities and credentials of the robots, as well as their life cycles. She does not want to rely on the 5G network operator for installing each new robot or for uninstalling and eliminating a robot's profile and credentials from the network.

B. Derived Requirements

As can be inferred from the use cases, there are a number of requirements for slice-specific AAC mechanisms which are summarized as follows:

- *R1: Provide embedded connectivity inside devices.* Future connected devices such as connected vehicles and future things for automation and assisted living are now believed to be best retailed when connectivity is directly commercialized with the device, for better customer experience. In these cases, a connectivity provider (i.e., the 5G network operator) sells connectivity to different verticals which in turn provide them to their own users in a B2B2C business model (Business to Business to Consumer). The 3rd parties (verticals) should then be able to manage the identities and credentials of their provided devices in order to control their subscriptions and connectivity usage.
- *R2: Allow 3rd parties to choose their own AAC methods.* The security requirements in each of the use cases are distinct. In other words, the sensitivity of the signaling and data messages between the devices and the network is not the same for all types of devices (nor for all use cases). Therefore the network should have the ability to allow the 3rd parties to choose the appropriate AAC mechanisms according to the security requirements of their proposed services.
- *R3: Allow 3rd parties to manage the lifecycles of their devices.* The fleet of devices belonging to a specific 3rd party is not static. New devices are regularly added to this fleet and old one uninstalled. The network should offer 3rd parties the ability to control the whole lifecycle from their devices, from enrollment to disenrollment processes.
- *R4: Provide AAC mechanisms for constrained devices.* The devices involved in each use case are different in terms of computational power and restricted in their energy supply. The network should give 3rd parties the ability to apply the most suitable AAC mechanisms for each type of constrained devices.
- *R5: Support for a massive number of devices.* A massive number of devices attempting to simultaneously connect to the 5G network operator's CN (by sending attachment and AAC requests) may cause congestions in the CN. Therefore the network should be able to give the ability to the 3rd parties to manage the AAC of their provided devices to avoid the congestions in the 5G network operator's core.

III. RELATED WORKS

AAC of UEs (User Equipment, refers here to any device that needs cellular connectivity, e.g., smartphones or IoT devices) in previous cellular networks (from 2G to 4G) is on a secure element, i.e. a SIM card: a globally unique identifier calls IMSI and a secret key shared between the UE and the network are physically provisioned on the card for each new subscription [11]. As for 5G phase 1 specifications, 3GPP decides to keep working with such a secure element in the device and with the AKA (authentication and key agreement) protocols for the UEs AAC as well (e.g., 5G-AKA and EAP-AKA protocols) [7].

Today, the use of eSIM (more precisely, eUICC) that means an embedded SIM instead of a plastic SIM card, is gaining more attention. Through eSIMs, users can choose which operators they would like to subscribe to. Over the air activation methods are proposed to provision the needed credentials to the eSIMs in a secure manner [12]. Although it is possible to add embedded connectivity features to some devices through the eSIMs, identity management and connectivity usage control of these devices are still done under the responsibility of the operator and not of the device providers (3rd parties). The 3rd parties are not able to choose their AAC mechanisms according to their security requirements and manage the lifetime of their devices. The AAC mechanisms in eSIMs are also based on the AKA protocols. However, AKA protocols used in cellular networks are not fully suitable for constrained devices. Moreover, when a massive number of devices is simultaneously attaching to the network, these protocols increases the computations overhead on the operator's network side as well [13, 14].

To overcome the shortcomings of AKA protocols in the presence of a massive constrained device, group-based AAC mechanisms have been proposed [15]. The general steps of

these mechanisms are forming a group of devices (based on their local communication areas, applications or behaviors),choosing a leader device for the group and forwarding signaling messages (AAC requests) of the group members to the network through this group leader [14, 16-18]. In [19], the devices form a group also, but they do not choose a group leader. The authentication is done between the first device who attempt to connect to the network and then continued locally with the remaining members of the group. These group-based AAC mechanisms address the requirements of constrained devices and solve the network congestion problems caused by a massive number of authentication requests. However, as the management of joining and leaving the devices in the group is done locally in the serving network, the CN is not aware of each individual device's behavior. It means that, although the CN provides services to each member of the groups, it is not able to control their connectivity usage and security issues [20] and provide different services to each member of the group (including AAC services) according to their different requirements.

There are also some AAC mechanisms designed for preserving the privacy of the UEs when trying to connect to a service provider network or foreign serving networks in the roaming scenarios. In [21] the authors propose an authentication procedure between the UEs and the IoT service providers, in addition to the existing 5G-AKA between the UEs and the 5G network provider. They try to protect the service data and UEs' privacy (UEs are able to anonymously ask for services) against the intermediate nodes like gNBs (i.e., 5G base station). [22] and [23] also provide anonymity when the UEs visit a serving network that is different from its home network. Although these papers show that it is possible to design AAC mechanisms based on the service providers or the visited serving networks security requirements, the network does never provide the ability to choose the AAC mechanisms in a dynamic way. They are not suitable for authenticating the massive number of constrained devices as well.

The different AAC methods and their compatibilities with the different requirements mentioned in the previous section are summarized in table 1. As we can see in this table, cellular AKA and service oriented and anonymity based methods fully meet none of the requirements; eSIM method just addresses embedded connectivity inside the device; while group-based AAC methods address the AAC requirements of the constrained devices and the mass number of devices' simultaneous connectivity request. We propose an approach to address these requirements by introducing a more loosely coupled AAC architecture, enabling to dynamically select the AAC method on a slice-specific basis.

TABLE I. DIFFERENT AAC METHODS AND THEIR COMPATIBILITY WITH THE DIFFERENT REQUIREMENTS

AAC method	R1	R2	R3	R4	R5
Cellular AKA	−	−	−	−	−
eSIM	+	−	−	−	−
Group based	−	−	−	+	+
Service-oriented and anonymity based	−	+/−	−	−	−

We propose an approach to address these requirements by introducing a more loosely coupled AAC architecture, enabling to dynamically select the AAC method on a slice-specific basis.

IV. THE PROPOSED 5G-SSAAC

While the current cellular RAN is mainly intended for forwarding signaling and data messages between the CN and the UEs and providing them the radio resources, we propose here to design a new RAN function that is able to host an authentication function from a 3rd party. The main challenge is to intercept the dependencies between the RAN and the CN in terms of the authentication and access control of the users. More precisely, we introduce three network functions in the RAN to enable a more loosely coupled architecture. One of them is developed and provided under the 3rd party's responsibility and the other two are under the responsibility of the MNO. These functions are in the form of a software code executable in the proximity data center located at the level of the 5G base station (gNB). By using these functions, the access network can register 3rd parties' slices and connect each UE to the adequate 3rd party's slice. These three network functions are as follows:

- 3rd GW Virtual Function: This function carries all the AAC for the devices owned by a given 3rd party on a given cell. It belongs to the 3rd party slice. The 3rd party decides how to design this function according to its requirements, and which AAC protocol to execute.
- 3rd GW Function Repository: This function is under the MNO's responsibility. It registers the 3rd GW Virtual Functions of the 3rd parties by keeping their local addresses. It is an anchor point between the 5G network operator and 3rd party. It provides to 3rd parties the ability to register their 3rd GW Virtual Functions in the 5G access network.
- RRC Connection Endpoint: This function is also under the MNO's responsibility. It is the termination point of the signaling messages with the UEs (on the MNO's side and not on the 3rd party's slice side). The RRC Connection Endpoint reuses the 5G RAN function, with some additional features detailed below.

V. EVALUATIONS

A. 5G-SSAAC Procedure

In this section, we describe and evaluate in detail the proposed 5G-SSAAC mechanism focusing on the first attachment procedure of the UE in the network. The procedure consists of four main phases.

1) 3rd Party's slice registration and UE' credential provisioning: Before starting to establish the connection between the UE and the network, two prerequisites are necessary: the 3rd party's slice registration and the UE credentials' provisioning. For the 3rd party's slice registration, a 3rd party organization provides its 3rd GW Virtual Function to a 5G network operator. The 5G network operator registers the 3rd GW Virtual Function's information, e.g. its address, in its 3rd GW Function Repository. For the UE credentials' provisioning, the 3rd

party organization provisions its UE with the Slice ID (the 3rd party's slice identifier) and the UE's subscription identities (that identify each UE in the 3rd party's slice).

2) Radio Link Synchronization: Each UE needs to have a communication link with a gNB to exchange messages. During the radio link synchronization procedure, the UE will get the necessary information to establish a connection with the gNB. This procedure is out of the scope of this paper (see the Random Access Procedure [24]).

3) Slice Connection Establishment: Fig. 1 shows this step in detail. This step consists of two sub-steps: The connection establishment between the UE and the gNB, and the connection establishment between the RRC Connection Endpoint and the 3rd GW Virtual Function. The connection between the UE and the RRC Connection Endpoint is called RRC Connection. the and the establishment procedure of it is the same as the RRC connection establishment procedure in LTE (i.e., 4G). After this procedure, the UE can use the radio resources. Next, the attachment request is sent from the UE to the gNB (step 3.a). The Attach Request consists of the UE's subscription identity and the UE's network capabilities (the UE's network capabilities' content depends on the security requirements of the 3rd party slice). This message also includes the slice's ID. The UE informs the gNB about the slice that it wants to connect to by using this ID.

Upon receiving the "Attach Req" message from the UE, the RRC Connection Endpoint gets the 3rd GW Virtual Function information, from the 3rd GW Function Repository to forward the UE's attach request to the right slice. It obtains this information by sending the "Slice Info Req" (step 3.b) message to the 3rd GW Function Repository, specifying the Slice ID. According to this Slice ID, the 3rd GW Function Repository finds the related slice information and sends it to the RRC Connection Endpoint through the "Slice Info Res" (step 3.c) message. The RRC Connection Endpoint is now able to establish a connection with the 3rd GW Virtual Function that is called S1 Signaling Connection by sending the "Attach Req Reroute" message to the 3rd GW Virtual Function (step 3.d). This completes the Slice Connection Establishment procedure and the UE is connected to the 3rd party's slice.

4) Authentication, Access Control, and Session Establishment: All of the processes of the authentication and access control of the UE and the session establishment for providing network services to the UE are conducted inside each 3rd party's slice. The AAC mechanism could be any AA mechanism; the 3rd party organization selects which AAC mechanism to use according to its own security requirements and the security requirements of its subscribers.

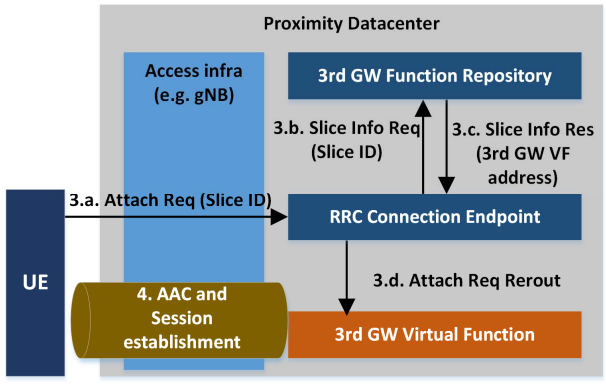

Fig. 1. Information flow of 5G-SSAAC. The main function is the 3rd GW Virtual Function (with the dashed borders)

B. Open Air Interface and Test Bed

In order to further evaluate the impact of our proposal on the RAN, we studied thoroughly its possible implementation with OAI (Open Air Interface). OAI is an open source platform that provides cellular network functions that are executable on general purpose processors (such as x86, ARM). The OAI code consists of two main parts, the OAI-RAN that implements the cellular RAN and the OAI-CN that implements the cellular CN. Both the core and the access network of the proposed solution are implemented based on the OAI (Open Air Interface) code. Our test bed setting is as follows: For making the radio access part (base station), the OAI-RAN is executed on a PC with an Intel Xeon W-2102 quad-core at 2.9 GHz, 16 GB memory; USB3 and Gigabit Eth. To have radio communications, we use an USRP B210 board. This SDR (software defined radio) supports 2*2 MIMO (multiple-input and multiple-output) and connects to the PC through the USB3 interface. The operating system is a 64-bit Ubuntu 14.04 with a low latency kernel. For making the CN part, it is enough to execute the OAI-CN on an Ubuntu 16.04 machine (with kernel 4.7). As the UE, we use Samsung Galaxy S4 and the programmable sim cards, sysmocom. For programming the sim cards, we use a Gemalto IDBridge K30 as card reader/programmer hardware.

C. Implementation impact on the RAN

For implementing our idea, we executed the OAI-CN on two systems and considered them as two network slices of two 3rd parties. Then we modified the OAI-RAN part and adding our functions to it. The OAI-RAN consists of three main parts, openair1, openair2, and openair3. These sections are designed based on the signaling plane and the data plane protocol stacks of the link between the UEs and the base station and also between the base station and the CN. Openair 1 is the implementation of the physical layer. Openair 2 is the implementation of the MAC, RLC, PDCP and RRC layers. Openair 3 is the implementation of the UDP, GTP, SCTP, S1AP and NAS layers. The detailed functionalities of each layer is out of the scope of this paper. In order to implement the four steps of the detailed procedure that we describe in this section, part A, we change the different parts of the OAI-RAN code for each step.

1) 3rd Party's slice registration and UEs' credentials provisioning. In the current OAI-RAN, when the eNB (4G base station) is booted up, it identifies the MME that it can have a connection with. We consider this process as the 3rd Party's slice registration process and in order to have two slices, we add another MME instance. The relevant changes are done in the s1ap_eNB_register_MME function of the Openair 3/S1AP/ s1ap_eNB.c file and in the eNB_app_register function of the Openair 2/ENB_AP/enb_app.c file.

2) Radio Link Synchronization. This step doesn't need any changes.

3) Slice Connection Esbablishment. The modified functions are as follow:
The rrc_eNB_send_S1AP_NAS_FIRST_REQ, the rrc_eNB_process_S1AP_DOWNLINK_NAS and the rrc_eNB_process_S1AP_INITIAL_CONTEXT_SETUP_REQ functions from the Openair2/RRC/LITE/rrc_eNB_S1AP.c file. And the s1ap_eNB_handle_nas_downlink function from the Openair3/S1AP/s1ap_eNB_nas_procedures.c file.

4) Authentication, Access Control and Session Establishment. The modified functions are as follow: The rrc_pdcp_config_security function from the Openair2/RRC/LITE/rrc_eNB_S1AP.c file and the pdcp_apply_security function from the Openair2/LAYER2/PDCP_v10.1.0/pdcp.c file.

Globally, 8 OAI functions are impacted by our proposal (831 lines of codes). Such modifications seem therefore potentially feasible by Radio Access Network manufacturers. In addition, we should also consider the additional works that have to be done by 3rd party players to provide their own security and AAC mechanisms. Moreover, each 3rd party should also design and operate IT solutions to manage the lifecycle of their devices – potentially linked with its existing IT. Network providers could here play a new role by offering pre-designed 3rd GW virtual functions for different types of needs and requirements, as well as the associated IT solutions.

VI. Conclusion and Future Work

In this paper, we propose an original 5G-SSAAC approach to design a new kind of radio access network for the fifth generation of mobile networks. We define three network functions in the RAN in order to enable the delegation of the AAC of the UEs to the 3rd parties which provide them. To do so, we introduce a connection between the UE and the corresponding 3rd party slice before the UE's AAC procedure. This enables to address the new requirements brought by the wholesales connectivity concept. We evaluate this approach via a detailed call flow and an initial study of the potential impact of it on an actual RAN, with the OAI. Our approach can be seen as the first step towards a more loosely-coupled design for 5G network architecture. However, many points are still to be considered to progress on this way such as mobility management of the UEs or security issues raised by our approach (e.g., lack of mandatory encryption between UE and gNB). In our future work, we will implement different AAC mechanisms in an OAI-based RAN for different 3rd parties' networks. Moreover, for addressing some of the security issues, we will also provide a new mechanism to secure the connection between the UE and the RAN without relying on the information coming from the 3rd party's network.

References

[1] 5G Ensure Project, "Deliverable D2.7 Security Architecture (Final)," 2017.

[2] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.

[3] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017.

[4] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," IEEE Communications Magazine, vol. 55, no. 5, pp. 94–100, 2017.

[5] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing & softwarization: A survey on principles, enabling technologies & solutions," IEEE Communications Surveys & Tutorials, 2018.

[6] 3GPP, "System Architecture for the 5G System," TS 23.501, Tech. Spec. V15.3.0, 2018.

[7] 3GPP, "Security architecture and procedures for 5G system," TS 33.501, Tech. Spec. V15.2.0, 2018.

[8] A. Boubendir, E. Bertin, and N. Simoni, "Flexibility and dynamicity for open network-as-a-service: From VNF and architecture modeling to deployment," in NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, pp. 1–6, 2018.

[9] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on, 2017, pp. 1292–1297, 2017.

[10] 5G Ensure Project, "Deliverable D2.1 Use Cases," 2016.

[11] 3GPP, "Security Architecture," *TS 33.401*, Tech. Spec. V15.5.0, 2018.

[12] GSMA, "Remote Provisioning Architecture for Embedded UICC," Tech. Spec. V3.1, 2016.

[13] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: a comprehensive survey," Security and Communication Networks, vol. 2017, 2017.

[14] B. L. Parne, S. Gupta, and N. S. Chaudhari, "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network," IEEE Access, vol. 6, pp. 3668–3684, 2018.

[15] 3GPP, "Service requirements for Machine-Type Communications (MTC)," *TS 22.368*, Tech. Spec. V14.0.1, 2017.

[16] J. Yao, T. Wang, M. Chen, L. Wang, G. Chen, "GBS-AKA: Group-based secure authentication and key agreement for M2M in 4G network", Proc. IEEE Int. Conf. Cloud Comput. Res. Innov. (ICCCRI), pp. 42-48, May 2016.

[17] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," IEEE Internet of Things Journal, vol. 3, no. 3, pp. 408–417, 2016.

[18] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 1017–1022, 2012.

[19] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," Computer Networks, vol. 57, no. 17, pp. 3492–3510, 2013.

[20] R. Giustolisi and C. Gerhmann, "Threats to 5G group-based authentication," in 13th International Conference on Security and Cryptography (SECRYPT 2016), 26-28 July 2016, Madrid, Spain, 2016.

[21] J. Ni, X. Lin, and X. S. Shen, "Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT," IEEE Journal on Selected Areas in Communications, vol. 36, no. 3, pp. 644–657, 2018.

[22] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, "CPAL: A conditional privacy-preserving authentication with access linkability for roaming service," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 46–57, 2014.

[23] J. K. Liu, C.-K. Chu, S. S. Chow, X. Huang, M. H. Au, and J. Zhou, "Time-bound anonymous authentication for roaming networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 178–189, 2015.

[24] 3GPP, "Medium Access Control (MAC) protocol," *TS 36.321*, Tech. Spec. V15.3.0, 2018.