Wireless Communications and Mobile Computing

Special Issue: Context-Based Resource Management and Orchestration in 5G Wireless Access Networks

Context-Awareness Enhances 5G Multi-Access Mobile Edge Computing (MEC) Reliability

Bin Han,1 Stan Wong,2 Christian Mannweiler,3 Marcos Rate Crippa,1 and Hans D. Schotten1,4

1 Institute of Wireless Communication, Technische Universität Kaiserslautern, 67655 Kaiserslautern, Germany.
2 UbiXpace, E3 4PU London, UK.
3 Nokia Bell Labs Germany, 81541 Munich, Germany.
4 Research Group Intelligent Networks, German Research Center for Artificial Intelligence (DFKI GmbH), 67663 Kaiserslautern, Germany.

Correspondence should be addressed to Bin Han; binhan@eit.uni-kl.de

Abstract

The fifth generation (5G) mobile telecommunication network is expected to support multi-access edge computing (MEC), which intends to distribute computation tasks and services from the central cloud to the edge clouds. Towards ultra-responsive, ultra-reliable and ultra-low-latency MEC services, the current mobile network security architecture should enable a more decentralized approach for authentication and authorization processes. This paper proposes a novel distributed authentication architecture that supports flexible, intelligent, and low-cost local authentication with the awareness to context information of network elements such as user equipment and virtual network functions.

Introduction

Fifth generation (5G) mobile telecommunication network has been expected to involve multi-access edge computing (MEC) [1-3]. MEC has evolved from mobile cloud computing, which shifts the important computation and storage tasks from the core network to the access network. Thus, mobile services can gain superiorities of low latency, power efficiency, context-awareness, and enhanced privacy protection [4], [5]. Furthermore, the security concerns become across the core network and the access network - from network elements to user equipment (UE) and from tenants to their network slices [6]. For example, the mobility management entity (MME) is set to be divided into few functions which can be co-existed in the access network and core network. This function decomposition gives the overall system flexibility, deployment efficiency and service agility.

The fourth generation (4G) long-term evolution (LTE) authentication and key agreement (AKA) has an architecturally inherited dependency on the core network, and can therefore constrain the exploitation of MEC. Nevertheless, there has been limited contributions on the
evolution of the LTE centralized security architecture, despite of demands of improved AKA efficiency in MEC [7]. However, delivering a flexible next generation telecommunication system is the main objective of 5G. All services at the edge of the network should be securely provided. Hence, the authentication and authorization processes can also exist at the edge of the network to increase the subscriber authentication efficiency and the reliability to the overall system.

Generally, authentication, authorization and accounting (AAA) processes require certain amount of cost from the system per registration of a subscriber. Putting these processes at the edge of the network would increase the efficiency of subscriber authentication and authorization. Also collecting valuable information helps to understand the context of the overall network situations, the connectivity availability and the traffic pattern [8]. With such knowledge we can increase the overall system reliability with minimal operations cost. In this paper, we will use the context-awareness technique to extract the network situation and reduce the traffic in between front-haul and back-haul when subscriber authentication and authorization take place. Particularly, we use network context information to distinguish the normal from emergency situation and deliver proactive control in facing any situation.

This paper introduces a novel distributed security approach for MEC in 5G networks, which aims at delivering a flexible and intelligent AKA executing within the edge cloud, and decouples the authentication process from the central cloud when backhaul connection outages are detected. The proposed approach is aware to network context information and able to predictively synchronize subscriber profiles to support local AKA procedures.

Materials and Methods

Security Architecture of Cellular Networks

A. Authentication and Key Agreement (AKA) in the 3GPP EPS

Security in the Third Generation Partnership Project (3GPP) Evolved Packet System (EPS) is divided into access stratum (AS) and non-access stratum (NAS) security. Security procedures rely on the EPS architecture; the most important elements are shown in Figure 1 and [9], [10].

Figure 1: Security Architecture of 3GPP LTE / EPS [11]
When a user equipment (UE) attaches to a LTE network, the AKA is executed between UE and mobility management entity (MME). As a result, keys are derived on the UE and the MME, that are used to secure the non-access stratum (NAS) signaling between these two entities. In addition, a key $K_{eNB}$ is derived with the same key of access security management entities ($K_{ASME}$) at both the UE and the MME sides, and passes from the MME to the evolved Node B (eNB) which the UE is connecting. This $K_{eNB}$ is used in the communication session as the basis of access stratum (AS) security, i.e. security on the radio link between the UE and the eNB. Three further keys are derived from $K_{eNB}$, one for control plane integrity protection, another for control plane encryption, and the last for user plane encryption. There is no general user plane integrity protection in LTE, a fourth key for this purpose is derived from $K_{eNB}$ only when required. The traffic protection keys do not remain valid over a long time. Instead, the eNB initiates an intra-cell handover to derive a new $K_{eNB}$ and new traffic protection keys $K_{RRCint}$, $K_{RRCenc}$ and $K_{UPenc}$.

LTE specifies three different pairs of cryptographic algorithms, each pair comprises an confidentiality protection algorithm and an integrity protection algorithm. The reason to have multiple algorithm pairs is to give LTE fallback options in case one of the pairs fails during the expected system lifecycle. Furthermore, the NAS and AS signaling procedures are specified to negotiate the algorithm pairs. Also, the backhaul link is protected by Internet key exchange (IKE) / Internet protocol security (IPsec). Generally, the IPsec tunnels are terminated by a dedicated security gateway (SEG), but they may also be terminated at the MME or serving gateway, for the control plane and user plane, respectively.

Note that in LTE, the eNB is considered as a physically exposed entity, with a notable risk of being compromised by an attacker with physical access. Therefore, it is designed to have no access to the NAS signaling that is protected end-to-end between UE and MME. However, it has access to the user plane traffic that is decrypted and re-encrypted at the eNB between radio interface and backhaul link. To mitigate the threat of unauthorized physical access, 3GPP requires all network elements installed in a “secure environment”. Particularly, the eNB also requires to protect the keys and other important processes. Therefore, the unauthorized access is prohibited.

For an overall security concept for an LTE network, additional non-standardized network security measures must be implemented, such as:

- Perimeter security, traffic filtering between network internal security zones,
- Traffic separation (separate data plane, control plane, management plane, etc.),
- Secure operation and maintenance (O&M),
- Secure operation of services / protocols such like DNS, NTP, IP routing, etc.

**B. Challenges in 5G Multi-Access Mobile Edge Computing**

The 3GPP security architecture specified for LTE/EPS cannot fulfill new requirements of emerging services in 5G. 5G networks requires to improve the flexibility of security functions with the MEC services.

The concept of MEC was proposed by the European Telecommunications Standards Institute (ETSI), suggesting to use the base stations instead of centralized cloud servers for offloading computation tasks from mobile users, in order to provide “IT and cloud-computing capabilities within the radio access network (RAN) in close proximity to mobile subscribers” [12].
Recently, it is extended and generalized to merge with the concept of Fog Computing proposed by Cisco, which aims at exploiting end-user device networks as edge computing units [13]. Differing from traditional mobile cloud computing systems, MEC systems with hierarchical controlling and management are more near to the end users, less coupled with the central cloud, less dependent on the backhaul network, and therefore with a better support to latency-critical applications [4]. The exploitation of MEC, however, can be constrained by the centralized 3GPP LTE/EPS security architecture.

The current AKA procedure deeply relies on the MME in central cloud, the backhaul latency in network attachment and mobility management can become a bottleneck for the quality of MEC services. When data congestions occur in the core network, this delay will significantly increase, and may violate the service latency requirement, especially for some ultra-reliable and ultra-low-latency emergency communication applications [14].

Additionally, the emerging concept of “5G Islands” [15], [16] might be expected to serve a group of devices in the same area autonomously and central-cloud-independently. On one hand, 5G Islands can be created in a scheduled manner to serve public events with requirement of dense MEC traffic but little dependency on core network functions (such like soccer games), or to maintain MEC services with planned disconnection from the core network (such as a cruise ship equipped with a sensor network). On the other hand, they can be also created in unexpected situations where the backhaul connection becomes seriously limited or even unavailable. Typical cases of this kind include cyber-attacks and extreme disasters that can cause tremendous damage to the network infrastructure (such like fires, explosions, earthquakes etc.). No matter if scheduled or unscheduled, in these 5G Islands, a basic set of network functionalities will be provided, regardless of the backhaul connection status. This concept is novel, but the development of its elements has already been launched. For example, [17] discusses how 5G networks will be able to support highly autonomous and smart decision making capabilities at various layers of the network, including the physical and media access control layers. Network architectures [18], [19] were proposed where MMEs autonomously perform UE management in a distributed manner as autonomous distributed MMEs. In this field, distributed edge security methods shall be developed to cope with non-static and unreliable backhaul connections. More specifically, the AKA procedures are expected to be decentralized at the network edge, and to provide stable quality of service of MEC in the 5G.

Decentralized Security Approach over Edge Clouds

A. 5G Authentication Authorization Accounting

Towards a flexible decentralized AKA mechanism for reliable 5G MEC services, we proposed a novel virtualized AAA approach: the 5G AAA [20]. It combines two independent international standard systems that are the 3GPP and the ETSI, as a single platform to manage and secure the subscribers, the tenants and the network slices under the 5G flexible network environment.

Generally, 5G AAA system is constructed by a virtualized-AAA (V-AAA) manager in core network and several V-AAA servers distributed in various edge clouds, and supported by hierarchical databases approaches for tenant data and tenant’s subscribers synchronization. This hierarchical database approach has been divided into two levels of synchronization.
Within the tenant network or dedicated resources of tenant network slice would have bi-directional replication across different regions. On the other hand, the tenant’s subscriber database would be applied many-to-one synchronization with the MNO core network subscriber database. This a directional synchronization. This logical illustration can be found in Figure 2. From the 3GPP view on 5G network architecture [21], the 5G AAA system is an advanced implementation of the access and mobility management function (AMF), which provides a complete generic AMF set in the central cloud with the V-AAA Manager, while offering specifically customized subsets of AMF for various 5G network slices in different local edge clouds with the polymorphic V-AAA servers. Similarly, the hierarchical databases and the Local Subscriber Servers (LSS) together construct the 3GPP unified data management (UDM). Taking the 4-layer-view on 5G network architecture proposed by the 5G Infrastructure Public Private Partnership (5G PPP) [21], the V-AAA Manager can be seen as part of the business supporting system (BSS) on the service layer, and each edge cloud V-AAA server is a virtual network function (VNF) dedicated to a particular network slice.

![Diagram of 5G AAA framework enhanced with Trust Zone in the 5G PPP architecture. The terms OSS, VIM, SDM-X, SDMO and SDM-C stand for operations support system, virtual infrastructure manager, software-defined mobile network (SDM) controller, SDM orchestrator and SDM coordinator, respectively. V/PNF denote virtual/physical network functions.]

Figure 2: The 5G AAA framework enhanced with Trust Zone in the 5G PPP architecture. The terms OSS, VIM, SDM-X, SDMO and SDM-C stand for operations support system, virtual infrastructure manager, software-defined mobile network (SDM) controller, SDM orchestrator and SDM coordinator, respectively. V/PNF denote virtual/physical network functions.
With such an architecture that distributes security functions and databases to all edge clouds, the 5G AAA approach enables a flexible and decentralized decision and application of security policies in every edge cloud. It is able to:

- Keep the centralized governance of tenants and mobile subscribers in the central cloud;
- Allow a degree of freedom of tenant governance their subscribers at the edge cloud;
- Use the AKA generated data to track and authenticate the mobile subscribers from the edge cloud and central cloud;
- Maintain the mobile subscribers and tenants with the point of attachment in the central cloud as well as in the edge cloud;
- Remain subscriber services even when the backhaul connection is limited or unavailable;
- Provide a trust platform collecting the trust value from the mobile subscribers to the NFV-based tenants, and from the physical network entities to the virtual network entities.

B. Trust Zone

The proposed 5G AAA [20] approach enables the AKA procedure in the local edge cloud to improve the MEC services. Nevertheless, its deployment still calls for novel solutions of adaptive AMF invocation. Due to the incomplete AMF set and probably limited budget on security measures, the local V-AAA servers are usually less secured than the central VAAA Managers. Therefore, it is generally preferred to invoke the AMF from the central cloud in common cases, and only to rely on the local version when the backhaul connection cannot satisfy the latency requirement of MEC services due to – intentional or unintentional – restrictions, congestions and collapses. To achieve this, the 5G AAA system must be able to adaptively switch between the centralized and local security modes with respect to the current backhaul connection status. The switching process must be carefully designed to mitigate data leaks.

Motivated by this challenge, we designed an edge cloud security architecture, the Trust Zone (TZ), in order to enhance and extend the 5G AAA approach to a cognitive solution [22]. The basic principle of TZ is to let the local edge cloud cognitively measure the quality of its backhaul connection. When the backhaul is healthy, the AMF is invoked at the V-AAA Manager in central cloud. When the backhaul connection is seriously limited or unavailable, the TZ relies on the V-AAA server that executes local AMF to maintain MEC services.

In a structural view, as illustrated in Figure 2, a TZ system consists of five entities:

1) **Central Cloud Connection Monitoring (CCCM)** – This entity periodically visits the NFV orchestrator in central cloud to evaluate the backhaul status. Additionally, when the backhaul connection is limited or unavailable, CCCM tries to diagnose the malfunction. This diagnose can be used by the software-defined network (SDN) management to assist backhaul recovery with backup resources, e.g. network redundancy and alternative routes such as satellite links. A dynamic network resource allocation in the SDN management can also be supported by the backhaul status information. When the backhaul connection becomes poor, specific network functions such as mobility management and fault management can obtain network resources with higher priorities.
2) **Zone Management (ZM)** – This is the core entity of TZ, which implements the most AMF and is connected with all other TZ entities. It triggers and coordinates the state transitions in TZ, when it receives reports about updated backhaul status. Integrated with interfaces to the central cloud and to the UEs, it also collaborates with the Local Access Assistant (LAA) to accomplish the AS security procedures in the local edge cloud. When the backhaul connection is healthy, ZM cooperates with the V-AAA Manager in central cloud to execute centralized AKA. When the backhaul is limited or unavailable, local authentication is needed, ZM will then collaborate with the LAA to execute local AKA instead.

3) **Local Access Assistant (LAA)** – This entity makes use of the subscriber information that is essential for authentication and stored in the LSS, in order to locally execute security measures such as AKA procedures. It can be considered as a lite AMF module migrated from the central cloud to the local edge cloud. LAA is deactivated by the ZM when the backhaul is reliably healthy, and activated otherwise. The LAA is isolated from the ZM mainly due to security concerns: the subscriber database should be decoupled from the ZM that is the central controlling unit of TZ and the priori target of potential cyber-attacks. To mitigate the risk that the LAA is attacked and manipulated to send fake information to the central cloud, an asymmetric trust relation between the central V-AAA manager and the local V-AAA server is needed, as will be introduced later.

4) **Security Auditing (SA)** – Mobile network operators (MNOs) usually keep logs of security critical operations for each subscriber. These logs can be audited to investigate all potential risks of illegal access and cyberattacks. Both the log database and the auditing center are usually located in the central cloud, so when the backhaul connection is unavailable, they cannot keep tracking the AAA operations executed by local V-AAA servers. To close this gap and provide a continuous audit, the SA module is designed. It is activated under the local security mode to record all local AAA operations. After the backhaul recovery, these records can be either actively pushed to the central auditing center, or passively pulled upon request.

5) **Emergency Services (ES)** – we have named some extreme disasters that can lead to backhaul outages earlier, such as fires, explosions and earthquakes. These events can be harmful not only to the network infrastructure, but also to human safety. A set of emergency services can be defined, which help users avoid personal injury and property damage under such disasters, even when their devices cannot be authenticated by the network. These services are implemented in the ES entity, including but not limited to public disaster alarm, evacuation guidance, positioning service, emergency call and short message service (SMS). Additionally, the ES is connected to the Internet-of-things gateway (IoT-GW) to collect context information about public disasters from external sensor networks. Such information can be visited by the NFV management and orchestration (NFV MANO) through the CCCM to assist the network diagnose and backhaul recovery processes.

Among those entities listed above, the first three entities are dedicated to a specific tenant or network slice, and within the edge cloud V-AAA server. However, CCCM and ES are defined as common functions and non-V-AAA server functions exist on both control plane and user plane.¹

---

¹Further details about the interfaces between TZ entities and a behaviour model of TZ are available in [22].
C. Asymmetric Trust to Safely Transfer Access Management

It should be noted that local V-AAA servers are less secured than the central V-AAA Manager, cyber-attackers may initiate attacks to disconnect the central cloud and the edge cloud, and hack the local TZ that is easier to target than the central cloud. Then they may eventually attempt to obtain access to the central cloud during the backhaul recovery, when the TZ hands the access management back over to the central cloud. To mitigate this risk, we designed an asymmetric approach of transferring the access management between the central cloud and the edge cloud, which can be briefly summarized as follows: When a degradation of backhaul connection occurs and the TZ switches to the local security mode, all devices already authenticated by the central V-AAA Manager before the mode switching will be considered as trusted by the local V-AAA server, and retain a seamless access to the local MEC services. In contrast, devices that newly arrive after the switching must go through a local authentication and authorization process to access the MEC services. Only the users that are successfully authenticated and authorized are considered as temporarily trusted to access the local MEC services, while for the rest devices only the emergency services will be available. When the backhaul connection recovers, all temporarily trusted devices in the local edge cloud have to reconnect to the network in a preplanned order, so that they are authenticated and authorized by the central V-AAA Manager again.

Context-Awareness in Trust Zone

A. Context-Aware Synchronization of Subscriber Profiles

The proposed local V-AAA server – or more specifically, the LAA – relies on the subscriber authentication information stored in the LSS to accomplish the local AKA procedure in the edge cloud. However, due to security concerns, parts of such information, such like the NAS key, cannot be locally generated in edge clouds, but only available in the central cloud. Thus, the subscriber authentication information must be synchronized from the central cloud to the LSS before the edge cloud switches to the local security mode, and periodically updated. Furthermore, taking the device mobility into account, users may enter an edge cloud from outer area while it is disconnected from the central cloud. Therefore, a LSS should not only synchronize the authentication information of devices in the local edge cloud, but also that of the devices in neighbor edge clouds nearby, which are able to arrive in the local edge cloud during the next synchronization interval.

Self-evidently, with respect to the mobility, various devices can move over different distances within the same synchronization interval. Thanks to the modern technologies of transportations and communications, people are nowadays able to travel over three hundred kilometers per hour, while continuously exploiting the cellular network services. Considering the limited area of a typical edge cloud, e.g. between 5×5 km² and 15×15 km² [23], the authentication information of every such high-mobility subscriber must be synchronized to 400 to 4000 different LSSs per hour. Accounting the large amount of user devices in the entire mobile network, this synchronization process will generate a considerably significant data traffic over the backhaul network, and hence leads to extra operating cost and raises the risk of data congestion. In other words, there is a conflict between the interests of subscribers (MEC service reliability) and of MNOs (operating cost). In this concern, we designed an advanced synchronizing mechanism with awareness to the context information of both UEs and edge clouds, which can be explained as follows.
The local security mode is activated only when the central security services fail to respond in time, the gain of subscriber authentication information synchronization is therefore not significant in the edge clouds with negligible probability of Central Security Service Outage (CSSO). Generally, to estimate this outage probability for a certain device in different edge clouds, the following factors should be taken into account:

1) **User arrival:** depending on the device-to-edge-cloud spatial distance and the user mobility, every edge cloud has its individual expectation about the user arrival probability in the next synchronization interval. The edge clouds located far from the device have less chance to serve the device than those located nearby. For still and low mobility users, the user arrival estimation can be simply accomplished through the handover prediction procedure of legacy networks. However, high-mobility users such like vehicles on highway and railway passengers can travel over multiple edge clouds during one backhaul outage, so that an additional position prediction in macro scale can be needed.

2) **User stay time:** upon arrival, depending on the user mobility, the coverage area of the edge cloud and the traffic model in that area, every edge cloud has its individual expectation about the duration of user’s stay in it. Some “important” edge clouds covering larger or more traffic-congested areas (e.g. the city center of Paris) are expected to serve a user for longer time, when compared to those “unimportant” ones (e.g. a small village aside a high-speed railway). The risk of CSSO during the user’s stay in these edge clouds, therefore, is also higher.

3) **Backhaul reliability:** depending on the current status of backhaul connection, every edge cloud has its individual expectation about the chance that a CSSO occurs during a certain period in the future. Generally, the edge clouds with worse current backhaul connection quality are more likely to suffer from CSSO.

Figure 3: Trust Zone extracts the context information of UEs & edge cloud to estimate the central security service outage probability.
Thus, from real-time information of devices (mobility and position) and edge clouds (coverage area, traffic model and backhaul throughput), we are able to extract high-level context information such as user motion pattern and backhaul outage probability, as illustrated in Figure 3. These context information can be used to estimate the CSSO risk for every certain device in different edge clouds. The subscriber authentication information of the device should only be synchronized to the edge clouds where the device has high CSSO risk above a predefined threshold, so that less redundant backhaul traffic is generated. By setting the threshold to different levels, the MNO is able to balance its interests in operating cost and MEC service reliability.

B. Modeling the Backhaul Connection Status

Although mature models and techniques are available to estimate user mobilities in mobile networks [24], which can be applied in the CSSO estimation procedure discussed above, a simple and efficient model for the backhaul status is still called for. Generally, a backhaul connection between the central cloud and the edge cloud can be evaluated with its average delay and packet error rate, which are easy to measure. With these metrics, we are able to estimate the probability that the central security server responses in time to support a certain edge computing service, when given its specific latency requirement. We define this probability as the Central Security Service Reliability (CSSR), which exhibits stochastic behavior in long term and can be modeled as a Markov chain, as shown in Figure 4.

![Central security service reliability as a Markov chain, circled numbers are state indexes.](image)

In our model, the backhaul network at any time instant is considered to be in one among several predefined states. Every state describes a specific combination of CSSR range and network state. According to the CSSR level, we defined three basic network states: healthy, unhealthy and disconnected. Additionally, the network operator may recognize network disasters and take necessary measures to repair the backhaul connection, for which we set an extra state under recovery.
Usually, the CSSR does not vary fiercely but smoothly, so only fluctuations between neighbor CSSR levels are considered, as we illustrate with solid arrows in Figure 4. Nevertheless, as aforementioned, some disasters and cyber-attacks, although rarely happen, can cause sudden disconnection of backhauls. In this case, the backhaul connection will fail to autonomously recover by itself, unless manual repair is taken. Therefore, in the model we enabled unidirectional transitions from the healthy and unhealthy states to the disconnected state, which are illustrated with dotted arrows in Figure 4. Furthermore, the network operator will take autonomous or manual measures to recover the backhaul network only when it is not healthy, and the recovery process will continuously improve the CSSR until it becomes healthy again, as denoted with the dashed arrows in Figure 4. By training the model with historical log data of the network operator, we are able to estimate the transition probabilities and predict the future CSSR. An example output of our Markov chain is depicted in Figure 5, where the state transition probability matrix is

\[
\begin{bmatrix}
0.8 & 0.1999 & 0 & 0 & 0 & 0 & 0 & 0 & 0.00001 \\
0.5 & 0.49 & 0.0099 & 0 & 0 & 0 & 0 & 0 & 0.00001 \\
0.25 & 0.5 & 0.15 & 0 & 0.0999 & 0 & 0 & 0 & 0.00001 \\
0 & 0 & 0.25 & 0.5 & 0.15 & 0 & 0.0999 & 0 & 0.00001 \\
0 & 0 & 0 & 0.2 & 0.6 & 0 & 0 & 0.1 & 0.1 \\
0 & 0.5 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0.5 & 0.5 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.3 & 0.7
\end{bmatrix}
\]

![Figure 5: An example simulation of backhaul quality generated by the proposed Markov chain](image)

**Results and Discussion**

We conduct numerical simulation to validate the effectiveness of the TZ approach, as to describe below.
Environmental Setup

An 8×8 km$^2$ region with UE density of 6250 km$^2$ is considered. An edge cloud covers a circular urban area with radius of 2 km that locates in the center of the region, which is surrounded by four suburban and rural areas, as illustrated in Figure 6.

Figure 6: Geographical map of the simulated region, EC is the coverage of the local edge cloud, while I – IV are neighbor suburban and rural areas.

The simulation initializes with number of UEs that are uniformly distributed across the region. Also, a mobility class is assigned to UEs. Those mobility class are HIGH, MEDIUM, LOW or STILL and also uniformly distributed on the UEs. We have extended the random walk model with 600 s steps, a random “basic speed” is generated for every moving UE according to its mobility class. This basic speed is then linearly scaled according to both the mobility class and the area where the UE is located, and combined with an uniformly distributed random direction, in order to obtain the UE’s movement. Details are listed in Tables 1 and 2. Once a UE leaves the region, a new arriving UE will be created to keep a constant overall UE density. We let the UEs move for 40 h so that the UE densities in all five areas converge to consistent levels.

| Mobility Class | STILL | LOW | MEDIUM | HIGH |
|----------------|-------|-----|--------|------|
| Basic Speed (m/s) | 0 | $\sim$N(1.5,0.5) | $\sim$N(10,2) | $\sim$N(40,5) |

| Mobility Class | EC | I | II | III | IV |
|----------------|----|---|----|-----|----|
| LOW            | 0  | 1 | 1  | 1   | 1  |
| MEDIUM         | 0.7| 1 | 0.9| 0.8 | 0.9|
| HIGH           | 0.2| 1 | 0.9| 0.85| 0.8|

Meanwhile, we take the Markov chain described earlier to generate the CSSR of unstable central security services in the edge cloud as a random process, which is updated by every simulation step. In every simulation step, depending on the current CSSR, there is a specific chance that a CSSO occurs in the edge cloud.

Testing the Trust Zone

We consider a TZ implemented in the edge cloud (EC) serving an urban area. It is assumed to have complete knowledge about the Markov chain parameters of the edge cloud’s CSSR. After
the convergence of UE densities in different areas, the TZ tracks the positions of UEs for 24 h to learn about the statistical motion patterns, in order to predict the arrival probability and stay time of every UE in the EC. After the training phase, the TZ is activated to estimate the CSSO risk in the next 30 min for every UE in the region. If and only if the risk exceeds a pre-defined critical level, the UE’s subscriber profile will be synchronized from the central cloud to enable TZ operation upon CSSO, and a backhaul traffic will be thereby generated. This operation repeats every 30 min. By every simulation step, if a CSSO occurs in the edge cloud, every UE that has not had its subscriber profile synchronized will suffer from the CSSO once, and therewith generate a CSSO report. This testing phase continues one month, and the performances of TZ under different specifications of critical CSSO risk levels are illustrated in Figure 7.

It can be observed that the deployment of TZ can effectively reduce the loss of user experience caused by CSSOs. Especially, by configuring the threshold of CSSO risk to different levels, we can achieve a flexible balance between the service reliability and the operations cost. Note that the required extra operations cost is increasing faster than proportionally to the gain in reliability.

Figure 7: Basic rocket ship design. The rocket ship is propelled with three thrusters and features a single viewing window. The nose cone is detachable upon impact.

Conclusions

In this paper, we have indicated the future 5G telecommunication networks with dense application of MEC services, and the current LTE/EPS security architecture in 3GPP Release 14 drawbacks with its centralized AKA mechanism. We proposed a solution integrated with our 5G AAA approach which enables the execution of AKA functionalities at the edge clouds, in order to support better deployment of 5G MEC services. An innovative edge cloud security architecture, the Trust Zone, has been introduced to enhance the 5G AAA with a cognitive access management with respect to the backhaul connection quality. Furthermore, we designed a context-aware mechanism of synchronizing subscriber authentication information to local subscriber databases, which helps in reducing the backhaul network traffic generated by the Trust Zone. Numerical simulation showed that our proposed method can effectively improve the reliability of edge cloud services in the context of unstable security network functions in
central cloud, while being capable to keep a flexible balance between the MEC reliability and operations cost.

We will continue to investigate better methods to improve the authentication process in 5G. In terms of increasing the service reliability, we will apply machine learning and deep learning techniques to improve the accuracy and efficiency of centralized security. Furthermore, the proposed distributed security mechanisms need to be evaluated with respect to their applicability of local authentication and authorization in hybrid private-public mobile networks as expected for 5G, e.g. 5G enterprise networks inter-working with 5G public land mobile networks.

**Data Availability**

The Python source code used to support the findings of this study is available from the corresponding author upon request.

**Conflicts of Interest**

The authors declare that there is no conflict of interest regarding the publication of this paper.

**Funding Statement**

This work has been performed in part in the framework of the H2020-ICT-2014-2 project 5G NORMA [grant number 671584]. The publication of this paper is supported by the DFG funding for open access.

**Acknowledgments**

This work has been performed in part in the framework of the H2020-ICT-2014-2 project 5G NORMA. The authors would like to acknowledge the contributions of their colleagues. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein.

**References**

[1] Barbarossa, Sergio, Stefania Sardellitti, and Paolo Di Lorenzo. "Communicating While Computing: Distributed Mobile Cloud Computing over 5G Heterogeneous Networks." *IEEE Signal Processing Magazine* 31.6 (2014): 45-55.

[2] Sabella, Dario, et al. "Mobile-edge computing architecture: The Role of MEC in the Internet of Things.” *IEEE Consumer Electronics Magazine* 5.4 (2016): 84-91.

[3] Corcoran, Peter, and Soumya Kanti Datta. "Mobile-Edge Computing and the Internet of Things for Consumers: Extending Cloud Computing and Services to the Edge of the network." *IEEE Consumer Electronics Magazine* 5.4 (2016): 73-74.

[4] Yuyi Mao, Changsheng You, Jun Zhang, et al., “A Survey on Mobile Edge Computing: The Communication Perspective”, *IEEE Communications Surveys & Tutorials* 19.4 (2017): 2322-2358.
[5] Nasir Abbas, Yan Zhang, Amir Taherkordi, et al. “Mobile Edge Computing: A Survey”, in IEEE Internet of Things Journal 5.1 (2018): 450-465.

[6] Shankar Lal, Tarik Taleb, and Ashutosh Dutta. “NFV: Security Threats and Best Practices”, IEEE Communications Magazine, Vol. 55, Issue 8, pp. 211–217. IEEE, 2017.

[7] Hongwei Li, Rongxing Lu, Jelena Misic, et al., “Security and Privacy of Connected Vehicular Cloud Computing”, IEEE Network, Vol. 32, Issue 3, pp. 4-6. IEEE, June 2018.

[8] A. Klein, C. Mannweiler, J. Schneider and H. D. Schotten, "Access Schemes for Mobile Cloud Computing," in 2010 Eleventh International Conference on Mobile Data Management, Kansas City, MO, USA, 2010, pp. 387-392.

[9] C. B. Sankaran, "Network Access Security in Next-Generation 3GPP Systems: A Tutorial," in IEEE Communications Magazine, vol. 47, no. 2, pp. 84-91. IEEE, February 2009.

[10] J. Cao, M. Ma, H. Li, Y. Zhang and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 283-302. IEEE, 2014.

[11] Ignacio Labrador Pavon, Jorge Rivas Sánchez, Alessandro Colazzo, et al., 5G NORMA Network Architecture – Intermediate Report, Technical Report, January 2017.

[12] ETSI, Mobile-Edge Computing – Introductory Technical White Paper, White Paper, September 2014.

[13] Flavio Bonomi, Rodolfo Milito, Jiang Zhu, et al., “Fog Computing and Its Role in the Internet of Things”, Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16. ACM, 2012.

[14] A. Osseiran, F. Boccardi, V. Braun, et al., “Scenarios for 5G Mobile and Wireless Communications: the Vision of the METIS Project”, IEEE Communications Magazine Vol. 52, Issue 5, pp. 26-35. IEEE, May 2014.

[15] Bin Han, Marcos Rates Crippa and Hans D. Schotten, “5G Island for Network Resilience and Autonomous Failsafe Operations”, 2018 European Conference on Networks and Communications (EuCNC), Ljubljana, Slovenia, June 2018.

[16] Jacob Kochems and Hans D. Schotten, “AMMCOA - Nomadic 5G Private Networks”, 23. VDE/ITG Fachtagung Mobilkommunikation), Osnabrück, May 2018.

[17] Meryem Simsek, Dan Zhang, David Öhmann, et al., “On the Flexibility and Autonomy of 5G Wireless Networks”, IEEE Access. IEEE, 2017.

[18] Hua Yang, Naoki Wakamiya, Masayuki Murata, et al., “An Autonomous and Distributed Mobility Management Scheme in Mobile Core Networks”, Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies. IEEE, 2016.

[19] Jeon, Seil, et al. "Distributed Mobility Management for the Future Mobile Networks: A Comprehensive Analysis of Key Design Options." IEEE Access 5 (2017): 11423-11436.

[20] Stan Wong, Nishanth Sastry, Oliver Holland, et al., “Virtualized Authentication, Authorization and Accounting (V-AAA) in 5G Networks”, IEEE Conference on Standards for Communications and Networking (CSCN), September 2017.

[21] 5G PPP Architecture Working Group, View on 5G Architecture, White Paper, July 2016.

[22] Bin Han, Stan Wong, Christian Mannweiler, et al., “Security Trust Zone in 5G Networks”, 24th International Conference on Telecommunications (ICT). IEEE, 2017.
[23] Aleksandra Checko, Henrik Lehrmann Christiansen, Ying Yan, et al., “Cloud RAN for Mobile Networks – A Technology Overview”, IEEE Communications Surveys & Tutorials Vol. 17, Issue 1, pp. 405–426. IEEE, 2015.

[24] Xiaohu Ge, Junliang Ye, Yang Yang, et al., “User Mobility Evaluation for 5G Small Cell Networks Based on Individual Mobility Model”, IEEE Journal on Selected Areas in Communications, Vol. 34, Issue 3, pp. 528–541. IEEE, 2016.