Enhancing Security and Trust in 5G Roaming Services: An LBO Architecture Leveraging Intel SGX Technology for Secure Charging and Authentication

Hyun Noh

Department of Future Convergence Technology Engineering

The Graduate School of

Sungshin Women's University

Enhancing Security and Trust in 5G Roaming Services: An LBO Architecture Leveraging Intel SGX Technology for Secure Charging and Authentication

A Master's Thesis
Submitted to the
Graduate School of Sungshin Women's University
in partial fulfillment of the requirements
for the degree of
Master of Future Convergence Technology
Engineering

Hyun Noh
Nov, 2023

This is to certify that we have examined the
Master's Thesis of
Hyun Noh
Submitted to Department of Future Convergence
Technology Engineering

Approved as to style and content:

Thesis Advisor Seongmin Kim

Committee Chairman Il-Gu Lee

Committee Member Yeon-sup Lim

The Graduate School of Sungshin Women's University

ABSTRACT

Commercially deployed 5G networks can enhance efficiency within roaming scenarios. The significance of billing and authentication in roaming extends beyond subscriber payments, as it is intricately linked to the assets of mobile network operators. However, the existing trust-based roaming architecture establishes a vulnerable security trust relationship, posing challenges in trusting and verifying mobile network operators during roaming. While previous research has predominantly focused on performance-related aspects in local breakout scenarios, studies addressing security concerns in billing and authentication are still nascent.

This paper delves into the billing and security intricacies of the local breakout in 5G stand-alone networks. It proposes a design that leverages Intel SGX technology to securely implement billing and authentication in local breakout. Based on the suggested local breakout architecture, our research utilizes the SGX framework to validate integrity through Remote Attestation and Sealing, concurrently ensuring optimal performance.

Contents

Table Contents

Figure Contents

Ⅰ. Introduction

The transition of the 5G network to a new paradigm of virtualized and software-defined networks based on Network Function Virtualization (NFV) and Software-Defined Networks (SDN) is underway. Specifically, the mobile packet core comprises Virtual Network functions (VNFs) running on the mobile edge cloud (MEC). Two modes, non-stand-alone (NSA) and stand alone (SA), are introduced by 5G standards to ensure compatibility with LTE. The 5G network comprises user equipment (UE), access network (RAN), and core network. The non-standalone method proposes a mix of 5G access networks and commercialized 4G packet core (EPC) for compatibility with the existing LTE network. In contrast, the stand-alone method implements access and core networks based on SDN/NFV, using a new 5G packet core designed according to 5G standards. As 5G matures, the paradigm shifts from NSA to SA, presenting opportunities to enhance the efficiency of the commoditized 5G network, particularly in a roaming scenario. 3rd Generation Partnership Project (3GPP) standards for 5G support roaming, with the SA mode's roaming architecture consisting of two implementations: HomeRouted and Local Breakout (LBO). LBO involves the direct routing of data traffic from the Visited Public Land Mobile Network (VPLMN). In contrast, the home-routed scenario directs traffic to the Home Public Land Mobile Network (HPLMN) for classification and routing. Of the two choices, LBO is deemed suitable for 5G SA mode in terms of latency, providing high data transmission speed and low latency compatible with roaming

LBO. However, the LBO model presents performance advantages, as it is tunneled from the visiting network. In contrast, the home-routed model involves sending all data plane traffic to the subscriber's HPLMN, resulting in latency due to additional round-trip time. However, MNOs do not prefer LBO despite its performance advantages because, in LBO, the HPLMN must bill the customer and pay the charges for the VPLMN. In LBO, VPLMN operators have complete control over data traffic, leading to significant security issues and potential problems such as over-billing, as the billing process cannot be audited. In contrast, home routed allows centralized control and data traffic monitoring, enabling implementation of policies and security measures, and is widely used by most MNOs. With the transition to 5G SDN, NFV introduces opportunities to utilize VNFs in existing legacy computing infrastructure, raising security and privacy concerns. To address this, an approach leveraging Software Guard Extensions (SGX) in the network functions of the 5G network, such as the Open Networking Foundation (OMEC) [1], has emerged. This approach is significant as a pioneering study, but it is not designed for a complete 5G SA mode. There remains a design space that does not consider how to charge in one network in the roaming scenario, how to form a safe relationship in a situation involving a third-party service provider, and whether it has been billed. MNOs trust based on business contracts, but no separate trusted entity in roaming makes verification challenging. From cellular networks to 5G network roaming, it is built on a vulnerable Trust model exchanging information that occurs between trusted parties. When a user is roaming,

considering the current roaming architecture, the user is not entirely protected for authentication accounting and billing. In order to fulfill these requirements, it is imperative to establish a framework aimed at fortifying the security of the 5G environment. This involves guaranteeing data integrity and operations within the system by utilizing Trusted Execution Environments (TEEs), which provide an isolated processing environment. This paper explores potential risks when utilizing LBO compared to HR, arguing that a mechanism for ensuring trustworthiness between HPLMN and VPLMN is required in the LBO architecture. This study designs a 5G network-based roaming architecture LBO that can maintain performance while meeting security requirements in the charging aspect by integrating Intel SGX into the 5G network function performing roaming charging, analyzing the current roaming threats of the 3GPP 5G roaming architecture LBO in the 5G roaming network.

In the LBO, the HPLMN can verify the trust relationship between the VPLMN and the HPLMN through Remote Attestation and protect the Charging Data Record (CDR) data in the enclave, a safe area protected during the charging process. Above all, the SGX Enabled Roaming network function guarantees control authority for the critical role of billing settlement in the LBO model. It verifies the existing control authority in the home routed model, securing reliability. The problems of being unable to use LBO despite its good performance in the 5G network due to the Weak Trust Model, Billing Transparency, other Security Issues, and Charging and Billing Issues are discussed.

To solve these problems, a design considering the 5G SA network function in two networks of roaming using Remote Attestation and Sealing of Intel SGX, a TEE technology, is proposed. Finally, it is evaluated that the SGX-enabled 5G network function guarantees performance while considering security. In summary, a novel 5G LBO roaming architecture leveraging SGX is proposed to guarantee secure charging and authentication, provide auditability, and address significant security concerns in LBO. The trust model is enhanced by explicitly spelling out what needs to be trusted and audited, ensuring compatibility with 5G SA standards.

Ⅱ. Background

1. Cellular network architecture

1.1 Basic Network

Cellular networks comprise UE, RAN, and core. A RAN refers to a wireless network between the UE and the base station. This base station is called Evolved Node B (eNB) in LTE and next-generation Node B (gNB) in 5G. More specifically, when it comes to the LTE Evolved Packet Core (EPC), the LTE plays a key role in providing cellular services, including user authentication, mobility management, and service billing (e.g., accounting). In 5G, the core takes the same roles as LTE, but each component is designed to be realized into separated NFVs.

1.2 Home network (HPLMN) and visited network (VPLMN)

Roaming is a feature where a UE uses services from a different mobile network operator while outside the coverage area of its home network. This home network is called HPLMN, which refers to the mobile network operator (MNO) with which the UE has a subscription. HPLMN generally identifies the UE by the inserted USIM card containing the subscription information. Likewise, the visited network is called VPLMN, where the UE has no subscription information while the HPLMN has a roaming agreement.

2. 5G Network

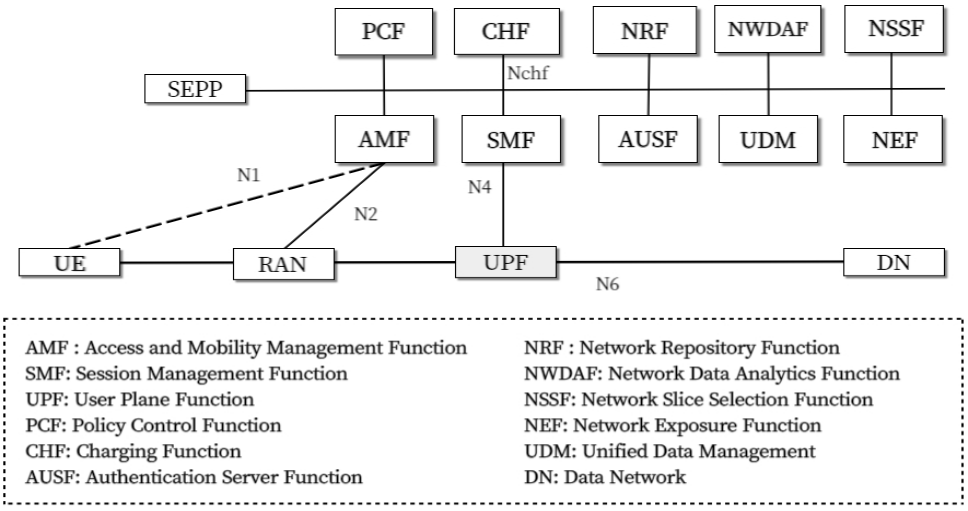

FIGURE 1. 5G Network Architecture

The network functions comprising the 5G network are illustrated in Figure 1. The fundamental elements of the network environment include SBI, SEPP, and HTTP/2 protocols. SEPP is defined in the 5G standard as a crucial feature for MNO interconnection in standalone 5G core-to-core roaming. It ensures the integrity and confidentiality of outbound HTTP/2 signaling messages through peer authentication and N32 roaming interconnects.

Within a service-based architecture, each NF serves as a service provider delivering specific services via a singular service-based interface. With authorized network supervision for any network function, a service infrastructure has been implemented, enabling the utilization of the services provided by the service provider as a service user.

3. Roaming Configuration

GSMA has provided two options for both EPS roaming and 5GS roaming: Home routed and Local-breakout architecture [2], [3].

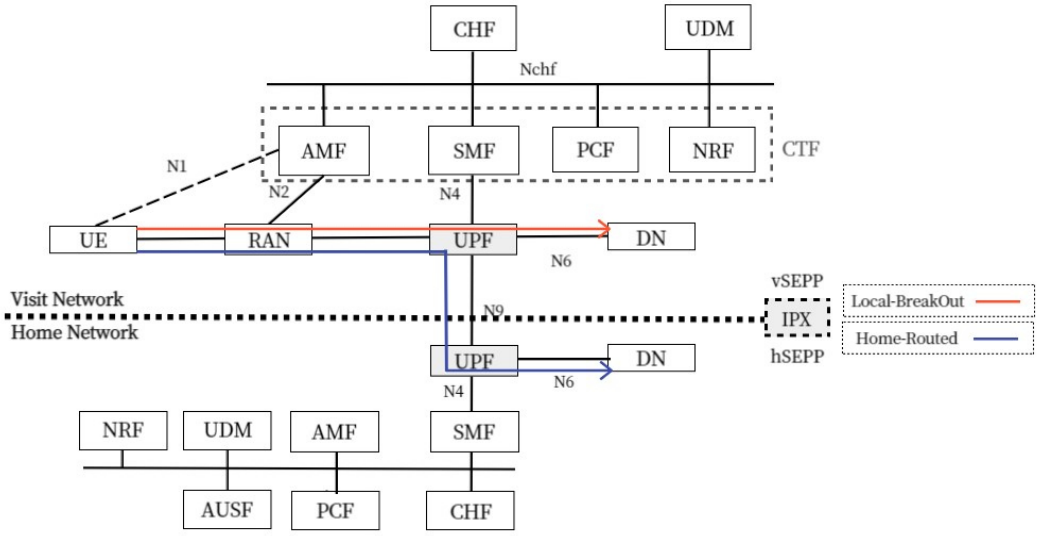

FIGURE 2. Roaming Configuration

3.1. Home Routed architecture (HR).

In the home routed architecture, all data plane traffic is directed to the subscriber's HPLMN network, typically located within their home country [3]. The HPLMN then processes and forwards the data traffic to its destination. By doing this, the HPLMN is able to provide the subscribers with access to services. In other words, this approach enables centralized control and data traffic monitoring. Thus, the HPLMN can enforce its policies and security measures. However, there are several disadvantages to the home-routed scenario. First, both the home

and visited operators must pay for interconnect hubs in between. This cost is high, resulting in expensive data roaming tariffs that are unappealing to most roamers. Second, home routed architecture results in higher latency for data traffic as it follows a longer path back to the home network and then to its destination. This home routed architecture is the primary roaming solution for voice and data today - and will also be used for 5GS roaming [4].

3.2. Local-Breakout (LBO).

GSMA has also provided an LBO architecture for roaming, where roaming subscriber's data can be sent directly to the destination server from the visited network. Unlike Home routing, the roaming traffic in LBO architecture is not routed to the HPLMN's infrastructure. Instead, the VPLMN provides the end-user direct access to external networks from its own UPF. This approach can provide several advantages. First, it results in lower latency for data traffic, as the traffic in LBO avoids the additional round-trip time for routing toward the HPLMN's User Plane Function (UPF) [5], [6]. Second, Local Breakout also helps reduce the load on the home network's infrastructure because not all roaming subscriber data needs to go through it.

4. Intel SGX

Intel SGX is a security processor architecture designed to ensure trust in platforms handling sensitive and valuable information. It utilizes an isolated secure region called the Enclave to restrict access to code and data exclusively to the program executing within it. Before creating an Enclave, it is essential to identify the assets requiring protection, the data structures encompassing these assets, and the code operating within these data structures. This step is crucial to ensure that untrusted or external components cannot read or modify the protected code once the Enclave is initialized and the code is loaded into memory. These assets are subsequently stored in a dedicated, trusted library. Furthermore, it is vital to establish their interfaces based on trustworthiness criteria after defining the trusted Enclave components and untrusted Host components within the Intel SGX program. A secure and trustworthy environment is maintained by delineating communication and interaction between the Enclave and Host.

4.1. Remote Attestation

Remote attestation is a process by which one party remotely verifies the integrity and trustworthiness of another party's hardware, software, or execution environment. It is commonly employed to establish trust between entities, typically clients and servers. Remote attestation software includes enclaves within the application and Intel-provided components such as the Quoting Enclave (QE) and Provisioning Enclave

(PvE).

The attestation hardware relies on Intel SGX-supported CPUs.

Remote attestation verifies three key aspects:

- the application's identity
- its integrity (ensuring it hasn't been tampered with)
- the secure execution of enclaves within an Intel SGXsupported platform

During remote attestation, the client generates an encrypted 'attestation' containing information about its current state and forwards it to the server. The server employs this attestation to ascertain the trustworthiness of the client's execution environment, confirming that it remains unaltered. Remote attestation is crucial for ensuring secure communication and establishing trust in distributed systems.

4.2. Sealing

Enclave sealing is vital in safeguarding sensitive information, such as encryption keys or user credentials, from unauthorized access or tampering. Enclaves utilize permanent hardwarebased encryption keys to securely encrypt and store critical data, allowing data retrieval only when a trusted environment is reestablished. Sealing mechanisms typically rely on hardware-based encryption keys unique to the execution environment. Data sealed within an enclave can only be decrypted and accessed within that enclave or a compatible, trusted environment.

Ⅲ 5G Network Framework Analysis

In this section, we explore the structure of the standard protocol in 5G networks, known as the Extensible Authentication Protocol (EAP) Framework, and conduct an analysis of the 5G-Authentication and Key Agreement (5G-AKA) Protocol. Additionally, we discuss the transition to 5G networks, focusing on the 5G Core and the associated motivation for this shift.

1. EAP Framework

In a 5G network, the primary authentication method within the EAP framework involves the use of 5G-AKA and Extensible Authentication Protocol-AKA' (EAP-AKA') during the first authentication, employing Subscription Permanent Identifier (SUPI) and Subscription Concealed Identifier (SUCI) for device authentication. In contrast, the authentication framework used in 4G networks is EPS-AKA, a mutual authentication system between user devices attempting to connect to the mobile network. It involves transmitting IMSI (International Mobile Subscriber Identifier) during the step where the cellular network requests authentication for the UE, serving the purpose of distinguishing subscribers in the cellular network.

The first authentication involves mutual authentication and key matching between the UE and the wireless core network, occurring in two stages. In the first stage, the UE initiates authentication by connecting to the Security Anchor Function (SEAF) and transmitting a

message. Importantly, the UE sends either a temporary identifier (5G-GUTI) or subscriber identifier information (SUCI) encrypted with public-key-based ECIES to SEAF. Thus, the subscriber's identification information is not transmitted in plaintext over the 5G wireless network. The UE's information is forwarded through SEAF to the Authentication Server Function (AUSF), which checks whether the service network requesting authentication has been authenticated. Upon success, AUSF forwards the authentication request to Unified Data Management (UDM) and Authentication Credential Repository and Processing Function (ARPF). When AUSF receives SUCI, it is decrypted through SIDF to identify the UE with SUPI. Subsequently, UDM/ARPF selects the authentication method (5G-AKA or EAP-AKA') for the first authentication based on UE's SUPI. The appropriate authentication method is selected in the second stage of the first authentication, and mutual authentication occurs. UE and AUSF rely on ARPF to perform mutual authentication and key exchange. This generates the anchor key (Kseaf), which is transmitted from AUSF to SEAF. After the first authentication for slice authentication, the recommended choice for the second authentication is an EAP-based authentication method. EAP combines and extends various authentication protocols, easily expanding the scope of authentication to third-party services. For instance, using EAP-TLS, identifiers can be transmitted in an encrypted form, enhancing privacy.

EAP's flexibility, supporting various authentication methods and credentials, efficiently supports authentication between IoT payment

systems with different credentials. In the 3GPP 5G security architecture, it is possible to adopt EAP-based extended types like EAP-TLS for the second authentication instead of the first authentication methods, 5G AKA or EAP-AKA'. EAP-TLS is used to establish a secure channel in vulnerable wireless environments and is one of the protocols defined in the 5G standard for providing core services in specific IoT environments.

1.1. 5G AKA Protocol

5G-AKA Protocol. In 3GPP TS 33.501, the sixth item, Security procedures between UE and 5G network functions, specifies the use of 5G-AKA and EAP-AKA' as standard protocols for the first authentication procedure. Section 6.1.3, Authentication procedures, in TS 33.501 defines and explains the procedures [7]. 5G-AKA, an enhanced version of the protocol based on 4G's EPS-AKA, facilitates mutual authentication of various devices and users in the network to establish a secure channel. EAP-AKA' is another authentication method supported in 5G, utilizing a protocol based on encryption keys to reduce the complexity of security management and support diverse access approaches. Both can be used in the 5G authentication framework for first-time authentication, and the choice considers differences in the role of the SEAF and the key generation process.

In the wireless environment of 5G, subscriber identification information required for device authentication is exchanged in an encrypted state [8]. TS 23.501 defines SUPI and SUCI in the fifth item, High-level features 5.9.2, 5.9.2. a and TS 33.501 in the fifth item, Security requirements, and

features, presents SUPI as a requirement for authentication and authorization. SUPI, a standardized technology integrating IMSI, is the unique subscriber identifier in 5G, assigned to the UE and provided by UDM/Unified Data Repository (UDR). SUCI is the encrypted form of SUPI and is protected using Elliptic Curve Integrated Encryption Scheme (ECIES).

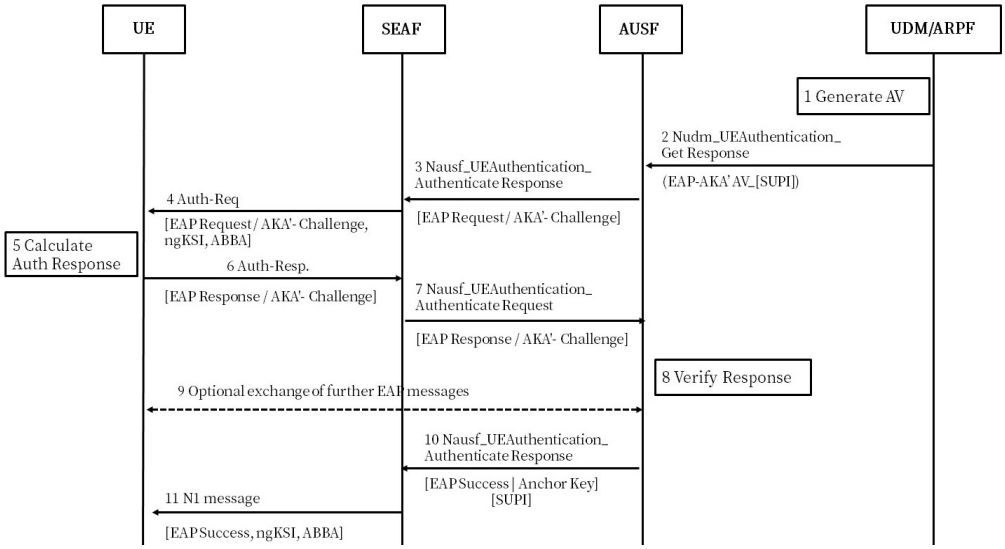

FIGURE 3. 33.501 - Authentication procedure for EAP-AKA'

In summary, unlike 4G, 5G enhances security in the first authentication through standardizing EAP framework protocols and introduces SUPI as an identifier to replace IMSI. Encrypted SUCI is used in the 5G device authentication process, while SUPI is exposed to the serving network, mitigating potential security vulnerabilities.

1.2. Qualitative Analysis

In the 5G security architecture, core network functions utilize OAuth 2.0 to protect the interaction between network functions. ETSI TS 133 501 [8], in section 12.1, specifies using the Network Exposure Function (NEF) to securely expose functionalities and events to third-party Application functions. It emphasizes that authenticated application functions must securely provide information from the 3GPP network. To achieve this, section 12.3 mandates the essential support of the TLS protocol. It mentions using the TLS protocol to ensure the integrity, replay, and confidentiality protection of the interface between NEF and application functions. Additionally, section 12.4 states that NEF must approve requests from application functions using OAuth-based authentication mechanisms. These regulations play a crucial role in the 5G security architecture, emphasizing enhancing authentication and protection features through OAuth and TLS protocols.

2. 5G Design Goal and Motivation

Deploying SDN/NFV to the 5G core network presents a challenge, with security being a significant concern. Isolating packet core entities, such as Mobile Management Entity (MME), Home Subscriber Server (HSS), and Policy and Charging Rules Function (PCRF), in 4G/5G NSA mode is particularly challenging. Additionally, executing each packet core entity in an untrusted cloud requires additional authentication and authorization for virtualized entities. The deployment of SDN also leads to an increase in participating entities due to the separation of control/data planes, resulting in a higher number of requests/responses during the authentication procedure.

To address these challenges, the OMEC has led efforts to utilize TEE technology, particularly hardware-based TEEs. Collaborating with Intel, they have employed SGX for a secure offline charging service (OFCS) in the LTE system [9]. The OMEC project proposes that in 5G NSA-based networks, network functions receive data packets from UE and RAN, and billing occurs in the OFCS. In the case of 5G SA, the packet flow and roles differ, with data packets being delivered to the Access Management Function (AMF), Session Management Function (SMF), and UPF. The existing billing process, which separates online and offline data delivery, transitions to a Converged Charging System in 5G SA, requiring additional design and evaluation.

The fundamental OMEC design focused on a single Telco and offline charging and billing services falls short in the context of 5G roaming,

where two Telcos are involved, and both online and offline billing processes are simultaneously required. This paper proposes a design leveraging SGX in the 5G core network to overcome these challenges and adhere to security objectives. These objectives include preventing user data in the application layer (ring-3) from being exposed to untrusted system software and providing a secure interface between modularized Network Functions (NFs). The proposed design, addressing the aforementioned challenges and objectives, will be discussed in the Design Section, emphasizing its significance for the evolution of the 5G core network.

Ⅳ. Why is LBO On the Shelf

Despite the benefits of Local breakout in roaming architecture, almost all MNOs have adopted Home routed architecture for their roaming in LTE [5]. In this section, the operational logic for charging and billing within the context of LBO is first reviewed. Subsequently, the main barriers that contribute to the dismissal of the adoption of the Local Breakout architecture considering both its service and security aspects, are investigated.

1. Charging and Billing in LBO

In this thesis, an exploration is undertaken into the operational logic of charging and billing in 5G when the LBO is adopted by the two PLMNs for their roaming architecture. The research primarily centers on the converged charging system (CCS), which incorporates the legacy online and offline charging systems [10]. Crucial roles in the charging and billing processes within the converged charging system are played by various functions, including the Charging Function (CHF), Rating Function (RF), Account Balance Management Function (ABMF), and Charging Gateway Function (CGF).

CHF is the primary function responsible for converged online and offline charging functionalities. The CHF takes the role of authorization and accounting by interacting with other components in the charging system. Also, it is exposed to other relevant network functions, such as AMF and SMF, which can request charging services.

CGF is a gateway for handling CDR files. It aggregates the CDR files, correlates with policies, and balances information from other components. Thus, CGF makes a bill and pushes it to the billing domain.

RF is responsible for determining the charges or costs associated with the usage of cellular services. It applies charging based on specific usage or event content and rules.

ABMF stores and maintains an account's credit, debit, and reserve balance data. This data is central to the real-time credit control mechanism.

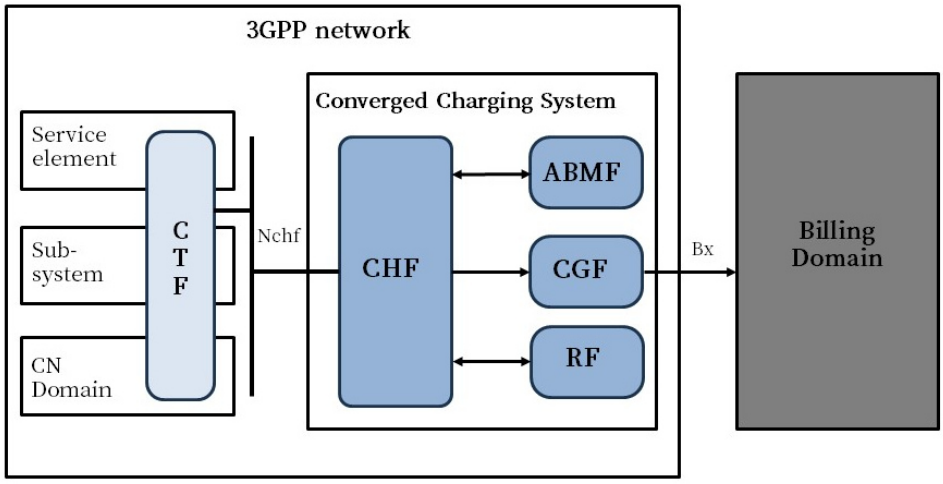

FIGURE 4. 3GPP 5G Converged Charging System

TABLE 1. Terminology Definitions

Terminology	Description
Charging	Supervise, gather, and oversee subscriber network utilization metrics (such as bytes, hours of usage, seconds, etc.) within the carrier network.
Billing	The procedure involves the creation and dispatch of invoices to customers, prompting them to settle outstanding financial obligations.

2. Operational logic of charging and billing.

In a typical LBO architecture, the roles between CDR movements and NFs, where billing occurs, are delineated as follows. Initially, the UE identified through inbound roaming connects from UPF in the User Plane area to the same region as the AMF and SMF in the Control Plane for data transmission. UPF processes roaming user data packets, recording information such as volume, speed, and delivery time in CDRs. It also encompasses data transfer, usage statistics, and events like fault reporting, warnings, and routing information. The UPF data is then transmitted to the AMF and SMF of the VPLMN, focusing on UE registration and mobility management. The AMF of a VPLMN can also engage with the CHF of the HPLMN to generate CDRs in the HPLMN.

Additionally, the SMF receives user plane information from UPF, obtains CDR data, gathers network events, and aggregates CDRs from charging trigger functions (CTFs) like SMF, transmitting them to CHF. Using this information, CHF performs CDR-related charging within CCS regions like CGF, AF, and AMBF, where CGF serves as an aggregator for multiple CDRs. The CGF then forwards the aggregated CDR to the Billing Domain. Subsequently, the user CDR in CHF is billed from the visiting network to the home network via Internetwork Packet Exchange (IPX).

Moreover, each CTF carries out distinct functions. The Network Repository Function (NRF) provides multi-HPLMN information

management and Roaming NRF integration through SEPP collaboration. The Authentication Server Function (AUSF) authenticates from HPLMN to UE based on user registration performed in AMF. The Policy Control Function (PCF) is responsible for provisioning policy and billing control decisions to the SMF. Although the PCF and CHF do not directly communicate, they exchange policy actions and enforcement through the SMF, and these network events are subsequently sent to CHF.

3. Charging and Service Issue

This section discusses issues that may arise during billing and service progression based on the LBO model, focusing on real-time charging, complicated wholesale agreements, and cost perspectives.

3.1. Hard to have real-time charging

In LBO architecture, since all control is with the visited network, billing for the roaming subscribers also takes place on the visited network [11]. Unlike HR, LBO may face constraints in providing real-time traffic information, as it relies on local infrastructure. This has been identified as a significant concern for MNOs that need a real-time view of customer traffic. LBO appears to be a natural choice for IP-based services, offering affordable data tariffs and lower operational costs. Simultaneously, it has been demonstrated that delays can be eliminated, and capacity for certain traffic types can potentially be increased, depending on the target. Although LBO relies on access to local infrastructure, providing this can act as a product differentiation factor for MNOs that offer this service first. In contrast, HR provides the home MNO all accounting and billing information. For MNOs that need to understand customer traffic almost in realtime for accounting reasons, HR has been identified as a major concern. HR plays a crucial role in providing information for accounting and billing by helping MNOs

have almost real-time insights into customer traffic, making it an important aspect of information provision for accounting and billing. On the other hand, LBO relies on local infrastructure, which can be a constraint in providing real-time traffic information. Therefore, LBO can be problematic for mobile operators who need almost real-time visibility into customer traffic.

3.2. Complicated wholesale agreement

As discussed in Basic Architecture, multiple components are involved in the current roaming system.

The LBO architecture manages roaming and billing information between operators, H-MNO and V-MNO. As a result, multiple contracts and financial transactions need to be processed between the two MNOs. In the case of direct contracts, separate agreements are required for each relationship, leading to high costs, overhead, and challenges when direct communication is only sometimes feasible (e.g., due to political obstacles).

For indirect contracts, connectivity between MNOs is achieved using a Clearinghouse. However, the presence of an intermediary introduces additional costs to the network and raises security and trust concerns by involving a third party. Consequently, contract and financial transactions become more intricate. For these reasons, Local Breakout may encounter

difficulties establishing the necessary contracts and financial transactions for roaming and interoperability between MNOs.

3.3. Cost

The LBO approach can offer lower operational costs and affordable data rates for IP-based services; however, it may increase operational costs for supporting network users. LBO can reduce roaming service latency and provide a better user experience by relatively reducing the user plane loop and necessary transmission resources. Nevertheless, it poses complexity in service control, policy control, and billing. The complexity in network management can lead to increased operational costs in aspects such as debugging issues, fault tracing, and traffic prediction. The time and resources required to address these problems can incur additional costs [5]. Many aspects that need to be changed due to HR and different networks require additional capital costs [12]. Moreover, it is unclear who should detect the fault and resolve the issue in case of service failures. IPX can help alleviate these impacts. Some solutions introduce additional proxy selectors and associated control functions to route traffic to the correct network and facilitate adjustments.

4. Security Issue

4.1 Weak Trust Model

All operators in the roaming scenario operate on the trust model, assuming information exchanges occur between trustworthy parties. Roaming operators work on the mutual trust model, assuming information exchanges occur between trustworthy parties, including HPLMN, VPLMN, and a third-party entity (i.e., Data Clearing House, DCH). While the HPLMN monitors the subscribers' service quality and accounts for the traffic, the VPLMN controls all network services provided to the roaming subscribers. A third-party entity can be placed to exchange information between HPLMN and VPLMN. However, with a naive trust model, HPLMN faces the challenges of having trust over VPLMN and DCH. While this trust model has worked on a best-effort basis, there are security concerns about emerging threats like SS7 attacks, which easily violate the trust model in roaming [13].

4.2 Billing Transparency

The HPLMN's lack of transparency on its subscribers roaming VPLMN in LBO can violate Network Operators' static agreements and pre-agreements [12]. First, there is a potential risk of MNOs accessing roaming user information illegally and imposing unfair charges on roaming users, leading to an over-billing attack [14]. While VPLMN records CDRs to bill roaming subscribers, the HPLMN has no method for authenticating and verifying the reported CDRs from VPLMN. Thus, the HPLMN in the LBO cannot monitor whether the VPLMN is appropriately delivering the roaming subscriber's subscribed services. Second, the CDRs can be maliciously tampered with by entities involved in the roaming, but there is no method to detect and give trust among various operators. Therefore, the HPLMN faces the challenge of placing complete trust in the VPLMN to ensure the validity and sanity of the received CDRs.

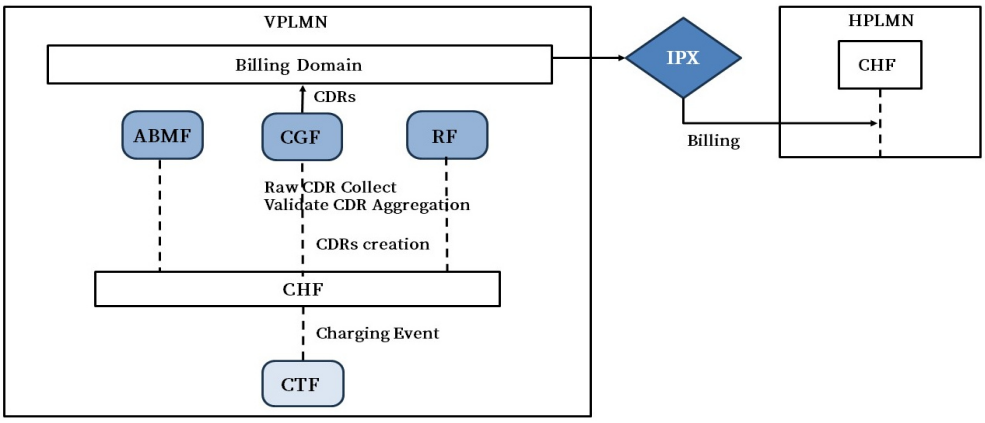

FIGURE 5. Billing Transparency

4.3 MNO Audit

MNOs cannot monitor VPLMNs for activities such as subscriber and fraudulent actions, making it difficult to identify issues like over-billing in real-time [14]. Roaming fraud is one of the most common problems in the telecommunications industry, costing over $38 billion annually. However, MNOs find monitoring and detecting roaming fraud in progress or responding in real-time challenging.

To bill consumers for roaming services, the visited network operator captures and records detailed usage information, and then the home network operator calculates the wholesale roaming charges to be paid. The home network operator bills the consumer. However, despite these processes, HPLMNs cannot charge for fraudulent activities and must bear the costs of the provided services. However, due to time delays in the settlement process between service usage and operators, billing information is not provided to consumers in real time during roaming.

In 5G roaming networks, as subscriber fraud increases, fraudsters create fake subscriptions using forged credentials, accumulating significant roaming charges without legitimate payment intent. Until the deception is discovered and terminated, fraudsters clandestinely exploit 5G roaming services, causing telecommunication companies to lose legitimate revenue.

TABLE 2. Summary of Threat Model

Threat Model	Description	Threat Entity	SGX-Enabled Security Approaches
Weak Trust Model	Dependence on third-party deployment and the necessity for absolute confidence in VPLMN is imperative.	Third-party (IPX provider, Clearing Houe) VPLMN in the context of LBO	Performing remote attestation for third party, VPLMN, and HPLMN.
Billing Transparency	Trust in network functions associated with charging and billing. Manipulation of CDR data. Challenges in Establishing Trust with MNO Subscribers.	UPF, CHF, CGF	Safeguarding CDRs within the Enclave region to ensure integrity.
MNO Audit	Challenges in Tracing and Auditing VPLMN Accounts. Utilizing falsified credentials with VPLMN and initiating billing roaming charges after registration.	VPLMN in the context of LBO AUSF, UDM	Verification for MNOs and Subscribers during Remote Attestation and Sealing.

V. Design

The billing process within the 5G LBO architecture, composed of SGX-enabled Network Functions (NFs), is illustrated in Figure 3. The SGX-enabled User Plane Function (UPF), Session Management Function (SMF), Policy Control Function (PCF), and Charging Function (CHF) constitute the network functions related to charging and billing, which exchange network and billing events based on user traffic in the 5G LBO architecture.

In this design, components not enabled with SGX (AMF, NRF, PCF) are protected by SGX-encrypted data. Hence, these components are considered within a non-trusted zone, eliminating the need for trust.

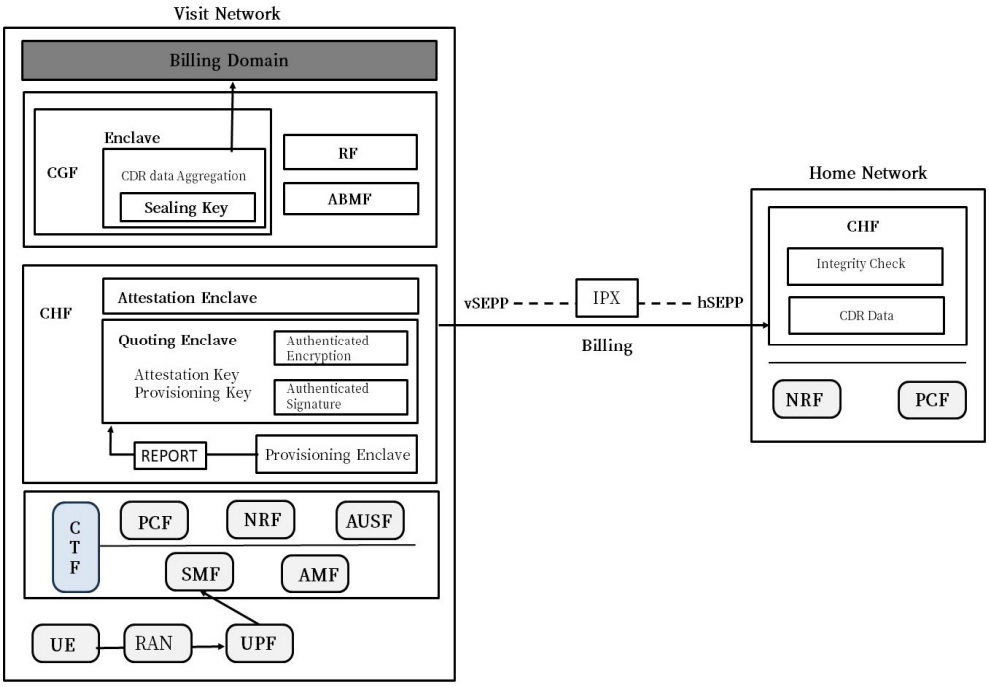

FIGURE 6. An overview of 5G LBO Enabled SGX Roaming

5.1 Security Requirement

The roaming agreement mandates strict adherence to the Roaming Network and its associated Network Functions during roaming events between VPLMN in the Local Breakout scenario. This agreement explicitly defines SGX-enabled network functions within the VPLMN, which is responsible for executing SGX operations such as Remote Attestation and Sealing. The VPLMN is obligated to promptly notify HPLMN about the usage of each Network Function. Operations of any undefined or unidentified Network Function on the roaming network are automatically blocked.

In cases where the storage of data protected by a Network Function or SGX is required for additional roaming activities, a verification process is initiated. The PCF manages this process, overseeing verification procedures on roaming networks and implementing roaming policies to prevent any alert-notification-defined Network Functions from impacting roaming activities. The HPLMN or SGX-Enabled Network Function must also adhere to the same policy.

The SGX-enabled V-CHF stores policy counter information related to subscriber plans and notifies the V-PCF when a subscriber exceeds a policy threshold based on usage consumption. Upon receiving this policy-trigger information, the V-PCF collaborates with V-SMF to enforce policy decisions, completing the process by informing the UPF about policy enforcement.

CDR replacement process, each CHF in VPLMN and HPLMN must conduct Remote Attestation to ensure proper replacement execution and

validate data integrity.

The UPF initially receives User IP Traffic from UE, conducting sealing operations within UPF. Subsequently, as data from the CTF stage is transmitted to the CHF, corresponding Remote Attestations occur in the Enclave and CGF Enclave within the CHF. This process extends to CDR exchanges between the two networks within CHF, with the HPLMN conducting integrity checks. Finally, the billing process is executed, delivering CDRs from the Billing Domain of the VPLMN to the HPLMN.

SGX Sealing operations are performed when UPF receives user traffic on the VPLMN. Data related to this event is encrypted to the Sealing Key inside the Enclave, securely generated, managed, and stored within. As encrypted data moves outside the Enclave, it is sealed and delivered. However, UPF's SealData is connected to the SMF. The untrusted application of the SMF protects its contents and unseals and decrypts seal data inside the Enclave of SMF with the Sealing Key. The UPF Raw data inside the Enclave is then decrypted and verified, with the Enclave of SMF checking the data and transmitting it back to CHF as a sealing operation.

The CHF is divided into untrusted and trusted areas, including Quote Enclave, Provisioning Enclave, and Enclave. Data collected from CTF's network and billing events through the Nchf interface is stored in the CHF's secure area. The trusted Enclave, operational only when functioning correctly, protects billing data. The Provisioning Enclave specifies the Enclave State, indicating its running and successful initialization. A report summarizing the hash value Measurement for

Enclave execution code and data is submitted to Quote Enclave, initiating Remote Attestation. The Provisioning Enclave generates a Provisioning Key and securely stores the Attestation and Sealing Key.

Quote Enclave leverages this report to validate the client's SGX environment and assert the client's credibility with the server. H-CHF meticulously examines reports received from Quote Enclave to corroborate the reliability of the V-CHF environment. Enclaves within SGX-enabled V-SMF and V-CGF ascertain reliability by ensuring secure data storage or authentication with an Attestation Key inside the Quote Enclave.

Within CHF, CDR data is consolidated within the Enclave area of CGF, engaging with other RFs and ABMFs to quantify billing. CDRs securely measuring billing within a CCS, comprising CHF, CGF, RF, and ABMF, are dispatched to the Billing Domain.

During roaming, CDRs are exchanged between networks, with CDRs generated by CCS in the VPLMN exchanging between H-CHF and V-CHF. At this juncture, data based on roaming usage is collected and managed by V-CHF, and the billing measurement process can be verified flawlessly within the Enclave Signature.

H-CHF can securely exchange CDRs delivered to the VPLMN over a protected communication channel using an Attestation mechanism for self-verification. CGF aggregates CDR data securely stored in Enclave, and upon delivery to the Billing Domain, Billing charges the HPLMN through Unsealing.

Ultimately, the billing process transpires while delivering CDRs from

the Billing Domain of the VPLMN to the HPLMN. Securing CDR data from VPLMN to SGX empowers roaming users to generate CDRs and network events incurred during roaming, subsequently delivering them to CTF, CHF, and Billing Domain, furnishing an audit trail that is challenging to verify or alter, preserving the integrity of the actual records.

5.2 Security analysis of the system

The home network is shielded from excessive charges beyond the actual usage, as the CDR is adjusted by roaming subscribers according to the activity conducted on the Visited Network. Ultimately, data protection is upheld throughout the process when the CDR charge from the VPLMN is transmitted through the IPX Operator. This ensures that the HPLMN can transfer trustworthy data without incurring additional expenses for transitioning to alternative CDRs or risking data leakage.

5.3 Experimental Setting

All experiments were conducted on SGX machines with Ubuntu 20.04 and the Linux kernel 5.5.0-91. The 5G SA network framework was implemented by deploying version 3.3.0 of Free5GC [15], an open-source software developed based on the 3GPP Release 15 standard [7]. UE and gNodeB use UERANSIM [16], and its version supports the CHF among the core network functions for 5G SA networks. The experimental environment of the SGX framework consists of 1.4.1 version EGO [17] and 1.6 version Gramine [18], which are frameworks that support Intel

SGX SDK and PSW by default. EGO is an open source SDK for running Confidential Applications on a GO language basis, and Gramine is also a library OS for Linux multiprocess applications that supports Go languages and supports Intel SGX.

Ⅵ. Discussion

Hard to provide differentiated service. The signaling of the Session Initiation Protocol (SIP) can be utilized to derive billing information for voice (and VoLTE) calls, while MNOs typically rely on records to generate invoices. Breakouts occurring at different points complicate accounting due to potential abuses from customers (e.g., billing delays allowing excessive roaming data traffic). Within cellular networks, traffic classes can be distinguished using Access Point Names (APN) and Quality of Service Class Identifiers (QCI). For instance, MNOs may implement HR for data, while LBO for VoLTE can leverage it. This raises questions about whether roaming agreements can be updated using the same principles to block some/all data traffic [5].

VII. Related Work

Relevant scholarly investigations are delineated within the subsequent two categories: security studies concerning billing measurement in roaming networks and the performance measurement of the LBO architecture.

Charging. In the context of security studies on billing measurement in 5G roaming networks, despite the popularity of 5G roaming services, research is still in its early stages. This is anticipated to be due to performance and billing cost issues related to billing measurement in roaming.

Chunyi Peng et al. [19] researched security vulnerabilities in usage-based billing in 3G/4G cellular networks and proposed countermeasures to prevent two attacks exploiting these vulnerabilities. Despite these initial efforts, security assessments for the roaming environment in 5G networks have not been extensively explored since the era of 3G/4G cellular networks.

Rogier Noldus et al. [20] address the impact on the architecture to achieve ARP and LBO services for controlling billing for roaming subscribers and covering content relevant to MNOs. However, the proposed ARP and LBO service architecture does not explicitly mention its limitations or drawbacks.

Ioannis Kaltsas [21] conducted a comparative study of VoLTE roaming architectures, proposing strategies for mobile network operators to cope with increasing traffic and decreasing roaming charges. However, this

study focuses solely on the comparative analysis of VoLTE roaming architectures. It does not provide additional security assessments, except for advocating that the S8HR architecture should disable encryption to eliminate lawful interception. While there have been studies on measuring billing and analyzing performance in existing networks, security analysis studies are lacking based on each roaming architecture.

The identified gap in the literature is addressed in this study, which endeavors to conduct a security analysis leveraging SGX for the establishment of reliable roaming capabilities within 5G SA networks.

LBO Performance. Recent research on the 5G network roaming LBO architecture has primarily focused on performance measurements. Studies such as [6] and [5] investigate the impact of international data roaming in Europe and compare and analyze the performance of roaming architectures, specifically Home Routing and LBO, to derive performance results. [6] examines the impact of international data roaming on user experience and analyzes detailed aspects of the infrastructure and user experience of international data roaming. In contrast, [5] measures the performance of international data roaming using LBO, discusses the performance advantages provided by LBO, and addresses considerations regarding service control, billing, and privacy. However, this research primarily focuses on the performance aspects of LBO and does not provide additional specific evaluations regarding billing and privacy. In this study, experimentation is conducted on the 5G network roaming LBO architecture, with a particular focus on billing and security

considerations. TEE technology, such as SGX, is employed to address these challenges without compromising the performance advantages inherent in LBO.

VIII. Conclusion and Future Work

Despite the advantages of LBO in roaming architecture, it is not actively implemented by many MNOs. Two significant security challenges have been highlighted in our study: the weak trust model and the lack of transparency to MNOs. To address these issues, the establishment of a mechanism to ensure trustworthiness between HPLMN and VPLMN is deemed crucial for the widespread adoption of LBO in roaming architecture. Consequently, to validate the integrity of roaming billing and authentication in the future, a design for an Intel SGX-based 5G SA LBO network function will be proposed, and its performance will be verified through experiments.

References

[1] G. Association, "Official document ir.88 - eps roaming guidelines." https://www.gsma.com/newsroom/wp-content/uploads/IR.88-v25.0-17.pdf, 2021.

[2] G. Association, "5gs roaming guidelines." https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v4.0.pdf, last viewed May 2021, 2021.

[3] 3rd Generation Partnership Project (3GPP), "System architecture for the 5G System (5GS)," 3GPP TS 23.501, 3GPP, December 2023. URL: https://www.3gpp.org//ftp/Specs/archive/23series/23.501/.

[4] R. Keller, D. Castellanos, A. Sander, A. Robison, and A. Abtin, "Roaming in the 5g system: the 5gs roaming architecture," tech. rep., Ericsson, 2021.

[5] A. M. Mandalari, A. Lutu, A. Custura, A. S. Khatouni, Alay, M. Bagnulo, V. Bajpai, A. Brunstrom, J. Ott, M. Trevisan, M. Mellia, and G. Fairhurst, "Measuring roaming in europe: Infrastructure and implications on users' qoe," IEEE Transactions on Mobile Computing, vol. 21, no. 10, pp. 3687 - 3699, 2022.

[6] A. M. Mandalari, A. Lutu, A. Custura, A. Safari Khatouni, O. Alay, M. Bagnulo, V. Bajpai, A. Brunstrom, J. Ott, M. Mellia, and G. Fairhurst, "Experience: Implications of roaming in europe," in Proceedings of the 24th Annual International Conference on Mobile Computing

and Networking, MobiCom '18, (New York, NY, USA), p. 179 - 189, Association for Computing Machinery, 2018.

[7] 3GPP, Technical Specification Group Core Network and Terminals, "5G System; Unified Data Repository Services; Stage 3 (Release 15)," Tech. Rep. TS 29.504, 3GPP. https://www.3gpp.org/.

[8] 3rd Generation Partnership Project (3GPP), "Security architecture an d procedures for 5g system," 3GPP TS 33.501, 3GPP, 2020. URL: htt ps://www.3gpp.org/ftp//Specs/archive/33series/33.501/.

[9] S. Chakrabarti, "Protecting telecom core with intel® sgx."https://ww w.intel.com/content/dam/www/public/us/en/documents/research/somna thchakrabarti-sgx-day-telco-security.pdf, 2020.

[10] 3rd Generation Partnership Project (3GPP), "Telecommunication ma nagement; Charging management; Charging architecture and principl es," 3GPP TS 32.240, 3GPP, September 2021. URL: https://www.3gp p.org/ftp//Specs/archive/32series/32.240/.

[11] G. Association, "International roaming explained." https://www.gsm a.com/latinamerica/wp-content/uploads/2012/08/GSMA-Mobile-roamin g-web-English.pdf, last viewed April 2010, 2012.

[12] I. K. Kaltsas, "Make yourself at home: A comparative study of vol te roaming architectures," 2017.

[13] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking atta cks for lte networks using the interworking functionality," in 2016 I FIP Networking conference (IFIP Networking) and workshops, pp. 3 15 - 322, IEEE, 2016.

[14] G. Macia-Fern ´ andez, P. Garc ´ ´ıa-Teodoro, and J. D´ıaz-Verdej o, "Fraud in roaming scenarios: An overview," Wireless Communicat ions, IEEE, vol. 16, pp. 88 - 94, 01 2010.

[15] free5gc, "free5gc." https://github.com/free5gc/.

[16] aligungr, "UERANSIM." https://github.com/aligungr/UERANSIM.git.

[17] edgelesssys, "EGO." https://github.com/edgelesssys/ego.git.

[18] gramineproject, "Gramine." https://github.com/gramineproject/gramin e.git.

[19] C. Peng, C.-y. Li, G.-H. Tu, S. Lu, and L. Zhang, "Mobile data ch arging: New attacks and countermeasures," in Proceedings of the 20 12 ACM Conference on Computer and Communications Security, CC S '12, (New York, NY, USA), p. 195 - 204, Association for Computin g Machinery, 2012.

[20] R. Noldus and L. Norell, "Roaming unbundling – challenges and o pportunities," in 2013 17th International Conference on Intelligence in Next Generation Networks (ICIN), pp. 118 - 125, 2013.

[21] I. Kaltsas, "Make yourself at home: A comparative study of volte r oaming architectures," 2017.

논문 개요

5G 로밍 서비스의 보안과 신뢰성 강화: 안전한 과금 및 인증을 위한 Intel SGX 기술을 활용한 LBO 아키텍처

노현
미래융합기술공학과
성신여자대학교 대학원

상용화된 5G 네트워크는 로밍 시나리오에서의 효율성을 향상시킬 수 있게 되었다. 로밍 시나리오에서의 과금 및 인증은 단순히 가입자의 지불뿐만 아니라 모바일 네트워크 사업자의 자산과 밀접한 관련이 있어 중요하다. 그러나 현재의 신뢰 기반 로밍 아키텍처는 보안 측면에서 취약한 신뢰 관계를 형성하며 로밍 과정에서의 모바일 네트워크 사업자를 신뢰하고 검증하기 어렵다. 주로 local breakout의 성능 위주 연구로 이루어져 왔지만 과금 및 인증을 위한 보안 측면의 연구는 초기 단계이다. 본 논문은 5G Stand Alone 네트워크에서 로밍 아키텍처 local breakout의 과금과 보안 측면에서의 문제점을 논의하고, local breakout의 안전한 과금 및 인증을 위한 Intel SGX 기술을 활용한 디자인을 제안한다. 제안된 local breakout 아키텍처를 기반으로 SGX 프레임워크를 사용하여 Remote Attestation과 Sealing을 통해 무결성을 증명하면서 동시에 성능을 보장하는 연구를 수행한다.

ACKNOWLEDGEMENTS

본 논문을 지도해주신 김성민 교수님과 공저자로서 도움을 주신
알파카네트웍스 배상욱 CTO님과 정은영 대표님께 감사드립니다.