





Article

Secure Secondary Authentication Framework for Efficient Mutual Authentication on a 5G Data Network

Seonghyeon Gong , Abir EL Azzaoui  and Jeonghun Cha  and Jong Hyuk Park * 

Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea; gongsh@seoultech.ac.kr (S.G.); abir.el@seoultech.ac.kr (A.E.A.); ckwjdgns@seoultech.ac.kr (J.C.)

* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Received: 22 November 2019; Accepted: 14 January 2020; Published: 20 January 2020



Abstract: The service-based architecture of the Fifth Generation(5G) had combined the services and security architectures and enhanced the authentication process of services to expand the coverage of the network, including heterogeneous devices. This architecture uses the secondary authentication for mutual authentication between the User Equipment (UE) and the Data Network (DN) to authenticate devices and services. However, this authentication mechanism can cause a signaling storm in the Non-Access Stratum (NAS) because the end node needs to communicate with the authentication server of the NAS area. This problem could affect the availability of the network when the network is extended. This research proposes a mutual authentication framework that can efficiently perform a mutual authentication process through secondary authentication between UE and DN. The proposed framework uses newly devised network functions: Secondary Authentication Function (SAF) and the Authentication Data Management Function (ADMF). This framework proposes a methodology at the protocol level for efficient mutual authentication using the mobile edge computing architecture. We analyzed the proposed framework in the point of security considerations, and we evaluated the effect of the framework on the traffic of the NAS layer and user experience. Our simulation results show that the proposed framework can reduce the NAS traffic by 39% and total traffic of the overall network by 10%.

Keywords: 5G network; secondary authentication; mutual authentication; edge computing

1. Introduction

The development of information and communication technology dramatically changed the form of services by maximizing connectivity between users and devices. Most information services today use cloud services as a platform. Platform as a Service(PaaS) [1] technology enabled several services to be integrated into cloud computing environments, and each service increased its efficiency through a centralized operating structure. Statistics show that the cloud market, which was \$127 billion in 2016, is expected to grow to \$163 billion by 2021 [2]. The change that began with the increased connectivity of the network led to the Internet of Things(IoT) technology and created an environment where not only services but also all devices connected to the network can create various additional services. The variety of technologies, such as smart cities, autonomous driving, and augmented reality, are being activated through the connection of various devices. Also, the requirements of 5G communication technology such as high communication speed, bandwidth, and low latency are expected to create synergies by integrating with IoT technology [3]. The convergence of these technologies makes high-level services available to many people and increases the efficiency of services through a unified management structure of the network.

However, this expansion of connectivity can cause problems in two perspectives. The first problem is that network traffic can explode as the number of devices connected to the network increase, and many services move to cloud platforms [4]. As data collected from a large number of nodes is transmitted to the cloud server, a vast amount of traffic is generated, and the amount of unnecessary traffic on the cloud server increases. The second is the security issue. As different heterogeneous devices are connected, they can cause security problems of communication and protocol to integrate and operate with each other. Functions such as mutual authentication and cryptographic communication are required for data communication between devices [5]. However, there is a limitation that all devices cannot communicate with the same protocol because the performance and operation environment of the devices are different. For compatibility of each device, there may be a point where sufficient security requirements are not satisfied in the operation of proper authentication and communication protocols. The more devices connected and the more diverse the network, the higher the number of these points, and the more difficult it becomes to prevent attackers from spreading malicious devices or data breaches through these points [6].

The 5G network architecture aims to improve the efficiency of communication and to solve security problems by including service areas in the network security architecture. To expand the area of network and to support various types of services and devices, the 5G architecture provides primary and secondary authentication for users and services [7]. When a user accesses a service network, the user can be authenticated not only on the network but also on the service network. This secondary authentication increases the compatibility between the device and the service area, solving the security vulnerabilities that may exist in the communication process [8]. However, this mutual authentication process can exacerbate the traffic problem of the network. The traffic generated by secondary authentication is transferred to the 5G home network area. When authentication for the terminal devices is frequently requested, this may put a load on the central home network [9]. Also, the fact that the authentication traffic is transmitted to the home network can cause a vulnerability that allows an attacker to intentionally generate traffic and perform a DoS attack on the entire network. For the functional purpose of authentication, 5G's authentication mechanism should be able to address and prevent these problems. Thus, the secure and scalable secondary authentication of 5G should give the proper answers about the following questions:

1. Does the authentication mechanism mitigate the problem of the NAS signaling storm?
2. Can the authentication mechanism provide enough scalability and auditability on the heterogeneous devices and services against the extension of the network?

The answers about the questions should be discussed in the standard of 5G, but secondary authentication is not standardized yet in the specification of 3GPP(3rd Generation Partnership Project)'s 5G system Phase 1 (release 15), and release 16 will address that standard in 2020 [10].

In this paper, we propose an authentication architecture that can mitigate the traffic problem of the 5G home network by relaying mutual authentication in the middle of the network. The proposed framework consists of nodes that perform mutual authentication in the serving network and nodes that manage authentication data of the connected device nodes. These nodes are authorized by the data network so that mutual authentication with the network for the user to access the data network can be performed at the middle layer of the network. Also, to efficiently manage the authenticated devices, the data network increases the efficiency of service by managing the authentication information of devices in the edge layer. The proposed network framework can improve the efficiency and security of the entire network by controlling the traffic generated during the mutual authentication of the entire network in the middle layer.

This paper is organized as follows. Section 2 describes the technical backgrounds, issues, and security requirements related to this research. Section 3 explained the state of the art researches related to the security architecture of 5G. The mechanisms and detailed operational structures of the proposed framework are described in Section 4. Section 5 shows the results of simulations and

evaluations of the proposed secondary authentication framework, and we conclude this research in Section 6.

2. Technical Backgrounds

This section addresses the technical backgrounds, related threats, and security considerations in the authentication mechanism of 5G.

2.1. Cloud Computing and Edge Computing

Edge computing and fog computing are concepts that process data from numerous devices connected to the network using the middle layer between the end device where the data is generated and the cloud [11]. Edge computing is a technology that efficiently operates a network by processing data in and around the device where the data is generated [12]. Edge computing can reduce traffic to the cloud or data centers by processing data locally without having to move the data to the cloud. Edge computing technology ensures that networks of heterogeneous devices have adequate security capabilities [13]. Fog computing is a technology that efficiently manages networks by placing nodes in the area of the local environment to process data [14]. The fog layer connects the terminal nodes of the edge layer and services of the cloud layer. Knowledge information from the data collected at the edge layer is used to efficiently manage the network and improve the capacity of the entire network [15]. These hierarchical network architectures are key technologies to meet the enhanced Mobile Broadband(eMBB), Ultra-Reliable Low Latency Communications(URLLC), and massive Machine Type Communications(mMTC) requirements of 5G networks [11].

2.2. 5G

Many industries and academia have extensively researched 5G for more advanced wireless technologies such as innovative speed, high bandwidth, and high availability [16]. 5G must meet many requirements, and to achieve this, integration of various technologies, rather than improved existing cellular communications, must be achieved. The integration of various technologies, such as edge computing to meet low latency, and high-density base station deployment for high availability, creates the complexity of 5G networks. As a result, 5G can efficiently manage complex networks through Software Defined Networking (SDN) and Network Function Virtualization (NFV), which are critical technologies in 5G configurations [17].

2.3. Threat Modeling on Authentication

5G communication is particularly vulnerable compared to the previous environment due to its structural characteristics. This section addresses the threats that may arise during the second authentication process in 5G environments: NAS signaling storm and diversity of access mechanism.

Converging with the IoT paradigm, the 5G communication network is expected to cover billions of heterogeneous devices and interact with them [18]. Interaction between devices requires mutual authentication. This authentication process occurs at the 3GPP NAS(Non-Access Stratum) layer. However, the packet data used in bearer activation [19] and location update for authentication may cause a NAS signaling storm [20]. NAS signaling storm means that the NAS layer service becomes difficult to operate correctly due to a large amount of traffic in the network environment. An attacker can exploit this phenomenon maliciously. An attacker can maliciously drive the NAS layer's traffic by requesting re-authentication by constantly modifying device information, or by continuously generating unnecessary authentication signals [16]. NAS signal traffic is affected by the number of devices connected to the network, which means that as the network expands, the entire network may become vulnerable. Also, encryption-based tunnel setup such as bearer activation and IPSec further increases the cost of network signals. These features can be regarded as a structural problem of the centralized core network. Therefore, the 5G network environment is required to prevent structural

DoS attacks that can be applied to signal traffic planes in the process of performing authentication between multiple devices.

Also, 5G networks provide connectivity to small cells such as femtocells and picocells, as well as general networks for connectivity between various devices [21]. These secondary open-access networks are used to increase the overall capacity of the network and have various advantages in terms of low cost and indoor coverage. However, the secondary network of various devices may not support sufficient strength of security due to the performance spectrum of each device [15]. Low-power devices used in open-access networks may not encrypt for availability during data communications and may use weak authentication mechanisms. Integration with open secondary networks requires a low complexity and efficient handover authentication mechanism to optimize power consumption [8].

2.4. Security Considerations and Requirements

Authentication mechanisms used in 5G environments, especially secondary authentication, must satisfy additional considerations in addition to those of the general authentication protocol. This section addresses four security considerations that should be considered by the secondary authentication in the 5G environment: Availability, Flexibility, Auditability and Independence of Authentication Authority.

2.4.1. Availability

The convergence of 5G communication and IoT technologies should be a network that can connect heterogeneous devices while requiring high communication performance, bandwidth, and low latency [17]. In a 5G environment where a significant number of devices are expected to be connected, rigorous optimization of the performance of the entire network must be performed to meet these requirements. In particular, 5G networks must be able to accommodate traffic from additional authentication. Moreover, the architecture for 5G communication should consider ways to solve the traffic load on the home network, reduce the amount of traffic delivered to the central network through the hierarchical structure, and have the structure to manage the end nodes efficiently [22].

2.4.2. Flexibility

Service-based architectures through network virtualization and network slicing are critical to the flexibility of 5G communication environments. These technologies enable the 5G network to provide various services at the network level, and network devices can provide various types of services through services implemented in the form of network functions. Many of the devices in a heterogeneous network are devices with limited resources. They are sensitive to the consumption of resources used in key generation and management, the operation of cryptographic algorithms, and mutual authentication. Some devices may not support these mechanisms. Therefore, a communication environment composed of heterogeneous networks should provide a basis for satisfying different performance and security requirements for each device by providing various protocols and communication mechanisms in the form of network services [17–19]. The communication architecture for 5G must be able to support a variety of protocols and devices based on this virtualization.

2.4.3. Auditability

5G networks must be able to monitor and manage the access of heterogeneous devices to data networks and services. The 5G network provides various types of services through various paths, and in the process, the environment may cause vulnerabilities that use inappropriate authentication and communication protocols [7]. These vulnerabilities can be mitigated by controlling the network through tiered and centralized architectures. The tiered architecture allows the network to efficiently understand and manage the configuration and behavior of each environment, while centralized architecture facilitates the coordination of the entire network [9,18,23,24]. Since 5G's security architecture uses two mutual authentication processes, it is necessary to manage the operation of authentication data efficiently [15].

2.4.4. Independence of Authentication Authority

The security architecture of 5G encompasses the service area and enhances security level through additional authentication between services and devices [5]. The enhanced authentication process for users through the concept of secondary authentication allows network and service providers to perform mutual authentication separately [25]. It can be considered that the mutual authentication authority that the network provider has in the existing network is also granted to the service provider, which requires the user to authenticate the data network additionally. That is, the service provider is independently granted the authority of mutual authentication for the user device, and this independent procedure cannot be omitted for the availability of the network. However, this new mutual authentication process puts an additional load on the overall network system, which puts security and availability in a trade-off relationship. Therefore, the security architecture for 5G should be designed to maintain the maximum independence of network providers and service providers' authority without sacrificing availability.

3. Related Work

Authentication in 5G network covers heterogeneous devices and networks considering the systematic requirements in terms of Availability, Flexibility, and Auditability. For this, Jianbing Ni et al. [26] proposed a framework that allows nodes to select proper network slice for anonymous data communication and grant authentication of users to IoT servers using service-oriented authentication and key agreement supporting network slicing and fog computing for 5G enabled IoT. Rajat Chaudhary et al. [15] introduced a concept of Kerberos Authentication server. Their approach aims to provide a fast and efficient authentication service at cloud computing that was significantly threatened by the DDoS attacks. Kerberos is designed for authentication of service to secure communication between authorized mobile devices and cloud server in 5G network. Ke Zhang et al. [13] focused on offloading both the computation and communication energy on the Mobile Edge Computing server in the 5G network by solving the optimization problem and designing an energy-efficient MEC cloud offloading resource allocation schemes in the 5G heterogeneous network. Mohammad Wazid et al. [27] designed a new secure key management and user authentication scheme called SAKA-FC for fog computing, and their proposal uses lightweight operations for smart devices as they are resource-constrained by nature. Furthermore, Ruei-Hau Hsu et al. [28] presented a new REconfigurable Solution for IoT security ReSIoT by using a group signature to practice anonymous authentication by signing a given message as a group-based public key credential among the connected devices based on the 5G Edge network. In Bin Han et al. [24] presented the TrustZone architecture to enhance the 5G AAA with cognitive access management, the authors designed a context-aware mechanism of synchronizing subscriber authentication information to local subscriber databases, thus reducing the backhaul network traffic generated by TrustZone and improving the authentication process in 5G. Liang Xiao et al. [23] discussed multiple security challenges in Mobile Edge Caching MEC, which are used in 5G by Mobile Edge Computing to reduce the computation overhead and latency. MEC is vulnerable to attacks like Jamming attacks, DoS, Spoofing attacks, to solve this problem, the authors proposed a security solution based on reinforcement learning such as RL(Reinforcement Learning)-based Anti-Jamming, RL-based Authentication. Their proposal can enhance the security and user privacy of mobile edge caching systems, thus having a reliable 5G network. While the authors of [12] discussed the value of MEC as a standardized solution for Edge Computing especially for use cases targeting fully connected cars, however, these cases require the fulfillment of challenging requirements, which are only possible with the use of 5G networks.

The following Table 1 shows the considerations of related works. As mentioned in Section 2, the authentication mechanism needs to consider four considerations: availability, flexibility, auditability, and independence on authentication authority. However, independence on authentication authority has not discussed to cover the heterogeneous network of 5G because secondary authentication is not standardized yet. Therefore, we propose an efficient secondary authentication framework

considering edge and fog computing architecture. The proposed framework achieves the features that (1) improved availability mitigating the threat of NAS signaling storm by performing the process through a hierarchical network based on cloud and edge computing; (2) flexibility covering various performance and security requirements for each device in a heterogeneous network by dividing large networks into several smaller networks and applying the optimal operation to each network for the compatibility of communication and authentication; (3) auditability by allowing operations in middle layer to efficiently manage total workload; (4) independence of authentication authority to satisfy the consideration of independence of secondary authentication.

Table 1. Comparison of considerations between the previous works and the proposed framework.

Research	Availability	Flexibility	Auditability	Independence
Ni et al. [26]	Efficient connection establishment mechanism on 5G core network	-	-	-
Chaudhary et al. [15]	Kerberos for communication security on mobile devices	Cloud mesh architecture for network service chaining	-	-
Zhang et al. [13]	Energy-efficient computational offload mechanisms for MEC	-	-	-
Wazid et al. [27]	-	Distributed device management mechanism for resource-limited devices	Key Management and User Authentication for Fog Computing	-
Hsu et al. [28]	Efficient mechanism for distribution of security module	Security architecture based on edge computing for flexibility of key management	-	-
Han et al. [24]	Low-cost local authentication	Distributed architecture for local authentication	Context-awareness on user equipment and virtualized network functions	-
Xiao et al. [23]	Solutions for DoS and Jamming attacks	-	Security architecture for mobile edge caching system	-
Sabella et al. [12]	SDN and NFV for MEC-based vehicle architecture	-	-	-
proposed framework	Traffic optimization with authentication relaying	Hierarchical architecture for authentication management	Data management node on the middle layer of architecture	Authorization on the trusted node as a virtualized network function

4. Secure 5G Network Architecture for Mutual Authentication

The overall structure of the framework proposed in this study is shown in Figure 1, and Table 2 shows the abbreviations used in the framework. To mitigate the impact of authentication traffic generated by secondary authentication on the home network of 5G, we designed two novel network functions: Secondary Authentication Function (SAF) and Authentication Data Management Function (ADMF). The role of SAF is to process primary operations of secondary authentication. The SAF receives requests for secondary authentication from the user, processes the request, and interacts with ADMF. The final goal of ADMF is to enhance the auditability of the communication environment. ADMF manages the identity and authentication information for users and DN-AAA(Data Network Authentication, Authorization and Accounting) servers and holds the authentication authority of DN-AAA. ADMF periodically sends a list of Data Networks it owns to SAFs in the surrounding serving network to announce its status. Also, ADMF periodically sends a list of authorized users it stores to the DN-AAA server for efficient management of connected users on the data network.

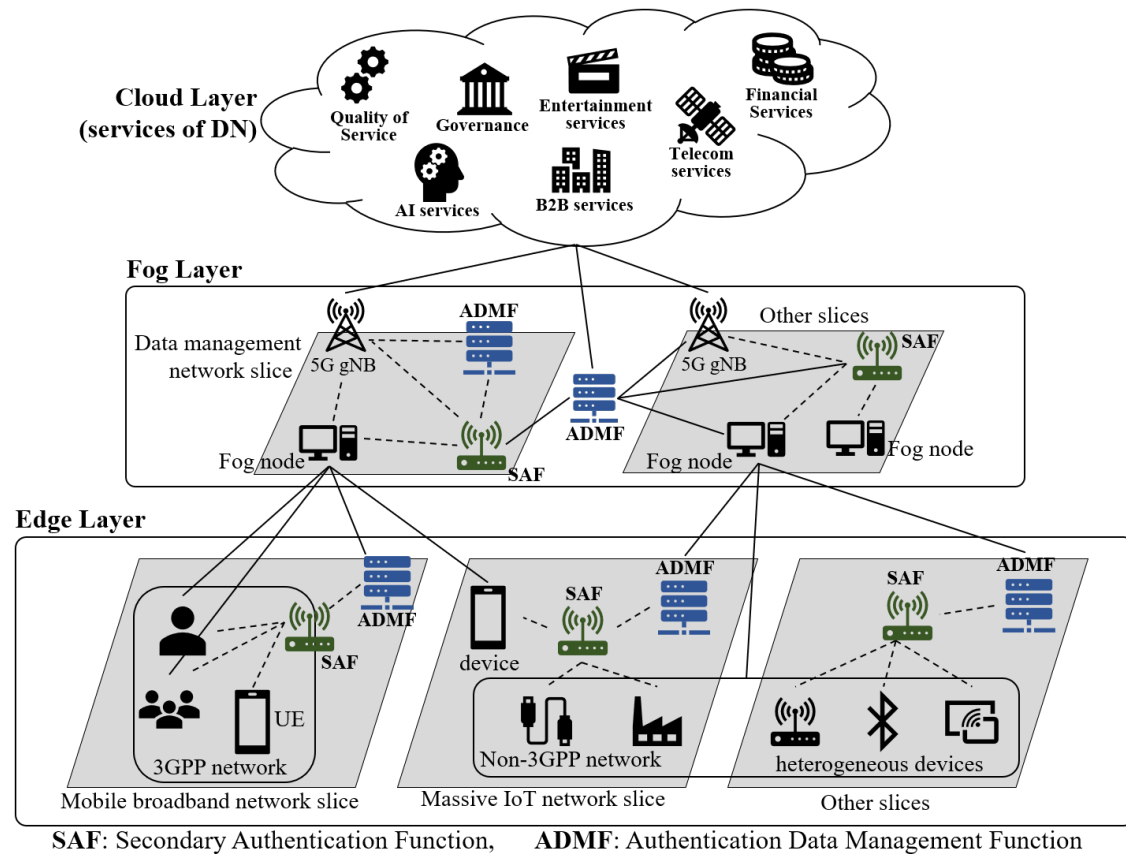


Figure 1. The proposed network architecture.

Table 2. Entities of Secondary Authentication in 5G's Security Architecture.

Abbreviation	Explanation
UE	User Equipment
AMF	Access and mobility Management Function
SMF	Session Management Function
SAF	Secondary Authentication Function
ADMF	Authentication Data Management Function
UPF	User Plane Function
AUSF	Authentication Server Function
DN-AAA	Data Network Authentication, Authorization and Accounting
N4	interface or bridge between control plane and user plane
SUPI	Subscription Permanent Identifier
NAI	Network Access Identifier
PDU	Protocol Data Unit
UDM	Unified Data Management

For the efficient operation of SAF and ADMF, the proposed framework consists of a hierarchical computing network architecture. SAF and ADMF, which are vital entities for efficient mutual authentication, are configured in the form of network functions and can be installed and operated in various types of equipment such as servers and general-purpose routers. In this way, the SAF can be freely located in a wide range of areas, from the network where the terminal nodes are located to the fog layer that controls the terminal node, and the SAF that handles secondary authentication requests from neighboring networks. ADMF is located in the fog layer to store and manage the information related to secondary authentication, collected and operated from SAFs. ADMF can only be located on nodes where network providers, such as carriers, can trust, so they are installed and operated on the base stations.

Mutual authentication in 5G is divided into initial and re-authentication processes to avoid duplicate authentication processes. Initial authentication is the process by which a user first authenticates to a data network and is initiated by the user equipment. The re-authentication process is used to validate the connection and maintain and renew the authentication status for networks and users that have been secondary authenticated. The re-authentication process can occur either by the user or by DN-AAA. The procedure of the initial authentication and re-authentication process of the mutual authentication framework proposed in this study is illustrated in the following Figures 2 and 3.

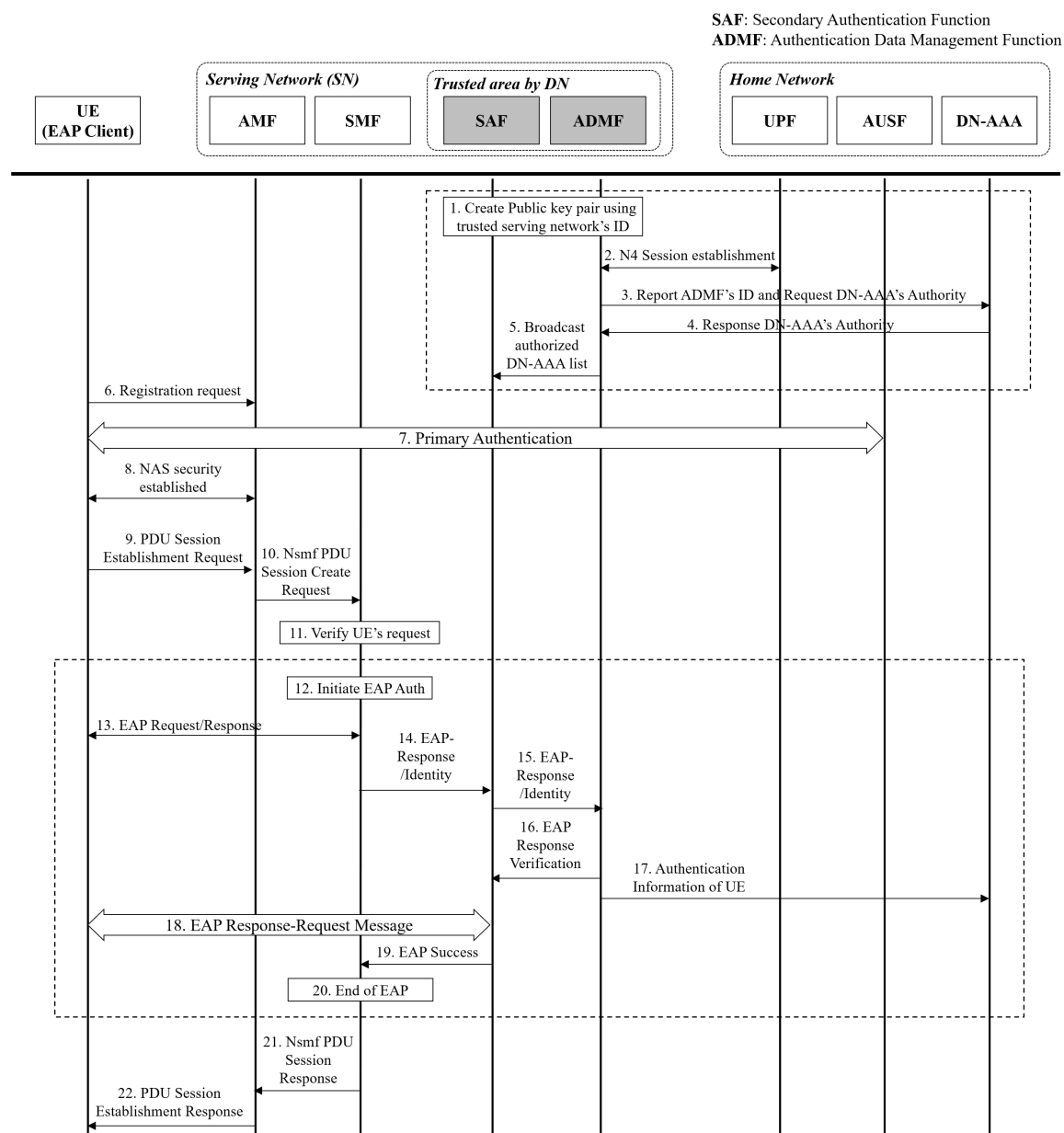


Figure 2. The initial secondary authentication with Secondary Authentication Function (SAF) and Authentication Data Management Function (ADMF).

The following describes the procedures of the initial authentication process described in Figure 2.

1. Base stations located in the Serving network area operate SAF and ADMF in the form of sliced network functions. Base stations that previously gained trust from service providers can operate SAF and ADMF internally, and ADMF runs on devices in the fog layer. Also, SAF can be operated in equipment such as servers, routers, and switches that exist at the edge layer and can

simultaneously perform authentication from a service provider. They relay mutual authentication of adjacent peripheral IoT devices. SAFs and ADMFs generate a public key pair using the node's resources, which are used to obtain the authentication authority of the DN-AAA server.

2. ADMF establishes an N4 session with the UPF to communicate with the DN-AAA server.
3. ADMF requests authorization from the DN-AAA server via the N4 interface. At this time, ADMF encrypts its ID information signed with the private key of the base station and transmits it with the public key of the DN-AAA server.
4. The DN-AAA server decrypts the input ADMF request packet with its private key. The DN-AAA server verifies the signature of the decrypted data using the public key of a base station. In the case of a trusted base station, its ID value and authentication authority information to be used for secondary authentication are encrypted using the base station's public key and transmitted to ADMF.
5. Authorized by the DN-AAA server, ADMF informs the SAFs of the other nodes that are connected to it about its data network.
6. The UE sends a registration request to the AMF for primary authentication.
7. AMF performs a primary authentication between the network provider and the UE using a predefined protocol.
8. The UE establishes a NAS security context with the AMF.
9. The UE sends a NAS message, including the PDU Session Establishment Request message, to the AMF to perform mutual authentication with the DN-AAA server.
10. The AMF delivers the message of the received UE to the SMF via the N1 SM container. At this time, SUPI information of the UE is delivered together.
11. The SMF checks the subscription information of the UE from the UDM using the received SUPI. The SMF checks with the local policy, whether the UE's request is legitimate.
12. If the UE request is justified, the SMF starts secondary authentication with DN-AAA.
13. The SMF delivers the EAP Request to the UE. The UE sends an EAP Response in response to this and transmits a message, including a network access identifier (NAI).
14. The SMF, having received the EAP Response from the UE, delivers the EAP Response message to the SAF existing in the neighbor node.
15. The SAF forwards the EAP Response message received from the SMF to the ADMF associated with it.
16. The ADMF checks the SUPI information of the NAI and the UE and the PDU Session Establishment Request message in the EAP Response received from the SMF. When a request for a service for which the user is authorized is confirmed, ADMF sends an EAP Response Verification message to the SMF.
17. The ADMF transmits the information on the UE for which authentication is requested to the DN-AAA server.
18. If ADMF confirms the suitability of authentication, SAF and UE exchange the EAP message.
19. If the EAP message is exchanged successfully, the SAF informs the SMF that the authentication was successful by sending an EAP Success message.
20. The SMF terminates the authentication procedure by storing the authentication details of the UE and the ID of the data network.
21. SMF delivers Nsmf PDU Session Response message to AMF.
22. The AMF informs the UE that the secondary authentication was successful by sending a PDU Session Establishment Response message. After that, the UE may access a data network and receive the service.

The following describes the re-authentication procedure for secondary authentication described in Figure 3.

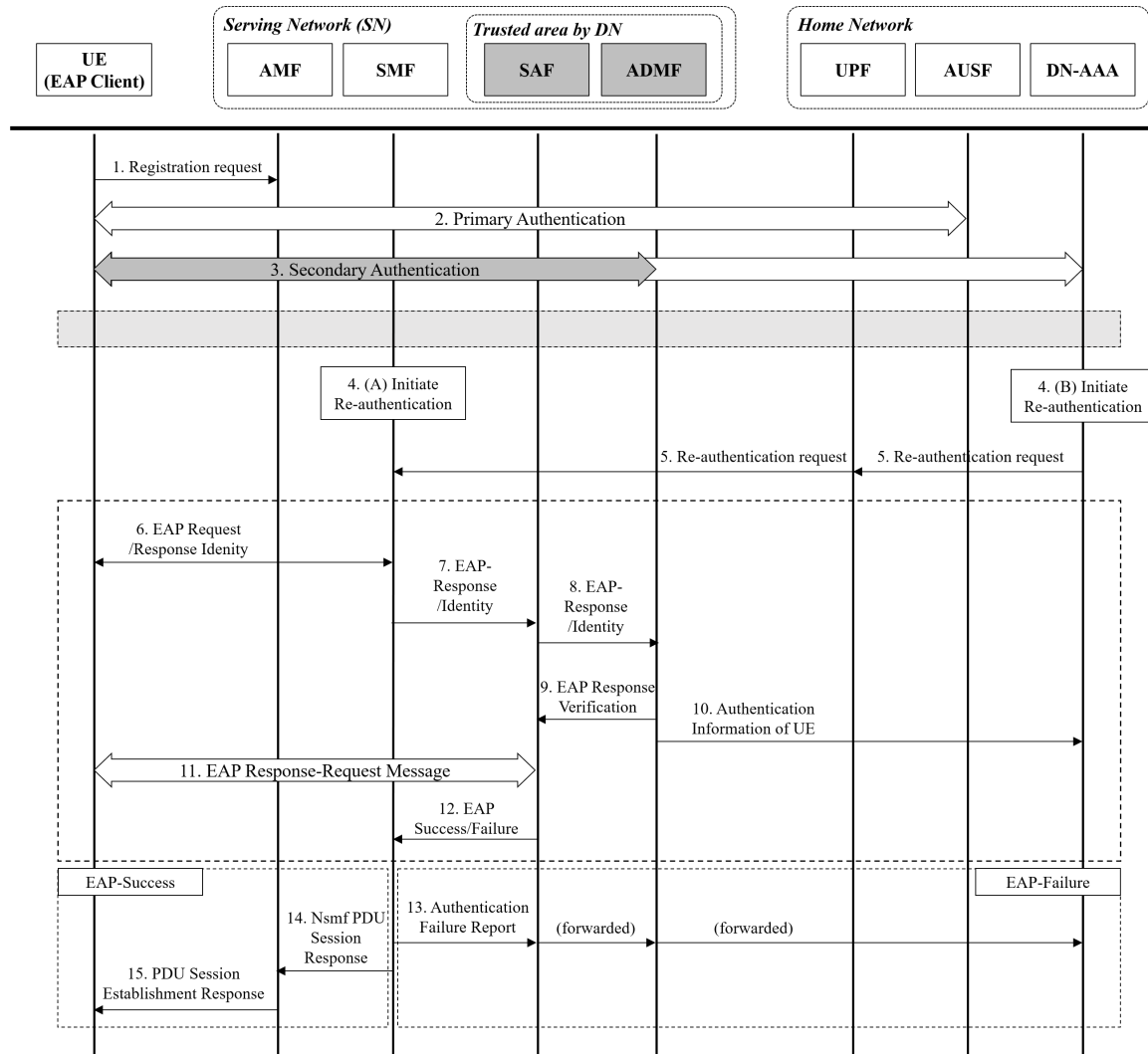


Figure 3. The Re-authentication of proposed secondary authentication framework.

1. The re-authentication process assumes that at least one initial secondary authentication should be performed beforehand. For initial authentication, the UE sends an initial authentication request message to the AMF.
2. UE and AUSF perform primary authentication. This process corresponds to procedure 7 of the initial secondary authentication process.
3. UE, SAF, and ADMF perform secondary authentication. This process corresponds to procedure 9–22 of initial authentication. After secondary authentication is successfully performed, the UE uses the service of DN. The secondary authentication established at this time may expire due to UE movement, timeout, change of policy of DN-AAA, and session coordination.
4. At any time, the UE and the DN-AAA server may request re-authentication, respectively.
5. If the DN-AAA requests re-authentication, the DN-AAA sends a message to the UPF. This message is transmitted via the N4 interface to send a re-authentication message to the SMF. UPF forwards this message to the SMF. If the UE requests a re-authentication process, this procedure is omitted.
6. The SMF delivers an EAP Request/Identity message to the UE to perform re-authentication, and the UE delivers an EAP Response/Identity message in response.
7. SMF delivers the EAP Response/Identity message to the SAF.
8. SAF forwards the EAP Response/Identity message to the ADMF.

9. The ADMF confirms the suitability of the re-authentication request for the UE from the message sent from the SAF. If conformance is verified, ADMF forwards the EAP Response Verification message to the SAF.
10. DMF transmits the information of the UE requested to be re-authenticated to the DN-AAA server.
11. If ADMF confirms the suitability of authentication, the EAP message is exchanged between SAF and UE.
12. The SAF informs the SMF whether the EAP succeeds or fails.
13. If EAP authentication fails, authentication failure information for the UE is passed to the ADMF and DN-AAA server via SAF. This process is skipped if EAP authentication succeeds.
14. SMF delivers Nsmf PDU Session Response message to AMF.
15. The AMF terminates the re-authentication process by sending a PDU Session Establishment Response message to the UE.

The proposed framework is designed for efficient secondary authentication performed in the process of receiving service from the data network. This framework relays secondary authentication traffic in the area of serving network through SAF and ADMF. This relaying minimizes the impact of authentication traffic that affects the home network. This approach mitigates the risk of NAS signaling storm of the home network by allowing secondary authentication to be performed in the serving network, achieving better efficiency of communication as the size of the network increase. Also, the proposed authentication mechanism is performed by SAF and ADMF, which are deputed the role of the DN-AAA server. ADMF nodes are located in trusted nodes, such as base stations, and are pre-authenticated by the DN-AAA server. ADMF then processes the secondary authentication requests from the UEs via SAF. ADMF retains the authentication authority received from the DN-AAA server for a specified period, which is determined by the service provider's policy. During this period, ADMF and SAF continuously process secondary authentication requests from UEs in neighboring networks. This approach can efficiently operate in a network of heterogeneous devices. Heterogeneous networks can use multiple SAFs to separate data networks by their limitations. Each SAF performs the authentication for specific requirements. Thus, a system that can cover all mutual authentications for the heterogeneous network could be configured. Therefore, network configuration through dedicated SAF can significantly improve the flexibility of the entire network. Also, the traffic problem that is relatively concentrated in the serving network can be effectively solved by distributing the size of the network through the edge computing architecture.

In 5G, the secondary authentication means that the network area and the service area are considered simultaneously at the point of security. However, secondary authentication is in a trade-off relationship with availability because it is an additional authentication procedure to be performed. Therefore, to satisfy the performance requirements and security considerations of 5G, mutual authentication mechanisms of a network area and an independent service area should be separated. To satisfy the consideration of independence of secondary authentication, the framework proposed in this study assumes that the ADMF, which performs mutual authentication, is located as a trusted base station. The reliable location of ADMF allows delegating the authority of authentication. The environment running ADMF must be an environment where the DN-AAA server can trust. In this environment, DN-AAA can grant authentication authority to ADMF through public key-based communication. This structure is the basis for the ADMF to operate the secondary authentication in the serving network.

5. Validation Procedures and Results

In this section, we perform a simulation to evaluate the efficiency of the proposed secondary authentication framework. To quantitatively express the performance of the proposed framework, we evaluate the communication cost as the performance of secondary authentication in the simulated environment. The ideal requirement of the 5G network's communication latency is 1ms or less of

end-to-end round-trip time [29]. However, to simulate the real-world latency of the 5G network is very challenging because to meet the ideal latency in real-world communication is infeasible. Thus, to concentrate on the NAS signaling storm problem, we define the communication cost as the amount of traffic at each network domain. In this experiment, we compare the performance of proposed our scheme with the secondary authentication scheme that is introduced in the 5G system release 15 specification [30] published by 3GPP.

To evaluate the number of packet transmission, we separated the type of transmission according to the participating nodes on each communication. Figure 4 shows the types of communication in the authentication mechanism of 5G. Communication between user equipment (UE) and serving network (SN) is wireless communications and performed in the access stratum (AS). Communications between nodes of SN such as AMF, SMF, SAF, and ADMF use wireless or wired communication and is performed in both edge and fog layer. Communications between serving network node (AMF, SMF, SAF, and ADMF) and home network node (UPF, AUSF, and DN-AAA) are the non-access stratum (NAS) communications. Moreover, some communication is performed within the home network nodes. According to these types of communication, we expressed the cost of each communication in Table 3.

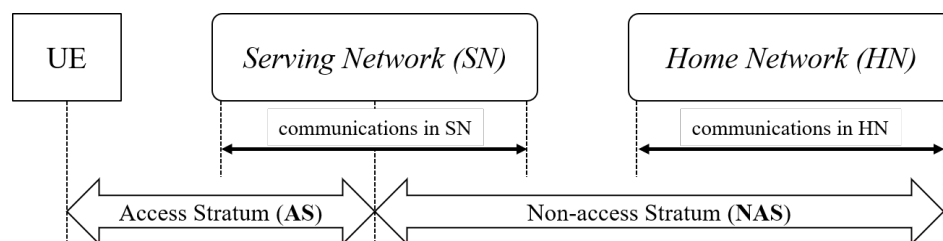


Figure 4. Types of Communications for Authentication in 5G.

Table 3. Cost Terms on Communication Types of 5G Authentication.

Term	Explanation
$n(T_{AS})$	The number of packet transmission between the UE and SN node
$n(T_{SN})$	The number of packet transmission between SN nodes
$n(T_{NAS})$	The number of packet transmission between the SN node and HN node
$n(T_{HN})$	The number of packet transmission between HN nodes

The NAS signaling storm affected by the number of NAS and HN traffics. Thus, $n(T_{NAS}) + n(T_{HN})$ affects the degree of NAS signaling storm problem. Moreover, the number of AS and SN traffics directly affects the user experiences. Thus, $n(T_{AS}) + n(T_{SN})$ means the availability of user on the 5G network. We evaluate the proposed secondary framework using these two perspectives: the degree of NAS signaling storm and user availability.

5.1. Simulation Settings

Proposed secondary authentication mechanisms in this research are composed of two schemes: initial secondary authentication and re-authentication. In Figure 2, steps 1 to 5 show the detailed process of initialization and steps 6 to 8 means the primary authentication process. Detailed procedures of secondary authentication are illustrated in steps 9 to 22 of Figure 2. Since the processes of primary authentication are already standardized and are out of our research scope, we evaluated the performances about the initialization and secondary authentication schemes. Likewise, in Figure 3, steps 1 to 3 mean the pre-procedures, and steps 4 to 15 mean the re-authentication. In the experiment, we evaluated the performance of re-authentications. According to the cost terms explained in Table 3, we analyzed the costs of each communication in the authentication process. Table 4 shows the analyzed costs of each communication.

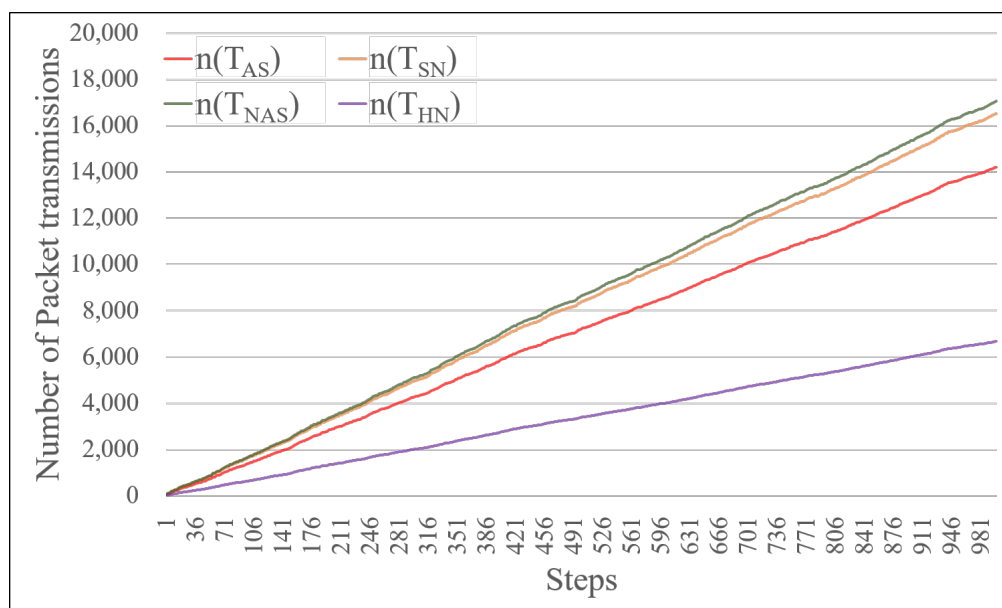
Table 4. Number of packets on Each Communication.

Scheme		$n(T_{AS})$	$n(T_{SN})$	$n(T_{NAS})$	$n(T_{HN})$
original (3GPP release 15 [30])	authentication	6	8	8	2
	re-auth (success)	5	5	5	2
	re-auth (failure)	5	5	7	3
proposed framework	initialization	-	1	4	-
	authentication	6	10	1	-
	re-auth (success)	5	9	2	1
	re-auth (failure)	5	10	3	1

The simulation environment consisted of 10 UEs, and the other nodes, such as SAF, ADMF, DN-AAA, etc. were configured one by one. In the experiment, we simulated the random actions of each UE repeatedly and calculated the number of packets generated in each step on communication types. For each step of the simulation, each UE repeats the action such as inter-network physical moving or using service, that can trigger the request of authentication, re-authentication, and the expiration of authentication. If the DN-AAA does not authenticate a UE, UE continuously requests a connection for secondary authentication with a specific probability (we had set the probability on authentication request to 0.8). If a UE is authenticated, the UE continuously take some actions that could trigger the expiration or re-authentication (we had set the probability of expiration to 0.2 and the probability of re-authentication to 0.8). Moreover, each success rate of the re-authentication had been set to 0.8. We performed the simulation repeatedly for 1000 steps.

5.2. Results and Analysis

Figures 5 and 6 show the number of packets generated by the original and the proposed secondary authentication framework. In Figure 5, the distribution of traffic in the original scheme relatively weighted on the traffic of UE($n(T_{AS})$), serving network($n(T_{SN})$), and NAS area($n(T_{NAS})$) and the amount of traffic in home network($n(T_{HN})$) is much smaller than other traffics. On the other hand, in Figure 6, the amount of traffic in the proposed framework is concentrated in the area of the serving network($n(T_{SN})$), and the number of home network traffic($n(T_{HN})$) is the smallest, like the traffic of the original framework.

**Figure 5.** Number of packets generated by the secondary authentication scheme of 3GPP release 15 [30].

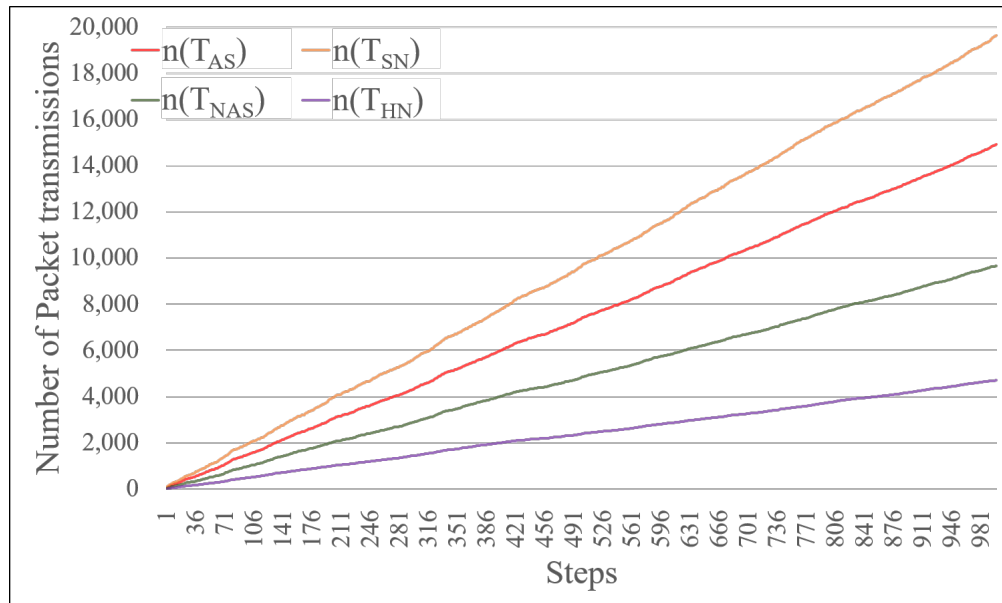


Figure 6. Number of packets generated by the proposed secondary authentication framework.

Traffic in the UE area and serving network are considered as the traffic of client-side and affect the user experience. On the other hand, traffic in the NAS area and home network, considered as server-side traffic, affects the risk and possibility of NAS signaling storm. To concentrate on the point of NAS signaling storm and user experience, we calculated the amount of traffic in the AS and NAS domain. Figure 7 shows the number of packets generated in the AS domain ($n(T_{AS}) + n(T_{SN})$). The result of the original scheme generated 30,742 packets for the communication of the AS and SN domain, while the proposed framework generated 34,555 packets. This result shows that the proposed framework generated 12.4% more packets in the AS and SN communication.

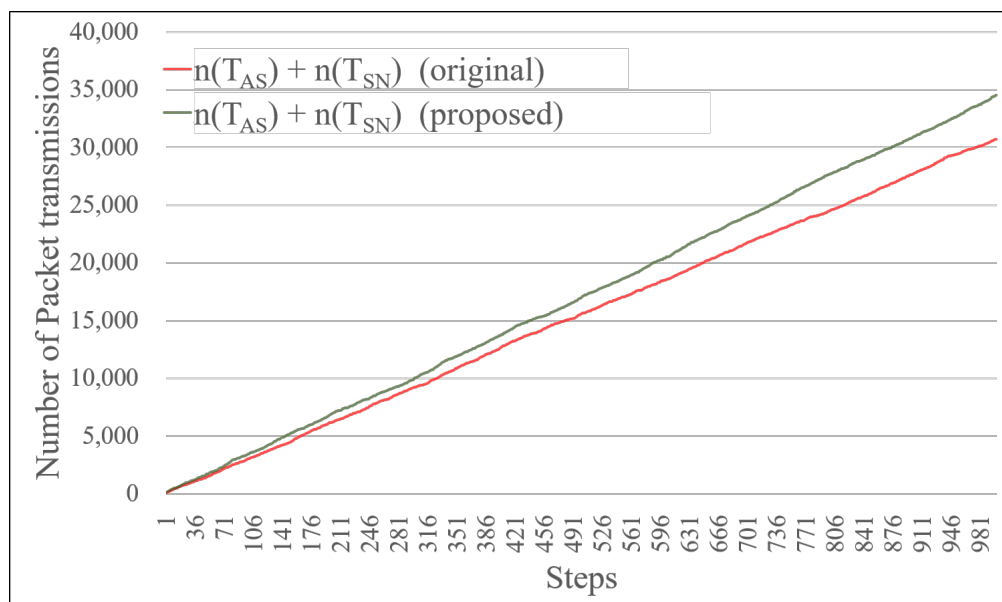


Figure 7. Number of packets transmitted in the access stratum (AS) domain.

On the other hand, Figure 8 shows the amount of traffic generated in the NAS and HN domain ($n(T_{NAS}) + n(T_{HN})$). As a result of the simulation with 1000 steps, the original scheme generated 23,732 packets, while our proposed framework generated 14,377 packets. This figure shows that the proposed framework that includes SAF and ADME, and reduces 39.42% of traffic in the NAS

and HN domain, mitigating the threat of NAS signaling storm. Also, Figure 9 shows the number of total packets generated in the whole secondary authentication process on each scheme. The original scheme generated 54,474 packets, while our proposed scheme generated 48,932 packets. Our proposed model reduced the total number of packets by 10.17%.

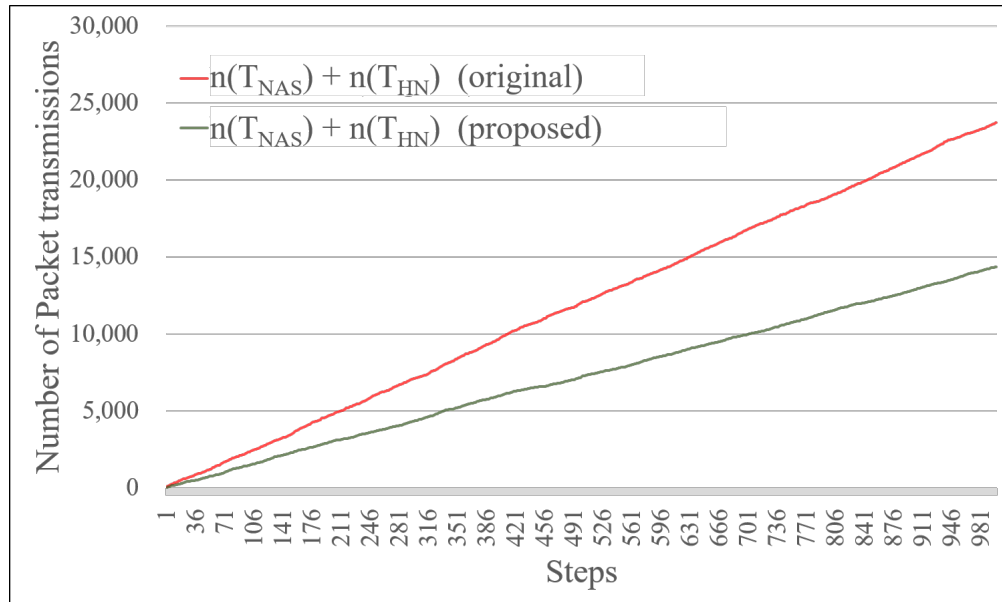


Figure 8. Number of packets transmitted in the Non-Access Stratum (NAS) domain.

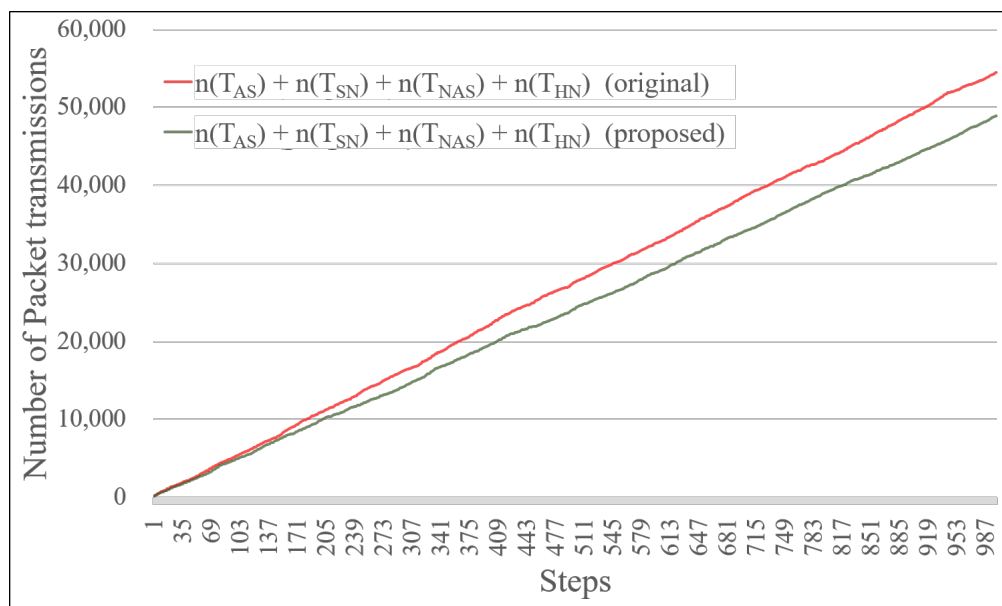


Figure 9. Number of total packets generated in each scheme.

Our simulation results show that the proposed framework generates about 12.4% more traffics in the AS and SN domain, which is related to the availability of users. However, the impact of traffic on the AS and SN domain could be alleviated through well-deployed medium nodes of the edge layer. Thus, the impacts on the user's availability could be considered as a minor problem. In contrast, the proposed framework dramatically reduced the amount of traffic in NAS and HN domain by 39.42%. This result can significantly mitigate the risk of the NAS signaling storm. Also, the proposed framework curtailed the overall traffics by 10.17%. Consequentially, the proposed framework can improve the availability and stability of the 5G network.

6. Conclusions

The proposed framework proposed a mutual authentication scheme based on the mobile edge computing network architecture. SAF and ADMF nodes, which are the core components of the proposed framework, are implemented in the form of network functions and relay the authentication mechanism as an intermediate of the mutual authentication process between the UE and DN-AAA. This approach could alleviate the risk of the NAS signaling storm that could be increased when the complexity of the network expanded. SAF and ADMF proposed in this research solve the signaling storm problem by performing mutual authentication for UE in the area of serving network. Based on the layered network architecture using edge and fog computing, the proposed model provide the ability to manage the availability, flexibility, auditability of the network. Also, as operating SAF and ADMF as a nodes of trusted third parties, our framework can guarantee independence of authentication authority. In the experiment, we provided the evaluation of the framework in terms of risk on NAS signaling storm and user's availability on the network. We simulated the result of the 5G authentication environment, and our result shows that the proposed framework can reduce the risk of NAS signaling storm by 39%, and the overall network traffic by 10%. In future research, we will study the model of network function that can detect an abnormality and abnormal behavior of network from the perspective of the security architecture to expand the coverage of security in the 5G network structure.

Author Contributions: S.G. and A.E.A. conceived of the presented idea. S.G., A.E.A. designed the proposed framework, performed the security analysis. S.G., A.E.A., J.C. discussed the related works, drafted the manuscript. S.G. conducted simulation and security analysis. J.H.P. supervised the research. All authors discussed the results and contributed to the final manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This study was supported by the Advanced Research Project funded by the SeoulTech(Seoul National University of Science and Technology).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lawton, G. Developing software online with platform-as-a-service technology. *Computer* **2008**, *41*, 13–15. [[CrossRef](#)]
2. Liu, S. *Cloud Computing—Statistics & Facts*; Statista: Hamburg, Germany, 2019.
3. Chen, S.; Zhao, J. The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication. *IEEE Commun. Mag.* **2014**, *52*, 36–43. [[CrossRef](#)]
4. Dillon, T.; Wu, C.; Chang, E. Cloud computing: Issues and challenges. In Proceedings of the 2010 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, Australia, 20–23 April 2010; pp. 27–33.
5. Ferrag, M.A.; Maglaras, L.; Argyriou, A.; Kosmanos, D.; Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. *J. Netw. Comput. Appl.* **2018**, *101*, 55–82. [[CrossRef](#)]
6. Chao, H.C.; Cho, H.H.; Shih, T.K.; Chen, C.Y. Bacteria-Inspired Network for 5G Mobile Communication. *IEEE Netw.* **2019**, *33*, 138–145. [[CrossRef](#)]
7. Patil, S.; Patil, V.; Bhat, P. A review on 5G technology. *Int. J. Eng. Innov. Technol. (IJEIT)* **2012**, *1*, 26–30.
8. Basin, D.; Dreier, J.; Hirschi, L.; Radomirovic, S.; Sasse, R.; Stettler, V. A formal analysis of 5G authentication. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 1383–1396.
9. Daoud, W.B.; Obaidat, M.S.; Meddeb-Makhlouf, A.; Zarai, F.; Hsiao, K.F. TACRM: Trust access control and resource management mechanism in fog computing. *Hum. Centric Comput. Inf. Sci.* **2019**, *9*, 28. [[CrossRef](#)]
10. Muruganathan, S.D.; Lin, X.; Maattanen, H.L.; Zou, Z.; Hapsari, W.A.; Yasukawa, S. An overview of 3GPP release-15 study on enhanced LTE support for connected drones. *arXiv* **2018**, arXiv:1805.00826.

11. Dolui, K.; Datta, S.K. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In Proceedings of the 2017 Global Internet of Things Summit (GloTS), Geneva, Switzerland, 6–9 June 2017; pp. 1–6.
12. Sabella, D.; Moustafa, H.; Kuure, P.; Kekki, S.; Zhou, Z.; Li, A.; Thein, C.; Fischer, E.; Vukovic, I.; Cardillo, J.; et al. *Toward Fully Connected Vehicles: Edge Computing for Advanced Automotive Communications*; White Paper; 5G Automotive Association: Munich, Germany, 2017.
13. Zhang, K.; Mao, Y.; Leng, S.; Zhao, Q.; Li, L.; Peng, X.; Pan, L.; Maharjan, S.; Zhang, Y. Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks. *IEEE Access* **2016**, *4*, 5896–5907. [\[CrossRef\]](#)
14. Asrar Baktayan, M.A.; Alhomdy, S. Fog Computing for Network Slicing in 5G Networks: An Overview. *J. Telecommun. Syst. Manag.* **2018**. [\[CrossRef\]](#)
15. Chaudhary, R.; Kumar, N.; Zeadally, S. Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges. *IEEE Commun. Mag.* **2017**, *55*, 114–122. [\[CrossRef\]](#)
16. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and Beyond. *IEEE Commun. Surv. Tutor.* **2019**. [\[CrossRef\]](#)
17. Agiwal, M.; Roy, A.; Saxena, N. Next generation 5G wireless networks: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [\[CrossRef\]](#)
18. Rost, P.; Mannweiler, C.; Michalopoulos, D.S.; Sartori, C.; Sciancalepore, V.; Sastry, N.; Holland, O.; Tayade, S.; Han, B.; Bega, D.; et al. Network slicing to enable scalability and flexibility in 5G mobile networks. *IEEE Commun. Mag.* **2017**, *55*, 72–79. [\[CrossRef\]](#)
19. Aijaz, A. Packet duplication in dual connectivity enabled 5g wireless networks: Overview and challenges. *arXiv* **2018**, arXiv:1804.01058.
20. Zhang, S.; Wang, Y.; Zhou, W. Towards secure 5G networks: A Survey. *Comput. Netw.* **2019**, *162*, 106871. [\[CrossRef\]](#)
21. Yang, N.; Wang, L.; Geraci, G.; El Kashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [\[CrossRef\]](#)
22. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G security challenges and solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [\[CrossRef\]](#)
23. Xiao, L.; Wan, X.; Dai, C.; Du, X.; Chen, X.; Guizani, M. Security in mobile edge caching with reinforcement learning. *IEEE Wirel. Commun.* **2018**, *25*, 116–122. [\[CrossRef\]](#)
24. Han, B.; Wong, S.; Mannweiler, C.; Crippa, M.R.; Schotten, H.D. Context-Awareness Enhances 5G Multi-Access Edge Computing Reliability. *IEEE Access* **2019**, *7*, 21290–21299. [\[CrossRef\]](#)
25. Xia, X.; Xu, K.; Wang, Y.; Xu, Y. A 5G-enabling technology: Benefits, feasibility, and limitations of in-band full-duplex mMIMO. *IEEE Veh. Technol. Mag.* **2018**, *13*, 81–90. [\[CrossRef\]](#)
26. Ni, J.; Lin, X.; Shen, X.S. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 644–657. [\[CrossRef\]](#)
27. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V. Design of secure key management and user authentication scheme for fog computing services. *Future Gener. Comput. Syst.* **2019**, *91*, 475–492. [\[CrossRef\]](#)
28. Hsu, R.H.; Lee, J.; Quek, T.Q.; Chen, J.C. Reconfigurable security: Edge-computing-based framework for IoT. *IEEE Netw.* **2018**, *32*, 92–99. [\[CrossRef\]](#)
29. Parvez, I.; Rahmati, A.; Guvenc, I.; Sarwat, A.I.; Dai, H. A survey on low latency towards 5G: RAN, core network and caching solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3098–3130. [\[CrossRef\]](#)
30. European Telecommunications Standards Institute. *5G: Security Architecture and Procedures for 5G System (3GPP TS 33.501 Version 15.2.0 Release 15)*; ETSI: Sophia Antipolis, France, 2018.

