Cross-Network-Slice Authentication Scheme for the 5^{th} Generation Mobile Communication System

Chun-I Fan, Yu-Tse Shih, Jheng-Jia Huang, and Wan-Ru Chiu

Abstract—**The fifth-generation mobile network (5G) integrates various application services in a heterogeneous network environment. Compared to the traditional networks, 5G is not just an extension of the 4th generation, which contains three important properties, enhanced mobile broadband (eMBB), massive machine type communications (mMTC), and ultra-reliable and low latency communications (URLLC). 5G applies the functionalities of Network Function Virtualization and Software-Defined Networking to support multiple services and proposes a new concept called Network Slicing. Users can access different services quickly in the 5G network supported by network slicing. In a traditional network like 4G, if a user wants to access different services, it will be necessary to perform different authentication procedures that cause additional burden and operation cost in the user's device. However, the 5G network inherits the previous network architecture. Hence, the user's device still needs to be authenticated by the core network. Besides, providing a guarantee of connecting to a correct network slice is one of the prime concerns. The paper presents an authentication scheme tailored for the 5G network. In the proposed scheme, the authentication is decentralized to the edge clouds to achieve low latency. Moreover, the authentication flow is no longer attached to the operator all the time to reduce time latency. The proposed scheme is secure against the attackers who aim to impersonate users, network operators, or even network slices, and it also provides secure session key exchange. Empirical performance assessment in terms of its functionalities gains better acceptability of the proposed scheme than other existing ones.**

Index Terms—**Authentication, 5G, network slicing, edge computing, low latency.**

Manuscript received May 13, 2020; revised October 25, 2020 and December 20, 2020; accepted December 29, 2020. Date of publication January 18, 2021; date of current version March 11, 2021. This work was partially supported by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU) and the Ministry of Science and Technology of Taiwan under grants MOST 109-2221-E-110-044-MY2, MOST 110-2923-E-110-001-MY3, MOST 109-2222-E-011-007-MY2, and MOST 109-2218-E-492-009. It also was financially supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan. The associate editor coordinating the review of this article and approving it for publication was B. Martini. *(Corresponding author: Jheng-Jia Huang.)*

Chun-I Fan is with the Department of Computer Science and Engineering and the Information Security Research Center, National Sun Yat-sen University, Kaohsiung 804, Taiwan, and also with the Intelligent Electronic Commerce Research Center, National Sun Yat-sen University, Kaohsiung 804, Taiwan (e-mail: cifan@mail.cse.nsysu.edu.tw).

Yu-Tse Shih and Wan-Ru Chiu are with the Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung 804, Taiwan (e-mail: d073040005@student.nsysu.edu.tw; sdspscindy@gmail.com).

Jheng-Jia Huang is with the Department of Information Management, National Taiwan University of Science and Technology, Taipei 106335, Taiwan (e-mail: jhengjia.huang@gmail.com).

Digital Object Identifier 10.1109/TNSM.2021.3052208

I. Introduction

The FIFTH-GENERATION mobile network (5G) inherits the functionalities of network function virtualization (NFV) and software-defined networking (SDN), and it enables multiple services through the network slicing with distinctive characteristics. However, providing a guarantee of connecting to a correct network slice is one of the prime concerns. This research aims to present a novel authentication technique tailored for 5G that satisfies the third-generation partnership project (3GPP). According to the IMT-2020 project proposed by the International Telecommunication Union Radiocommunication Sector (ITU-R) [1], the 5G standard was published in 2020, and the new system of 5G is commercialized to demonstrate diversified services such as enhanced mobile broadband, ultra-high reliability, and low latency applications, massive Internet of Things (IoT), etc. Fig. 1 depicts the scopes and requirements of the 5G network as defined by ITU-R [1]. In the 5G network, Enhanced Mobile Broadband provides high speed while Ultra-Reliable Low-Latency Communication guarantees extremely-low latency, and Massive Machine Type Communication assists lots of devices to connect each other.

Based on the 5G Concept white paper published by IMT-2020 (5G) Promotion Group in Feb, 2015 [2], the 5G technology development was broadly divided into four parts:

1) *Seamless Wide-Area Coverage:* It provides a better user experience with a data rate of over 100Mbps. Users can also experience high coverage of the 5G network in high-speed mobile environments and border areas.
2) *High-Capacity Hot Spots:* It supports high-capacity hot spots and high-traffic services. The challenge of this scenario is to give users 1 Gbps user experienced data rate, tens of Gbps peak data rate, and tens of Tbps/km^2 traffic volume density.
3) *Low-Power Massive-Connections:* The main applications of the 5G are smart cities, smart health care systems, environmental monitoring, and even prevention of forest fires. These application scenarios have some common characteristics, such as large numbers of packets transmission, numerous devices, and a wide range of areas. To support these applications, 5G must achieve the 10^6 /km^2 connection density with low power consumption and low cost.
4) *Low-Latency With High-Reliability:* Driverless and industrial control are two of the most critical applications in this scenario. It must guarantee that the minimum latency can support data transfer delays below

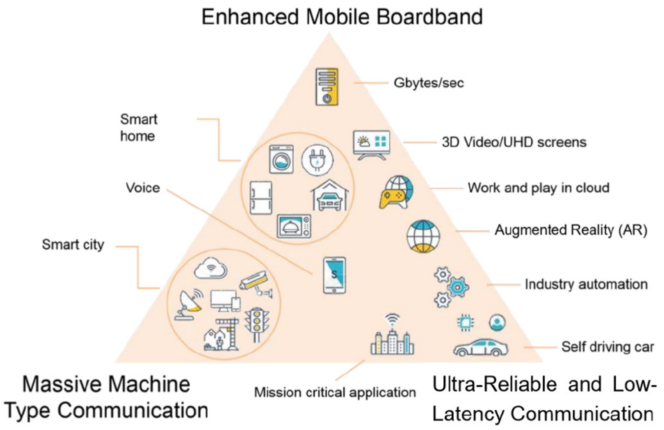

Fig. 1. 5G Scenarios.

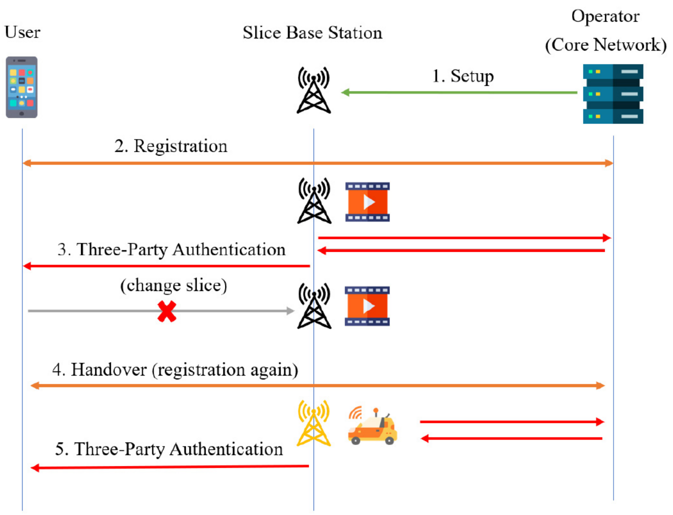
User
Slice Base Station
Operator (Core Network)
1. Setup
2. Registration
3. Three-Party Authentication
(change slice)
4. Handover (registration again)
5. Three-Party Authentication

Fig. 2. Slice Crossing in the 5G Network.

one-thousandth of a second and maintain high reliability to ensure application security.

With the aforementioned four properties, the 5G network environment requires high-speed data rates while providing various services to different devices and users. It is not just the pursuit of high speed as it used to be. Given the diversity of services and the balance of network speeds, the traditional network architectures cannot meet the 5G requirements. Therefore, 5G has proposed a new type of network architecture called network slicing. In the traditional network environment, no matter the core network (CN) or the radio access network (RAN) has a dedicated hardware device to provide services, a set of devices only corresponds to a single service. It would easily cause that any minor adjustments may lead to an overall service suspension, inefficiency, and huge hardware cost. Since 5G communication requires a lot of network access, the concept of network slicing is introduced to divide a physical network into multiple virtual networks, where each virtual network can flexibly correspond to different services. Therefore, it is no longer necessary to map each service to a dedicated network environment when deploying, which significantly reduces network hardware costs.

According to the consumers' demands, network slicing can be adjusted without suspending the overall service's operation. Specifically, 5G adopts NFV and SDN to implement the functionalities of network slicing. Specifically, it virtualizes the network functions through the NFV technology, and then utilizes the SDN technology to control the flow of packets uniformly. Thus, a single network function no longer requires support from a single hardware device, which can reduce the cost of telecommunication operators. Since the SDN technology is used as a packet flow control system, all service network packets can be managed in a unified manner and integrated into a complete 5G network. With the cooperation of NFV, SDN, and cloud computing, the 5G communication provides a highly flexible network. The traditional vertical network can be divided into many pieces, each of which is independent and does not interfere with each other. The operator can impose virtual network services that satisfy the customers' requirements.

Fig. 2 shows the 5G network environment, where different network slices and infrastructures provide different services. Therefore, a user's device will be required to be authenticated by the core network each time the user wants to access another network slice. In the proposed scheme, we aim to reduce the authentication cost when a device crosses network slices. If the user wants to access a different slice, he needs to be authenticated by the slice rather than the core network to achieve fast handover. Thus, we can reduce the time latency and communication cost between the slice base station and the core network.

Besides, for security concerns, the framework of security authentication must be innovated. In the past generations, the authentication framework only certified one service at a time. For a new type of network containing a large number of access networks and supporting large numbers of services, the traditional network authentication framework is inefficient and costly. According to the security white paper "Security challenges and opportunities for 5G mobile networks" [3] released by NOKIA in 2017, and "5G SECURITY: SCENARIOS AND SOLUTIONS" [4] released by Ericsson in 2015, the 5G security authentication framework needs to consider the following aspects:

1) *Multiple access networks (heterogeneous networks)*
2) *Fast service switching (network slicing)*
3) *Fast authentication*
4) *Reduction of the computation cost of the operator*

Since the appearance of heterogeneous networks and network slicing, the network society becomes more complicated than before, so we need a mechanism for rapid authentication and computation to support a diverse network society. In addition to the support of rapid authentication, reducing the computation cost is also an essential topic in these white papers. The security white paper also mentions the attacks that 5G systems may suffer from. For example, hackers may launch DDOS attacks on a large number of IoT devices. Compared with traditional single-user devices, 5G networks face this threat more seriously than before. Not only are the technical attacks increasing, but also there are more social engineering attacks. Therefore, we must design the 5G systems very carefully and automate them as much as possible to reduce manual management and build a secure network environment.

In addition to the white papers, 3GPP explicitly defined the network slice architecture in the TS 23.501 [5] standard. For example, in Network Slice Selection Assistance Information (NSSAI), each slice Single-Network Slice Selection Assistance Information (S-NSSAI) has its Slice/Service Type (SST) and the Slice Differentiator (SD). The NSSAI is a collection of max eight S-NSSAIs (that is, each user can access at most eight services) and so on. Through the above white papers or standards, we can learn that switching between slices in a secure way is urgently required. Therefore, designing a fast and light-weight authentication for the 5G network environment is a crucial goal for 3GPP and the operators.

A. Contribution

Devices are able to support diverse wireless communication systems now, which are also known as heterogeneous networks, but the current authentication mechanisms do not address adequate strategies for heterogeneous networks. In tradition, there is a corresponding authentication framework for an access network. However, there is no complete cross-network-slice authentication framework in the traditional architecture, also in the 5G study. Only the need of integrating heterogeneous network authentication was proposed, but no corresponding solution has been put forward. It is still an open problem to provide a cross-slice authentication. Therefore, in this article, we will design a fast authentication mechanism tailored for the 5G network environment. Through this mechanism, we integrate the access authentication of heterogeneous networks. Due to the integration of the heterogeneous networks, it is unnecessary to spend a lot of time repeatedly running the authentication process, and we can achieve low-latency with high-reliability mechanism in 5G.

B. Organiazation

In Section II, we review some backgrounds of knowledge, including the 5G environment and the 3GPP standard TS 33.501. In Section III, we briefly review an authentication scheme and give some comments on the scheme. In Section IV, we describe the proposed authentication scheme in the 5G environment. We provide the security analysis of the proposed scheme in Section V. The comparisons are presented in Section VI and a concluding remark is given in Section VII.

II. Preliminaries

In this section, we will briefly introduce some 3GPP standards and technologies related to our work.

A. IMT Vision–Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond [1]

The social and economic evolution of the past few decades is an essential driving factor for the evolution of mobile communications, which has promoted the economic and social development of developed and developing countries. Mobile communication has been closely integrated into the daily life of the entire society. It is expected that social technology trends and the evolution of mobile communication systems will remain tightly coupled and become the foundation of the society. However, it is expected that in the future new requirements, such as more traffic, more devices, and different service requirements, a better quality of the user experience (QoE) and better affordability to further reduce costs will require more and more innovative solutions. The goal of this recommendation [1] is to define IMT's vision, describe potential users and application trends, traffic growth, technology trends, and spectrum impact, and provide guidelines for the IMT framework and capabilities in the future.

B. 5G Network Environments

The 5G network has stretched much of flexibility due to the concept of network slicing comparing with traditional networks. The 5G networks not only enhance broadband but also connect the whole smart devices to construct the mMTC property. Moreover, it provides ultra-low latency and high reliability network transmission in this environment. Furthermore, the original access network and core network must be adjusted according to the target: the connection of many Internet of Things devices, low-latency, high-reliability network transmission, and the realization of speed in a high-speed transmission environment. Therefore, whether it is base station deployment or network data packet transmission, 5G networks are entirely different from traditional networks.

In a traditional mobile network, all user devices attached with an access network are further connected to the core network. The data computation units are unified in the core network. However, this method may increase latency unnecessarily. In order to address the aforementioned aspect and to satisfy the diversified services of 5G, the core network and the access network partially utilize the concept of center cloud and edge cloud. The edge cloud is the collective name for the access network and a small part of the core network. In order to easily connect to the base station, the edge cloud is being set up near to the base station. Therefore, the functionalities of the original core network are moved with low latency to the edge cloud. Hence, the consumer needs to connect its nearby base station to avail the permissible network computing and storage features. Center cloud is a small part of the core network. If the number of service requests are high enough, such as the mMTC scenario, the data are still processed in the center cloud just as a traditional network.

As a result, the latency of the package switching can be greatly reduced. Fig. 3 shows the different service slices with different functionalities deployed between the center cloud and the edge cloud. The eMBB service has a great demand for bandwidth, so the user plane of the core network and the cache memory can be placed in an edge cloud which is closer to the user. Thus, it can increase the user's favorability to the service. URLLC service is designed for automatic driving and remote management. It is more demanding for the latency related to the package switching. To achieve the goal,

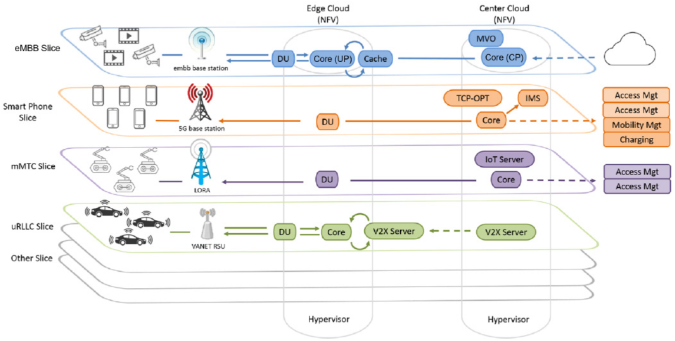

Fig. 3. 5G Network Environments.

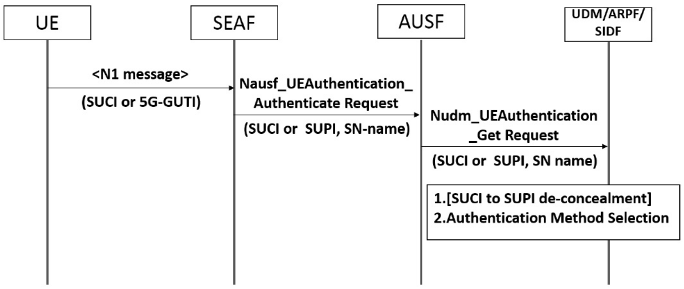

Fig. 4. A TS 33.501 Flow.

the core network and the corresponding server (such as V2X Server) are moved to the edge cloud to reduce the data transmission time. Through the collocation between the edge cloud and the center cloud, the edge cloud can separate and distribute the complexity of the calculation to the center cloud. Due to the power of partial calculations is decentralized to the edge cloud, the demand for low-latency service can be easily achieved.

C. Technical Specification 33.501

A unique International Mobile Subscription Identity (IMSI) [6] shall be allocated to each mobile subscriber in the GSM/UMTS/EPS system. In the traditional 2G, 3G, and even 4G network environments, the problem of leaking private locations of mobile phones, the so-called IMSI Catcher, has not been properly solved. Due to the considerations of network functionality, cost, and security, this issue is a significant concern whenever a new generation of communication network standards is formulated. According to TS 33.501 [7] published by 3GPP in 2018, the 5G IMSI security standard has been clearly defined. In 5G, the true identity of a mobile phone is called SUbscription Permanent Identifier (SUPI), which is similar to IMSI, and the ciphertext encrypted by the public key is called SUbscription Concealed Identifier (SUCI). In 4G, the IMSI is sent in cleartext from the UE to the network. To solve this problem, 5G conceals the SUPI by encrypting it.

According to TS 33.501, 5G introduces a public/private key system. The operator stores its public key in the secure element of a UE and keeps the private key by itself. Besides, the UE will encrypt the SUPI with the operator's public key, and it does not send its identity in a cleartext. In this way, only the carrier can decrypt the real identity information of the mobile phone. Attackers can only obtain the encrypted information and cannot catch the IMSI without the private key. After the SUCI is transmitted to the base station, the base station directly forwards it to the core network. Fig. 4 shows the transmission flow of the device identity from the user side to the core network in TS 33.501.

In the 5G core network, NFV virtualizes the original core network into many functions with different features one another. However, in the paper, we will not go into details about the functions and the operating mode between functions. We refer to the core network functions in TS 33.501 as "core network." A mobile device initiates a transmission flow by sending a request to the base station gNB for accessing the network and transmitting SUCI (i.e., encrypted SUPI) or Globally Unique Temporary UE Identity (GUTI). After receiving the information, the base station gNB forwards the information to the core network. The core network receives the message and judges if it is a GUTI or SUCI. If the message is a GUTI, it matches the corresponding SUPI and then the network service information (SN-Name) corresponding to the carried process in the core network will be analyzed to determine whether the mobile phone is within the service range of the network or not. After confirming the above information, the core network will decrypt SUCI to obtain SUPI and configure the corresponding authentication procedure for mobile phones through SUPI.

We know that encrypting SUPI and decrypting SUCI are a major issue for mobile phone identity verification during the authentication and transmission process. Based on elliptic curve cryptography (ECC), there are two pairs of keys. One is the pair of the terminal side ephemeral (Eph.) public key and private key, where both of the keys are generated by Eph.key pair generation. The other pair comes from the home network. The user has the public key of the home network stored in the SIM card.

D. Slice Specific Authentication and Access Control for 5G [8]

In 2020, Behrad [8] pointed out that each network slice can be dedicated to a third party. Moreover, they proposed a 5G slice-specific authentication and access control mechanism. On the other hand, the Mobile Network Operator (MNO) is not responsible for Authentication and Access Control (AAC) of all devices in the network, which decreases the signalling load on the operator's network. The architecture of the AAC mechanisms consists of an AC server and AC clients. When an AC client wants to access the network, the AC client needs to send queries to the AC server to process the authentication protocol.

When a device needs to be authenticated by the network slice service, the device will perform the authentication protocol based on the AAC information provided from the network slice service. This information includes the slice ID of the third party and the device identifier. These identifiers may be distinct from the globally unique identifiers used in the current cellular systems and the 3GPP specifications (IMSI and SUPI). According to the AAC mechanism selected by the third party, the information provided to the devices may contain some security credentials. It determines the format of the subscription identifiers, and they do not need to be specific to 5G.

E. Some Related Authentication Schemes in LTE-A

In 2019, Panda and Chattopadhyay proposed an improved authentication and security scheme for LTE/LTE-A networks [9]. It adopted elliptic curve encryption (ECC), elliptic curve Diffie-Hellman (ECDH) and Salsa20 algorithms to improve end-to-end security and provide faster data transmission for 4G environments. The scheme [9] used a variety of robust encryption techniques while providing proper mutual authentication between the user equipment (UE) and the message management entity (MME).

In 2019, Ma *et al.* proposed a privacy-preserving secure handover authentication scheme [10] in LTE-A networks. They proposed a secure handover identity verification scheme based on a certificateless symbol encryption technology. Their solution can realize a secure and unified handover procedure without sacrificing efficiency. Security and performance measurement show that their scheme can satisfy various security properties, including perfect forward/backward confidentiality and privacy protection. At the same time, their solution achieves the desired efficiency.

In 2019, Zhou *et al.* proposed a hybrid authentication protocol for LTE/LTE-A network [11]. They discussed the main weaknesses of the Long Term Evolution (LTE) authentication process and proposed a new method, the Hybrid Evolutionary Packet System (HEPS) protocol to solve the vulnerability. Their protocol has been logically verified, using the Burbu-Abadi-Needum (BAN) logic. The HEPS agreement will optimize the performance of the LTE authentication process and fundamentally cope with the security problems of the process.

In 2019, Parne *et al.* proposed a Performance and Security Enhancement (PSE-AKA) protocol for LTE/LTE-A networks [12]. It supports Internet of Things and the proposed protocol follows the cocktail therapy, generates an authentication carrier, and improves performance in terms of computing and communication overhead. The agreement protects the privacy of the object, protects KSI, and avoids identification attacks on the communication network. It used the BAN logic and the AVISPA tools to perform verification and security analysis on the proposed protocol, respectively. Security analysis demonstrates that the protocol meets the security goals and can resist various known attacks.

F. A Formal Analysis of 5G Authentication

The mobile communication network connects most of the world's population. For the 5G network, the 3GPP group has standardized the 5G AKA protocol for the purpose. The protocol provides the first comprehensive official model from the AKA series of agreements: 5G AKA. It also extracts precise requirements from the 3GPP standards that define 5G and identify missing security goals. Using Tamarin, a security protocol verification tool, they conducted a comprehensive, systematic, and security assessment of the 5G security target model. This work [13] gave a formal analysis of 5G authentication and the first formal model of the 5G AKA protocol. Moreover, it identified the assumptions required for each security goal and pointed out some critical security goals missing from the 3GPP standards.

G. An Overview of the 3GPP 5G Security Standard

In 2019, this work [14] was posted on the website. It shows an overview of the 3GPP 5G security standard, including the authentication framework, subscriber privacy, service-based architecture and interconnection security, and user plane protection. LTE/4G and 5G have many similar functions. In these two systems, security mechanisms can be divided into two groups. The first group contains all of the network access security mechanisms. These are security functions which provide users with secure access to services via devices (usually phones), and can prevent attacks on the air interface between the device of a user and the radio node (eNB in LTE or gNB in 5G). This includes functions that enable nodes to exchange signaling data and user data safely, such as between radio nodes and core network nodes.

III. Related Works

The 3GPP did not specify how to perform authentication when a device needs to access another network slice. The straightforward method is to authenticate the device by the core network again. Our proposed scheme can speed up the authentication by authenticating the device in the slice side. Comparing to 5G-AKA and EAP-AKA, the device does not need to be authenticated by the core network in the proposed scheme in the above situation. After we surveyed the 5G network slice authentication schemes, the concept of Ni *et al.*'s scheme [15] is more suitable for our scheme.

Based on the framework of the 3GPP TS 23.501 System Architecture [5] for the 5G System, Ni *et al.* proposed an efficient service-oriented authentication protocol, but we found a disadvantage. The scheme performs the same identity verification process for each slice base station, but the scheme does not consider the situation where different slices may have different infrastructures and specifications. The operator can find the slices which a user can access without knowing the slice/service type (SST) and SD of each slice, and the user can anonymously access the slice services. Hence, the scheme can protect the information included in each slice. Nevertheless, the scheme ignores the different services which are provided by each slice. For the service with less latency, the computing unit should be decentralized to the edge cloud. Therefore, we do not recommend that a service should be authenticated in the center cloud since it will increase the latency.

There have been several schemes proposed in recent years; hence we analyze these works that are similar to our proposed scheme. In the following subsections, we briefly introduce some related works.

A. Authentication and Access Control for 5G [16]

In 2020, Behrad *et al.* proposed a work called "Authentication and Access Control for 5G" [16]. They showed some surveys

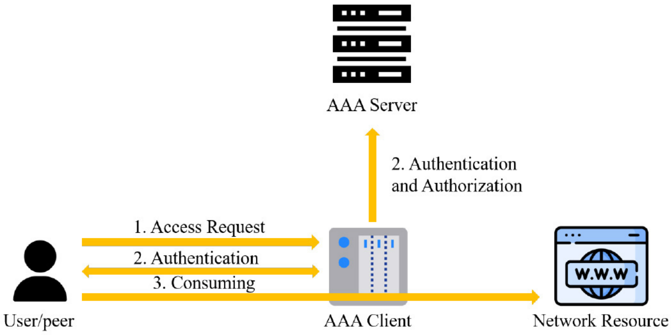

Fig. 5. Functions of an AAC System from [17].

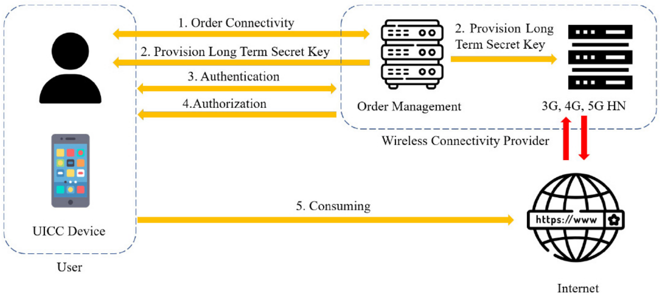

Fig. 6. An AAC Model in the Cellular Networks.

on the network architecture, AKA protocol, access control, specific use cases, and requirements of 5G.

1) Basics of Authentication and Access Control: The main purposes of Authentication and Access Control (AAC) are to protect user privacy and network security. Fig. 5 shows the flow of an AAC system.

2) Overall Architecture of the AAC in 3G, 4G, and 5G: From the perspective of AAC, cellular networks (such as 3G, 4G, and 5G) are composed of three main parts: ES (user equipment) or equipment, SN (service network), and HN (home network). HN is the network to which UEs subscribe. The service network is the ES service network changing the network in the roaming plan. SN is an AC client and HN is the AC server. Fig. 6 illustrates the AAC model in a cellular network.

3) Authentication and Access Control in 5G: The 5G architecture provides some new design options for authentication and access control, but it also brings many continuities. The most essential continuity involves symmetric key-based authentication through security elements. In TS 33.501 of the 5G specification, secure elements in UEs or devices (such as UICC in 4G and 3G, and SIM card in 2G) were kept to handle subscription authentication and process subscription credentials [7]. This credential can also be an ESIM (Embedded User Identity Module) provided by the device makers. The operator can provide its profile through the air when subscribing. The authentication methods introduced in the 5G specification are 5G-AKA, EAP+AKA and EAP+TLS (Transport Layer Security).

4) 5G-AKA Protocol: Without losing versatility, the protocol focused on the 5G-AKA agreement (and its differences with the EPS + AKA agreement) because it is the main authentication and key agreement that meets the AAC requirements in 5G. The authentication mechanism in the 5G system will follow the same principles with some subtle differences in the 4G system. These differences in the AKA mechanism will only be from the network perspective, not from the UE perspective. The AKA mechanism in the 5G system (such as the mechanism in the 4G system) takes the "service network name" (such as the SNid in 4G) to derive the anchor key (KSEAF); therefore, the anchor key will belong to a specific service network, and this service network cannot pretend to be another service network. Unlike EPS+AKA, there are four participants in 5G-AKA, and this section will further explain these participants. Another difference in the AKA mechanism of the 5G system is that the anchor key (KSEAF) derived in 3GPP access also is able to be used for non-3GPP access without a new authentication process. The authentication process will involve the UE in the service network, the security anchor function, the AUSF in HN, and the UDM/ARPF (Authentication Repository and Processing Function) in HN [18]. SEAF will be included in AMF and interact with AUSF in order to obtain authentication data from UDM. It completes the UE authentication of different access networks. ARPF stores subscriber profiles and security-related information. It also selects the authentication method (such as 5G-AKA, EAP + AKA, EAP + TLS) according to the identity of the subscriber, and calculates the key material of AUSF. The call flow of 5G-AKA is as follows [19].

(1) Initially, the UE transmits its SUCI to SEAF.

(2) After receiving the signaling message from the UE, SEAF will send a 5G-AIR (Authentication Initiation Request) message to AUSF. 5G-AIR includes the UE's SUCI or SUPI and the name of the service network. This message also shows that the UE is using a 3GPP access or non-3GPP access.

(3) After verifying the authorization of the service network requesting the authentication service, AUSF will send an AIR message to UDM/ARPF. If AUSF sends SUCI in this message, the SIDF (Subscription ID De-hiding Function) parallel to UDM/ARPF will decrypt SUCI to obtain SUPI. After receiving a request for authentication information from AUSF, UDM/ARPF will generate AVs (as in 4G), and then convert them into new AVs specific to 5G systems. Depending on the selected authentication method, this conversion will vary.

(4) UDM/ARPF sends the AV containing AUTN, XRES*, KASUF, and SUPI to AUSF in the authentication information response message. When receiving this message, AUSF calculates HXRES*, which is the hash value of XRES*, and stores KAUSF.

(5) AUSF sends 5G-AIA (Identity Verification Information Acceptance) (including HXRES*) to SEAF. This message does not include SUPI. AUSF (in the home network) only sends SUPI to SEAF (in the service network) after successful UE authentication.

(6) After storing HXRES*, SEAF transmits the AUTN token in the authentication request message to the UE. The UE verifies the validity of AUTN (by using the key shared with HN). If AUTN is valid, the network

identity verification in the UE is successful. If AUTN is invalid, the UE will send a MAC failure message (message authentication code) to SEAF. Next, as in the ESP+AKA process, the UE verifies the sequence number (SQN) derived from AUTN to control the freshness of AUTN. If this verification fails, the UE will send a synchronization failure message to SEAF. The UE also calculates RES*.

(7) The UE transmits RES* to SEAF in the authentication response message. SEAF verifies the validity of RES* by calculating HRES* and comparing it with HXRES*.

(8) In order to make the final decision about UE authentication through the home network, SEAF sends 5G-AC (identity verification confirmation) messages (including RES*) to AUSF. AUSF verifies the validity of RES* by comparing it with XRES*. Sending 5G-AC messages from SN to HN is to prevent possible billing cheating proposed by SN [20].

5) *New Concepts in 5G:* These different goals and use cases have an important impact on the security of the system. When designing appropriate authentication and access control mechanisms for 5G networks (such as fast communication requiring fast AAC processes), service-specific security requirements should be considered [21]. Another example is that in IoT, many devices may access the network at the same time, so the network should be able to control the large amount of signaling traffic and correctly authenticate the devices to withstand the DDoS (distributed denial of service) attacks. IoT devices have low power consumption and cannot support the strong authentication process. In addition, they are usually able to connect to the network through the authentication and access control of the 5G non-3GPP access options (some of these options will not have 5G radio accesses and will use Wi-Fi or Bluetooth) [22]. In view of these limitations, some IoT gateway solutions based on group-based authentication were proposed to reduce the number of complete AKA process executions [23], [24]. But these group-based AKA solutions also have their own weaknesses. Some of these include the traditional AKA weaknesses mentioned in the previous section, and some attacks are group-based specific to these methods. For example, attackers can impersonate group members and access the Internet [25].

B. Ni et al.'s Scheme

In 2018, Ni *et al.* proposed an efficient service-oriented authentication scheme [15], which is the compliance with the 3GPP standard for the 5G architecture. We will briefly introduce Ni *et al.*'s scheme and give a summary. They proposed an efficient, secure, and service-oriented authentication framework to support network slicing and fog computing for 5G IoT services. Specifically, users can effectively establish a connection with the 5G core network and anonymously access the IoT service assigned by the fog node according to the correct 5G infrastructure network slice selected by the slice/service type of the access service. A privacy-preserving slice selection mechanism is introduced to retain the configured slice type and users who access the service type. In addition, a session key is negotiated among the user, the fog, and the IoT server to ensure that the service data in the fog cache and the remote server are safely accessed with low latency. They evaluated the performance of the proposed framework through simulations to demonstrate its efficiency and feasibility under the 5G infrastructure.

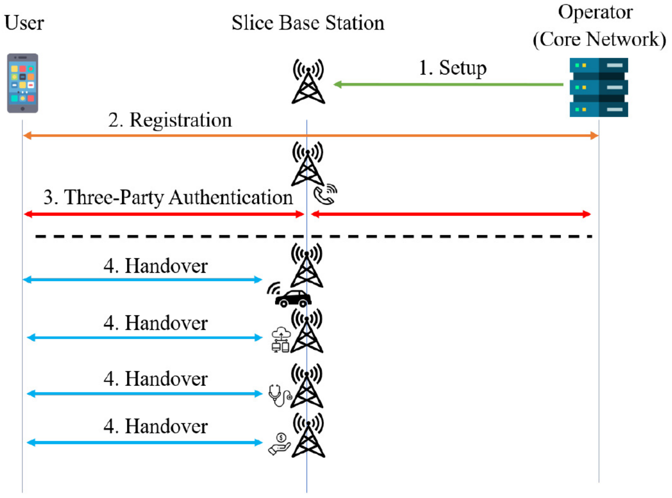

Fig. 7. The Proposed System Model.

Since, in Ni *et al.*'s scheme, the core network needs to re-authenticate a device when it accesses a different slice, it will be time-consuming. In our proposed scheme, the devices only need to be authenticated by slices after the registration phase. As compared to Ni *et al.*'s scheme, our scheme can reduce the latency time of the authentication. A detailed comparison will give in Section VI.

IV. The Proposed Scheme

We present an efficient and lightweight authentication scheme for the 5G network. In the proposed scheme, there are three roles: User, Slice, and Operator. The proposed scheme consists of four phases: *Setup, Registration, Three-Party Authentication,* and *Handover,* as illustrated in Fig. 7. The Setup algorithm publishes security parameters that will be used to provide authentic communication. Next, users will register with the operator in the Registration phase. A user can send a request to a slice that the user wants to access in the three-phase authentication phase. The 5G setting allows one device to have at most eight slices at a time. After the operator authenticates a slice with a user, if the user wants to access a different slice, he will be authenticated by the new slice rather than the core network to achieve fast handover.

A. Setup

Each slice is deployed by the operator, and the operator shares a long-term secret key slk_i with each slice SID_i at the time of deployment. Let n be the number of slices. We define

- $slk = \{slk_1, slk_2, \ldots, slk_n\}$ as the set of the long-term secret keys of the n different slices.
- $SID = \{SID_1, SID_2, \ldots, SID_n\}$ as the set of the identities of the n slices.
- $sSecret = \{\kappa_1, \kappa_2, \ldots, \kappa_n\}$ as the set of the identity secrets of the n slices.

We define a Single-NSSAI (S-NSSAI) as an identity secret κ_i, which consists of a slice/service type (SST) and some optimal information called a slice differentiator (SD). Every slice has its unique feature. It is easier to find slices that provide services through these features by users or the operator. When the demand for various services increases or decreases, the set *slk*, *SID*, and *sSecret* will be added or deleted by the operator.

According to 3GPP TS 33.501, the encryption and decryption between the operator and the users are under the Elliptic Curve Integrated Encryption Scheme (ECIES) [26]. Based on the ECIES scheme:

- The operator generates a pair of keys (*pk*, *sk*) where *pk* is its public key and *sk* is the secret key corresponding to *pk*.
- *pk* is stored in every SIM card where *pk* is legally published and *sk* is kept secret by the operator.
- A key generator *keygen* is stored in every SIM card, which can generate a different pair of keys for a user in each different session.
- (E_{key}, D_{key}) is a pair of symmetric encryption and decryption functions.
- *H* is a one-way hash function defined in ECIES, which maps an arbitrary-length byte string to a byte string of a predefined output length.

B. Registration

A user is able to register with the operator as follows.

1) The user must provide his identity *ID* and the identities of the slices which he wants to access to the operator.
2) Let $\Gamma_{ID} \subseteq [1, n]$ be the index set of the slices the user wants to access. The operator gives a SIM card *SIM* to the user where *SIM* contains $\{pk, keygen, slice = \{E_{slk_j}(\kappa_j)||SID_j \mid j \in \Gamma_{ID}\}, ulk\}$.

where *ulk* is the long-term secret key shared by the operator and the user only. The operator should maintain a list to record the information.

C. Three-Party Authentication

- *Step 1:* A user *ID* sends a request for accessing a service to a slice SID_i
  1) The user randomly chooses a string α as the session number.
  2) The user executes *keygen* to generate a public-private key pair (*upk*, *usk*) for this session.
  3) The user takes the operator's public key *pk* which had been stored in *SIM* and *usk* to generate a shared key $x = H(usk \cdot pk)$ (According to ECIES [26], $H(usk \cdot pk) = H(sk \cdot upk) = x$).
  4) The user forms $SUCI = E_x(E_{ulk}(SUPI||ID||\alpha)||ID)$ where *SUPI* is the user device identification code (similar to IMSI in 4G).
  5) Let $c_1 = E_{slk_i}(\kappa_i)||SUCI||upk$. The user sends c_1 to SID_i, where $E_{slk_i}(\kappa_i)$ had been stored in *SIM*.
- *Step 2:* SID_i verifies the correctness of $E_{slk_i}(\kappa_i)$
  1) After receiving c_1, SID_i takes slk_i to decrypt $E_{slk_i}(\kappa_i)$ and then verifies if the output of the decryption is identical to its κ_i. If not, SID_i will abort the query.
  2) SID_i computes $c_2 = E_{slk_i}(c_1||\kappa_i||ts_1)||SID_i$ and sends c_2 to the operator where ts_1 is the timestamp.
- *Step 3:* The operator authenticates the slice and verifies the user
  1) The operator authenticates the slice: The operator first parses $c_2 = c_2'||SID_i$. According to SID_i, the operator retrieves (*slk*$_i$, κ_i) from its database and decrypts c_2'. Let $c_1||\kappa_i'||ts_1 = D_{slk_i}(c_2')$. The operator checks if both $\kappa_i' = \kappa_i$ and ts_1 is fresh. If true, the operator will authenticate SID_i; otherwise, it will abort the request.
  2) The operator verifies the user: The operator takes *upk* in c_1 and its private key *sk* to create the shared key $x = H(sk \cdot upk)$. It performs the following tasks.
     - Decrypt *SUCI* in c_1 with x to get $E_{ulk}(SUPI||ID||\alpha)||ID$.
     - Decrypt $E_{ulk}(SUPI||ID||\alpha)$ with *ulk* of user *ID* and then parse the result as $SUPI||ID'||\alpha$.

     If $ID' \neq ID$, the operator aborts the request.
- *Step 4:* The operator sets the parameters for handover and sends the parameters to the slice

  Since the operator knows the services the user can access, it can retrieve the long-term secret keys and identity secrets of those slices and perform the following tasks.
  1) Compute $slice' = \{E_{slk_j}(\kappa_j||uslk_j)||uslk_j \mid j \in \Gamma_{ID}\}$ where $uslk_j$ is randomly chosen and will act as the common secret key shared by user *ID* and slice SID_j for each j after the three-party authentication is successfully completed.
  2) Compute $c_3 = E_{slk_i}(E_{ulk}(slice'||\alpha||\beta)||\kappa_i||\alpha||\beta||ts_2)$ where β is a randomly-chosen string and ts_2 is the timestamp.

  The operator transfers c_3 to SID_i.
- *Step 5:* The slice authenticates the operator and sends the parameters to the user

  After receiving c_3, SID_i decrypts c_3 and extracts the second component $\tilde{\kappa_i}$ from the output of the decryption. If both $\tilde{\kappa_i}$ is identical to its κ_i and ts_2 is fresh, SID_i will authenticate the operator; otherwise, it will abort the session. It sends $c_4 = E_{ulk}(slice'||\alpha||\beta)$ to the user.
- *Step 6:* The user authenticates the system and stores the parameters for handover

  After receiving c_4, the user decrypts it and extracts the second component α' from the output of the decryption. If $\alpha' = \alpha$, the user will authenticate the system; otherwise, he will abort the session. He keeps $slice'$ for later handover and sends $H(\beta)$ to SID_i. Finally, the user sets $H(\alpha||\beta)$ to be the session key with SID_i.
- *Step 7:* The slice authenticates the user

  SID_i verifies if $H(\beta)$ is correct by applying H to the β it received from the operator. If true, it will authenticate user *ID*; otherwise, it will abort the request. Finally, SID_i sets the session key with the user to be $H(\alpha||\beta)$.

D. Handover

In the 5G environment, it is allowed that one device has at most eight network slices at a time. In certain situations, a device may need to switch between the slices quickly. Suppose that slice SID_t is the one which user *ID* wants to handover to. The slice and the user can authenticate each other and establish a session key as follows.

1) User *ID* retrieves $E_{slk_t}(\kappa_t||uslk_t)$ and $uslk_t$ from his stored *slice*$'$, and then he randomly chooses a string α and computes $E_{uslk_t}(\alpha)$. He sends $E_{slk_t}(\kappa_t||uslk_t)$ and $E_{uslk_t}(\alpha)$ to slice SID_t.
2) SID_t decrypts $E_{slk_t}(\kappa_t||uslk_t)$ to obtain κ_t and $uslk_t$. If the κ_t is identical to its own one, SID_t will set $uslk_t$ to be the common secret key shared with user *ID*; otherwise, it will abort the request. SID_t decrypts $E_{uslk_t}(\alpha)$ by using $uslk_t$ and gets α. It randomly chooses a string β and then computes and sends $E_{uslk_t}(H(\alpha)||\beta)$ to the user.
3) User *ID* decrypts $E_{uslk_t}(H(\alpha)||\beta)$ to obtain $H(\alpha)$ and β. He verifies if the $H(\alpha)$ is correct by applying *H* to the α he chosen in step 1). If true, he will authenticate SID_t and set the session key to be $H(\alpha||\beta)$; otherwise, he will abort the session. Finally, he computes and sends $H(\beta)$ to SID_t.
4) SID_t verifies if $H(\beta)$ is correct by applying *H* to the β it chosen in step 2). If true, it will authenticate user *ID* and set the session key to be $H(\alpha||\beta)$; otherwise, it will abort the request.

V. Security Analysis

The security of mutual authentication and session key establishment can be guaranteed based on the security of public-key cryptosystems, symmetric encryptions, and one-way hash functions. The challenge-response mechanism and the timestamp approach have been applied to withstand replay attacks. We show how to achieve the security as follows.

A. Mutual Authentication Between Slice SID_i and the Operator in Three-Party Authentication

The slice long-term secret key slk_i had only been shared by slice SID_i and the operator in the Setup phase. In Step 2 of Three-Party Authentication, slice SID_i sends $c_2 = E_{slk_i}(c_1||\kappa_i||ts_1)||SID_i = c_2'||SID_i$ to the operator. A correct c_2' can be constructed by using slk_i only and a fresh c_2' can only be generated in the current session (i.e., c_2' is not a replayed one). Therefore, in Step 3, after decrypting c_2', once the κ_i extracted from the decryption result is the identity secret of SID_i and ts_1 is fresh, the operator will learn that c_2' is correct and fresh and thus it will authenticate SID_i.

In Step 4 of Three-Party Authentication, the operator sends $c_3 = E_{slk_i}(E_{ulk}(slice'||\alpha||\beta)||\kappa_i||\alpha||\beta||ts_2)$ to SID_i. In Step 5, SID_i decrypts c_3. Similarly, SID_i will authenticate the operator if the κ_i extracted from the decryption result is its identity secret and ts_2 is fresh. From the above, mutual authentication between SID_i and the operator can be guaranteed.

B. Mutual Authentication and Session Key Agreement Between User ID and the System (Slice + Operator)

The long-term secret key *ulk* had been shared by user *ID* and the operator in the Registration phase. In Step 1 of Three-Party Authentication, α is randomly chosen by user *ID* as a challenge material to the system and then *SUCI* $= E_x(E_{ulk}(SUPI||ID||\alpha)||ID)$ is sent to the system. In Step 5, the user receives the response $c_4 = E_{ulk}(slice'||\alpha||\beta)$ from the system. In Step 6, after decrypting c_4, if the α in the decryption result is identical to the one the user chosen in Step 1, then he will authenticate the system since only the operator and he know *ulk* and both the operator and SID_i had authenticated each other.

The string β is randomly chosen by the operator in Step 4 to be a challenge material to the user and $c_4 = E_{ulk}(slice'||\alpha||\beta)$ is sent to the user in Step 5. In Step 6, after decrypting c_4 and getting β, the user computes and sends the response $H(\beta)$ to the system. If the response is correct, the system will authenticate the user since β is randomly chosen by the operator and *ulk* is only known to the user and the operator. Therefore, mutually authentication between the user and the system can be achieved.

Consider the session key agreement. After the mutual authentication, user *ID* and slice SID_i have shared α and β secretly, each of which has been protected by either encryption or one-way hashing. Hence, $H(\alpha||\beta)$ can form as a session key between user *ID* and slice SID_i for the following secure communication in this session.

C. Mutual Authentication and Session Key Establishment Between User ID and Slice SID_t in the Handover Phase

After performing Three-Party Authentication successfully, user *ID* has obtained an authenticated *slice*$' = \{E_{slk_j}(\kappa_j||uslk_j)||uslk_j \mid j \in \Gamma_{ID}\}$ from the system. In the Handover phase, the user retrieves $E_{slk_t}(\kappa_t||uslk_t)$ and $uslk_t$ from *slice*$'$ and sends $E_{slk_t}(\kappa_t||uslk_t)$ to SID_t. After decryption, SID_t can obtain the common secret key $uslk_t$ shared with the user.

The user randomly chooses α and sends $E_{uslk_t}(\alpha)$ as a challenge to the slice. If the response $H(\alpha)$ from the slice is correct, the user will authenticate the slice since none can decrypt $E_{uslk_t}(\alpha)$ to obtain α and then compute $H(\alpha)$ without $uslk_t$. On the other hand, the slice randomly chooses β and sends $E_{uslk_t}(H(\alpha)||\beta)$ to the user. If the response $H(\beta)$ from the user is correct, the slice will authenticate the user since none can decrypt $E_{uslk_t}(H(\alpha)||\beta)$ to obtain β and then compute $H(\beta)$ without $uslk_t$.

After performing the mutual authentication successfully, user *ID* and slice SID_t have secretly shared α and β, each of which has been protected by either encryption or one-way hashing. Therefore, $H(\alpha||\beta)$ can form as a session key between user *ID* and slice SID_t in this session.

VI. Comparisons

In this section, we show the comparison between the proposed scheme and Ni *et al.*'s scheme [15]. Ni *et al.*'s

TABLE I
COMPUTATION COSTS

	Ni *et al.*'s Scheme				The Proposed Scheme			
		User	Slice	Operator		User	Slice	Operator
Three-Party Authentication	T_m	8	—	7	T_s	1	—	1
	T_{e1}	16	5	21	T_{e1}	—	—	—
	T_{e2}	1	—	4	T_{e2}	—	—	—
	T_p	5	6	12	T_p	—	—	—
	T_{AES}	2	—	5	T_{AES}	3	3	5 + n_s, ($n_s \leq 8$)
	T_h	8	4	17	T_h	3	2	1
	Total (us)	208.1475	173.283	421.075875	Total (us)	0.647625	0.04125	$\leq$ 0.713625
		User	Slice	Operator		User	Slice	Operator
Handover	T_m	8	—	7	T_s	—	—	—
	T_{e1}	16	5	21	T_{e1}	—	—	—
	T_{e2}	1	—	4	T_{e2}	—	—	—
	T_p	5	6	12	T_p	—	—	—
	T_{AES}	2	—	5	T_{AES}	2	3	—
	T_h	8	4	17	T_h	3	3	—
	Total (us)	208.1475	173.283	421.075875	Total (us)	0.04125	0.0495	—

scheme satisfies the 3GPP standard, but it does not satisfy some 5G network environment characteristics. The 5G network allows one device to have at most eight slices simultaneously. It means that each device may have more than one slice at the same time. In Ni *et al.*'s scheme, whenever a user wants to access a different slice, it will be necessary for the core network to authenticate the user. It is time-consuming and will be getting worse when the user crosses slices frequently. We will provide the same scenario in both of the schemes for comparisons where a user equipment, network slices, and the operator are included. Since Ni *et al.*'s scheme is based on a credential system, the authentication performance may not be as good as that of our scheme while it has the advantage of the storage of the slice information. However, Ni *et al.*'s scheme needs more computation cost and more time latency whenever switching among the slices.

TABLE II
NOTATIONS

Notation	Meaning
T_m	the cost of a multiplication computation
T_s	the cost of a scalar multiplication in an additive group
T_{e1}	the cost of an exponentiation computation of $\mathbb{G}_1, \mathbb{G}_2$
T_{e2}	the cost of an exponentiation computation of $\mathbb{G}_T$
T_p	the cost of a pairing computation
T_{AES}	the cost of an AES encryption
T_h	the cost of a one-way hash computation
n_s (≤ 8)	the number of slices where the user has access rights

TABLE III
PROPERTY COMPARISON

	Ni *et al.*'s Scheme	The Proposed Scheme
Satisfaction of TS 33.501	Yes	Yes
Without pairing	No	Yes
Time latency	High	Low

A. Performance Comparison

The performance comparison between Ni *et al.*'s scheme and our scheme is shown in Table I and some notations are defined in Table II. We count the computation costs of Ni *et al.*'s scheme by measuring the computation cost of each cryptographic primitive used in Ni *et al.*'s scheme, such as Hash, ECC, and AES. In the Three-Party Authentication phase and the Handover phase, Ni *et al.*'s scheme needs 8 multiplications, 17 exponentiations, 5 pairings, 2 AES encryptions, and 8 one-way hash computations in the user side. It requires 5 exponentiations, 6 pairings, and 4 one-way hash computations in the slice side. And it needs 7 multiplications, 25 exponentiations, 12 pairings, 5 AES encryptions, and 8 one-way hash computations in the operator side. Our three-party authentication needs 1 multiplication, 3 AES encryptions, and 3 one-way hash computations in the user side. And it requires 3 AES encryptions and 2 one-way hash computations in the slice side, and it needs 1 multiplication, $(5 + n_s)$ AES encryptions, and 1 one-way hash computation in the operator side. The proposed handover requires 2 AES encryptions and 3 one-way hash computations in the user side and it needs 3 AES encryptions and 3 one-way hash computations in the slice side. According to [27], we have $T_m \approx 66$ clock cycles. We execute the computations on a computer with Intel Core i7-8700 CPU @3.2GHz and 8.00GB memory. Hence, the clock cycle is approximately 0.3125 ns. According to [28], [29], [30], [31], we have that T_{e1} and T_{e2} are 240 times of T_m. T_p is 5 times of T_{e1}. T_h and T_{AES} are 0.4 times of T_m. T_s is 29 times of T_m.

B. Properties Comparison

Based on the discussions in Section III, we compare the proposed scheme with Ni *et al.*'s in three-party authentication and handover. Regarding the satisfaction of the TS 33.501 standard, both of the proposed scheme and Ni *et al.*'s scheme achieve it. Furthermore, our scheme is based on elliptic curves and we can complete the entire authentication without pairing. It turns out that the time latency of the proposed scheme is much lower than that of Ni *et al.*'s. The property comparison between Ni *et al.*'s and the proposed scheme is summarized in Table III.

Here, we show a practical example to demonstrate the efficiency of the proposed scheme. As we mentioned in a previous section, the 5G network allows one device to have at most eight slices simultaneously. Assume that a user called Bob has a 5G device such as a smart phone. And this device has eight slices like Smart Home using an eMBB slice, Smart City

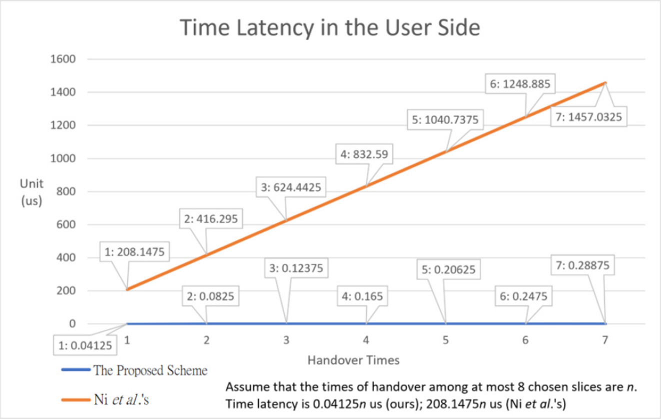

Fig. 8. Time Latency in the User Side.

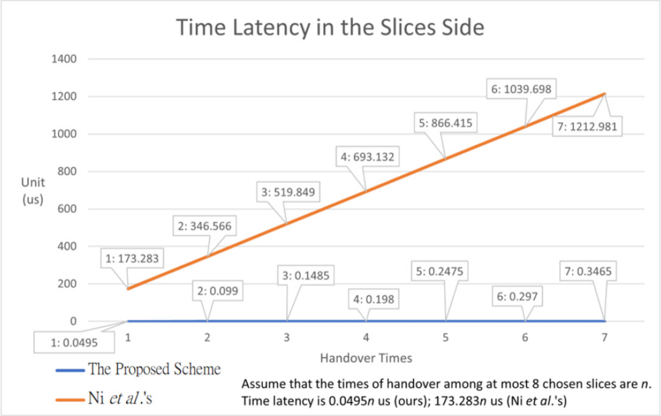

Fig. 9. Time Latency in the Slices Side.

using an MMTC slice, and Self-Driving Car using a uRLLC slice. When Bob works at home or plays a game, he will need one slice in this situation. When Bob wants to control some IoT devices like lights or air conditioners in his Smart Home, he will need another slice to control them. After Bob finishes his work and he wants to watch an AR/VR video, he requires another eMBB slice again. At last, he wants to go outside and takes a Self-Driving Car. He will need a uRLLC slice to achieve ultra-low latency. In the above example, Bob are accessing several slices and switching among his slices frequently. We illustrate the comparisons on the latency time regarding the user side in Fig. 8 and the slices side in Fig. 9 to demonstrate how fast the proposed scheme will be as compared with Ni *et al.*'s scheme in a sequence of handovers. Since in the 5G environment, three-party authentication is executed one time; however, handover will be executed lots of times when a device wants to switch among the slices.

VII. Conclusion

This article demonstrated a new authentication technique suitable for effective communication in the 5G network. The scheme is based on the concept of the elliptic curve integrated encryption strategy. It leverages the functionalities of the edge cloud and the center cloud to reduce the latency for 5G communication. Further, it showed an efficient handover mechanism where IoT devices need to switch network slices based on the requirement. The security of the proposed scheme is based on the security of public-key cryptosystems, symmetric encryptions, and one-way hashing. It is immune to replay attacks under the protection from the challenge-response mechanism and the timestamp approach. The performance of the proposed scheme is measured based on the overheads of different cryptographic operations. Moreover, it is found that the proposed scheme is better than Ni *et al.*'s scheme in terms of the computation cost and the latency. We will look for relevant open-source software and plan to implement the proposed scheme in our future work.

Acknowledgment

The authors would like to thank Prof. Arijit Karati for his valuable comments on the paper.

References

[1] “IMT vision—Framework and overall objectives of the future development of IMT for 2020 and beyond,” Int. Telecommun. Union, Geneva, Switzerland, ITU-Recommendation M.2083, Sep. 2015.

[2] I.-G. P. Group, “5G concept,” IMT-2020(5G) Promotion Group, Beijing, China, Rep., Feb. 2015. [Online]. Available: http://www.imt2020.org.cn/en/documents/3

[3] “Security challenges and opportunities for 5G mobile networks,” NOKIA, Espoo, Finland, Rep., 2017. [Online]. Available: https://onestore.nokia.com/asset/201049?_ga=2.41812066.1968491423.1611722503-172889078.1611722503

[4] “5G security: Scenarios and solutions,” Erricsson, Stockholm, Sweden, Rep., 2017. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security—enabling-a-trustworthy-5g-system

[5] *System Architecture for the 5G System*, 3GPP Standard TS 23.501, 2017.

[6] *Numbering, Addressing and Identification*, 3GPP Standard TS 23.003, 2020.

[7] *Security Architecture and Procedures for 5G System*, 3GPP Standard TS 33.501, 2018.

[8] S. Behrad, “Slice specific authentication and access control for 5G,” Ph.D. dissertation, Dept. Comput. Sci. Netw., Inst. Polytechnique de Paris, Palaiseau, France, 2020.

[9] P. K. Panda and S. Chattopadhyay, “An improved authentication and security scheme for LTE/LTE-A networks,” *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 5, pp. 2163–2185, 2020.

[10] R. Ma, J. Cao, D. Feng, H. Li, Y. Zhang, and X. Lv, “PPSHA: Privacy preserving secure handover authentication scheme for all application scenarios in LTE-A networks,” *Ad Hoc Netw.*, vol. 87, pp. 49–60, May 2019.

[11] J. Zhou, M. Ma, and S. Sun, “A hybrid authentication protocol for LTE/LTE-A network,” *IEEE Access*, vol. 7, pp. 28319–28333, 2019.

[12] B. L. Parne, S. Gupta, and N. S. Chaudhari, “PSE-AKA: Performance and security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks,” *Peer-to-Peer Netw. Appl.*, vol. 12, no. 5, pp. 1156–1177, 2019.

[13] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, “A formal analysis of 5G authentication,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2018, pp. 1383–1396.

[14] (Jul. 17, 2019). *An Overview of the 3GPP 5G Security Standard.* [Online]. Available: https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

[15] J. Ni, X. Lin, and X. S. Shen, “Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.

[16] S. Behrad, E. Bertin, and N. Crespi, *Authentication and Access Control for 5G*. Hoboken, NJ, USA: Wiley, May 2020, pp. 1–19.

[17] S. Behrad, S. Tuffin, E. Bertin, and N. Crespi, “Network access control for the IoT: A comparison between cellular, Wi-Fi and LoRaWAN,” in *Proc. 22nd Conf. Innovat. Clouds Internet Netw. Workshops (ICIN)*, 2019, pp. 195–200.

[18] “Study of security aspects of the next generation system,” 3GPP, Sophia Antipolis, France, Rep. 33.899, 2017.

[19] H. Khan and K. M. Martin, "On the efficacy of new privacy attacks against 5G AKA," in *Proc. ICETE*, 2019, pp. 431–438.

[20] R. P. Jover, "The current state of affairs in 5G security and the main remaining security challenges," 2019. [Online]. Available: arXiv:1904.08394.

[21] P. Schneider and G. Horn, "Towards 5G security," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1165–1170.

[22] C. S. Näslund, P. Ståhl, I. Innov, G. Correndo, V. Krivcovs, and S. Philips, "Deliverable D2.7 security architecture (final)," [Online]. Available:https://5gensure.eu/sites/default/files/5G-ENSURE_D2.7_SecurityArchitectureFinal.pdf

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

[24] W.-T. Su, W.-M. Wong, and W.-C. Chen, "A survey of performance improvement by group-based authentication in IoT," in *Proc. Int. Conf. Appl. Syst. Innovat. (ICASI)*, 2016, pp. 1–4.

[25] R. Giustolisi and C. Gerhmann, "Threats to 5G group-based authentication," in *Proc. 13th Int. Conf. Security Cryptogr. (SECRYPT)*, Jul. 2016, pp. 360–367.

[26] V. Shoup, "A proposal for an ISO standard for public key encryption (version 2.1)," *IACR e-Print Archive*, vol. 112, pp. 1–56. Dec. 2001.

[27] R. L. A. Mrabet and N. El-Mrabet, "A systolic hardware architectures of montgomery modular multiplication for public key cryptosystems," Cryptol. ePrint Archive, Int. Assoc. Cryptol. Res., Lyon, France, Rep. 2016/487, 2016, [Online]. Available: https://eprint.iacr.org/2016/487

[28] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs Codes Cryptogr.*, vol. 19, pp. 173–193, Mar. 2000.

[29] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2001.

[30] M. Scott, "Implementing cryptographic pairings," in *Proc. Pairing-Based Cryptogr.*, 2007, pp. 177–196.

[31] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Trans. Dependable Secure Comput.*, vol. 3, no. 4, pp. 386–399, Oct./Dec. 2006.

Chun-I Fan received the M.S. degree in computer science and information engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1993, and the Ph.D. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 1998. From 1999 to 2003, he was an Associate Researcher and a Project Leader with Telecommunication Laboratories, Chunghwa Telecom Company, Ltd., Taoyuan, Taiwan. In 2003, he joined as a faculty with the Department of Computer Science and Engineering, National Sun Yat-sen University (NSYSU), Kaohsiung, Taiwan. He has been a Full Professor since 2010 and a Distinguished Professor since 2019. He also is the Dean of College of Engineering and the Director of Information Security Research Center at NSYSU, and he was the CEO of "Aim for the Top University Plan" Office, NSYSU. And he is currently an outstanding faculty in Academic Research in NSYSU. His current research interests include applied cryptology, information security, and communication security. He received the Best Student Paper Awards from the National Conference on Information Security in 1998, the Dragon Ph.D. Thesis Award from Acer Foundation, the Best Ph.D. Thesis Award from the Institute of Information and Computing Machinery in 1999, and the Y. Z. Hsu Science Paper Award (Information and Communication Science and Technology Category) in 2020. He won the Engineering Professors Award from Chinese Institute of Engineers—Kaohsiung Chapter in 2016, and the Outstanding Technical Achievement Award from IEEE Tainan Section in 2020. He is the Chairman of Chinese Cryptology and Information Security Association, and was the Chief Executive Officer of Telecom Technology Center in Taiwan.

Yu-Tse Shih was born in Taichung. He is currently pursuing the Doctorate degree in computer science and engineering with National Sun Yet-sen University, Kaohsiung, Taiwan. His research interests include communication security, information security, applied cryptography, and biometric authentication.

Jheng-Jia Huang was born in Kaohsiung, Taiwan. He received the M.S. degree in information management from National Kaohsiung First University of Science and Technology, Kaohsiung, in 2012, and the Ph.D. degree in computer science and engineering from the National Sun Yat-sen University, Kaohsiung, in 2019. From 2019 to 2020, he has been a Director of the InfoCom Security Division, a Quality Control/Quality Assurance Supervisor, and the Chief Security Officer of Telecom Technology Center, Kaohsiung. In 2020, he joined the faculty with the Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan. He also is the Deputy Secretary General of the Chinese Cryptology and Information Security Association. His current research interests include cloud computing and security, social network security and authentication, network and communication security, information security, and applied cryptography. He won the Phi Tau Phi Award and the Best Ph.D. Thesis Award from the National Sun Yat-sen University in 2019, the Best Ph.D. Thesis Award from the Taiwan Association for Web Intelligence Consortium and the Taiwan Institute of Electrical and Electronic Engineering in 2019, and the Best Ph.D. Thesis Award from the Taiwan Association of Cloud Computing, the Chinese Cryptology and Information Security Association, and the Institute of Information & Computing Machinery in 2020.

Wan-Ru Chiu was born in Changhua City, Taiwan. She received the master's degrees in computer science and engineering from National Sun Yat-sen University, Kaohsiung, Taiwan, in 2018. Her research interests include communication security, cloud computing, network security, and information security.