Hindawi
Security and Communication Networks
Volume 2021, Article ID 6697155, 18 pages
https://doi.org/10.1155/2021/6697155

Research Article

A Composable Multifactor Identity Authentication and Authorization Scheme for 5G Services

Yurong Luo, Hui Li, Ruhui Ma, and Zhenyang Guo

School of Cyber Engineering, State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, China

Correspondence should be addressed to Yurong Luo; yurongluo@stu.xidian.edu.cn

Received 26 December 2020; Revised 25 March 2021; Accepted 31 March 2021; Published 19 April 2021

Academic Editor: Chengzhe Lai

The fifth-generation (5G) mobile communication technology has already deployed commercially and become a global research focus. The new features of 5G include unlimited information exchange, a large variety of connections with independent energy, and diversified high transmission rate services. Collective synergy of services is expected to change the way of life and future generations and introduce new converged services to the ICT industry. Different application services have to meet differentiated security demands. From the perspective of security, in order to support the multiservice of 5G services, it is necessary to consider the new security mechanism driven by the service. Based on 5G massive data stream, the 5G system can provide customized real-world services for potential users and reduce the user experience gap in different scenarios. However, 3GPP Extensible Authentication Protocol (EAP), which is the present entity authentication mechanism for the 5G service layer, is only an individual authentication architecture and unable to fulfill the flexible security objectives of differentiated services. In this paper, we present a new hierarchical identity management framework as well as an adaptable and composable three-factor authentication and session key agreement protocol for different applications in 5G multiservice systems. Finally, we propose an authorization process by combining with the proposed three-factor authentication mechanism and Service-Based Architecture (SBA) proposed by the 3GPP committee. The proposed mechanism can concurrently provide diverse identity authentication schemes corresponding to four different security levels by easily splitting or assembling three-factor authentication protocol blocks. The proposed scheme can be simultaneously applied to a variety of applications to improve the efficiency and quality of service and reduce the complexity of the whole 5G multiservice system, instead of designing or adopting several different authentication protocols. The performance evaluation results indicate that the proposed scheme can guarantee the multiple security of the system with ideal efficiency.

1. Introduction

At present, the global 5th generation mobile communication technology (5G) commercial development has begun to take shape and been recognized as main supporting technologies of mobile networks. It has become the focus of global mobile communication research and technology competition. Compared with the existing 4G network, 5G network aims to provide high quality and reliable services such as higher data rate, ultralower latency, massive connectivity, high energy efficiency, and accurate quality of experience (QoE) [1]. The 5G network can realize more kinds of dynamic customization and scalable network services by adopting software-defined network (SDN) and network function virtualization (NFV) technologies. Due to its powerful bandwidth and service capability, a significant number of new applications are introduced into the 5G network platform, such as augmented reality, multimedia video business, mobile industrial internet, autonomous driving, and mobile electronic health services.

There are new security requirements and challenges in 5G, so it is not enough to provide the traditional security mechanism. 5G network will support massive smart devices and various forms of terminals; thus, 5G network is driven to introduce new identity management methods. The generation, distribution, and other lifecycle management of users' identification involved in the identity management method will change [2].

The growing demand for diversified applications has brought about widely different services, as well as security issues such as service authentication. Moreover, due to the openness of services, a variety of different mobile terminals need to be connected to the 5G network, which also raises corresponding security trust issues and attacks [3, 4]. In diverse application scenarios, different kinds of terminals have different security demands. For example, large-scale machine-type communication (MTC) devices need lightweight security mechanisms to adapt to low energy storage; meanwhile, high-speed mobile services need more efficient and secure authentication schemes, and video services need to meet the security requirements of low latency and high reliability. If the same security scheme is used for differentiated applications, it may seriously affect the user's service experience. The 5G intelligent computing technology, which is user centric, reconfigures the appropriate security scheme after collecting user and scene data, so as to provide better services. It is significant to provide hierarchical security protection for different services in order to better provide security services for the vertical industry. In the traditional networks, multiservice system adopts different authentication schemes for different kinds of terminals, which increases the complexity of the system and reduces the quality of user experience. According to the current 3GPP standard [5], 5G employs Extensible Authentication Protocol (EAP) to realize the entity identity authentication for third-party services and applications, yet EAP is an identity authentication architecture that can merely adopt unitary authentication schemes such as symmetric key cryptography or digital certificate system alone. Diverse services and applications in EAP adopt a variety of independent authentication mechanisms, which cannot support differentiated and adventurous 5G services. Consequently, a flexible and secure composable authentication and service authorization framework is urgently needed to provide comprehensive and fine-grained entity trusted security support for the vertical industry in the 5G network.

In this paper, we design a new flexible and composable multifactor authentication and session key agreement protocol under a diversified identity management architecture in 5G multiservice systems and finally give an authorization process based on the 5G unified authentication and service authorization framework. In our scheme, a new diversified identity, which includes the security levels of services and applications, is assigned by the 5G Network Repository Function (NRF) and deployed to 5G user equipment (UE) in the initial stages. Subsequently, the biometrics and password are employed in conjunction with the smart card to construct the multifactor service authentication and session key agreement protocol, which can be separated or combined according to 4 different security levels or requirements. Finally, the improved service authorization process based on the 5G service architecture is executed to provide required services for users. Without the separate implementation of different identity authentication protocols, this scheme can greatly improve the quality of service of users and reduce the complexity of the whole 5G multiservice system.

The main contributions of the paper are threefold. (1) A hierarchical identification data structure for the 5G application layer is designed. (2) A composable and potent multifactor service authentication and session key agreement protocol is proposed, which provides 4 grades of security levels of authentication. Furthermore, the proposed protocol is not the simple combination of three authentication factors but flexibly integrates them to ensure the security and the feasibility of the 5G service system. (3) We give an authorization process based on the proposed authentication mechanism and SBA architecture. (4) The BAN logic and the formal verification tool, Scyther tool, have been employed to prove that the proposed scheme can achieve multiple security functions and resist attacks.

Compared with the conference version [6], which barely proposed a conceptual classified mutual authentication scheme without high efficiency, formal security analysis, or detailed performance evaluation in the 5G multiservice system, we optimize the multifactor authentication scheme and provide key agreement and service authorization protocol in new design. Moreover, the formal analysis including BAN logic and CK model security analysis are employed to verify the scheme security. Then, we evaluate the computational cost, communication cost, and storage cost of our proposed scheme by comparing it with the typical EAP protocol based on the NIST standard and show the protocol performance under unknown attacks.

The rest of the paper is organized as follows. In Section 2, we investigate the related work. Section 3 introduces the biometric authentication fuzzy extractor function. Section 4 presents the security and network model. Section 5 details the processes of the proposed scheme. The security and performance analysis are revealed in Section 6 and Section 7, respectively. Finally, Section 8 summarizes the paper.

2. Related Work

The research works on the network entity authentication and process for services and applications in 4G/5G networks [7, 8] were very lacking. Shin and Kwon [9] proposed an anonymous three-factor authentication and access control scheme for real-time applications in WSNs. However, the scheme is liable to user collusion and desynchronization attacks. Ni et al. [8] designed a service-oriented anonymous authentication mechanism for enabling 5G IoT. In the scheme, an anonymous authenticated key agreement mechanism is proposed to ensure the secure connection and authentication for IoT devices and will not disclose user privacy. However, both of the schemes in [7, 8] employ the complex public key cryptosystem to design the related protocol and only achieve the single authentication method, which is not fit for 5G multiservice systems. Due to the introduction of the IoT service, users can also interactively control other devices in the 5G network, such as controlling the startup of the home appliance in the smart home scenario, so stricter authentication methods, such as biometric authentication, are required to ensure that the identity is true. Besides, there are a large number of authentication schemes based on the same authentication factors proposed

in [10–14]. These schemes can achieve efficient and high-strength entity authentication, but cannot complete dynamic multifactor authentication which can adjust the security strength in the 5G multiservice network. Furthermore, some authentication mechanisms for the multiserver environment have been proposed in [15, 16]. Huang et al. [15] proposed a robust multifactor authentication protocol for fragile communications which can be separated to finish dynamical authentication. However, this scheme can only discuss two stand-alone schemes but cannot be composable or achieve the mutual authentication. Liao and Wang [16] proposed a dynamic ID-based remote user authentication scheme based on the smart card and password for the multiserver architecture. This scheme can achieve the mutual authentication and key agreement between the user and server by the use of hash function. However, Li et al. [17] pointed out that the scheme [16] is vulnerable to masquerade attacks.

3. Preliminary

Biometrics with certain probability distribution characteristics such as facial recognition are not completely random and limited. In order to protect the user's biometric data and privacy, biometrics cannot be stored on the remote server and must be fuzzed. Fuzzy extractor can compact a pseudo-random eigenvalue string from a low-entropy string and is generally used to extract and recover secret features from biometrics. Based on the definition in [18], a fuzzy extractor can be described as a quintuple of $(\mathcal{M}, m, \ell, t, \epsilon)$ including the following functions.

3.1. Metric Space. It is a set $\mathcal{M}$ with a distance function *dis*: $\mathcal{M} \times \mathcal{M} \longrightarrow \mathbb{R}^+ = [0, \infty)$. The function $\mathrm{dis}(\omega, \omega\prime)$ is a measure of the difference between two variables, for example, Hamming distance.

3.2. Min Entropy. $\mathbf{H}_\infty(A) = -\log(\max_a \Pr[A = a])$ is the minimum-case entropy of a random variable A.

3.3. Statistic Distance. The statistical distance between two probability distributions A and B is defined as $\mathrm{SD}(A, B) = (1/2)\sum_v |\Pr(A = v) - \Pr(B = v)|$.

3.4. Fuzzy Extractor. A fuzzy extractor is represented as a quintuple of $(\mathcal{M}, m, \ell, t, \varepsilon)$ including a pair of procedures, "generate" (Gen) and "reproduce" (Rep).

(1) The probabilistic generation procedure Gen: $\mathcal{M} \longrightarrow^R \{0,1\}^\ell \times \{0,1\}^*$ is

$$\mathrm{Gen}(\omega) = (R, N). \tag{1}$$

Any input $\omega \in \mathcal{M}$ is a low-entropy string. In the output pair, R is called as a characteristic string, and N is an auxiliary string. For any distribution W on $\mathcal{M}$ of min-entropy m, the string R is nearly random even for those who observe N: if $(R, N) \leftarrow \mathrm{Gen}(\omega)$; then, we have $\mathrm{SD}((R, N), (U_\ell, N)) \leq \epsilon$, where U_ℓ represents the uniform distribution on l–bit binary strings.

(2) The deterministic reproduction procedure Rep: $\mathcal{M} \times \{0,1\}^* \longrightarrow^D \{0,1\}^\ell$ is

$$\mathrm{Rep}(\omega\prime, N) = R \quad \text{if } \mathrm{dis}(\omega, \omega\prime) \leq t. \tag{2}$$

For all $\omega, \omega\prime \in \mathcal{M}$, if $(R, N) \leftarrow \mathrm{Gen}(\omega)$ and $\mathrm{dis}(\omega, \omega\prime) \leqslant t$, the fuzzy extractor can recover the pseudo-random string R from P by computing $\mathrm{Rep}(\omega\prime, N)$.

Thus, fuzzy extractors are capable of extracting pseudo-random string R from a low-entropy string ω such as biometrics and then reproduce R from any string $\omega\prime$ extremely similar to ω with the unclassified auxiliary string N.

4. System and Security Model

4.1. Network Model. 5G network needs to establish different trust models according to the characteristics of different services and provide flexible management modes according to the demands of industry users. Operators already have relatively complete security capabilities, such as authentication, ID management, and key management. In order to reduce operating and maintenance costs, vertical industries can entrust service authentication to operators. Operators can perform network and service authentication in a unified manner to achieve direct network access to multiple services. The authentication capability of the operator not only greatly facilitates the user but also provides a vertical industry as a value-added service to help it rapidly deploy the service.

Based on the principle of the service center, the 3GPP committee has designed a new 5G service secure architecture which describes the authentication and authorization of 5G services and applications: Service-Based Architecture (SBA) [19], as shown in Figure 1. There are 3 roles of the 5G SBA authentication and authorization framework including user equipment (UE), network repository function (NRF), and network function (NF) service producer. PLMN and gNB in Figure 1 are the public land mobile network and 5G base station, respectively.

The NF service producers are various 5G vertical service providers. The entity user that owns a UE obtains NF service producers' 5G services through NRF. Users can subscribe to a variety of services provided by service providers according to users' needs. NRF is located in the 5G core network, which is responsible for the discovery and selection of network functions, and provides appropriate peer-to-peer services for UE. As a 5G service configuration management server, NRF is able to support the mutual authentication and service authorization between UEs and NF service producers. EAP [5] is the identity authentication architecture proposed by the 3GPP committee to realize the user application layer authentication, which is compatible with a series of authentication protocols such as EAP-AKA [20] and EAP-TLS [21] in diverse application scenarios.

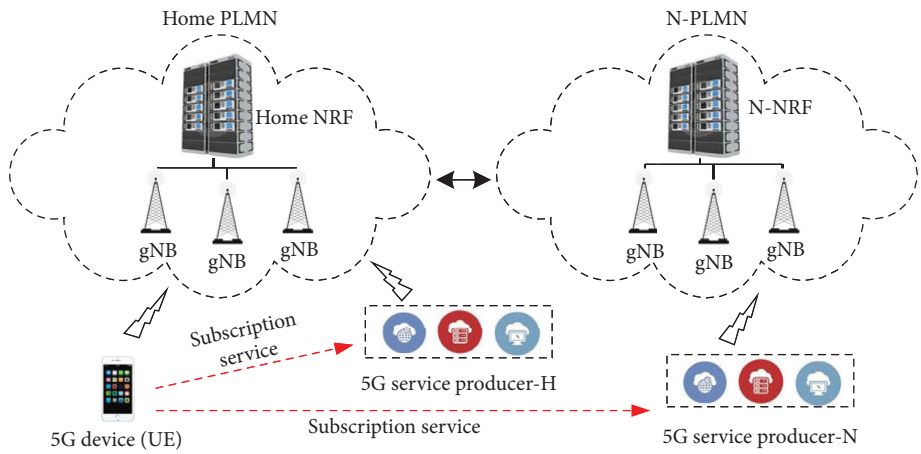

Figure 1: Network architecture.

4.2. Security Model. The authentication architecture of the proposed protocol includes 3 participants: the 5G entity user C, the 5G UE owned by a 5G entity C, and the service configuration management server NRF who supports authentication. In a basic CK-adversary model [22], the air interface channel between a UE and the NRF is public and unsecure, where a probabilistic polynomial-time (PPT) attacker $\mathscr{A}$ can monitor, tamper, and forge any wireless transmission of messages between 5G UEs and the NRF. Other than the basic adversary capabilities, $\mathscr{A}$ may collect the secret information stored in the UE's memory and NRF's database via explicit attacks. The security attacks are divided into three categories according to the type of information mastered by the adversary. We assume that the secure connection between the NRF and service producers has been established and is not within the scope of our scheme. The authentication framework and system secure model is as shown in Figure 2.

The design objective of this scheme is to achieve the composable and secure multifactor authentication for differentiated services and applications in the 5G network. The goal includes the following secure functions and capabilities:

(i) Multifactor authentication: to meet different security demands of various services, the mechanism should be able to easily combine multiple authentication factors to increase the security strength of the authentication protocol. Considering the convenience of 5G users, this scheme is mainly made up of password, smart card, and biometric authentication technology to accomplish multifactor authentication.

(ii) Composable authentication: considering the complexity of the system, the scheme should be an authentication protocol which can be divided into several blocks and flexibly combined to achieve different security strengths and goals. Without multiple authentication protocols, only a common authentication architecture does not affect the integrity of the protocol.

(iii) Efficient differentiated-service authentication: aimed at the differences in services over the 5G network, the proposed scheme can accommodate to multiservice authentication by splitting and assembling the authentication procedures. The flexible and composable authentication mechanism can largely improve the efficiency and quality of service. Aiming at the difference of applications in the 5G network, the scheme can adapt to multi-service authentication by separating and composing the authentication process. The flexible and fine-grained authentication mechanism could greatly increase the efficiency and quality of 5G service.

(iv) Session key agreement: to ensure the security of the subsequent communication process, the proposed scheme should negotiate a secret session key between the UE and the NRF to encrypt and protect the integrity of the communication information.

(v) Service authorization: after the successful authentication between the UE and NRF, users access resources and obtain services by means of legitimate NRF authorization. Depending on the authorized credential, the service providers deal with the service request and supply services to UE securely.

(vi) Withstanding existing protocol attacks: the proposed scheme should withstand the existing protocol attacks such as replay attack, MitM attack, and forgery attack.

5. The Proposed Authentication Scheme

This section introduces a new 5G hierarchical identity management mechanism, a flexible and composable three-factor authentication and session key agreement protocol, and a service authorization scheme for differentiated services in the 5G application system.

5.1. Security Assumptions. Without loss of generality, the following security assumptions are proposed for the authentication model:

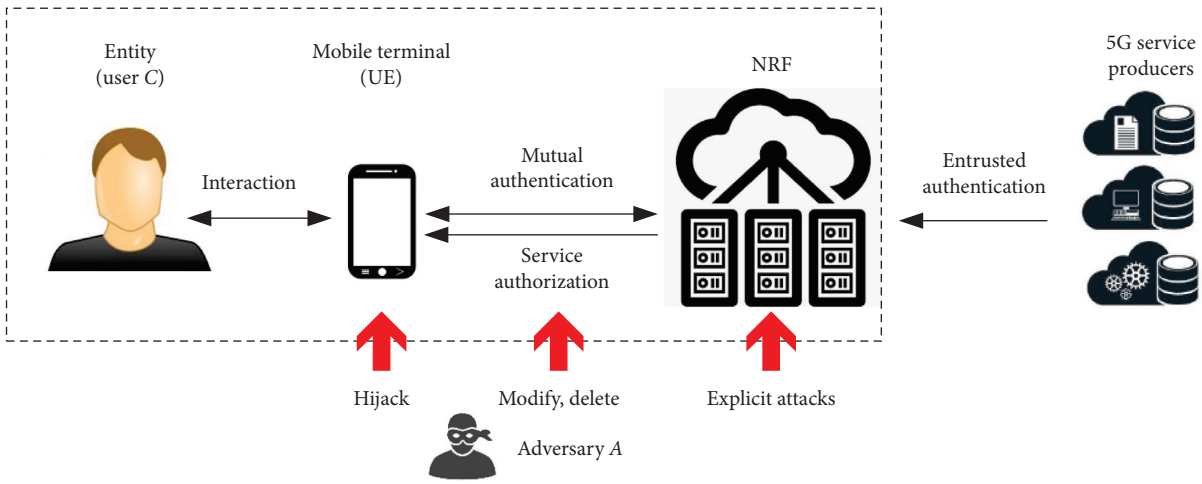

Figure 2: Secure model.

(1) In this scheme, some measures will be taken by the authentication server NRF to prevent the dictionary attack and guessing the password of a valid user.

(2) When the 5G user uses a UE, all security-related operations are implemented in the trusted execution environment [23]. Thus, the communication between the smart card function calculation such as the fuzzy extractor is secure and cannot be monitored.

(3) In the registration phase, the UE can distinguish the right NRF, and the secret information is transmitted through a trusted channel.

5.2. 5G Diversified Identity Management Mechanism. In order to adapt to differentiated applications in the 5G network, a new 5G diversified identity management framework is proposed. As shown in Figure 3, the 5G identity model includes three data blocks: physical identification, functional identification, and security level.

(i) Physical identification: the physical identification generated by the equipment manufacturer or operators satisfies the characteristic of global or network uniqueness. It represents the unique identification of a device, such as the UE's international device identification (IMEI) or the user's ID number.

(ii) Function identification: function identification is generated by telecom operators and application service providers, which points to specific services or applications that users can access. Since a device can have multiple different service resources, a physical ID can be related with several functional IDs. Function codes indicate the service authority of a user and can be changed and adjusted quickly and flexibly.

(iii) Security level: each function identification can be nominated with only one security level which shows the security requirements of functional services. According to the security requirements of service providers, we divide services or applications into four security levels: 0, 1, 2, and 3 followed by low to high, which will lead to single-factor, two-factor, and three-factor authentication protocol, respectively. Among them, 1 and 2 represent the same security strength because both of them can trigger two-factor authentication, but the authentication factors are different. For different security levels, the differentiated authentication subprotocol between UE and application server will be adopted. Ordinarily, browsing public web pages belongs to security level 0, while high-risk e-health services belong to security level 3. Service providers should demarcate security levels for services according to their defined security rules or authentication requirements.

5.3. Flexible and Composable Three-Factor Authentication Mechanism for Different Applications. This section proposes an entity authentication mechanism in the 5G multiservice system. In this scheme, the service authentication protocol can be implemented in the form of a subprotocol according to several security levels. The proposed scheme consists of the following five phases: initialization, registration, authentication, session key agreement, and biometrics and password updating, which are described in detail as follows. The notations used in our proposed scheme are shown in Table 1.

5.3.1. Initialization. Based on a system security parameter k, the authentication server NRF generates a symmetric key for authentication and a public-private key pair for authorization. And the NRF generates an elliptic curve E shared between the NRF and the user C's smart card SC for session key agreement.

(1) NRF implements public key generation algorithm PUB.KGen(k) to obtain a pair $(\mathrm{PK}_{\mathrm{NRF}}, \mathrm{SK}_{\mathrm{NRF}})$

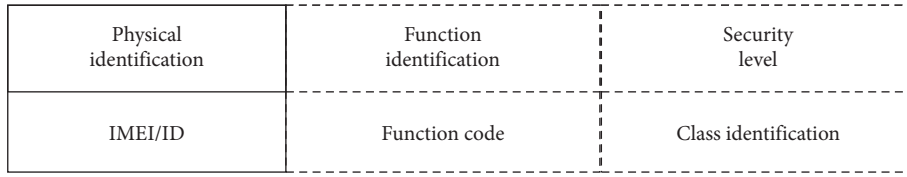

Figure 3: 5G diversified identity model.

Table 1: Notations.

Notation	Description
PUB.KGen(k)	Public key generation algorithm
$(PK_{\mathrm{NRF}}, SK_{\mathrm{NRF}})$	Public-private key pair of the authentication server NRF
SKE.KGen(k)	Symmetric key generation algorithm
$\mathrm{SKE.Enc}_{\mathrm{SK}}$	Symmetric encryption with SK
$\mathrm{SKE.Dec}_{\mathrm{SK}}$	Symmetric decryption with SK
$\mathrm{Sign}_{\mathrm{SK}}$	Sign with SK
Hash	Cryptographic hash function
MAC	Message authentication code function
ID_C	Identification of C
PW	Password chosen by C
Bio	Biometric data
SC	Smart card
D_{Bio}	Biometric data
D_C	Password data
RN	Random number
T_i	Current timestamp
Ks	Session key of NRF and C
K_{ij}	Session key between i and j

(2) NRF runs symmetric key generation algorithm SKE.KGen(k) to obtain SK_C

(3) NRF calculates the base point P on the elliptic curve E, and n is the order of P

The parameter $(\mathrm{PK}_{\mathrm{NRF}}, E, P)$ is public, and the secret parameter $(\mathrm{SK}_{\mathrm{NRF}}\mathrm{SK}_C)$ is kept secret by the NRF.

5.3.2. Registration. The registration process consists of the following steps:

(1) Biometrics registration:

(i) NRF generates ID_C with the security level designed in Section 5.2 and notifies it to user C.

(ii) User C collects the biometric data in his device UE, and a pair (R, N) is generated by C's biometric template Bio. Algorithm Gen is defined as the fuzzy extractor generation as shown in Section 3. $\mathrm{Gen}(\mathrm{Bio}) \longrightarrow (R, N)$.

(iii) C extracts MAC key $K_B = \mathrm{Hash}(R)$ and sends (K_B, N) to NRF.

(iv) After receiving (K_B, N), NRF chooses a random number RN_1 and encrypts K_B with SK_C by using the symmetric key encryption algorithm SKE.Enc.

$$D_K = \mathrm{SKE.Enc}_{\mathrm{SK}_C}(\mathrm{ID}_C \| K_B \| \mathrm{Hash}(\mathrm{ID}_C \| K_B \| \mathrm{RN}_1)),$$

where $\mathrm{Hash}(\mathrm{ID}_C \| K_B \| \mathrm{RN}_1)$ is used for integrity detection. And $\overline{D_K} = (\mathrm{SKE.Enc}_{\mathrm{SK}_C}(K_B \| \mathrm{RN}_1), \mathrm{ID}_C)$.

(v) NRF sets $D_{\mathrm{Bio}} = (N, D_K, \mathbf{Hash}, \mathbf{Rep})$ and $\overline{D_{\mathrm{Bio}}} = (N, \overline{D_K}, \mathbf{Hash}, \mathbf{Rep})$, where **Rep** is the reproduction algorithm in the fuzzy extractor.

(2) Password registration:

(i) NRF chooses two new random numbers RN_2 and RN_3 and calculates D_E and $\overline{D}$ as follows:

$$\begin{aligned} D_E &= \mathrm{Hash}\left(\mathrm{ID}_C \left\| \left(\mathrm{SK}_C \oplus \mathrm{RN}_2\right)\right.\right) \oplus \mathrm{RN}_3, \\ \overline{D} &= \mathrm{Hash}\left(\mathrm{ID}_C \left\| \left(\mathrm{SK}_C \oplus \mathrm{RN}_3\right)\right.\right). \end{aligned} \tag{3}$$

(ii) NRF sets $D_C = (\mathrm{ID}_C, \mathrm{RN}_2, D_E, \overline{D}, \mathbf{Hash})$.

(3) Smart card registration:

(i) A smart card is sent to user C containing D_C, D_{Bio}, elliptic curve E, and its base point P securely. Here, according to the 3GPP 5G standard [19], the smart card such as USIM has been deployed in a trust execution environment on each 5G device. Thus, the 5G device only requires to keep D_C and D_{Bio} in secret in the smart card which are sent by NRF.

(ii) User C encrypts D_{Bio} with K_B and stores it in .

(iii) Upon receiving, user C inputs his random password PW. Then, the device generates a random number RN_4 and computes

$D = \overline{D} \oplus \text{Hash}(\text{PW} \oplus \text{RN}_4)$ to replace the local old $\overline{D}$.

Finally, user C keeps and password securely. NRF also stores $(\overline{D_{\text{Bio}}}, D_C, E, P)$ in its database and erases RN_3 and D_{Bio}.

5.3.3. Authentication. Firstly, user C inserts the smart card and tries to request service. User C sends the service request message including the predefined identity ID_C with the service security level. Upon the receipt of the message, the authentication server NRF verifies if the identity ID_C is valid and checks the security level of ID_C to ensure user's access rights. Here, PW′ and Bio′ are represented as the collected password and biometrics during each authentication process, respectively. According to different security levels, different mutual authentication processes are executed in detail as shown in Algorithm 1.

According to the implementation method of the authentication protocol, the authentication protocol is able to divide into four protocol blocks: no authentication (attach request phase), biometrics and smart card-based authentication (biometrics authentication phase), password and smart card-based authentication (password authentication phase), and password and biometrics and smart card-based authentication which is the entire protocol as shown in Figure 4. When the service security level SR = 0, for example, the user wants to skim some public information without any privacy or sensitive data; he only needs to read his identity from the smart card and runs in two steps without any authentication. From a user experience perspective, the biometric authentication is more convenient than the password authentication for 5G users. Thus, the biometrics authentication phase and the password authentication phase are designed for the service security level SR = 1 and SR = 2, respectively. The user must implement all of the protocol blocks for the highest security level SR = 3. The proposed authentication protocol can be adopted dynamically by composing some protocol blocks and steps to balance the efficiency and security.

5.3.4. Session Key Agreement. In the subsequent authorization of NF service access processes, user C and NRF need to negotiate a session key to securely communicate with each other. The session key agreement process is executed after a successful authentication and based on the elliptic curve Diffie–Hellman (ECDH) protocol. The session key agreement is described in Algorithm 2.

In this phase, when SR = 2 or 3, NRF and user C can derive bP and aP, respectively, since

$$D^{\text{new}} \oplus \text{Hash}\left(\text{PW} \oplus \text{RN}_4^{\text{new}}\right) = \text{Hash}\left(\text{ID}_C \| \text{SK}_C \oplus \text{RN}_3^{\text{new}}\right). \tag{4}$$

5.3.5. Biometrics and Password Updating. To avoid the attacker who obtains only one of the valid features (biometrics or password) distorting the information maliciously, we suppose that the biometrics and password update phase are implemented after the successful and complete authentication (SR = 3). Users select the following phases to update the biometrics and password.

(1) Biometrics Update Phase. The user who wants to update the biometrics needs to perform a complete authentication protocol and executes some steps similar to biometrics registration. The biometrics update phase is described in Algorithm 3.

(2) Password Update Phase. To improve system security, the users are advised to change the password on a frequent basis. Likewise, the password updating phase begins with an authentication process but is slightly different from the password registration. The password update phase is described in Algorithm 4.

5.4. Authorization Scheme of NF Service Access. According to the 3GPP 5G service authentication and authorization architecture, Service-Based Architecture (SBA), we design a new authorization scheme for the 5G multiservice system, which is described in Algorithm 5.

The authorization process is shown in Figure 5. The validity parameter lifetime in Token_C is associated with the service security level SR, which is set up by the service producer NF_h in advance.

6. Security Analysis

Our proposed scheme can provide the following security objectives.

6.1. Protocol Verification

6.1.1. Authentication of C to NRF. When service SR = 1, NRF verified the legal user C by computing if the challenge response result Tag is $\text{MAC}_{K_B}(\text{RN}_6 \oplus \text{Hsah}(D_K) \| T_3)$. The attacker cannot extract correct K_B and decrypt $\text{SKE.Enc}_{K_B}(D_{\text{Bio}})$ in the smart card SC. Therefore, the attacker is not able to derive the correct Tag without K_B or D_K. When the security level is 2, NRF verifies if $\text{Hash}(\text{RN}_3 \oplus T_3) \stackrel{?}{=} M_1 = \text{Hash}(\text{Hash}(D \oplus \text{Hash}(\text{PW}' \oplus \text{RN}_4) \oplus D_E) \oplus T_3)$. As a result of PW′ = PW,

$M_1 = \text{Hash}(\text{Hash}(D \oplus \text{Hash}(\text{PW} \oplus \text{RN}_4) \oplus D_E) \oplus T_3) = \text{Hash}(\text{Hash}(\overline{D} \oplus D_E) \oplus T_3) = \text{Hash}(\text{RN}_3 \oplus T_3)$

Due to the collision resistance of hash function, an adversary cannot derive correct M_1 without the user random password. When the security level is 3, the complete authentication process is executed between C and NRF.

6.1.2. Authentication of NRF to C. When the security level is 1, C verifies NRF by checking $M_K \stackrel{?}{=} \text{Hash}(\text{Hash}(D_K) \oplus \text{RN}_5 \| T_2)$. The attacker cannot extract D_K from smart card or NRF's database without K_B or SK_C. When the security level is 2, C checks if $\text{Hash}(\text{Hash}(D \oplus \text{Hash}(\text{PW}' \oplus \text{RN}_4) \oplus D_E^{\text{new}}) \oplus T_4) = M_2$ and $\text{Hash}(\text{Hash}(D \oplus \text{Hash}(\text{PW}' \oplus \text{RN}_4) \oplus \overline{D}^{\text{new}}) \oplus T_4) = M_3$. Here, M_3 and M_2 are calculated with the server's secret parameters $(\text{SK}_C, \text{RN}_3)$. Attackers cannot disguise legitimate NRF to

Require: the user identity ID_C; the password $PW\prime$; the biometric data $Bio\prime$; the smart card.
Ensure: authentication result: 0 for failure; 1 for success.
(1) : 5G user C sends a service request message including ID_C and security level of the access service read from the smart card.
(2) : NRF checks the highest security level SR in the service request message. **If** SR = 0, then
Output 1 and **Terminate** the authentication process.
Else **if** SR = 1, then go to Step 3.
Else **if** SR = 2, then go to Step 8.
Else **if** SR = 3, then go to Step 3.
NRF sends an attach response $(SR, Attach)$ to notify C.
(3) 5G user C chooses a new random number RN_5 and sends (ID_C, T_1, RN_5) to NRF.
(4) Upon the receipt of the message, NRF works as follows.
(i) **If** the timestamp T_1 is invalid, **Output** 0. **Else**, go ahead.
(ii) Search $\overline{D_K}$ by ID_C in the database and decrypt $\overline{D_K}$ with SK_C to obtain K_B.
(iii) Generate a new random number RN_6 and compute $D_K = SKE.Enc_{SK_C}(ID_C \| K_B \| Hash(ID_C \| K_B \| RN_1))$ and $M_K = Hash(Hash(D_K) \oplus RN_5 \| T_2)$.
(iv) Send $(T_2 \| RN_6, M_K)$ to user C.
(5) Upon the receipt of the message, C works as follows.
(i) **If** the timestamp T_2 is invalid, **Output** 0. **Else**, go ahead.
(ii) Compute $R\prime = Rep(Bio\prime, N)$ and $K_B' = Hash(R\prime)$.
(iii) Decrypt $SKE.Enc_{K_B}(D_{Bio})$ with K_B' to obtain D_K.
(iv) Compute $M_K \stackrel{?}{=} Hash(Hash(D_K) \oplus RN_5 \| T_2)$. **If** the equation is established, then go ahead. **Else**, **Output** 0.
(v) Compute $Tag = MAC_{K_B'}(RN_6 \oplus Hash(D_K) \| T_3)$ and send (Tag, T_3) to NRF.
(6) Upon the receipt of the message, NRF works as follows.
(i) **If** the timestamp T_3 is invalid, **Output** 0. **Else**, go ahead.
(ii) Verify $Tag \stackrel{?}{=} MAC_{K_B}(RN_6 \oplus Hsah(D_K) \| T_3)$. **If** it is, then go ahead. **Else**, **Output** 0.
(7) **If** SR = 1, then **output** 1. **Else**, **if** SR = 3, go ahead.
(8) C computes $M_1 = Hash(Hash(D \oplus Hash(PW\prime \oplus RN_4) \oplus D_E) \oplus T_4)$ and sends $(ID_C, RN_2, D_E, M_1, T_3)$ to NRF.
(9) Upon the receipt of the message, NRF works as follows.
(i) **If** the timestamp T_4 is invalid, **Output** 0. **Else**, go ahead.
(ii) Compute $RN_3 = D_E \oplus Hash(ID_C \| (SK_C \oplus RN_2))$.
(iii) Verify $Hash(RN_3 \oplus T_4) \stackrel{?}{=} M_1$. **If** the equation is established, go ahead. **Else**, **Output** 0.
(iv) Generate new numbers (RN_2^{new}, RN_3^{new}) and calculate $D_E^{new} = Hash(ID_C \| (SK_C \oplus RN_2^{new}))$ and $\overline{D}^{new} = Hash(\overline{D} \oplus RN_2^{new}) \oplus Hash(ID_C \| SK_C \oplus RN_3^{new})$.
(v) Calculate $M_2 = Hash(Hash(\overline{D} \oplus D_E^{new}) \oplus T_5)$ and $M_3 = Hash(Hash(\overline{D} \oplus \overline{D}^{new}) \oplus T_5)$.
(vi) Send $(RN_2^{new}, D_E^{new}, \overline{D}^{new}, M_2, M_3, T_5)$ to C.
(10) Upon the receipt of the message, C works as follows.
(i) **If** the timestamp T_5 is invalid, **Output** 0. **Else**, go ahead.
(ii) Calculate $Hash(Hash(D \oplus Hash(PW\prime \oplus RN_4) \oplus D_E^{new}) \oplus T_5) \stackrel{?}{=} M_2$ and
(iii) $Hash(Hash(D \oplus Hash(PW\prime \oplus RN_4) \oplus \overline{D}^{new}) \oplus T_5) \stackrel{?}{=} M_3$. **If** the two equations are established, then go ahead. **Else**, **Output** 0.
Generate RN_4^{new} and $D^{new} = Hash(D \oplus Hash(PW\prime \oplus RN_4) \oplus RN_2^{new}) \oplus \overline{D}^{new} \oplus Hash(PW\prime \oplus RN_4^{new})$.
(iv) Replace (D_E, D, RN_2, RN_4) with $(D_E^{new}, D^{new}, RN_2^{new}, RN_4^{new})$. **Output** 1.

Algorithm 1: Composable three-factor authentication.

cheat C without the secret parameters. Similarly, C runs the above two subprotocols of authentication when SR is 3.

6.1.3. Session Key Agreement. In the session key agreement phase, K_C sent to NRF and K_{NRF} sent to C are composed of the hashed authentication secret information and string generated by using the ECDH algorithm. Firstly, without biometrics Bio, password PW, or NRF's secret information RN_3, an adversary is unable to deduce aP or bP from K_{NRF} and K_C. Secondly, even if an adversary obtained the part of the user and NRF's data accidentally and calculated the correct aP and bP, he is unfeasible to compute the session key $Ks = abP$ since our proposed scheme is based on the elliptic curve Diffie–Hellman problem (ECDHP) and elliptic curve discrete logarithm problem (ECDLP).

6.2. Attack Analysis. The proposed scheme can resist several protocol attacks as follows.

6.2.1. Replay Attack. The attacker can disguise the previously transmitted message as a legitimate user and send it to the disguised user. By using the timestamp and the new nonce, our proposed scheme can resist replay attacks. Based on the timestamps and fresh nonces, the proposed scheme can defend against the replay attack. In Steps 1 to 6, C and NRF check the validity of the timestamp from the other side, and the attacker cannot forge the Tag or M_K without K_B and the private key SK_C. In addition, the random numbers RN_6 and Tag calculated with RN_6 are updated in each session. In Steps 8 to 10, the random numbers RN_2, RN_3, and RN_4 are used for authentication, which are updated at the end of each authentication protocol.

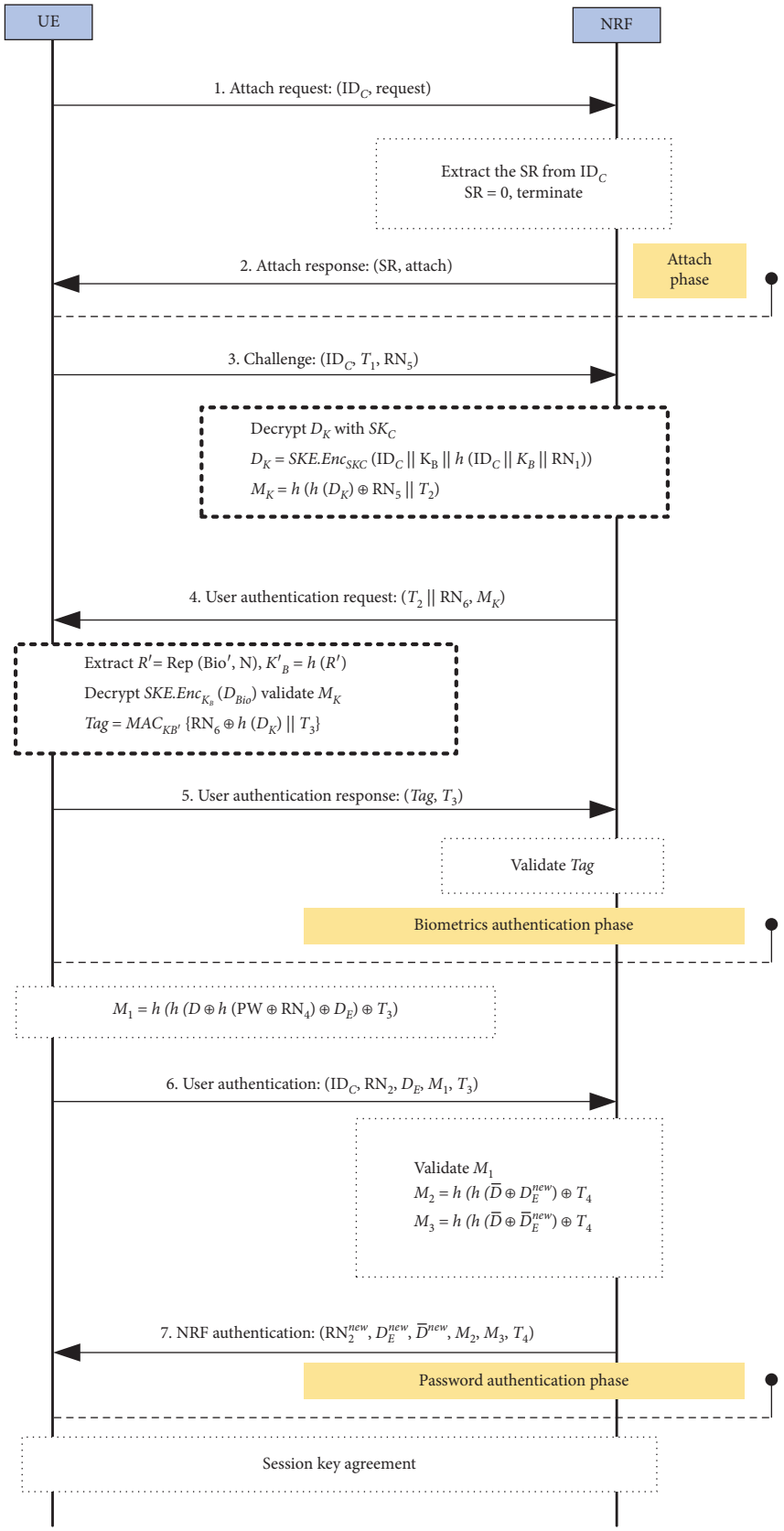

Figure 4: Authentication process.

Require: the user identity ID_C; the password $\mathrm{PW}\prime$; the biometric data $\mathrm{Bio}\prime$; the smart card.
Ensure: agreement result: Ks.
(1) NRF executes the following commands.
(i) Check the highest security level SR in the authentication process. **If** SR = 0, then **Output** 1, and **Terminate** the process. **Else**, go ahead.
(ii) Choose random number $a \in Z_n^*$.
(iii) Compute the secret auxiliary message $\mathrm{SM}_{\mathrm{NRF}}$
If SR = 1, then set
$\mathrm{SM}_{\mathrm{NRF}} = \mathrm{Hash}(\mathrm{ID}_C \| K_B \| \mathrm{RN}_6)$.
If SR = 2, then set
$\mathrm{SM}_{\mathrm{NRF}} = \mathrm{Hash}(\mathrm{Hash}(\mathrm{ID}_C \| \mathrm{SK}_C \oplus \mathrm{RN}_3^{\mathrm{new}}))$.
If SR = 3, then set
$\mathrm{SM}_{\mathrm{NRF}} = \mathrm{Hash}(\mathrm{ID}_C \| K_B \| \mathrm{RN}_6) \oplus \mathrm{Hash}(\mathrm{Hash}(\mathrm{ID}_C \| \mathrm{SK}_C \oplus \mathrm{RN}_3^{\mathrm{new}}))$.
(iv) Calculate $K_{\mathrm{NRF}} = \mathrm{SM}_{\mathrm{NRF}} \oplus aP$.
(v) Send K_{NRF} to C.
(2) Upon the receipt of the message, C works as follows.
(i) Choose random number $b \in Z_n^*$.
(ii) Compute the secret auxiliary message SM_C.
If SR = 1, then C sets
$\mathrm{SM}_C = \mathrm{Hash}(\mathrm{ID}_C \| K_B \| \mathrm{RN}_6)$.
If SR = 2, then C sets
$\mathrm{SM}_C = \mathrm{Hash}(D^{\mathrm{new}} \oplus \mathrm{Hash}(\mathrm{PW} \oplus \mathrm{RN}_4^{\mathrm{new}}))$.
If SR = 3, then C sets
$\mathrm{SM}_C = \mathrm{Hash}(\mathrm{ID}_C \| K_B \| \mathrm{RN}_6) \oplus \mathrm{Hash}(D^{\mathrm{new}} \oplus \mathrm{Hash}(\mathrm{PW} \oplus \mathrm{RN}_4^{\mathrm{new}}))$.
(iii) Calculate $K_C = \mathrm{SM}_C \oplus bP$.
(iv) Calculate $Ks = b(K_{\mathrm{NRF}} \oplus \mathrm{SM}_C)$.
(v) Send $(K_C, \mathrm{SKE.Enc}_{Ks}(aP))$ to NRF.
(3) Upon the receipt of the message, NRF works as follows.
(i) Calculate $Ks = a(K_C \oplus \mathrm{SM}_{\mathrm{NRF}})$.
(ii) Decrypt $\mathrm{SKE.Enc}_{Ks}(aP)$ with Ks. And if the decryption is aP, NRF confirms success.
(iii) Send $\mathrm{SKE.Enc}_{Ks}(bP)$ to C.
(4) C decrypts $\mathrm{SKE.Enc}_{Ks}(bP)$ with Ks. And if the decryption is bP, C confirms success, and the process terminates.

Algorithm 2: Session key agreement.

Require: the user identity ID_C; the password $\mathrm{PW}\prime$; the biometric data $\mathrm{Bio}\prime$; the smart card.
Ensure: update the result: 0 for failure; 1 for success.
(1) NRF and user C execute the mutual authentication process. The security level SR is set to 3. **If** the authentication failed, **Output** 0. Otherwise, go ahead.
(2) User C works as follows.
(i) Input new biometric data as same as those in the biometrics registration phase. The trusted device generates a new pair $(R^{\mathrm{new}}, N^{\mathrm{new}})$.
(ii) Calculate new $K_B^{\mathrm{new}} = \mathrm{Hash}(R^{\mathrm{new}})$.
(iii) Send $(\mathrm{SKE.Enc}_{Ks}(K_B^{\mathrm{new}}, N^{\mathrm{new}}))$, biometrics update request( ) to NRF.
(3) Upon the receipt of the message, NRF works as follows.
(i) Choose a new number $\mathrm{RN}_1^{\mathrm{new}}$ and encrypt K_B^{new} with SK_C by using SKE.Enc.
(ii) Calculate $D_K^{\mathrm{new}} = \mathrm{SKE.Enc}_{\mathrm{SK}_C}(\mathrm{ID}_C \| K_B^{\mathrm{new}} \| \mathrm{Hash}(\mathrm{ID}_C \| K_B^{\mathrm{new}} \| \mathrm{RN}_1^{\mathrm{new}}))$ and $\overline{D_K}^{\mathrm{new}} = (\mathrm{SKE.Enc}_{\mathrm{SK}_C}(K_B^{\mathrm{new}} \| \mathrm{RN}_1), \mathrm{ID}_C)$.
(iii) Set $D_{\mathrm{Bio}}^{\mathrm{new}} = (N^{\mathrm{new}}, D_K^{\mathrm{new}}, \mathbf{Hash}, \mathbf{Rep})$ and $\overline{D_{\mathrm{Bio}}}^{\mathrm{new}} = (N, \overline{D_K}^{\mathrm{new}}, \mathbf{Hash}, \mathbf{Rep})$
(iv) Store $\overline{D_{\mathrm{Bio}}}^{\mathrm{new}}$ in its database.
(v) Send $\mathrm{SKE.Enc}_{Ks}(D_K^{\mathrm{new}})$ to C.
(4) After receiving the message, C encrypts $D_{\mathrm{Bio}}^{\mathrm{new}}$ with K_B^{new} and stores in the smart card. And **Output** 1.

Algorithm 3: Biometrics update.

6.2.2. Forgery Attack. In our scheme, it is impossible for any attacker to forge the legal $M_K = \mathrm{Hash}(\mathrm{Hash}(D_K) \oplus \mathrm{RN}_5 \| T_2)$ without the secret key SK_C. Moreover, the calculation results of M_2 and M_3 need to use secret parameters SK_C and RN_3 kept secretly by NRF. According to the irreversibility of one-way hash function, it is too hard for any attacker to recover one of SK_C and RN_3 from the public parameters. The attacker has $\mathrm{ID}\prime$ which is not ID_C and hopes to deduce the

Require: the user identity ID_C; the password $PW\prime$; the biometric data $Bio\prime$; the smart card.
Ensure: update the result: 0 for failure; 1 for success.
(1) NRF and user C execute the mutual authentication process. The security level SR is set to 3. **If** authentication failed, **Output** 0. Otherwise, go ahead.
(2) User C works as follows.
(i) Choose a new password PW^{new}, and the smart card generates new RN_4^{new} to compute $M_{PU} = \text{Hash}(D \oplus \text{Hash}(PW \oplus RN_4) \oplus RN_2) \oplus \text{Hash}(PW^{new} \oplus RN_4^{new})$.
(ii) Send $(\text{SKE.Enc}_{Ks}(M_{PU})$, password update request$(\,)$ to NRF.
(3) Upon the receipt of the message, NRF works as follows.
(i) Derive $\text{Hash}(PW^{new} \oplus RN_4^{new})$ from $M_{PU} \oplus \text{Hash}(\text{Hash}(ID_C \| SK_C \oplus RN_3) \oplus RN_2)$.
(ii) Choose RN_2^{new} as well as RN_3^{new}, and calculate $\overline{D}^{new} = \text{Hash}(\text{Hash}(ID_C \| SK_C \oplus RN_3) \oplus RN_2^{new}) \oplus \text{Hash}(PW^{new} \oplus RN_4^{new}) \oplus \text{Hash}(ID_C \| SK_C \oplus RN_3^{new})$.
(iii) Calculate $D_E^{new} = \text{Hash}(ID_C \| SK_C \oplus RN_2^{new}) \oplus RN_3^{new})$.
(iv) Send $\text{SKE.Enc}_{Ks}(RN_2^{new}, D_E^{new}, \overline{D}^{new})$ to C.
(4) Upon the receipt of the message, C computes $D^{new} = \text{Hash}(D \oplus \text{Hash}(PW \oplus RN_4) \oplus RN_2^{new}) \oplus \overline{D}^{new}$.
(5) C and NRF store D^{new}, D_E^{new}, and $\overline{D}^{new}$ to replace the old information. And **Output** 1.

Algorithm 4: Password update.

Require: the user identity ID_C; the session key Ks; the smart card .
Ensure: authorization result: 0 for failure; 1for success.
(1) **If** user C holds a valid token for his desirable service, then go to Step 5. Otherwise, go ahead.
(2) User C and NRF execute the proposed authentication mechanism as mentioned above. **If** the authentication failed or key agreement failed, **Output** 0. Otherwise, go ahead.
(3) User C sends the service authorization request $M_{RS} = (ID_C, \text{Service Request})$.
(4) Upon the receipt of the message, NRF works as follows.
(i) Confirm SR of the service authorization request is less than SR in the authentication process. **If** SR of the service authorization request is bigger than SR in the authentication process, then go to Step 2. **Else**, go ahead.
(ii) Generate $\text{Token}_C = \text{Sign}_{SK_{NRF}}(ID_C, NF_h, K_{Ch}, SR, T_5, \text{lifetime})$.
(iii) Send $\text{SKE.Enc}_{Ks}(\text{Token}_C, NF_h, K_{Ch})$ to user C (the message is not encrypted when SR = 0). Suppose that NRF has told NF_h the session key K_{Ch} between NF_h and C securely after the NF discovery process described in [24] is executed.
(5) User C sends $\text{SKE.Enc}_{K_{Ch}}(\text{Token}_C, ID_C)$ to the service producer NF_h.
(6) NF_h verifies Token_C through NRF. **If** the validation failed, **Output** 0. Otherwise, go ahead.
(7) NRF informs the verification result to the service producer NF_h.
(8) NF_h sends a service response to C and executes requested services if the token has been successfully verified. **Output** 1.

Algorithm 5: Service authorization.

authentication information from M_1, for instance, the password of C in another. The attacker has to find an integer i' in which $i \neq i'$ satisfying that

$$\text{Hash}(ID' \oplus PW \oplus i') = \text{Hash}(ID_C \oplus PW \oplus i), \quad (5)$$

which is impossible due to the collision resistance of hash function. In the biometric authentication, an adversary cannot obtain the correct biometric data to generate K_B and achieve the response challenge.

6.2.3. Man-in-the-Middle Attack. In the session key agreement phase, if the attacker hijacks and forges the agreement message between the NRF and user after the authentication phase, the attacker may make man-in-the-middle attack. In the proposed scheme, aP is hidden by the use of $\text{Hash}(ID_C \| K_B \| RN_6))$ or $\text{Hash}(\text{Hash}(ID_C \| SK_C \oplus RN_3^{new}))$, and bP is also hidden by the use of $\text{Hash}(ID_C \| K_B \| RN_6))$ or $\text{Hash}(D^{new} \oplus \text{Hash}(PW \oplus RN_4^{new}))$. The attacker cannot drive the middle key taP and tbP from the transmitted messages K_C and K_{NRF} over the public channel without possessing the secret K_B, password, and RN_3.

In addition, there are some other attacks aimed at password/smart card authentication protocol. We proved the proposed scheme can resist the following attacks.

6.2.4. Stolen Smart Card Attack. When the smart card of a valid user is hijacked by an attacker, first case, even if an attacker obtains a smart card, he cannot guess the password from $D = \overline{D} \oplus \text{Hash}(PW \oplus RN_4)$ in D_C owing to using one-way hash function. In addition, the biometric information is not stored in the smart card in the plaintext but protected and encrypted with K_B. To gain the biometric information, the attacker requires to record the biometric information immediately to finish the authentication. To sum up, it is unable for any attacker to complete the authentication when the security level is greater than 0.

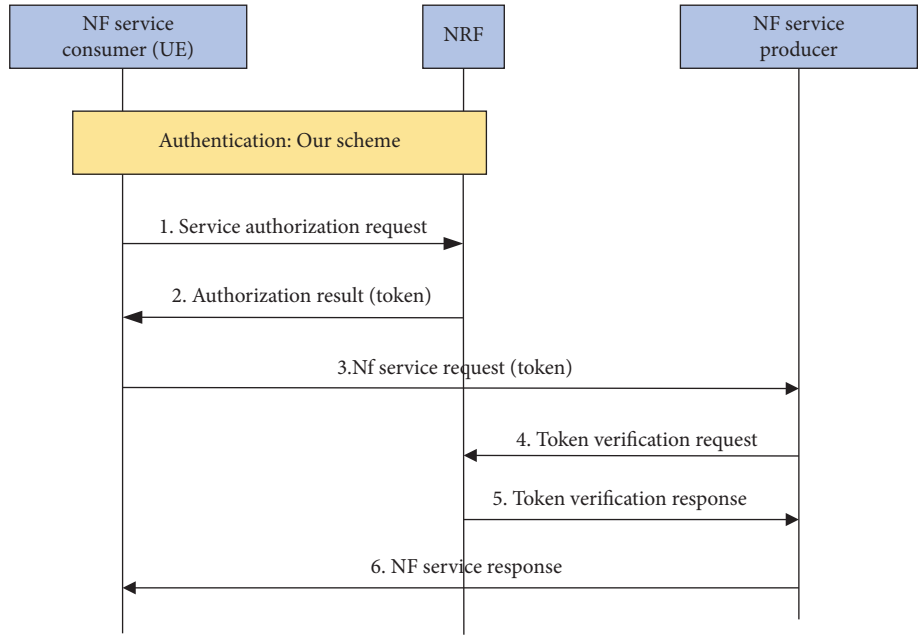

Figure 5: Service authorization of 5G SBA.

We summed up the proposed scheme and other related schemes for the protocol security properties. Table 2 shows several important security properties of our scheme, scheme in [10], and the standard mechanism proposed by the 3GPP committee including EAP-AKA (marked as AKA) and EAP-TLS (marked as TLS).

6.3. Scyther Simulation. The formal verification tool Scyther [25] is employed to verify security simulation analysis of our proposed scheme. Scyther is a tool which can be used to find problems that arise from the way the protocols are constructed and support multiprotocol parallel analysis. Scyther tool has a clear description of the state set trajectory. Based on the model improvement algorithm, Scyther is conveniently used to protocol attack search, role execution, and security proof. Scyther uses a set of claims to represent many security goals such as secrecy and several authentications including aliveness, weak agreement, agreement, and synchronization. Secret claim is used to mean confidentiality and expresses that certain information is not revealed to an adversary, even though these data are communicated over an untrusted network. In order to provide different degrees of authentication strength, several forms of authentication claims including Alive, Weakagree, Niagree (noninjective agree), and Nisynch (noninjective synchronization) are employed to detect potential protocol attacks such as replay, reflection, and man-in-the-middle attacks. For a detailed description of the formal definition of all Scyther claims, please see [26].

In our proposed scheme, there are two main roles: UE and NRF; they represent the user C's equipment and network repository function NRF, respectively. Since the register of our proposed protocol is supposed to be secure, we only consider the three-factor authentication and session key agreement phase. We structure the proposed scheme in the Security Protocol Description Language (SPDL) to describe and analyze protocols and specify the security properties of our proposed scheme by a series of claims of Scyther as shown in Figure 6. Here, the Dolev–Yao intruder model is employed in which the attacker can completely control the network and conduct a series of attacks to be the implementation scenario of the proposed scheme. According to Figure 6, our scheme successfully makes certain all Scyther secrecy and authentication claims; moreover, there are no attacks found under the verification of the Scyther tool.

6.4. Authentication Proof Using BAN Logic. We use the BAN logic [27] to prove the security of our proposed protocol. By our proposed scheme, the authentication and session key process when SR = 3 is composed of the biometrics and smart card authentication (SR = 1) and password and smart card authentication process (SR = 2) as shown in Section 4. Therefore, if both the biometrics authentication and password authentication process are demonstrated to achieve security goals, the complete authentication process (SR = 3) can also be proven to achieve security goals obviously. Consequently, we mainly demonstrate the security of the biometrics and smart card authentication process and password and smart card authentication process, respectively.

6.4.1. Biometrics and Smart Card Authentication. According to the analytic procedures of the BAN logic, the biometrics and smart card authentication protocol must satisfy the following goals:

Table 2: Comparison of security properties.

	Yu et al. [10]	AKA	TLS	Ours
Mutual authentication	Y	Y	Y	Y
Multifactor authentication	Y	N	N	Y
Key agreement	N	Y	Y	Y
Authorization	N	N	N	Y
Composability resisting	Y	N	N	Y
Protocol attack resisting	Y	N	N	Y
Dictionary attack resisting	N	—	—	Y
Stolen smart card attack	Y	N	N	Y

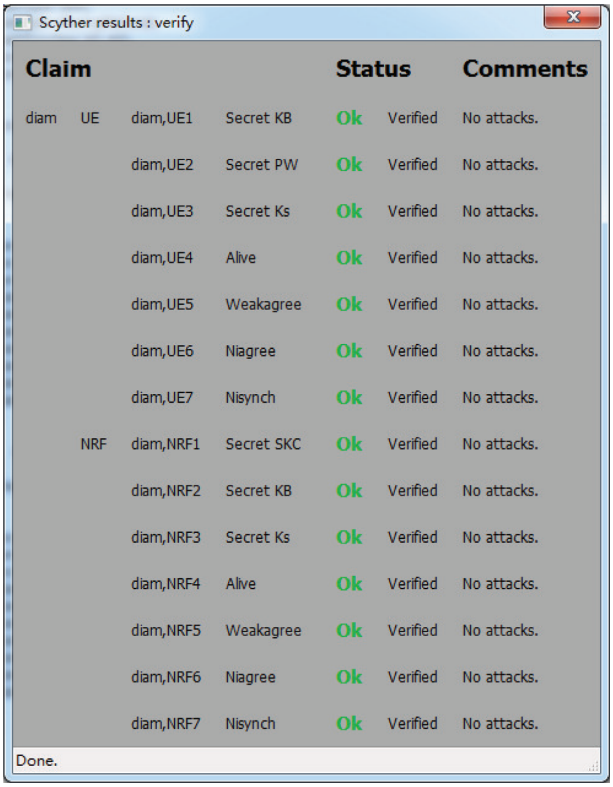

Figure 6: Formal verification results under the test of the Scyther tool.

(i) Goal 1. $C| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$
(ii) Goal 2. $\mathrm{NRF}| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$
(iii) Goal 3. $C| \equiv \mathrm{NRF}| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$
(iv) Goal 4. $\mathrm{NRF}| \equiv C| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$

Firstly, the protocol is described in the following idealized form:

(i) Msg 1. $\mathrm{NRF} \longrightarrow C$: $\{aP\}_{\langle K_B \rangle_{RN_6}}$
(ii) Msg 2. $C \longrightarrow \mathrm{NRF}$: $(\{bP\}_{\langle K_B \rangle_{RN_6}}, \{aP\}_{Ks})$, where $Ks = abP$
(iii) Msg 3. $\mathrm{NRF} \longrightarrow C$: $\{bP\}_{Ks}$

Secondly, we make the following initial status and hypotheses:

(i) A1. $\mathrm{NRF}| \equiv \sharp(a)$
(ii) A2. $C| \equiv \sharp(b)$
(iii) A3. $\mathrm{NRF}| \equiv C| \Rightarrow b$
(iv) A4. $C| \equiv \mathrm{NRF}| \Rightarrow a$
(v) A5. $\mathrm{NRF}| \equiv (\mathrm{NRF} \overset{K_B}{\leftrightarrow} C)$
(vi) A6. $C| \equiv (\mathrm{NRF} \overset{K_B}{\leftrightarrow} C)$

Based on the assumptions and the rules of the BAN logic, the proofs are presented as follows.

According to Msg 1, we have

$$C \triangleleft \{aP\}_{\langle K_B \rangle_{RN_6}}. \tag{6}$$

Before the key agreement process, user C has verified the NRF's signature by using the public key of NRF. With the successful confirmation, A6, and the message-meaning rule, we can derive

$$C| \equiv \mathrm{NRF}| \sim \{aP\}. \tag{7}$$

Based on the random number and freshness rule, A1, and A4, we can derive

$$C| \equiv \sharp\{aP\}. \tag{8}$$

Based on the nonce verification rule, we can derive

$$C| \equiv \mathrm{NRF}| \equiv \{aP\}. \tag{9}$$

According to A4 and the jurisdiction rule, we can derive

$$C| \equiv \{aP\}. \tag{10}$$

C can compute $Ks = b * aP$, and according to the belief rule, we can derive Goal 1:

$$C| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C). \tag{11}$$

Equally, according to Msg 2 and the same deductions, we can derive Goal 2. From Msg 3, we have

$$C \triangleleft \{bP\}_{Ks}. \tag{12}$$

According to Goal 1 we have proved and the message-meaning rule, we can derive

$$C| \equiv \mathrm{NRF}| \sim \{bP\}. \tag{13}$$

Based on A2, the random number and freshness rule, and the nonce verification rule, we can derive

$$C| \equiv \mathrm{NRF}| \equiv \{bP\}. \tag{14}$$

According to $C| \equiv \mathrm{NRF}| \equiv \{aP\}$ and the belief rule, we can derive Goal 3:

$$C| \equiv \mathrm{NRF}| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C). \tag{15}$$

Equally, according to Msg 2 and the same deductions, we can derive Goal 4.

6.4.2. Password and Smart Card Authentication. According to the analytic procedures of the BAN logic, the password and smart card authentication protocol must satisfy the following goals:

(i) Goal 1. $C| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$
(ii) Goal 2. $\mathrm{NRF}| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$
(iii) Goal 3. $C| \equiv \mathrm{NRF}| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$
(iv) Goal 4. $\mathrm{NRF}| \equiv C| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C)$

Again, the protocol is described in the following idealized form:

(i) Msg 1. $\mathrm{NRF} \longrightarrow C$: $\{aP\}_{h(h(\mathrm{ID}_C \| \mathrm{SK}_C \oplus \mathrm{RN}_3^{\mathrm{new}}))}$
(ii) Msg 2. $C \longrightarrow \mathrm{NRF}$: $(\{bP\}_{h(D^{\mathrm{new}} \oplus h(\mathrm{PW} \oplus \mathrm{RN}_4^{\mathrm{new}}))}, \{aP\}_{Ks})$, where $Ks = abP$
(iii) Msg 3. $\mathrm{NRF} \longrightarrow C$: $\{bP\}_{Ks}$

In the same way, we make the following initial status and hypotheses:

(i) A1. $\mathrm{NRF}| \equiv \sharp(a)$
(ii) A2. $C| \equiv \sharp(b)$
(iii) A3. $\mathrm{NRF}| \equiv C| \Rightarrow b$
(iv) A4. $C| \equiv \mathrm{NRF}| \Rightarrow a$
(v) A5. $\mathrm{NRF}| \equiv (\mathrm{NRF} \overset{K_P}{\leftrightarrow} C)$
(vi) A6. $C| \equiv (\mathrm{NRF} \overset{K_P}{\leftrightarrow} C)$

Specifically, K_P is defined by the use of the sharing secret between NRF and C, $K_P = h(D^{\mathrm{new}} \oplus h(\mathrm{PW} \oplus \mathrm{RN}_4^{\mathrm{new}})) = h(h(\mathrm{ID}_C \| \mathrm{SK}_C \oplus \mathrm{RN}_3^{\mathrm{new}}))$.

According to Msg 1, we have

$$C \triangleleft \{aP\}_{h(h(\mathrm{ID}_C \| \mathrm{SK}_C \oplus \mathrm{RN}_3^{\mathrm{new}}))}. \tag{16}$$

This is the equivalent as follows:

$$C \triangleleft \{aP\}_{K_P}. \tag{17}$$

Before the key agreement process, user C has verified the NRF by using the secret information RN_3. With the successful confirmation, A6, and the message-meaning rule, we can derive

$$C| \equiv \mathrm{NRF}| \sim \{aP\}. \tag{18}$$

Based on the random number and freshness rule, A1, and A4, we can derive

$$C| \equiv \sharp\{aP\}. \tag{19}$$

Based on the nonce verification rule, we can derive

$$C| \equiv \mathrm{NRF}| \equiv \{aP\}. \tag{20}$$

According to A4 and the jurisdiction rule, we can derive

$$C| \equiv \{aP\}. \tag{21}$$

C can compute $Ks = b * aP$, and according to the belief rule, we can derive Goal 1:

$$C| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C). \tag{22}$$

Equally, according to Msg 2 and the same deductions, we can derive Goal 2.

From Msg 3, we have

$$C \triangleleft \{bP\}_{Ks}. \tag{23}$$

Based on Goal 1 we have proved and the message-meaning rule, we can derive

$$C| \equiv \mathrm{NRF}| \sim \{bP\}. \tag{24}$$

According to A2, the random number and freshness rule, and the nonce verification rule, we can derive

$$C| \equiv \mathrm{NRF}| \equiv \{bP\}. \tag{25}$$

From $C| \equiv \mathrm{NRF}| \equiv \{aP\}$ and the belief rule, we can derive Goal 3:

$$C| \equiv \mathrm{NRF}| \equiv (\mathrm{NRF} \overset{Ks}{\leftrightarrow} C). \tag{26}$$

Equally, according to Msg 2 and the same deductions, we can derive Goal 4.

7. Performance Analysis

This section evaluates the performance of our proposed scheme including the efficiency parameters' computational cost, storage cost, and communication cost by comparing our proposed scheme with the effective three-factor authentication scheme in [10] and the current 3GPP standard [5]. Since the 3GPP committee employs the Extensible Authentication Protocol (EAP) as the identity authentication architecture to achieve the user authentication for services and applications, we mainly compare our proposed scheme with the typical EAP including EAP-AKA and EAP-TLS to evaluate the performance.

Without loss of generality, we set that the system adopts AES as the symmetric encryption algorithm and elliptic curve digital signature (ECDSA) as the digital signature algorithm. Meanwhile, both ID and PW are 128 bits in length. We assume the request and response information is 16 bits (2 bytes). To achieve the same security level with AES 128 bits, we assume that the key size for algorithms based on ECC is 256 bits [28]. Moreover, the output of the hash function is 128 bits, the length of the random number is 128 bits, and the size of the timestamp is 32 bits [29].

On the computational cost, we mainly refer to the time consumed by each cryptographic algorithm or operation including the hash operation N_h, symmetric encryption (or decryption) operation SKE, digital signing operation Sign, and verification operation SigVer, respectively. We test the above operations or algorithms on a laptop PC with Intel (R) Core i5-4210U 1.70 GHz CPU as a server and Huawei Mate 40 device with Kirin 9000 5G SOC 3.13GHZ processor as a client by using the Eclipse Java IDE. The testing results are shown in Table 3. Table 4 shows the comparison of the computational cost of related schemes. According to Table 4, our scheme outperforms the scheme in [10] and EAP-TLS. When SR = 3, the computational cost of our scheme is little larger than that in EAP-AKA for flexibility and security.

On the storage cost, the client has to preserve (D_{Bio}, D_C) stored in the smart card. The total storage overheads of related schemes are shown in Table 5. From Table 5, the overall storage overhead of our proposed scheme is lower than that of EAP-TLS, which is little larger than that of EAP-AKA and the scheme in [10]. Some additional overheads are involved because of the multifactor authentication and protocol flexibility.

On the communication overhead, our complete authentication protocol runs 4 message exchanges. According to the size of all of interaction messages, we compared the communication overhead in each security level of the proposed scheme with the scheme in [10], EAP-AKA, and EAP-TLS as shown in Table 6. From Table 6, the communication cost of our scheme is major observable better than that of the scheme in [10] and EAP-TLS, which is little larger than that of the EAP-AKA.

Performance with attacks: we analyze the performance of our proposed protocols when there are unknown attacks or uncertain attacks. We do not know when the unknown/uncertain attacks occur either. To be precise, we assume that the probability of unknown attacks occurred in the i step is $(1/n_{\text{msg}})$, where n_{msg} is the number of signal messages in one execution of protocols. Considering the consistency, we elaborately evaluate the authentication computational cost of our scheme when the attacks occur, and other performance evaluations with attacks are the same as that of the computational cost. We define an instability index ISI to evaluate the influence of performance with attacks for one success execution of the protocol, which is described as follows, where C_i represents the total computational cost before the attack occurs in the i step and C_{scs} shows the total computational cost for one success execution of the protocol with no attack.

$$\text{ISI} = \frac{p \times \sum_{i=1}^{n_{\text{msg}}} \left(1/n_{\text{msg}}\right) C_i + (1-p) \times C_{\text{scs}}}{(1-p) \times C_{\text{scs}}}. \tag{27}$$

For our proposed protocol when SR is 0, 1, 2, and 3, respectively, ISIs are shown as follows:

$$\begin{aligned} \text{ISI}_{\text{SR0}} &= 1, \\ \text{ISI}_{\text{SR1}} &= \frac{221726p}{1285355(1-p)} + 1, \\ \text{ISI}_{\text{SR2}} &= \frac{227061p}{1801044(1-p)} + 1, \\ \text{ISI}_{\text{SR3}} &= \frac{889481p}{4951324(1-p)} + 1. \end{aligned} \tag{28}$$

For the scheme in [10],

$$\text{ISI}_{Yu} = \frac{97468738p}{199161000(1-p)} + 1. \tag{29}$$

For the scheme in EAP-AKA,

$$\text{ISI}_{\text{AKA}} = \frac{685695p}{8526625(1-p)} + 1. \tag{30}$$

For the scheme in EAP-TLS,

$$\text{ISI}_{\text{TLS}} = \frac{4533024p}{9151771(1-p)} + 1. \tag{31}$$

Figure 7 shows the result of instability index ISI of different security-level authentication process and other related schemes. According to Figure 7, no matter what SR is, our scheme outperforms the scheme in [10] and EAP-TLS even if there are some unknown attacks occurred. However, the instability index of our scheme is little higher than that of EAP-AKA due to the introduction of the multiple authentication factors of the proposed scheme. ISI of different security levels in our scheme is close to each other, and it is a good sign that the computation overheads of the three authentication phases are evenly distributed. Therefore, our scheme has better performance under the unknown attacks.

Based on the above results of comparison and analysis, our scheme outperforms the scheme in [10] and EAP-TLS in terms of computation cost, communication overhead, and stability under unknown attacks without the loss of flexibility and security. Our proposed scheme requires more

Table 3: Computational cost of the cryptography operations (μs).

Operation	Symbol	Client	Server
Hash	N_h	21.9	0.429
Symmetric encryption	SKE	36.7	0.713
Digital signing	Sign	7755.6	102
Signing verification	SigVer	11919.1	173.4

Table 4: Computational cost (μs).

	Client	Server
Ours:SR = 0	0	0
Ours:SR = 1	$5N_h$ + 1SKE= 146.2	$5N_h$ + 2SKE= 3.571
Ours:SR = 2	$12N_h$ = 262.8	$9N_h$ = 3.861
Ours:SR = 3	$17N_h$ + 1SKE= 409	$14N_h$ + 2SKE= 7.432
Yu et al. [10]	$3N_h$ + 1SigVer+1SKE + 2Sign= 27532.7	$4N_h$ + 2SigVer+1SKE + 1Sign= 451.2
EAP-AKA	5SKE = 183.5	5SKE = 3.565
EAP-TLS	$4N_h$ + 1SignVer+2SKE= 12080.1	$4N_h$ + 1SignVer+2SKE= 176.542

Table 5: Storage cost (bytes).

	Client	Server
Memory contents	D_{Bio}, D_C	$\overline{D_{\text{Bio}}}, D_C$
Storage space in ours	134	134
Storage space in [10]	80	96
Storage space in EAP-AKA	32	32
Storage space in EAP-TLS	480	480

Table 6: Communication overhead (bytes).

Task	Rounds	Overhead
Ours:SR = 0	2	18 + 2 = 20
Ours:SR = 1	5	20 + 36 + 36 + 20 = 112
Ours:SR = 2	4	20 + 68 + 84 = 172
Ours:SR = 3	7	20 + 92 + 152 = 264
Yu et al. [10]	5	558
EAP-AKA	5	76
EAP-TLS	10	986

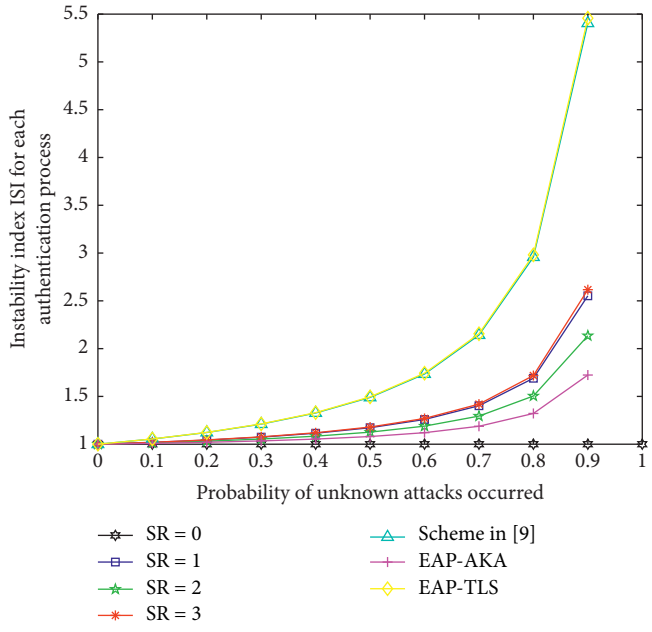

Figure 7: Comparison of the ISI of the authentication protocols.

storage than EAP-AKA and the scheme in [10] because of the composability of the authentication process. The overall performance of our scheme is worse than the EAP-AKA's; however, the proposed scheme can achieve more types of security properties, such as multifactor authentication, protocol composability, and resisting protocol attacks.

8. Conclusions

This paper presents an efficient and dynamically composable service authentication and authorization mechanism in 5G multiservice systems. By integrating and utilizing three authentication factors subtly, our proposed scheme is able to achieve four security intensities for different 5G application scenarios as well as session key agreement independently, and that greatly reduces system complexity. Based on the 3GPP SBA and our proposed protocol, we design an authorization process to implement service access control. We have corroborated that the proposed mechanism can achieve the ideal efficiency, meanwhile, realize the mutual authentication and service authorization, and resist the password guessing attack, stolen smart card attack, and existing protocol attacks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key R&D Program of China (no. 2017YFB0802700), the National Natural Science Foundation of China (nos. U1836203 and 61772404), and the Key Research and Development Program of Shaanxi (no. 2020ZDLGY08-08).

References

[1] P. Agyapong, M. Iwamura, D. Staehle, W. Kiess, and A. Benjebbour, "Design considerations for a 5G network architecture," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 65–75, 2014.

[2] C. Kalogiros, G. Zois, G. Darzanos et al., "The potential of 5G experimentation-as-a-service paradigm for operators and vertical industries: the case of 5G-VINNI facility," in *Proceeding of the IEEE 5G World Forum*, pp. 327–352, Dresden, Germany, November 2019.

[3] J. Cao, M. Ma, H. Li et al., "A survey on security aspects for 3GPP 5G networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 170–195, 2020.

[4] L. Wu, X. Du, and J. Wu, "Effective defense schemes for phishing attacks on mobile computing platorms," *IEEE Transactions on Vehicular Technology*, vol. 65, no. No. 8, pp. 6678–6691, 2016.

[5] ETSI, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Aspects; Study one Security Aspects of the 5G Service Based Architecture (SBA)*, ETSI, Sophia Antipolis, France, 2020.

[6] Y. Luo, J. Cao, M. Ma et al., "DIAM: Diversified identity authentication mechanism for 5G multi-service system," in *Proceeding of International Conference on Computing, Networking and Communications*, pp. 1–8, Honolulu, HI, USA, April 2019.

[7] D. He, "An effientient remote user authentication and key agreement protocol for mobile client-server environment from pairing," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1009–1016, 2012.

[8] J. Ni, X. Lin, and X. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE Journal of Selected Areas in Communications*, pp. 1–14, 2018.

[9] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of things," *IEEE Access*, vol. 8, pp. 67555–67571, 2020.

[10] J. Yu, G. Wang, Y. Mu, and W. Gao, "An efficient generic framework for three-factor Authentication with provably secure instantiation," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2302–2313, 2014.

[11] M. A. Nematollahi, H. Gamboa-Rosales, F. J. Martinez-Ruiz, J. I. D. L. Rosa-Vargas, S. A. R. Al-Haddad, and M. Esmaeilpour, "Multi-factor Authentication model based on multipurpose speech watermarking and online speaker recognition," *Multimedia Tools & Applications*, vol. 76, no. 5, pp. 1–31, 2017.

[12] D. Wang and P. Wang, "Two birds with one stone: two-factor Authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[13] C. Wang and G. Xu, "Cryptanalysis of three password-based remote user authentication schemes with non-tamper-resistant smart card," *Security and Communication Networks*, vol. 2017, no. 3, Article ID 1619741, 2017.

[14] S. Shin and T. Kwon, "A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes," *Sensors*, vol. 19, no. 9, 2012.

[15] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust multi-factor Authentication for fragile communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568–581, 2014.

[16] C. C. Lee, T. H. Lin, and R. X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using cards," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13863–13870, 2011.

[17] X. Li, Y. Xiong, J. Ma, and W. Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 763–769, 2012.

[18] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractor: how to generate strong keys from biometrics and other noisy data," *Proceeding of EUROCRYPT Lecture Notes in Computer Science*, vol. 3027, pp. 529–551, 2004.

[19] ETSI, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Architecture and Procedures for 5G System*, ETSI, Sophia Antipolis, France, 2020.

[20] J. Arkko and H. Haverinen, "Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA)," *IETF RFC*, vol. 4187, 2006.

[21] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS authentication protocol," *IETF RFC*, vol. 5216, 2008.

[22] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," *Lecture Notes in Computer Science*, Springer, Berlin, Germany, pp. 453–474, 2001.
[23] Y. Cheng, X. Fu, X. Du, B. Luo, and M. Guizani, "A lightweight live memory forensic approach based on hardware virtualization," *Information Sciences*, vol. 379, pp. 23–41, 2017.
[24] "3rd generation partnership project; technical specification group services and system Aspects; procedures for the 5G system," *3GPP TS*, vol. 23, 2020.
[25] C. Cremers, *The Scyther Tool*, University of Oxford, Department of Computer Science, Oxford, UKhttp://www.cs.ox.ac.uk/people/cas.cremers/scyther.
[26] C. Cremers, *Scyther-Semanticas and Verification of Security Proocols*, Ph.D.dissertation, Eindhoven University of Technology, Institute for Programming research and Algorithmics, Eindhoven, Netherlands, 2006.
[27] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.
[28] National Institute of Standards and Technology, *Special Publication 800-57: Recommendation for Key Management Paet 1: General (Revision 4)*, National Institute of Standards and Technology, Gaithersburg, MA, USAhttps://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf.
[29] National Institute of Standards and Technology, *Special Publication 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revision 2)*, National Institute of Standards and Technology, Gaithersburg, MA, USA, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf.