2024 International Conference on Networking and Network Applications (NaNA) | 979-8-3503-7677-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/NaNA63151.2024.00077

UE-detectable Authentication and Key Agreement Method Resisting Serving Network Forging

Jia Cao
Shanghai Jiao Tong University
Shanghai, China
Email: cj2000@sjtu.edu.cn

Jiayue Zhou
Shanghai Jiao Tong University
Shanghai, China
Email: balala@sjtu.edu.cn

Jianan Hong
Shanghai Jiao Tong University
Shanghai, China
Email: hongjn@sjtu.edu.cn

***Abstract*—The authentication protocol is important for secure mobile communication. To resist the threat of false base station or serving network in the Fifth generation (5G) network, the 3GPP Group has standardized the 5G AKA scheme, which leveraged the serving network name ($SNname$) to validate the identity of the network. However, according to existing work that analyzed the 5G authentication, the security requirement of implicit authorization of the serving network by the user equipment (UE) is not satisfied. The basic problem is that the $SNname$ check is done by the home network, rather than the UE. Due to the problem, the UE cannot detect the false serving network in the authentication phase, which may result in security threats in some emergent cases. Current repairs on this problem cannot work on the existing 5G/6G architectures, as they require a procedure redesign for the USIM module. This paper hence proposes a new authentication and key agreement (AKA) protocol, which lets UE detect the false serving network name directly from the MAC (one information element in legacy AKA), but without any modification of the USIM procedure. To realize the above effect, the most important mechanism in our scheme is to embed the SNname to the random nonce before the USIM procedure. Such slight and extremely lightweight modifications strongly bind the MAC with the claimed serving network name. Further security analysis shows that the proposed scheme is secure, especially against the attack of a false serving network.**

***Index Terms*—5G AKA, false serving network, SNname, random nonce**

I. Introduction

Nowadays, the mobile communication system, with its anytime and anywhere connectivity feature, has become an integral part of daily activities [1]. The popularity of smartphones has further expanded the range of applications for this technology. Evolved from 2G to 3G and then to 4G, the development and advancement of the technology has been driven by the increasing variety and requirements of supported mobile network services [2]. Today, a vast array of network services, including high-definition video streaming, the Internet of Things (IoT), mobile healthcare, and telecommunications, are in high demand for fast yet ubiquitous networks. Therefore, 5G, the next generation of mobile telecommunication networks, must offer greater capacity, higher speeds, greater dynamism, and highly secure connectivity than any previous generation has provided.

Considering the demand for connectivity that the 5G standard has to cope with, the 5G document has placed much importance on privacy and security [3], and one important issue among others is the malicious serving networks (SN) that users may encounter in roaming [2]. Therefore it is important to assure the security properties of the AKA protocol, which is responsible for the authentication between the subscriber and the serving network, and key establishment between the two. To prevent identity fraud of malicious SNs, the idea of binding network (SNid) to the key generation was adopted in 4G's EPS-AKA. In the 5G AKA document, the serving network name ($SNname$) is used in the authentication and derivation of the anchor key. Apart from that, 5G requires an additional transmission round for the confirmation between SN and the home network (HN). In this way, in the HN's sight, the SN can no longer pretend others' names [4].

Yet problems still exist in the authentication of the SN from the subscriber's point of view. A formal analysis of version v15.1.0 for Release 15 has been conducted in [5]. The evaluation studies weaknesses and security concerns in the protocol using Tamarin Prover, a tool for formal verification. As is pointed out in [5], the UE authenticates the SN identifier through an "implicit key authentication" [6]. In other words, the verification of SN's identity by the user equipment (UE) is handed over from the authentication phase to subsequent communications between UE and SN. If there's no problem in subsequent communication, the UE will consider that the SN has obtained the same anchor key from the HN, which indicates that the HN has authenticated the SN's identity. Such an approach is risky since there's no specification in the 5G document concerning the type of subsequent communication. The SNs may initiate dangerous actions or communications that don't require the anchor key, arousing security concerns.

In the latest version v15.4.0 of Release 15, modifications were added to the authentication procedure: for example, the HN sends the anchor key K_{SEAF} to the SEAF in SN only after confirmation of successful authentication. But the previous problem remains unsolved. The authors of [7] themselves propose either to bind the authentication message to the SN's identifier or to add a message flow from the SN for key confirmation.

Their solution is straightforward but hard to adopt since the MAC validation is executed in the USIM module, in addition, we want to make as few changes to the protocol flow as possible. As will be discussed later in Section III, the USIM module is difficult to exchange, taking into account the compatibility

979-8-3503-7677-7/24/$31.00 ©2024 IEEE
DOI 10.1109/NaNA63151.2024.00077

for legacy subscribers before 5G. Such compatibility will also affect the future security protocol design, such as 6G.

Faced with this technical problem, in this paper, we propose a new AKA protocol for future mobile communication. Without any modification USIM procedure, including the algorithm, input, or output interfaces, the user can detect whether the relevant SNname is validated before its verification to the network is completed. The modification is lightweight and brings in quite a slight protocol evolution for the legacy system. The security analysis indicates that the seemingly adventurous scheme shows a significant advantage in security.

The main contribution of this paper can be summarized as follows:

1) We study the malicious SN problem from 5G and define the non-modification for the USIM procedure in solving the problem.
2) We propose a new AKA protocol to fix the UE's authentication to the serving network without any modification of USIM, thus showing its advantage in compatibility. The scheme is also the first in academia to our best knowledge.

II. Related Work

Recent years have witnessed substantial advancements in the domain of wireless communication, notably transitioning from 1G to 5G technologies [8]. Presently, over 5.4 billion mobile users connect to networks through their USIM cards [9], benefiting from robust security measures designed to protect user data confidentiality (such as voice communications and SMS). These security protocols ensure that subscribers are accurately billed for the services they use while safeguarding them against threats posed by malicious base stations and other adversarial elements.

Security mechanisms should be designed to achieve mutual authentication of subscribers and their carriers, as well as to establish a secure channel to protect communications[5]. Since the 3G generation, the Authentication and Key Agreement (AKA) protocol has been a standardized method developed by 3GPP to facilitate this process [10]. These protocols are designed to ensure mutual authentication between subscribers and HNs, and to enable the establishment of a session key between subscribers and SNs [7]. Security measures have been significantly strengthened in the transition to 4G, as seen with the 4G/LTE EPS-AKA protocol, which enhanced security for connectivity across different networks [11]. This evolution introduced a new set of cryptographic safeguards, including improved ciphering and integrity checking of signaling data exchanged between the User Equipment (UE) and the core network. This integration of EPS-related cryptographic keys enables a UE to authenticate the identity of a SN. However, the authentication process in 4G, which requires a home network to rely on a serving network for UE authentication, introduces some vulnerabilities. In particular, this dependency allows for potential exploitation by sophisticated adversaries who can imitate serving networks to monitor subscribers [12], [13].

5G has undergone a significant upgrade in terms of both security architecture and authentication protocols, intending to satisfy a service-oriented network model. This upgrade has also addressed numerous vulnerabilities that were present in previous versions of the technology. In fact, 5G is the first standard to have its authentication architecture as a unified framework [14], which offers enhanced protection for user equipment (UE) identities compared to 4G. 5G technology has introduced the Subscription Concealed Identifier (SUCI), a cryptographic variant of the Subscription Permanent Identifier (SUPI), designed to obscure the user's actual details during the authentication phase [11]. This enhancement ensures that a UE's permanent identifier, e.g., the IMSI, will not be sent over 5G networks in plaintext, representing a significant improvement in network security compared to previous generations.

In the 5G network, three principal authentication protocols are outlined in the relevant 3GPP documents [15]. These include the 5G AKA (Authentication and Key Agreement) protocol [6], EAP-AKA$'$ [6], and the 5G EAP-TLS protocol [16]. These standard protocols are predominantly formulated as RFCs—informal documents that offer comprehensive guidance for protocol engineers. However, it may be a potential source of significant security vulnerabilities in their implementations, according to [17]. This informal setup can often lead to ambiguities that compromise the security of the network systems relying on these protocols.

Nevertheless, researchers have also identified numerous issues with 5G. For instance, the researchers [5] have conducted a comprehensive examination of the security characteristics of the 5G AKA protocol (and its variant EAP-AKA$'$) as outlined in 3GPP$'$s specifications [6], [18] based on the protocol analyzer TAMARIN [19], a useful tool for resolving ambiguities and validating the correctness of the protocol design.

In [5], the authors have identified several authentication issues, including the absence of key confirmation, the lack of integrity protection for service network identities, and the binding assumption on the channel between the serving network and the home network. Furthermore, they analyze the EAP-AKA$'$ protocol and demonstrate the existence of a failure message linkability attack in 5G-AKA [20]. Subsequently, in [21] the authors propose a novel version of the 5G AKA protocol to overcome the currently identified weaknesses in [7]. However, their solutions require modifications to the protocol format. Moreover, although 5G-AKA can defeat IMSI-catcher attacks, researchers of [7] have identified that user tracking is still possible in 5G by observing the occurrence of synchronization failure messages over time [22], [23]. Besides, the issue of using a rogue base station to fool user equipment (UE) into disclosing its unique subscriber identity (SUPI), for example, by leveraging a spoofed pre-authentication message, has not yet been resolved in 5G [23]. Furthermore, in response to the Linkability Attack [24], Wang *et al.*[20] proposed an improved scheme called 5G-AKA', encrypting the challenge value $RAND$ with a transient key encrypted with $SUPI$ at both the user equipment (UE) and the home network (HN) ends. Since the transient key is updated with each protocol

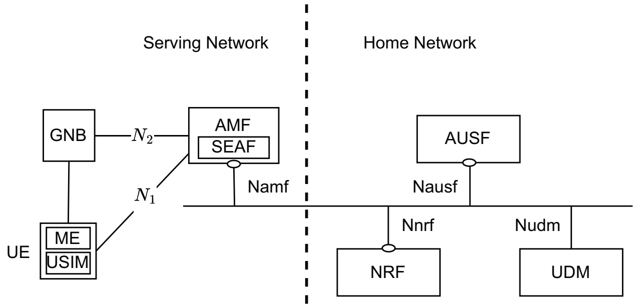

Fig. 1. Architecture of 5G's Service-Based Model

establishment, replayed messages will result in the incorrect $RAND$, which will cause the MAC verification to fail. The target UE will return a MAC failure, as do other devices, thus ensuring the freshness of the message and resisting various attacks brought about by message replay. However, the 5G-AKA scheme [20] does not address network identity spoofing attacks. Network identity spoofing attacks do not typically result in effective attacks against ordinary UEs.

For the future, the consensus is that many 5G features will not disappear, but will be fully supported with further security enhancements for 6G use. The common authentication framework and security isolation in 5G technologies will continue to play a central role in 6G [25] to converge the authentication features for multi-access networks. However, the security capabilities of the 5G AKA framework will be the target of further improvements. Some researchers have proposed the use of an eSIM [26] (a SIM card embedded in a mobile device) or a non-SIM model, but as SIM cards and the identity management model has not changed significantly since 2G, this shift will require a fundamental change in identity storage or sharing, which is not compatible with previous generation mobile networks.

III. System Model and Legacy AKA

This section describes the system model based on legacy 5G technology. We briefly present the general process of the legacy protocol, point out its weaknesses, and define the security feature of our scheme.

A. System Model

In the communication system, an authentication procedure requires three parties: the user (UE), the visited serving network (SN), and the home network (HN). Let us use 5G SBA (service-based architecture) as the instance. Figure 1 presents the necessary function elements as well as their reference points. A brief description of the roles of each party, as well as different entities belonging to them, is provided below:

1) **UE (ME, USIM):** The user is equipped with user equipment (UE), typically a piece of mobile equipment (ME) carrying a Universal Subscriber Identity Module (USIM), the latter is uniquely identified by its Subscription Permanent Identifier (SUPI). The USIM is subscribed to a specific home network (HN) and shares a long-term secret K with the HN's Unified Data Management (UDM). The UE is connected to the serving network (SN) through a gNodeB in the 5G access network.
2) **Serving Network (AMF/SEAF):** In the serving network, an entity called Security Anchor Function (SEAF) participates in the 5G AKA procedure. Its functionality of authentication is provided through the Access and Mobility Management Function (AMF) in the SN.
3) **Home Network (AUSF, UDM/ARPF):** In the home network, the authentication server function (AUSF) is an entity that serves as the backend authenticator in the 5G AKA procedure. In the protocol flow, a challenge generated by the HN is sent to the user, and the AUSF is responsible for the verification of the user's response to this challenge. The Unified Data Management (UDM) in the HN stores the subscriber's data. Co-located with the UDM is the Authentication Credential Repository and Processing Function (ARPF), which stores the long-term secret shared with the UE. The UDM is responsible for the generation of messages essential for the authentication.

According to the 5G documents, the 5G core network is moving to a service-based architecture (SBA) to achieve better flexibility, scalability, resilience and reduce expenses. Hence, the Network function Repository Function (NRF) was introduced. The NRF is a centralized repository for all Network Functions (NF) and is responsible for the discovery of other NF services. In SBA, a client-server model is adopted for communication between different NFs within the core network. All those communications go through the NRF, where mechanisms such as NF authorization can be implemented to enhance the core network security. According to 5G requirements, secure network communication protocols such as HTTPS are used. Therefore, in this article, we assume that the channel between SEAF and AUSF, and that the communication within the HN is secured, whereas the one between the UE and the SEAF is insecure.

B. 5G AKA protocol

To clarify the problem, we briefly introduce the legacy 5G AKA protocol, Figure 2 is the message flow for both the legacy and our schemes. Since the channel between the UE and the SEAF is not secure, it is important to check SEAF during the AKA. This is what the 5G AKA authentication protocol aims to achieve.

The whole procedure can be divided into 2 phases: the initialization phase and the authentication phase. During the initialization phase, the user encrypts its SUPI with its HN's public key pk_{HN}. Together with Id_{HN}, the user transmits this message to SEAP. The whole message is referred to as SUCI. The SEAP in SN relays SUCI to the HN together with the serving network name ($SNname$). In HN, the ARPF decrypts the received message and acquires SUPI, with which it looks up the long-term key K shared with USIM.

Then in the authentication phase, a challenge-response mechanism is used for authentication. In HN, the ARPF is responsible for the construction of the authentication vector. We explain the role of some interesting items in the AV as follows:

1) The random nonce R is selected by the ARPF.
2) The message authentication code MAC is generated from a one-way function that takes the shared secret K, the challenge R, and the sequence number stored for the subscriber SQN_{HN} as input. A correct MAC value implies that the UE is communicating with the correct HN, and in this case, the UE considers the authentication successful and generates the anchor key K_{SEAF}.
3) The hashed expected response $HXRES^*$. It is the hash output of R and $xRES^*$, while $xRES^*$ is bound to K, R and $SNname$ (SN's identifier). When the UE has verified the correctness of the MAC value, it generates an RES^* in the same way as $xRES^*$. By comparing the values of $SHA256(< R, RES^* >)$ and $HXRES^*$, the SN can verify the UE's legitimacy (the UE possessed the correct K required for the generation of correct $RES^* = xRES^*$).
4) If the previous check was passed, the SEAF forwards the RES^* to the HN. Similarly, by comparing RES^* and $xRES^*$, the HN verifies the legitimacy of the UE.

At the end of the protocol, an agreement on the anchor key K_{SEAF} should be established between the UE and the SEAF. For the UE, K_{SEAF} can be calculated from $(K, R, SQN_{NH}, SNname)$. For the SN that doesn't know the value of K, the K_{SEAF} is received from the HN in a confirmation message after the HN has verified the legitimacy of the UE.

C. Weakness

We can find that, in standard 5G AKA, the validation of SNname is executed in Step 4. Whereas UE's verification for the network is already completed in Step 3. It means that the validation check is too late.

The validation subject also indicates the problem. We let the home network (AUSF) verify the SNname by checking the received RES^*, while the only element is MAC for UE to check the network. However, MAC does not contain the SNname. To add a new parameter is difficult, it means an additional input interface for USIM and a new procedure design. It is not secure to use the same binding method as RES since the malicious serving network can derive the MAC to mislead the UE.

Thus, a thorough solution to this problem is technically difficult.

IV. Proposed Scheme

A. Overview

For the clarity of the scheme description, the message flow and relevant components will be discussed according to the 5G systems. But it should be mentioned that our mechanism suits the future 6G communications as well.

The message flow is as Figure 2. According to our discussion above, the only chance for the UE to check the validity of the network (including the HN and SN) is the verification of $xMAC$ (MAC). Hence, our primary goal is to soundly bind the Serving Network Name ($SNname$) in the MAC without altering the USIM procedure.

In the original version, the nonce R is randomly selected by the ARPF, and directly used in the calculation of the MAC. Note that the calculation of MAC only requires knowledge of the random nonce R, the sequence number $SQN_{HN/UE}$, and the long-term secret key K. Upon the reception of AV, the UE gets R directly and acquires $SQN_{HN/UE}$ once the AK is recovered. Thus, it can calculate an expected MAC (xMAC) with its stored K and compare it with the MAC.

Our modification is a venture but is secure according to later analysis. We directly bind the random nonce R with the $SNname$ and use the bound value (denoted as R_1) to generate MAC, as well as other elements. In the transmission of AV, the nonce is still the plain nonce R.

With this method, if the SN wants to cheat UE, the MAC relayed to the UE cannot be tampered to the form of its asserted $SNname$. The detailed scheme is described as follows.

B. Initialization phase

1) In the initialization phase, when the UE receives the SN's authentication request and stores the $SNname$ contained in the request. Unlike the standard protocol, the value will be used to verify the SN's authenticity. The UE then generates its authentication message SUCI to SEAP:

$$SUCI =< aenc(pk_{HN}, SPUI), Id_{HN} >$$

2) The SEAP transmits the SUCI to AUSF together with its valid serving network name $SNname$. The AUSF sends the two messages to ARPF.
3) Upon reception of the message, the UDM/ARPF de-conceals SUCI with HN's secret key sk_{HN} and obtains SUPI.

C. Authentication phase

1) The UDM/ARPF uses the de-concealed SUPi to look up the corresponding long-term key K shared with the UE and the sequence number SQN_{HN} and generates the authentication vector as follows: First, a random nonce R is generated as in the standard protocol. Then the ARPF calculates $R_1 = f*(SNname, R)$, where $SNname$ is the SN's serving network name received in the initialization phase, and $f*$ is a hash function with an output size equal to the previous R value. The ARPF continues to calculate the other items as follows:

$$\begin{aligned} MAC &= f_1(K, AMF, SQN_{HN}, R_1) \\ AK &= f_5(K, R_1) \\ CONC &= SQN_{HN} \oplus AK \\ AUTN &= CONC||AMF||MAC \end{aligned} \quad (1)$$

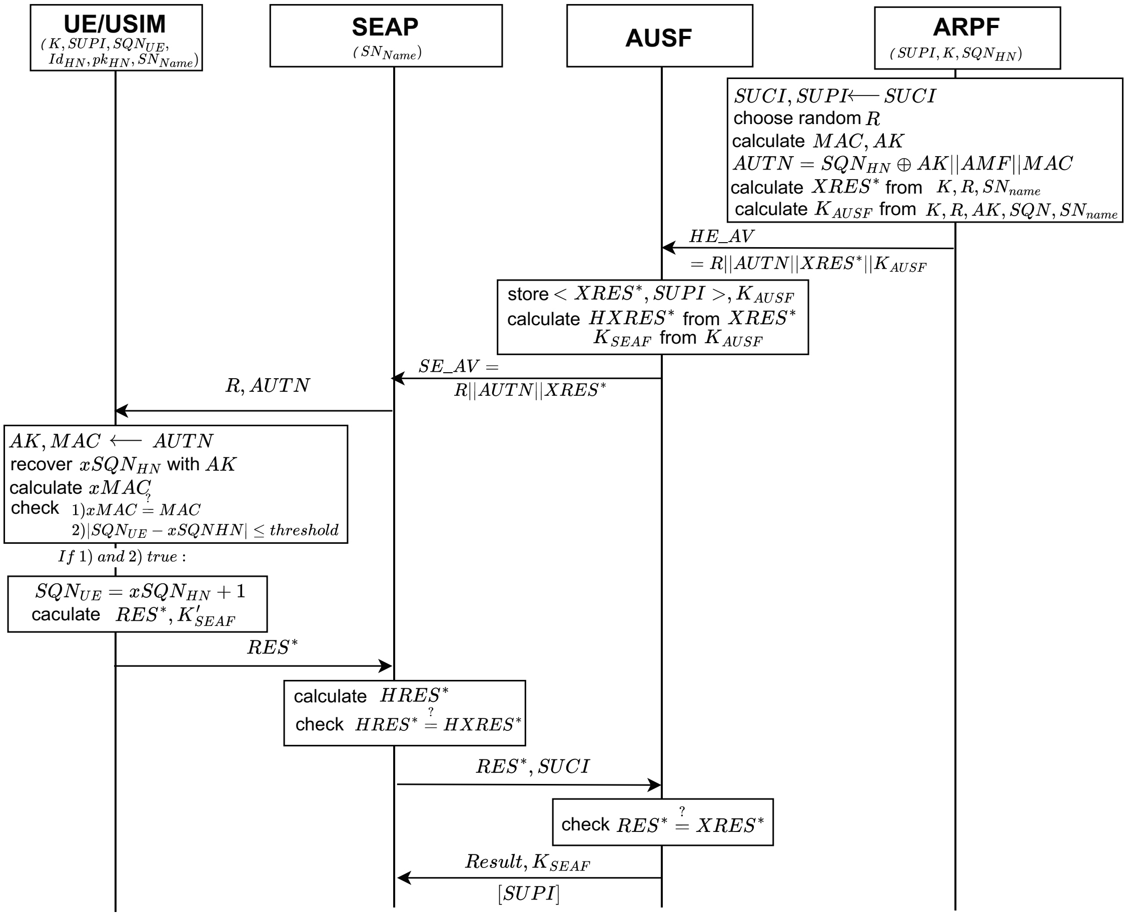

Fig. 2. Message Flow of AKA (Compatible for both 5G and our Scheme)

$$
\begin{aligned}
IK &= f_3(K, R_1)\\
CK &= f_4(K, R_1)\\
XRES &= f_2(K, R_1) \qquad (2)\\
K_{AUSF} &= KDF(CONC, SNname, CK, IK)\\
5G\_HE\_AV &= R||AUTN||XRES*||K_{AUSF}
\end{aligned}
$$

Our scheme differs from the standard protocol in that all R previously used in the calculation of AV items are replaced by R_1. Note that the random nonce R in the 5G HE AV to send to AUSF remains unchanged.

2) Upon reception of 5G HE AV from ARPF, the AUSF stores XRES* and calculates HXRES* and K_{SEAF} and constructs 5G SE AV as follows:

$$
\begin{aligned}
&HXRES* = SHA-256(R, XRES*)\\
&K_{SEAF} = KDF(SNname, K_{AUSF})\\
&5G\_SE\_AV = R||AUTN||HXRES*
\end{aligned}
$$

The 5G SE AV is transmitted to the SEAF.

3) The SEAF parses the SE AV and gets the random nonce R, the AUTN, and the HXRES*. It stores HXRES*, R, and sends $(R, AUTN)$ to the UE.

4) Upon reception of AUTN and R, the UE/USIM can recover AK and SQN_{HN} and calculate an expected xMAC to compare it with the MAC value sent in AUTN. Before forwarding the messages received to USIM, an additional operation in UE is required:

$$R_1 = f^*(SNname, R)$$

Unlike the standard 5G AKA, it is not $(R, AUTN)$, but $(R_1, AUTN)$ that is forwarded to USIM.

$$
\begin{aligned}
&(CONC, AMF, MAC) \leftarrow AUTN\\
&AK' = f_5(K, R_1)\\
&xSQN_{HN} = AK' \oplus CONC\\
&xMAC = f_1(K, AMF, xSQN_{HN}, R_1)
\end{aligned}
$$

Then the USIM checks if the obtained $xMAC$ matches the MAC received in AUTN and if the sequence number stored in the USIM $SQN_{UE} < xSQN_{HN}$. If the two previous conditions were satisfied, the USIM calculates

RES, CK, and IK:

$$RES = f_2(K, R_1)$$
$$IK = f_3(K, R_1)$$
$$CK = f_4(K, R_1)$$

The three output values are sent to UE, which continues to calculate RES* and K_{SEAF}:

$$RES^* = KDF(R, RES, SNname)$$
$$K_{AUSF} = KDF(SQN_{HN} \oplus AK, SNname, CK, IK)$$
$$K_{SEAF} = KDF(SNname, K_{AUSF})$$

The UE stores the anchor key K_{SEAF} and sends the RES^* to SEAF.

5) The SEAF receives the RES^* and checks if the following equation holds:

$$SHA - 256(R, RES^*) \overset{?}{=} HXRES^*$$

If true, it forwards the RES^* with the corresponding SUCI to AUSF.

6) In the HN, the AUSF checks if the received RE^* is equal to the previously stored $XRES^*$ and indicates the SEAF the result. If the two values match, the authentication is considered successful, and the AUSF should include in the result the anchor key K_{SEAF} and the previously stored SUPI.

V. Analysis

The proposed scheme resists false SN's attacks well. To analyze this property, we can formulate the malicious SN's behavior as the following attack target.

Definition 1: With the reception of a valid authentication vector $AV = (R, MAC, xRES, SQN_{HN} \oplus AK)$, according to our proposed protocol with serving network's validated name N_1, replacing a new vector AV', allowing the SN to change any of the elements, but can be verified with its asserted name N_2.

The best way for the SN to achieve the above goal is to replace R. Since it can easily derive the nonce of the practical USIM module as $R_1 = f*(N_1, R)$. The remaining task is to get a new R', which satisfies that $R_1 = f^*(N_2, R')$. However, based on the unidirectionality of f^*, it is computationally impossible.

Apart from this way, the SN has to forge a new AV to realize the Definition 1. Its difficulty can be reduced to the difficulty of hacking the basic AKA method: the only difference between them is the range of valid SQN. In basic AKA, the adversary should use an SQN, whose value is a little larger than the previous AVs; in this goal, the valid SQN can be the same as the current AV.

Luckily, as has been discussed, the nonce R_1 cannot be the same, the $AK = f_5(K, R_1)$ is different, the component of $SQN_{HN} \oplus AK$ cannot bring any benefit for this adversary.

The above analysis has shown that the SN cannot convince the UE of its claimed false name. It is best to prove it formally, due to the space limitations, we will realize it using Tamarin Prover in our future work.

VI. Conclusion

In this work, we have proposed a variant to the existing 5G standard AKA authentication protocol to eliminate a weakness arousing security concerns over the threat of malicious SNs. An important change is to replace the random nonce challenge selected by the HN with a challenge committed to the SN's identifier. This change enables the UE to detect serving network forging in the authentication procedure and ensures "explicit" SN authorization by the HN. In addition, our scheme requires few changes to the existing scheme and imposes no modification on the USIM functions.

Acknowledgement

This work was supported by Natural Science Foundation of China (Grant Nos. 62202290), Research and Development Program of Department of Industry and Information Technology in Xinjiang Autonomous District (No. SA0304173).

References

[1] G. Liu, Y. Huang, N. Li, J. Dong, J. Jin, Q. Wang, and N. Li, "Vision, requirements and network architecture of 6G mobile network beyond 2030," *China Communications*, vol. 17, no. 9, pp. 92–104, 2020.

[2] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks," *IEEE Access*, vol. 7, pp. 64 040–64 052, 2019.

[3] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. Wiley Online Library, 2018.

[4] S. Behrad, E. Bertin, and N. Crespi, "A survey on authentication and access control for mobile networks: from 4G to 5G," *Annals of Telecommunications*, vol. 74, pp. 593–603, 2019.

[5] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 2018, pp. 1383–1396.

[6] 3GPP, "TS 33.501: Security architecture and procedures for 5G system," Technical Specification, 9 2023. [Online]. Available: https://www.3gpp.org/ftp/Specs/latest

[7] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A Formal Analysis of 5G Authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. Toronto Canada: ACM, Oct. 2018, pp. 1383–1396.

[8] M. R. Bhalla and A. V. Bhalla, "Generations of Mobile Wireless Technology: A Survey," *International Journal of Computer Applications*, vol. 5, no. 4, pp. 26–32, Aug. 2010.

[9] "Global Mobile Trends 2024." [Online]. Available: https://data.gsmaintelligence.com/research/research/research-2024/global-mobile-trends-2024

[10] Muxiang Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 734–742, Mar. 2005.

[11] V. O. Nyangaresi, Z. A. Abduljabbar, M. A. Al Sibahee, I. Q. Abduljaleel, and E. W. Abood, "Towards Security and Privacy Preservation in 5G Networks," in *2021 29th Telecommunications Forum (TELFOR)*, Nov. 2021, pp. 1–4.

[12] S. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," *Network and Distributed Systems Security (NDSS) Symposium 2018*, Feb. 2018.

[13] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information," in *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2019.

[14] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.

[15] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif," *IEEE Access*, vol. 8, pp. 23 674–23 688, 2020.

[16] E. Rescorla and T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force, Request for Comments RFC 5246, Aug. 2008, num Pages: 104.

[17] D. Basin, C. Cremers, K. Miyazaki, S. Radomirovic, and D. Watanabe, "Improving the Security of Cryptographic Protocol Standards," *IEEE Security & Privacy*, vol. 13, no. 3, pp. 24–31, May 2015, conference Name: IEEE Security & Privacy.

[18] 3GPP, "TS 33.102: 3G security; Security architecture," Technical Specification, 4 2024. [Online]. Available: https://www.3gpp.org/ftp/Specs/latest

[19] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The TAMARIN prover for the symbolic analysis of security protocols," in *Computer Aided Verification*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, vol. 8044, pp. 696–701, series Title: Lecture Notes in Computer Science.

[20] "Privacy-Preserving and Standard-Compatible AKA Protocol for 5G."

[21] A. Braeken, M. Liyanage, P. Kumar, and J. Murphy, "Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks," *IEEE Access*, vol. 7, pp. 64 040–64 052, 2019.

[22] "IMSI-catcher," page Version ID: 1192994246. [Online]. Available: https://en.wikipedia.org/w/index.php?title=IMSI-catcheroldid=1192994246

[23] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5g specifications," *IEEE Access*, vol. 7, pp. 24 956–24 963, 2019.

[24] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar, "New privacy issues in mobile telephony: fix and verification," in *Proceedings of the 2012 ACM conference on Computer and communications security*. Raleigh North Carolina USA: ACM, Oct. 2012, pp. 205–216.

[25] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, "6G White paper: Research challenges for Trust, Security and Privacy," *arXiv preprint arXiv:2004.11665*, 2020.

[26] H. Goswami and H. Choudhury, "An eSIM-based remote credential provisioning and authentication protocol for IoT devices in 5G cellular network | Semantic Scholar," *Internet of Things*, vol. 23, p. 100876, 2023.