IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 July 2022, accepted 19 July 2022, date of publication 25 July 2022, date of current version 28 July 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3193372

RESEARCH ARTICLE

A New Tracking-Attack Scenario Based on the Vulnerability and Privacy Violation of 5G AKA Protocol

YA-CHU CHENG AND CHUNG-AN SHEN, (Member, IEEE)
Department of Electronic and Computer Engineering, National Taiwan University of Science and Technology, Taipei 106, Taiwan

Corresponding author: Chung-An Shen (cashen@mail.ntust.edu.tw)

This work was supported in part by the Ministry of Science and Technology, Taiwan.

ABSTRACT The security architecture and procedure for 5G systems (TS 33.501) is based on the 3rd Generation Partner Project (3GPP) security specification draft that is released in 2018. Since its debut, the security violations in the 5G security protocol have been intensively studied and discussed. Based on the 5G security protocol, this paper illustrates a new tracking-attack scenario that feasibly makes subscribers suffer in a breakdown of personal privacy. Specifically, it is shown in this paper that patterns of personal behavior are leaked without any awareness during the synchronization procedures in the 5G protocol. An in-depth analysis of the privacy violations is presented in this paper and potential countermeasures for protecting the sensitive information of genuine subscribers are given. A lemma model based on the TAMARIN Prover is illustrated to analyze the privacy vulnerabilities in the depicted attack scenario. Furthermore, a practical experiment based on the srsLTE framework is setup to demonstrate how the privacy information of genuine subscribers are violated based on the scenario that is reported in this paper.

INDEX TERMS Tracking and monitoring attack scenario, vulnerability, exploit, 5G AKA protocol, 3GPP, authentication and key agreement, privacy violation, TAMARIN prover, srsLTE.

I. INTRODUCTION

The mutual authentication scheme has been employed in mobile communications for enforcing the identity, authentication and verification between users and the network [1]–[4]. Through handshaking protocols between different parties, a mutual-based and challenge-response security protocol, Authentication and Key Agreement (AKA), become the global standards of authentication protocols [1]. The AKA protocol is based on a counter known as sequence number (SQN) and symmetric keys [2], [3]. Specifically, the SQN is employed for counting the number of times of successful handshaking and symmetric keys are stored in user equipment and the network respectively for identifying genuine users. The AKA protocol has evolved from the original version to support generations of mobile communications. For instance, the identifying features of AKA protocols in 3G are a cipher key CK, an integrity key IK [2], and an authentication token AUTN [5]. Moreover, the 4G was published with strong encryption and integrity protection algorithms, and the updated key hierarchy was vital to confidentiality [6]. In addition, the AKA-based 5G security specification is also released in 2018 [4].

While the security system has been strengthened, the security violations based on the vulnerability of AKA still exist. These violations occur during the security attacks such as IP address spoofing [6], replay [7], man-in-the-middle [7], denial of service (DoS) [8] and IMSI-catchers [9], [10]. The AKA-related security violations have been widely studied and are categorized as confidentiality, authentication, and privacy [11]. In particular, the confidentiality violation specifies that genuine subscribers leak sensitive information because of the incomplete secrecy [11], [12]. Furthermore, the authentication violation is related to the failure of agreement and subscription ID check [13], [14]. In addition, the privacy violation is categorized as "traceability" or "linkability" [11]

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

and [15]. It is mentioned in [11] that the leakage of identifying data such as the SQN makes the subscribers become traceable. On the other hand, the logic vulnerability of leveraging a counter can be exploited by an attacker to monitor the genuine subscribers known as the "linkability" [15]–[18].

This paper studies the vulnerability of the 5G AKA protocol and reveals a tracking-attack scenario that has never been reported in literature. In particular, it is shown in this paper that the sensitive information of subscribers such as personal behavior patterns can be violated and deduced without any awareness through the frequent connection between subscribers and the network. Main contributions of this paper are summarized as follows.

- The procedure of the revealed tracking-attack includes eavesdropping, interception, and injection. During this procedure, the attacker is able to steal personal information of a genuine subscriber by purposely triggering a synchronization failure. An in-depth analysis of the privacy violations based on the revealed attack is illustrated in this paper.
- In order to validate the illustrated tracking-attack, Lemma models based on the state-of-art verification tool for security protocols, TAMARIN Prover [19], are built to analyze the privacy vulnerabilities in the disclosed attack scenario and the 5G specifications.
- A practical experiment based on an open-source platform for LTE experimentation, srsLTE [20], is conducted to demonstrate how the adversaries attack the genuine subscribers based on the illustrated procedure.
- Potential countermeasures to address the attack and recommendations for protecting the sensitive information of genuine subscribers are given in this paper.

The rest of the paper is organized as follows. The background of 5G security and the AKA mechanism is presented in Section II. The illustrated tracking-attack scenario is presented in Section III and the countermeasure is shown in Section IV. The experiments with srsLTE and the TAMARIN lemma model are shown in in Section V. The paper is concluded in Section VI.

II. BACKGROUND AND RELATED WORK

A general architecture of 5G security and AKA mechanism based on the specification 3GPP TS 33.501, is reviewed in this section [4]. The studies related to the privacy vulnerabilities are also discussed in this section.

A. 5G SECURITY ARCHITECTURE AND AKA MECHANISM

A simplified architecture of communication network contains three main entities such as user equipment (UE), serving network (SN) and home network (HN) [1]. The user equipment (UE) is the subscriber's device where the universal subscriber identity module (USIM) is the most commonly used UE. Furthermore, the serving network (SN) represents the base station and the home network (HN) is the database server to contain subscribers' carrier information. Based on this architecture, the channel between each entity requires a mutual authentication before the subscribers can successfully access to the registered network. Therefore, the authentication and key Agreement (AKA) mechanism [2], [4] is presented for mobile communications. The overview of the 5G AKA protocol [4] is shown in Fig. 1 and key functions are defined as follow:

- **USIM**: universal subscriber identity modules
- **SEAF**, security anchor key function in SN
- **AUSF**, authentication server function in HN
- **ARPF**, authentication credential repository and processing function in HN
- **SIDF**, subscription identifier de-concealing function in HN

Furthermore, a long-term symmetric key (K), the subscription permanent identifier(SUPI), and a sequence number counter (SQN) are three essential components that are stored in both UE (USIM) and HN [11]. The K is a source key for key hierarchy, derivation and distribution. The SUPI is an identity of subscriber which can be encrypted into subscription concealed identifier (SUCI). The SQN is a counter for counting the number of successful handshake [2].

It is shown in Fig. 1 that initially a subscriber sends the subscriber identity SUCI to SN where SN initiates the authentication by sending SUCI and its own identity $\mathrm{SN_{name}}$ to HN. The HN retrieves SUPI from SUCI for verifying the identity of the subscriber. The function ARPF in HN then generates a 5G home environment authentication vector (5G HE AV) that is composed of a random number (RAND), an authentication token (AUTN), a derived key($\mathrm{K_{AUSF}}$) and an expected response (XRES$*$). The RAND is processed by HN and will be used in the subsequent AKA protocol procedures. The AUTN contains a CONC which consists of $\mathrm{SQN_{UE}}\oplus$ AK, an authentication and key management field (AMF) and a message authentication code (MAC). The 5G HE AV is combined with SUCI and is sent to AUSF. In the following, the AUSF generates 5G serving environment authentication vector (5G SE AV) which consists of a newly derived key $\mathrm{K_{SEAF}}$ from $\mathrm{K_{AUSF}}$, a hashed HXRES$*$ by RAND, RAND, and AUTN. The $\mathrm{K_{AUSF}}$ and XRES$*$ are both stored in the AUSF. The AUSF sends 5G SE AV with SUCI to the function SEAF in SN whereas $\mathrm{K_{SEAF}}$ and HXRES$*$ are stored in the SEAF from the received response. The RAND and AUTN are sent to UE where UE performs two key checks as below:

$$\mathrm{xMAC} = \mathrm{MAC} \tag{1}$$

$$SQN_{UE} < SQN_{HN} \tag{2}$$

The Eq. (1) checks if the received MAC is the same as expected MAC calculated by UE (xMAC). The Eq. (2) is to ensure the challenges and responses between UE and HN remain freshness [2]. Possible results for the checks include:

a. **Authentication success** if both Eq. (1), Eq. (2), and the subsequent verification succeed

b. **MAC failure**if xMAC $\neq$ MAC

c. **Synchronization failure** if $SQN_{UE} \nless SQN_{HN}$

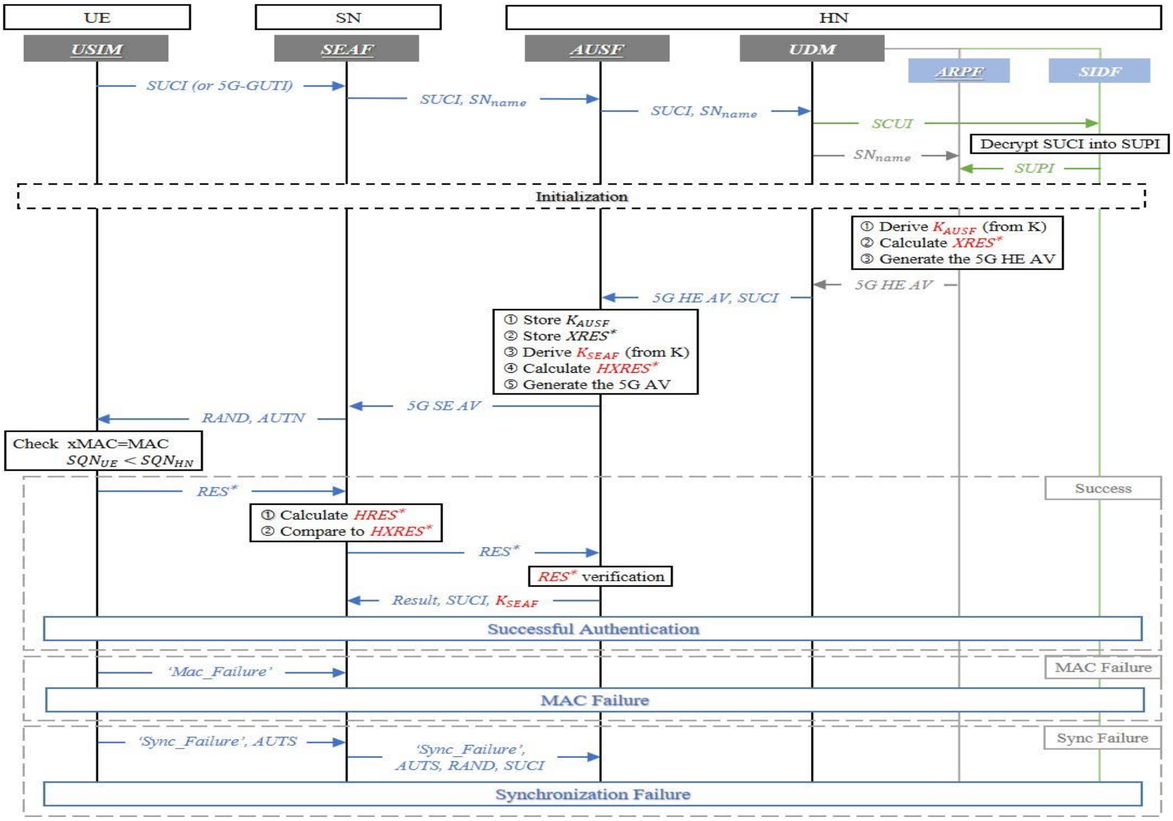


FIGURE 1. The overview and procedures of 5G AKA protocol [4].

It succeeds, UE sends RES* to response SEAF and the SEAF calculates a hashed RES* known as HXRES* by RAND. The HXRES* is compared with HXRES* that it stored before and, as long as the comparison succeeds, the SEAF sends RES* to AUSF as the final verification. The protocol ends with authentication success after SEAF receive Result, SUCI and K_{SEAF}. As for *b.* and *c.*, they are failed in Eq. (1) and Eq. (2) respectively, and only *c.* sends failure message back to HN due to the re-sync process which is to ensure AKA protocol be triggered with $SQN_{UE} = SQN_{HN}$ in the next time.

B. THE VULNERABILITY RELATED TO THE SQN MECHANISM

In the 5G AKA protocol, SQN_{UE} and SQN_{HN} are stored in UE and HN respectively. The initial values of both SQNs are identical and both are incremented by one whenever a handshake succeeds. Specifically, after the HN receives the N_{UDM}*_UE_Authentication_Get_Request* and the identity of the subscribers is confirmed, the SQN_{HN} is incremented by 1. Similarly, when Eq. (1) and Eq. (2) in UE are checked successfully, the SQN_{UE} is incremented by 1. Thus, the two SQNs are identical again in the end of the protocol. Figure 2 illustrates a scenario of synchronization failure after initialization. It is assumed that a subscriber starts at time $t = 1$ with the initial $SQN_{UE} = SQN_{HN} = 1$ and finishes successfully with $SQN_{UE} = SQN_{HN} = 2$ in the end of the protocol. The AKA protocol is executed again at time $t = i$ with the initial $SQN_{UE} = SQN_{HN} = 5$. At this time an unexpected Authentication Request, $(RAND, AUTN)_{t=0}$ instead of $(RAND, AUTN)_{t=i}$is received. The Authentication Request $(RAND, AUTN)_{t=0}$ represents the information that is fetched in a previous time due to the failure. When receiving re-use challenge, the SQN_{HN} in $(AUTN)_{t=0}$ is lower than the SQN_{HN} in expected $(AUTN)_{t=i}$since the AKA protocol succeeded at least once (at $t = 0$) before $t = i$. As a result, the comparison of SQN_{UE} and SQN_{HN} fails because of $SQN_{UE} = 5 \geq SQN_{UE} = 1$ as the example in Fig. 2.

C. RELATED WORK

The security and privacy issues related to the 5G AKA protocol have been studied in literature [16], [17], [21] where K_{SEAF}, SUPI and SQN are identified as essential security features. Furthermore, the authentication properties of 5G AKA protocol are investigated in [14] and the violation of authentication related to K_{SEAF} is studied in this work. The security properties are modeled in the TAMARIN Prover by using lemma models. Moreover, it is illustrated in [11] that the identifying data such as SQN and SUPI need to remain secret, otherwise a classical location attack (i.e. the traceability of the subscribers) is resulted. The TAMARIN Prover is also used in [11] to show the underspecified and missing security goals and assumptions in TS 33.501. It is also indicated in [11] that the SQN mechanism in 5G AKA is vulnerable to the replay attack. On the other hand, the work [15] exploits the logic vulnerability of leveraging SQN to monitor the genuine subscribers. The attack scenario discovered in [15] is to deduce

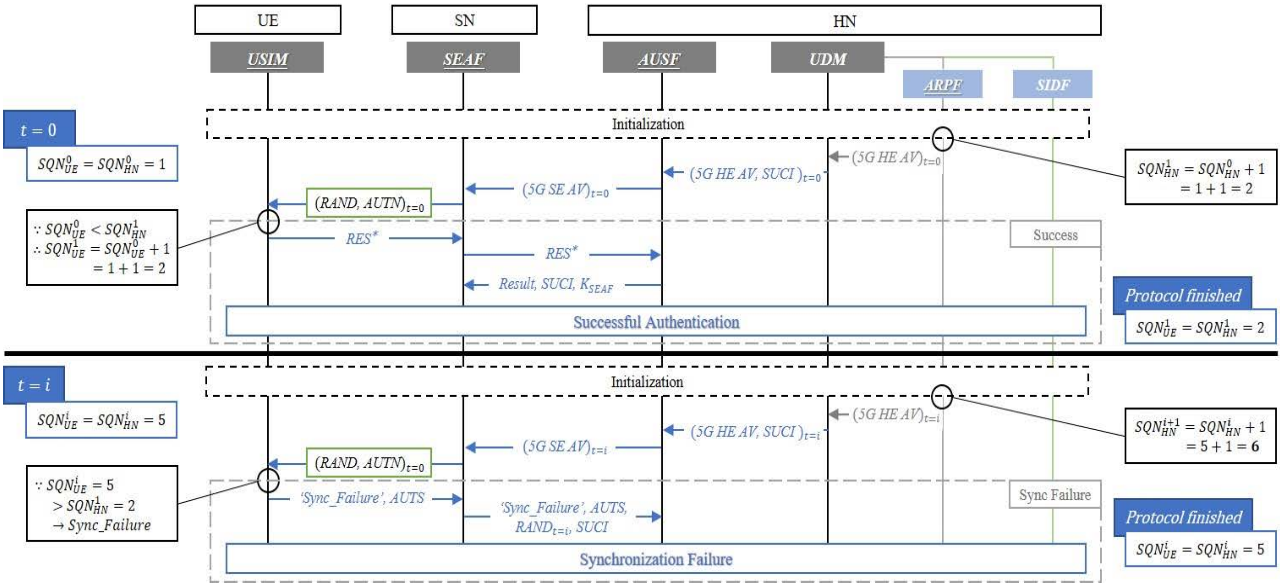

UE
SN
HN
USIM
SEAF
AUSF
UDM
ARPF
SIDF
t = 0
$SQN_{UE}^0 = SQN_{HN}^0 = 1$
Initialization
$(5G\ HE\ AV)_{t=0}$
$(5G\ HE\ AV,\ SUCI)_{t=0}$
$(5G\ SE\ AV)_{t=0}$
$(RAND,\ AUTN)_{t=0}$
$SQN_{HN}^1 = SQN_{HN}^0 + 1 = 1 + 1 = 2$
$\because SQN_{UE}^0 < SQN_{HN}^1$
$\therefore SQN_{UE}^1 = SQN_{UE}^0 + 1 = 1 + 1 = 2$
RES*
RES*
Result, SUCI, K_{SEAF}
Success
Protocol finished
$SQN_{UE}^1 = SQN_{HN}^1 = 2$
Successful Authentication
t = i
$SQN_{UE}^i = SQN_{HN}^i = 5$
Initialization
$(5G\ HE\ AV)_{t=i}$
$(5G\ HE\ AV,\ SUCI)_{t=i}$
$(5G\ SE\ AV)_{t=i}$
$(RAND,\ AUTN)_{t=0}$
$SQN_{HN}^{i+1} = SQN_{HN}^i + 1 = 5 + 1 = 6$
$\because SQN_{UE}^i = 5 > SQN_{HN}^1 = 2 \rightarrow Sync\_Failure$
'Sync_Failure', AUTS
'Sync_Failure', AUTS, $RAND_{t=i}$, SUCI
Sync Failure
Protocol finished
$SQN_{UE}^i = SQN_{HN}^i = 5$
Synchronization Failure

FIGURE 2. An example of synchronization failure in SQN mechanism [4].

the typical service consumption of targeted subscribers by the SQN inference algorithm.

In addition, it is demonstrated in [18] that the traces of subscribers can be leaked by triggering the authentication failure. On the other hand, a port-scan scheme is proposed in [22] for the IoT so that the security of the network is improved while the degradation of the performance can be minimized. Furthermore, an approached is proposed in [23] to protect the data privacy for IoT by using the AI technology, whereas a method is presented in [24] to detect the malicious adversaries in the IoT. Therefore, the SQN mechanism in 5G AKA is vulnerable to both traceability and linkability security issues. In this paper, we show how the subscribers suffer in privacy violations only in few procedures in our discovered attack.

III. THE TRACKING-ATTACK BASED ON THE 5G AKA PROTOCOL

A. THE OVERVIEW OF THE TRACKING-ATTACK SCENARIO

The types of attack are categorized as passive attackers or active attackers. Passive attackers, without having any extra knowledge, obtain the information by eavesdropping. On the other hand, passive attacker doesn't have abilities of interception, injection and manipulation. Active attackers can encrypt, decrypt and hash. They also have knowledge of key hierarchy or protocols procedures [25]. Based on the capabilities of passive and active attackers, it is shown in this paper that privacy violations can be resulted through exploiting the vulnerability of the SQN scheme. The conceptual overview of such violation is illustrated in Fig. 3 where an active attacker impersonates as a malicious base station and triggers a synchronization failure at different time. The sync failure message containing the message of AUTS is retrieved by the attacker. Since the SQN_{UE} is included in AUTS, that is, AUTS $=$ CONC*||MAC-S; $\oplus$CONC* $=$ $SQN_{UE}AK^*$, the attacker can learn the value of SQN_{UE} at different time whenever the synchronization failure is triggered. The attack then leverages the values of SQN_{UE} at different time to retrieve sensitive information, such as personal behavior patterns, preference and daily routines, of the subscriber.

Based on the concept illustrated in Fig. 3, the procedure for the presented tracking-attack scenario is shown in Fig. 4. It is shown in Fig. 4 that this procedure contains an online phase and an offline phase where the purpose of the online phase for the attacker is to obtain AUTS by triggering synchronization failure of the genuine subscribers. Based on the monitoring of the targeted genuine subscriber, the attacker eavesdrops the genuine subscriber and intercepts the valuable data such as SUPI and authentication request from SN. In the following, the attacker impersonates as a base station and eventually injects the authentication request towards the network so that the synchronization failure is triggered and the message AUTS is obtained. The obtained AUTS is then used in the offline phase to retrieve the SQN_{UE}. The patterns and behaviors of the genuine subscriber are obtained through the vulnerability of SQN mechanism.

B. THE ONLINE PHASE OF THE ATTACK

The protocol of the online phase for the presented attack is shown in Fig. 5. Assuming that the attack starts at time $t = t_0$ where the attacker eavesdrops the genuine subscriber using sniffer tools such as the packet analyzer Wireshark [26]. The subscriber's SUPI/SUCI and the authentication request ($RAND_{t_0}$, $AUTN_{t_0}$) that is sent from the network to the subscriber are obtained by the attacker. In the following time at $t = t_1$, the attacker impersonates a base station. The attacker forwards the challenges and responses between the genuine subscriber and the network to check if the attacker is connected with both UE and the network. The AKA protocol proceeds successfully and the SQN_{UE} and SQN_{HN} are incremented as normal procedures. Furthermore, at time $t = t_2$, the

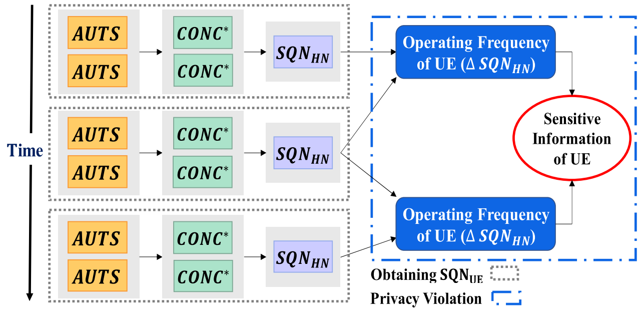


FIGURE 3. An overview of deducing the sensitive information in the discovered tracking-attack scenario.

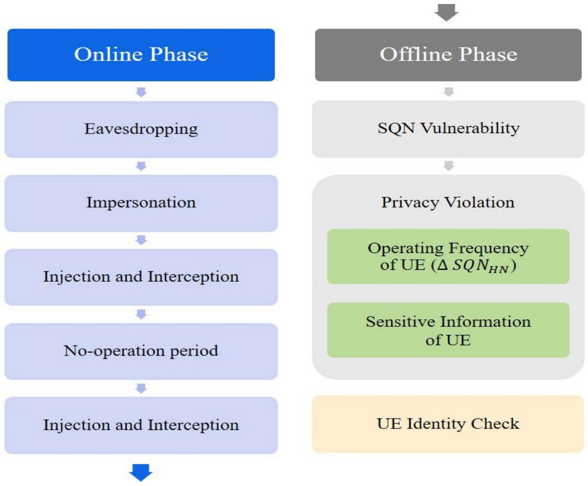


FIGURE 4. The procedure of the discovered tracking-attack.

attacker sends the authentication request ($RAND_{t_0}$, $AUTN_{t_0}$) that is obtained from the genuine subscriber at time $t = t_0$ to the subscriber. From the perspective of genuine subscriber, this is the second time that the same authentication request message is received. It is noted that the SQN_{UE} has been increased in the previous success of 5G AKA protocols at $t = t_1$. Furthermore, the SQN_{HN} of the authentication request ($RAND_{t_0}$, $AUTN_{t_0}$) that is injected by the attacker is from the time at $t = t_0$. As a result, at time $t = t_2$, the value of SQN_{UE} is no longer smaller than the SQN_{HN} and the synchronization failure is triggered, i.e., a violation of the Eq. (2). The replied message $AUTS_{t_2}$ from the genuine subscriber at time $t = t_2$is stored by the attacker.

The attacker then waits for a no-operation period noted as $t = i$ in Fig. 5 where $t_2 < i < t_3$. During this period, the attacker only forwards the challenges and responses so that the UE executes a successful 5G AKA protocol. After no-operation period, the attacker repeats the same attack at $t = t_3$ as $t = t_2$ to trigger another synchronization failure and to obtain $AUTS_{t_3}$. As a result, when the online phase of the attack completes, the attacker possess AUTS messages, $AUTS_{t_2}$ and $AUTS_{t_3}$, that are obtained at $t = t_2$ and $t = t_3$ respectively. It is noted that the no-operation period is dependent on different schemes of SQN_{UE}. For example, the SQN wraps around after 2^n seconds where n is based on the setting of the service provider. Based on Profile 1 in [2], n is equal to 24 so that the AUTS needs to be fetched within 2^{24} seconds (approximately 194 days.)

C. THE OFFLINE PHASE OF THE ATTACK

The two messages $AUTS_{t_2}$ and $AUTS_{t_3}$ that are retained by the attacker during the online phase are used to derive sensitive information about the UE during the offline phase. It is noted that the AUTS contains CONC∗, i.e., AUTS = CONC∗ || MAC-S where $\oplus CONC^* = SQN_{UE}AK^*$. Since the attacker obtains $AUTS_{t_2}$ and $AUTS_{t_3}$ at two different time, the attacker can retrieve two CONC∗ from two AUTS shown as below.

$$CONC^*_{t_2} = SQN^{t_2}_{UE} \oplus AK^*_{t_2} \tag{3}$$

$$CONC^*_{t_3} = SQN^{t_3}_{UE} \oplus AK^*_{t_3} \tag{4}$$

Since the RAND is generated in HN and sent in plaintext that defined in TS 33.501 [4], the attacker has injected the same authentication request ($RAND_{t_0}$, $AUTN_{t_0}$) twice in the online phase in advance. Therefore, it can be derived that

$$AK^*_{t_2} = f5^*_K\left(RAND_{t_0}\right) = AK^*_{t_3} \tag{5}$$

Thus, the attacker can deduce that

$$\begin{aligned} CONC^*_{t_2} \oplus CONC^*_{t_3} &= \left(SQN^{t_2}_{UE} \oplus AK^*_{t_2}\right) \\ &\quad \oplus (SQN^{t_3}_{UE} \oplus AK^*_{t_3}) \\ &= SQN^{t_2}_{UE} \oplus SQN^{t_3}_{UE} \end{aligned} \tag{6}$$

By leveraging Eq. (6) and through the derivation, the attacker infers $SQN^{t_2}_{HN}$ by utilizing the algorithm presented in [15].

D. LEAKAGE OF SENSITIVE INFORMATION BY THE ATTACK

It is shown in Section III-A, III-B, and III-C that the SQN_{HN} can be obtained by the attacker through the procedures shown in Fig. 3, Fig. 4, and Fig. 5. This subsection illustrates how the inferred SQN_{HN} are used by the attacker to derive sensitive information of the targeted subscriber. Consider a scenario where an attacker attempts to acquire the information about the footprint of a subscriber such as how frequent does this subscriber visit a place or how much time does this subscriber spend in a specific location. The attacker starts the attack to acquire the information about SQN_{HN} by following the procedure shown in Fig. 5 at different time. For example, the attacker obtains a SQN^1_{HN} on Day-1. The attacker then repeats the attack to obtain a SQN^2_{HN} on Day-2. In the following, the attacker can calculate the different between these two SQNs, that is, $\Delta = SQN^2_{HN} - SQN^1_{HN}$. The attacker repeats the procedure and retains multiple Δ periodically in a given period of time. As a result, personal preferences of the targeted subscriber can be inferred from the multiple Δ. For instance, whether the targeted subscriber spends more time in this location during a certain period of time or how often does this subscriber visit this location in a certain period of time. Even further, if the attacker setup the attack environment in multiple locations, the frequency of the targeted subscriber appearing in certain location, and the daily routine and activities of the targeted subscriber can be derived.

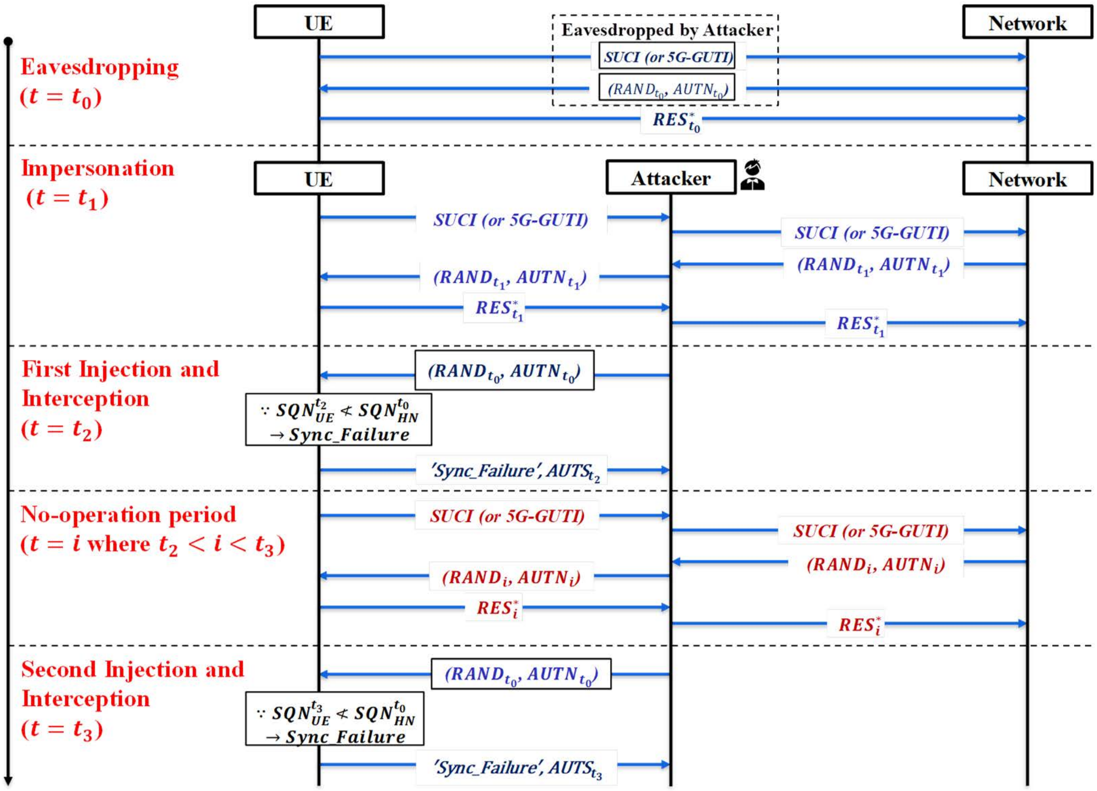

UE
Eavesdropped by Attacker
Network
Eavesdropping
($t = t_0$)
SUCI (or 5G-GUTI)
($RAND_{t_0}$, $AUTN_{t_0}$)
$RES^*_{t_0}$
Impersonation
($t = t_1$)
UE
Attacker
Network
SUCI (or 5G-GUTI)
SUCI (or 5G-GUTI)
($RAND_{t_1}$, $AUTN_{t_1}$)
($RAND_{t_1}$, $AUTN_{t_1}$)
$RES^*_{t_1}$
$RES^*_{t_1}$
First Injection and Interception
($t = t_2$)
($RAND_{t_0}$, $AUTN_{t_0}$)
$\because SQN^{t_2}_{UE} \nless SQN^{t_0}_{HN}$
$\rightarrow Sync\_Failure$
'Sync_Failure', $AUTS_{t_2}$
No-operation period
($t = i$ where $t_2 < i < t_3$)
SUCI (or 5G-GUTI)
SUCI (or 5G-GUTI)
($RAND_i$, $AUTN_i$)
($RAND_i$, $AUTN_i$)
RES^*_i
RES^*_i
Second Injection and Interception
($t = t_3$)
($RAND_{t_0}$, $AUTN_{t_0}$)
$\because SQN^{t_3}_{UE} \nless SQN^{t_0}_{HN}$
$\rightarrow Sync\ Failure$
'Sync_Failure', $AUTS_{t_3}$

FIGURE 5. The protocol of the online phase for the presented attack. It is noted that the network here consists of SN and HN.

E. COMPARISONS WITH EXISTING METHODS

The idea of K_{SEAF} violation mentioned in paper [14] is that if the adversaries obtain the K_{AUSF}, the K_{SEAF} can be derived easily. While analysis about vulnerabilities of 5G AKA protocols by the lemmas of TAMARIN Prover is presented in [14], how those exploits occur is not illustrated in a full scenario. As a result, subscribers have no clues how they may suffer in a leakage of personal privacy. On the other hand, this papers provide a concrete scenario with detailed procedures based on the vulnerabilities. Moreover, the work [15] exploits the logic vulnerability of leveraging SQN to monitor genuine subscribers. The main idea of [15] is about how to deduce the SQN from the collected data by adversaries. The work in [15] does not provide a step-by-step scenario, and how the required data is collected by adversaries is not clearly depicted. On the contrary, this paper shows that that only few steps are taken that personal information is leaked, and a clear procedure is presented.

IV. A POSSINLE CUNTERMEASURE

It is shown in Section III that the subscribers have a huge risk in leaking sensitive personal information without any notice and suffering in the privacy violations. Although many countermeasures for 5G AKA protocols are proposed in order to solve security weakness such as the authentication properties [11] and mutual anonymity [17], there are still cases that haven't been approached yet. To overcome the logical vulnerability of SQN mechanism and the attacking scenario illustrated in Section III, it is suggested in this paper that the UE generates RAND by itself instead of using the random number (RAND) that is generated in the ARPF of HN. To be specific, based on TS 33.501 [4], RAND for 5G AKA protocol is generated by ARPF of HN. After generating RAND, ARPF calculates 5G home environment authentication vector (HE AV) based on the RAND. The rest of the parameters in the 5G AKA protocol use the same RAND generated in ARPF. In other words, the following parameters of messages are generated by utilizing the same RAND in previously received messages. It can be seen from Eq. (5) that the same $\boldsymbol{RAND_{t_0}}$ is encrypted by $\boldsymbol{f5^*_K}$ in two different $\boldsymbol{AK^*}$ and can be leveraged by the attacker to inference SQN_{HN}.

On the other hand, assuming different RANDs are used, the two AK* would not equal to each other. As a result, the Eq. (6) would be invalid and the logical vulnerability of SQN mechanism would no longer exists. The procedure based on the proposed countermeasure is shown in Fig. 6. With the suggested scheme of RAND generated by UE, RAND_{UE}, the parameters generated by UE utilizes the latest RAND_{UE} in UE instead of the RAND in the previously received messages. When UE receives Authentication Request from network and triggers the synchronization failure, UE generates AK* with the latest RAND_{UE} instead of the RAND in the received Authentication Request message. For the disclosed tracking-attack scenario, when the attacker injects the Authentication Request ($\text{RAND}^{\text{t}_0}_{\text{UE}}$, AUTN_{t_0}) to the UE at $\text{t} = \text{t}_2$, the UE returns AUTS_{t_2} which $\text{AK}^*_{t_2} = \text{f5}^*_{\text{K}}\left(\text{RAND}^{\text{t}_2}_{\text{UE}}\right)$.

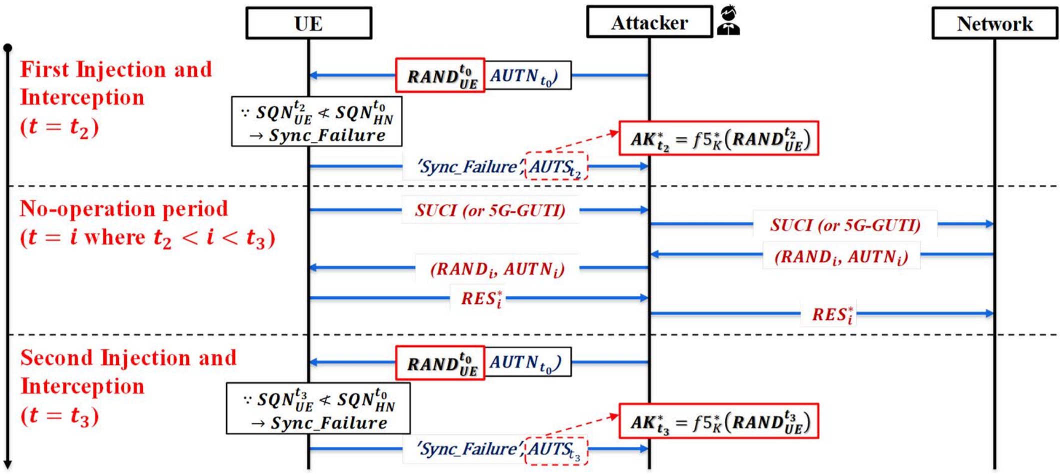

UE
Attacker
Network
First Injection and Interception
$(t = t_2)$
$RAND_{UE}^{t_0}$, $AUTN_{t_0}$
$\because SQN_{UE}^{t_2} \nless SQN_{HN}^{t_0}$
$\rightarrow Sync\_Failure$
$AK_{t_2}^{*} = f5_K^{*}(RAND_{UE}^{t_2})$
'Sync_Failure', $AUTS_{t_2}$
No-operation period
$(t = i$ where $t_2 < i < t_3)$
SUCI (or 5G-GUTI)
SUCI (or 5G-GUTI)
$(RAND_i, AUTN_i)$
$(RAND_i, AUTN_i)$
RES_i^{*}
RES_i^{*}
Second Injection and Interception
$(t = t_3)$
$RAND_{UE}^{t_0}$, $AUTN_{t_0}$
$\because SQN_{UE}^{t_3} \nless SQN_{HN}^{t_0}$
$\rightarrow Sync\_Failure$
$AK_{t_3}^{*} = f5_K^{*}(RAND_{UE}^{t_3})$
'Sync_Failure', $AUTS_{t_3}$

FIGURE 6. A possible countermeasure for the logical vulnerability of SQN mechanism which UE generates RAND instead of ARPF of HN.

Similarly, the attacker will receive AUTS_{t_3} which $\mathrm{AK}^{*}_{t_3} = \mathrm{f5}^{*}_{\mathrm{K}}\left(\mathrm{RAND}^{t_3}_{\mathrm{UE}}\right)$ when injecting again at $\mathrm{t} = \mathrm{t}_3$. As a result, the attacker in tracking-attack can't leverage Eq. (5) again. Instead, the attacker receives

$$AK^{*}_{t_2} = f5^{*}_{K}\left(RAND^{t_2}_{UE}\right) \neq AK^{*}_{t_3} = f5^{*}_{K}\left(RAND^{t_3}_{UE}\right) \qquad (7)$$

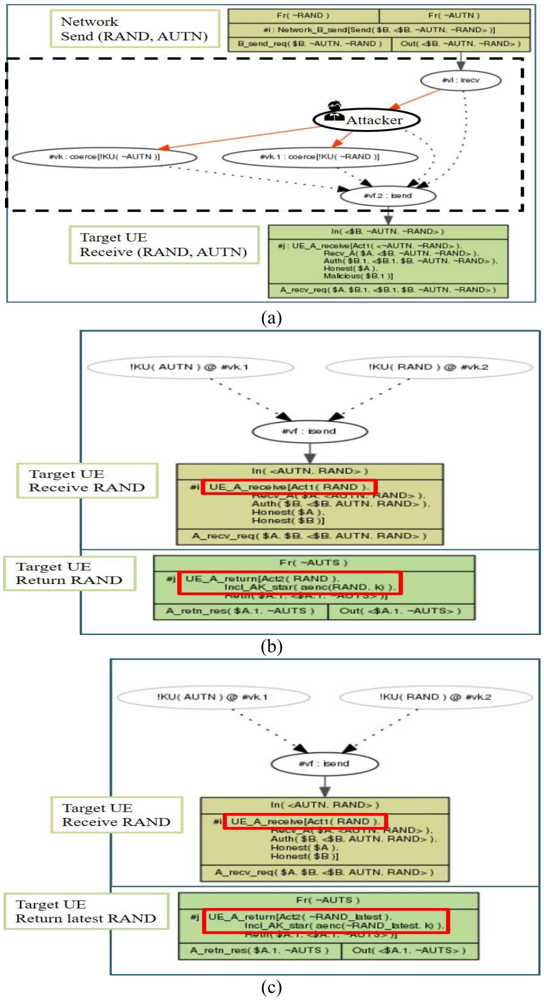
V. EXPERIMENT AND VALIDATION

This section illustrates the validation of the disclosed attacking scenario. The TAMARIN Prover [19] is used to validate the procedures of protocols and to show that the messages between each entity can be easily intercepted by the attacker. The countermeasure mentioned in Section IV is also validated. Furthermore, a practical experiment based on the open source platform srsLTE [20] is conducted so that the discovered tracking-attack scenario is emulated in a complete network architecture.

A. THE LEMMA MODELS OF THE TAMARIN PROVER

The TAMARIN prover [19] is used to demonstrate the procedure illustrated in this paper for validating the attack scenario on 5G AKA protocol. The TAMARIN prover is a validation tool for modling and analysis of security protocols where the multiset rewriting rules are used to define the procedures of 5G AKA protocol and the lemma model is employed for proving the exploits within these specific rules. The diagrams of constrain systems generated from the TAMARIN Prover are shown in Fig. 7. Through the result of the constraint systems in TAMARIN, it can be shown that an attacker can easily fetch the messages. The rectangle blocks in the constraint system represent the procedures of the given rules, that is, the procedures of 5G AKA protocol. The ellipse blocks denote the capabilities of an active attacker.

In particular, the constrain system shown in Fig. 7(a) shows that the attacker intercepts the authentication request, i.e., the eavesdropping step shown in Fig. 6. It is shown in Fig. 7 (a) that when Authentication Request (RAND, AUTN) is sent by SEAF of SN in plaintext, an active attacker intercepts the message and utilizes it to send to other entities or for other usages since the parameters in the message can be fetched separately. Furthermore, it is shown in Fig. 7 (b) that,

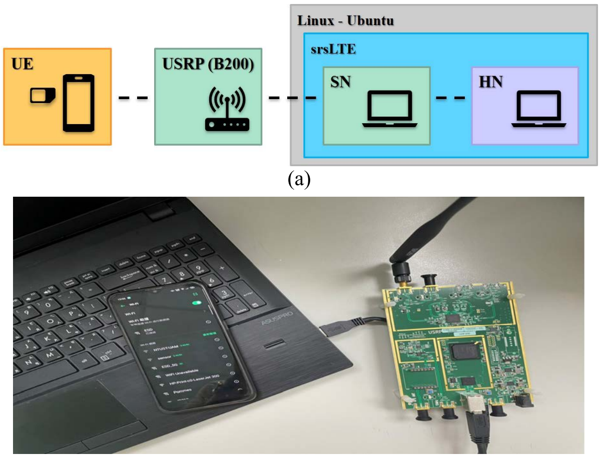


(a)

(b)

(c)

FIGURE 7. (a) The attacker fetches RAND and AUTN in the constraint system of lemma model in TAMARIN Prover. (b) The target UE receives and returns RAND in TAMARIN Prover. (c) The lemma model of receiving latest RAND in TAMARIN Prover.



(a)

(b)

FIGURE 8. (a)The architecture of experiment in srsLTE and (b) The photo of the experiment of tracing-attack scenario in srsLTE.

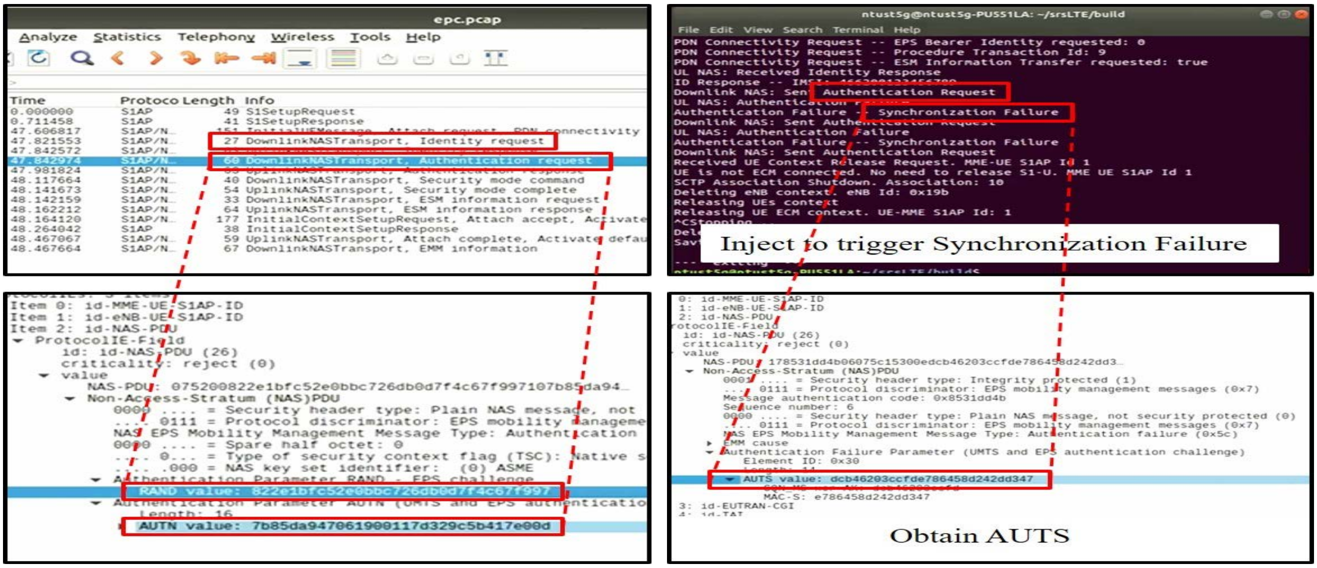
based on the specification TS 33.501, when the UE receives the Authentication Request (RAND, AUTN) from the attacker, the UE utilizes the same RAND to encrypt AK∗. As a result, the same RAND is used by the attacker to infer the $\mathrm{SQN_{HN}}$. As long as the attacker can easily fetch the sensitive messages such as AUTN and RAND, the SQN_{HN} of subscribers can be inferred. Once the attacker obtains the SQN_{HN} as shown in Fig. 3 and follows the procedures that are discovered and demonstrated in Section III, the UE using frequency can be deduced by observing the values changing between different timing SQN_{HN}. The privacy for the target subscriber is then violated and the personal behavior patterns is leaked.

For the countermeasure that is proposed in Section IV, it has been shown that when the attacker injects Authentication Request (RAND_UE, AUTN) toward UE, the AK∗ in the returning failure message form UE will be encrypted by the latest RAND_UE instead of the RAND_UE of injection. Although the AK∗ in AUTS in Fig. 7(c) is as Eq. (7), and the attacker can't leverage as Eq. (6) anymore, the constraint system shows that the attacker can still intercept the AUTS easily.

B. THE EXPERIMENT WITH srsLTE PLATFORM

A practical experimental testbed is setup based on the open source srsLTE to emulate the online phase of the discovered tracking-attack scenario. The overview for the setup of the testbed is shown in Fig. 8(a) where the testbed includes a cellphone with a programmable USIM module to represent the UE. Furthermore, a computer with Ubuntu Linux OS 16.04 is installed with the srsLTE software package and to represents the network. Both EPC (HN) and eNodeB (SN) are resided in the computer and the SN emulates the imperosnated base station. The (Universal Software Radio Peripheral) USRP B200 is employed as the wireless interfance to connect the UE and to the network. After the setup of srsLTE, a blank USIM card is programmed to procide UE a virtual identity IMSI (as SUCI) in order to connect with the network. The photo of the experiment testbed is shown in Fig. 8(b).

At the begining, the SN eavasdrops IMSI and Authentication Request ($\mathrm{RAND_{t_0}}$, $\mathrm{AUTN_{t_0}}$) from the network to UE at t=$\mathrm{t_0}$. The intercepted parameters are shown in Fig. 9(a) where the RAND and AUTN are acquired by the SN. It is noted that the IMSI of UE is assumed to be known. After obtaining these two critical information, the SN impersonate the eNodeB again at t=$\mathrm{t_1}$ and rewrite the file hss.cc for the preparation of the injection in the subsquet step. As long as UE still has connection with the USRP, whether the request is received from the UE or not, the attacker always can inject the Authentication Request ($RAND_{t_0}$, $AUTN_{t_0}$) which is intercepted previously toward UE at t=$\mathrm{t_2}$. In the following,


epc.pcap
Analyze Statistics Telephony Wireless Tools Help
ntust5g@ntust5g-PU551LA: ~/srsLTE/build
File Edit View Search Terminal Help

```
Time          Protoco Length  Info
0.000000      S1AP       49  S1SetupRequest
0.711458      S1AP       41  S1SetupResponse
47.606817     S1AP/N..  151  InitialUEMessage, Attach request, PDN connectivity
47.821553     S1AP/N..   27  DownlinkNASTransport, Identity request
47.842572     S1AP/N..
47.842974     S1AP/N..   60  DownlinkNASTransport, Authentication request
47.981824     S1AP/N..
48.117664     S1AP/N..   40  DownlinkNASTransport, Security mode command
48.141673     S1AP/N..   54  UplinkNASTransport, Security mode complete
48.142159     S1AP/N..   33  DownlinkNASTransport, ESM information request
48.162212     S1AP/N..   64  UplinkNASTransport, ESM information response
48.164120     S1AP/N..  177  InitialContextSetupRequest, Attach accept, Activate
48.264042     S1AP       38  InitialContextSetupResponse
48.467067     S1AP/N..   59  UplinkNASTransport, Attach complete, Activate defau
48.467664     S1AP/N..   67  DownlinkNASTransport, EMM information
```

```
Item 0: id-MME-UE-S1AP-ID
Item 1: id-eNB-UE-S1AP-ID
Item 2: id-NAS-PDU
 ProtocolIE-Field
    id: id-NAS-PDU (26)
    criticality: reject (0)
  value
      NAS-PDU: 075200822e1bfc52e0bbc726db0d7f4c67f997107b85da94…
    Non-Access-Stratum (NAS)PDU
        0000 .... = Security header type: Plain NAS message, not
        .... 0111 = Protocol discriminator: EPS mobility manageme
        NAS EPS Mobility Management Message Type: Authentication
        0000 .... = Spare half octet: 0
        .... 0... = Type of security context flag (TSC): Native s
        .... .000 = NAS key set identifier:  (0) ASME
      Authentication Parameter RAND - EPS challenge
          RAND value: 822e1bfc52e0bbc726db0d7f4c67f997
      Authentication Parameter AUTN (UMTS and EPS authenticatio
          Length: 16
          AUTN value: 7b85da9470619001117d329c5b417e00d
```

(a)

```
PDN Connectivity Request -- EPS Bearer Identity requested: 0
PDN Connectivity Request -- Procedure Transaction Id: 9
PDN Connectivity Request -- ESM Information Transfer requested: true
UL NAS: Received Identity Response
ID Response -- IMSI: 
Downlink NAS: Sent Authentication Request
UL NAS: Authentication Failure
Authentication Failure -- Synchronization Failure
Downlink NAS: Sent Authentication Request
UL NAS: Authentication Failure
Authentication Failure -- Synchronization Failure
Downlink NAS: Sent Authentication Request
Received UE Context Release Request. MME-UE S1AP Id 1
UE is not ECM connected. No need to release S1-U. MME UE S1AP Id 1
SCTP Association Shutdown. Association: 10
Deleting eNB context. eNB Id: 0x19b
Releasing UEs context
Releasing UE ECM context. UE-MME S1AP Id: 1
^CStopping ..
```

Inject to trigger Synchronization Failure

```
0: id-MME-UE-S1AP-ID
1: id-eNB-UE-S1AP-ID
2: id-NAS-PDU
rotocolIE-Field
 id: id-NAS-PDU (26)
 criticality: reject (0)
 value
    NAS-PDU: 178531dd4b06075c15300edcb46203ccfde786458d242dd3…
  Non-Access-Stratum (NAS)PDU
      0001 .... = Security header type: Integrity protected (1)
      .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
      Message authentication code: 0x8531dd4b
      Sequence number: 6
      0000 .... = Security header type: Plain NAS message, not security protected (0)
      .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
      NAS EPS Mobility Management Message Type: Authentication failure (0x5c)
    EMM cause
    Authentication Failure Parameter (UMTS and EPS authentication challenge)
        Element ID: 0x30
        Length: 14
      AUTS value: dcb46203ccfde786458d242dd347
          SQN_MS xor AK: dcb46203ccfd
          MAC-S: e786458d242dd347
3: id-EUTRAN-CGI
4: id-TAI
```

Obtain AUTS

(b)

FIGURE 9. The results in srsLTE showing that (a) eavesdropping Authentication Request (RAND, AUTN) and (b) injection and interception.

the syncronization failure is triggered since an unexpected request ($SQN_{UE}^{t_2} \nless SQN_{HN}^{t_0}$) is recied by the UE. This is presented in Fig. 9(b). At this moment, the AUTS is obtained due to the syncronization failure. After a period of no-operation time after the first injection, the injection steps mentioned above are repeated. Afterwards, the attacker obtains another timing AUTS at $t = t_3$ to infer the $SQN_{HN}^{t_2}$ and deduce service consumption of UE and other personal sensitive information.

VI. CONCLUSION

A tracking-attack scenario making subscribers suffer in a leakage of personal privacy is shown in this paper. The analysis of the attacking scenario is illustrated in this paper and potential countermeasures for protecting the sensitive information of genuine subscribers are given. A lemma model based on the TAMARIN Prover is used to analyze the privacy vulnerabilities in the attack. A practical experiment based on the srsLTE framework is setup to demonstrate how the genuine subscribers are attacked based on the scenario that is depicted in this paper.

REFERENCES

[1] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5G specifications," *IEEE Access*, vol. 7, pp. 24956–24963, 2019.

[2] *3G Security; Security Architecture*, document TS 33.102, Version 16.0.0, 3GPP, Jul. 2020.

[3] *3GPP System Architecture Evolution (SAE); Security Architecture*, document TS 33.401, Version 16.3.0, 3GPP, Jul. 2020.

[4] *Security Architecture and Procedures for 5G System*, document TS 33.501, Version 17.0.0, 3GPP, Dec. 2020.

[5] V. Niemi and K. Nyberg, *UMTS Security*. Hoboken, NJ, USA: Wiley, 2003.

[6] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283–302, 1st Quart., 2014.

[7] M. A. Abdrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, "LTE authentication protocol (EPS-AKA) weaknesses solution," in *Proc. IEEE 7th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2015, pp. 434–441.

[8] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Proc. Int. Symp. Wireless Pers. Multimedia Commun. (WPMC)*, Jun. 2013, pp. 1–9.

[9] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, New Orleans, LA, USA, Dec. 2014, pp. 246–255.

[10] M.-F. Lee, N. P. Smart, B. Warinschi, and G. J. Watson, "Anonymity guarantees of the UMTS/LTE authentication and connection protocol," *Int. J. Inf. Secur.*, vol. 13, no. 6, pp. 513–527, Nov. 2014.

[11] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," Presented at the ACM SIGSAC Conf. Comput. Commun. Secur., Toronto, ON, Canada, 2018.

[12] M. Dehnel-Wild and C. Cremers, "Security vulnerability in 5G-AKA draft," Dept. Comput. Sci., Univ. Oxford, Tech. Rep., Feb. 2018.

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

[14] C. Cremers and M. Dehnel-Wild, "Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion," Presented at the Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA, Feb. 2019.

[15] R. Borgaonkar, L. Hirschi, S. Park, and A. Shaik, "New privacy threat on 3G, 4G, and upcoming 5G AKA Protocols," *Proc. Privacy Enhancing Technol.*, vol. 2019, no. 3, pp. 108–127, Jul. 2019.

[16] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.

[17] 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. 64040–64052, 2019.

[18] 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 *Proc. ACM Conf. Comput. Commun. Secur.*, 2012, pp. 205–216.

[19] D. Basin, C. Cremers, J. Dreier, S. Meier, R. Sasse, and B. Schmidt, "5G-AKA tamarin models," Dept. Comput. Sci., Univ. Oxford, Tech. Rep., 2019.

[20] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srsLTE: An open-source platform for LTE evolution and experimentation," in *Proc. ACM Int. Workshop Wireless Netw. Testbeds, Exp. Eval., Characterization*, 2016, pp. 25–32.

[21] M. Li, L. Zhu, Z. Zhang, C. Lal, M. Conti, and F. Martinelli, "Privacy for 5G-supported vehicular networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1935–1956, 2021.

[22] S. Verma, Y. Kawamoto, and N. Kato, "A network-aware internet-wide scan for security maximization of IPv6-enabled WLAN IoT devices," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8411–8422, May 2021.

[23] J. Xiong, M. Zhao, M. Z. A. Bhuiyan, L. Chen, and Y. Tian, "An AI-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 2, pp. 922–933, Feb. 2021.

[24] J. Zhang, M. Z. A. Bhuiyan, X. Yang, T. Wang, X. Xu, T. Hayajneh, and F. Khan, "AntiConcealer: Reliable detection of adversary concealed behaviors in EdgeAI assisted IoT," *IEEE Internet Things J.*, early access, Aug. 6, 2021, doi: 10.1109/JIOT.2021.3103138.

[25] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[26] Z. Trabelsi and H. Saleous, "Teaching keylogging and network eavesdropping attacks: Student threat and school liability concerns," in *Proc. IEEE Global Eng. Educ. Conf. (EDUCON)*, Apr. 2018, pp. 437–444.

YA-CHU CHENG received the master's degree from the Department of Electronic and Computer Engineering, National Taiwan University of Science and Technology, in July 2021.

CHUNG-AN SHEN (Member, IEEE) received the B.Sc. degree from the National Taiwan University of Science and Technology (NTUST), Taipei, Taiwan, in 2000, the M.Sc. degree from Ohio State University, Columbus, OH, USA, in 2003, and the Ph.D. degree from the University of California, Irvine, in 2012. He joined at the Department of Electronic and Computer Engineering, NTUST, in 2012, where he is currently an Associate Professor. His research interests include signal processing, protocol, and security for wireless communication networks.