FTGPHA: Fixed-Trajectory Group Pre-Handover Authentication Mechanism for Mobile Relays in 5G High-Speed Rail Networks

Ruhui Ma, *Student Member, IEEE*, Jin Cao, *Member, IEEE*, Dengguo Feng, *Member, IEEE*, Hui Li, *Member, IEEE*, and Shiyang He

***Abstract*—For high-speed rail networks, data transmission suffers from severe penetration loss and when the train moves from one base station to another, a large number of User Equipments (UEs) on board carry out the handover authentication procedure simultaneously, which incurs a lot of handover overheads. The introduction of Mobile Relay Node (MRN) can improve the link quality and decrease the handover overheads. However, MRNs still suffer from several protocol attacks and frequent handovers and thus, the introduction of MRNs deteriorates the handover success rate and handover performance. At the same time, considering the diversity of future 5G high-speed rail networks, in this paper, we propose two fixed-trajectory group pre-handover authentication schemes for MRN: the first proposed scheme FTGPHA1 which establishes most of the important security properties and costs low handover overheads, and the second proposed scheme FTGPHA2 which furnishes better security properties than the first one. In these two schemes, since all of the MRNs in the same train and the next base station can accomplish the handover authentication with the help of the donor software defined networking controller before the MRN arrives, the handover delay can be ignored and thus, uninterrupted services can be provided for UEs on board. The security and performance evaluations demonstrate that the two proposed schemes outperform other related schemes.**

***Index Terms*—High-speed rail networks, Group handover authentication, Mobile relay node, Tamarin.**

I. Introduction

With the rapid development of science and technology, more and more individuals pick the fast and convenient high-speed railway as the traffic tool. However, due to the rapid mobility of the high-speed railway, data transmission suffers from severe penetration loss, severe doppler frequency shift and so on [1]. Besides, in high-speed rail networks, when the train leaves one base station to another, a large number of User Equipments (UEs) on board perform the frequent handovers simultaneously, which incurs a lot of communication and computational overheads and thus, may result in handover failure [2]. In order to solve the above problems, the Mobile Relay Node (MRN), which can increase the handover success rate by employing the group handover procedure and ensuring the stability of the link between the MRN and its attached UEs, has been proposed by the third Generation Partnership Project (3GPP) committee [3], [4]. However, since MRNs connect to the 5G core network via an insecure air interface and the introduction of MRNs still incurs frequent handovers in high-speed rail networks [2], it is indispensable to accomplish a secure and seamless handover authentication scheme for MRNs.

Related works: According to the 3GPP standard [4], the MRN handover procedure is identical with the handover procedure of UE defined in [5], [6]. However, the defined handover procedure in [5], [6] exists some security threats such as replay attacks, missing key confirmation attacks, traceability attacks and so on [7]. As far as we know, only a few of handover authentication schemes for MRNs in high-speed rail networks have been proposed [1], [2], [8]–[12] in recent years. Kong *et al.* [1] raised a secure handover session key management scheme based on proxy re-encryption technique in LTE-A. In this scheme, the session keys are initially generated and encrypted with the public key of Mobility Management Entity (MME) by the on-board UEs. Further, these ciphertexts are re-encrypted with the re-encryption key of the target evolved Node B (eNB) by the MRN. Therefore, the target eNB can decrypt these ciphertexts without the direct involvement of the MME. This scheme can successfully establish session keys and achieve the Forward/Backward Key Separation (FKS/BKS). However, this scheme suffers from several protocol attacks such as lacking of Perfect Forward/Backward Secrecy (PFS/PBS), missing key confirmation attacks and so on, and consumes a lot of computational overheads simultaneously. Pan *et al.* [2] put forward an enhanced handover scheme for MRNs, which is backward compatible with the LTE-A layer 2/3 protocols. However, this scheme only focuses on the measurement procedure during handover and thus, the whole handover execution process except for measurement procedure is the same as that in LTE-A, which is vulnerable to several protocol attacks. Tian *et al.* [8]

Manuscript received May 12, 2019; revised September 27, 2019; accepted December 10, 2019. Date of publication December 17, 2019; date of current version February 12, 2020. This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802700, and in part by the National Natural Science Foundation of China under Grants 61772404 and U1836203. The review of this article was coordinated by Prof. W. A. Krzymien. *(Corresponding author: Jin Cao.)*

R. Ma, J. Cao, H. Li, and S. He are with the State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: rhma@stu.xidian.edu.cn; caoj897@gmail.com; lihui@mail.xidian.edu.cn; syhe@xidian.edu.cn).

D. Feng is with the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing 100190, China (e-mail: fengdg@263.net).

This article has supplementary downloadable material available at http://ieeexplore.ieee.org, provided by the authors.

Digital Object Identifier 10.1109/TVT.2019.2960313

0018-9545 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

presented a seamless handover scheme. In this scheme, in order to reduce the handover overheads, the handover request message of each UE collected by Access Points (APs) will be forwarded to the MRN and then the MRN represents all UEs on board to perform the handover process with the ground eNB. Huang *et al.* [9] proposed a mobile relay-based fast handover scheme in LTE-A. In this scheme, in order to improve the performance of handover, the pre-preparation message containing the context information, position and velocity information shall be sent to the target eNB before handover. Once the MRN arrives at the target eNB, the target eNB initiates the handover process, which can reduce handover execution time. However, the schemes in [8], [9] do not consider the handover security. Cao *et al.* [10] designed a handover authentication mechanism based on trajectory prediction. In this scheme, all eNBs deployed along the vehicle route form a route-eNB group and share a group key. The mutual authentication and key agreement process between the MRN and the target eNB is achieved with ideal efficiency. However, this scheme does not implement some important security properties, such as privacy preserving, PFS/PBS and so on. Cao *et al.* [11] put forward a group-to-route handover authentication scheme for mobile relays. By this scheme, all of the Donor evolved NodeBs (DeNBs) deployed along the route construct a route-DeNB group and all of the MRNs on board build a MRN group. The source DeNB generates a Handover Ticket (HT) for each MRN and then the HT is employed to accomplish the mutual authentication and key agreement between the MRN group and the target DeNBs. However, this scheme cannot achieve the FKS/BKS, PFS/PBS, anonymity and unlinkability. Haddad *et al.* [12] introduced a privacy-preserving intra-MME group handover via MRN in LTE-A networks for repeated trips. By this scheme, each user possesses a number of one-time public/private key pairs and chooses one of his one-time private keys to generate a signature. The MRN aggregates all these signatures and transmits them to the target eNB. This scheme establishes anonymous authentication and preserves the user's privacy. However, the scheme incurs a lot of communication and computational overheads due to the use of the multiple bilinear pairing operations.

For these schemes in [1], [8]–[10], [12], only a single MRN on board is taken into account. With the rapid development of 5G high-speed railway, there will be more and more UEs on the train and thus, a single MRN may not provide high quality service for massive UEs on board. For these schemes in [2], [11], several MRNs on board are considered to guarantee high quality service and group handover procedure is employed to further shorten the handover overheads. However, for the scheme in [2], the master MRN performs the handover procedure first and then the general MRNs start the handover procedure, which shall result in lengthening the handover time. In addition, both of these schemes in [2], [11] suffer from a lot of protocol attacks. Therefore, it is meaningful to design a secure and seamless group handover authentication scheme for several MRNs on board.

Until now, several group handover authentication schemes for other networks have been proposed [13]–[17]. In these schemes [13]–[15], all security contexts of group members are transmitted by the source eNB to the target eNB when the first UE performs the handover procedure. Thus, the rest of the group members can directly perform the handover procedure without the re-assistance of the source eNB. However, these schemes still incur a lot of handover costs and do not implement some important security properties, such as privacy preserving, PFS/PBS and so on. Lai *et al.* [16] put forward a secure and efficient group roaming scheme based on a novel certificateless aggregate signature technique. By this scheme, group members can be simultaneously authenticated by the access networks. However, the access networks cannot be trusted by the group members and thus, the mutual authentication cannot be accomplished. Cao *et al.* [17] raised a uniform group-based handover authentication for MTC in LTE-A networks. Owing to the use of the multi-signature and Aggregate Message Authentication Code (AMAC) techniques, this scheme can largely reduce the signaling costs and thus, avoid signaling congestion. However, this scheme cannot fulfill these important security properties including privacy preserving, PFS/PBS and so on, and it consumes a lot of computational costs on the UE due to the use of multiple modular exponentiation operations.

Contributions: In this paper, we adopt the group pre-handover authentication mechanism, which can perform the handover authentication procedure in advance and thus provide uninterrupted services for UEs. Further, considering the diversity of future 5G high-speed rail networks, in some scenarios, users have poor performance and need relatively low security requirements, while in other scenarios, the opposite is true. Thus, in this paper, we propose two fixed-trajectory group pre-handover authentication schemes: FTGPHA1 and FTGPHA2. By the FTGPHA1, the standard handover mechanism is slightly enhanced to achieve the fast pre-handover for a group of MRNs. By the FTGPHA2, each MRN generates a private/public key by using the partial private/public key generated by itself and another partial private/public key obtained from the access network and then employs the generated key pair to finish the pre-handover procedure based on the aggregate signcryption technique. Our contributions made in this paper can be summarized up as follows.

1) In these two schemes, since the Donor Software Defined Networking controller ($D-SDN$) obtains the fixed-trajectory information of the train from the MRN group in advance and thus, determines which base station the MRN group will connect to, the MRN group and the next base station can perform the handover authentication and negotiate the session key before the MRN group arrives at the next base station. Thus, the handover delay can be ignored. Besides, considering the fast handover in fast moving trains with the deployment of small cell in 5G networks [2], the collaborative handover procedures are taken into account in these two schemes and the signaling, communication and computational overheads can be shortened.
2) The proposed FTGPHA1 is a lightweight pre-handover authentication scheme, which can achieve most of the security properties and only consume a small amount of signaling, communication and computational overheads.
3) The proposed FTGPHA2 is a secure-enhanced pre-handover authentication scheme, which can accomplish

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

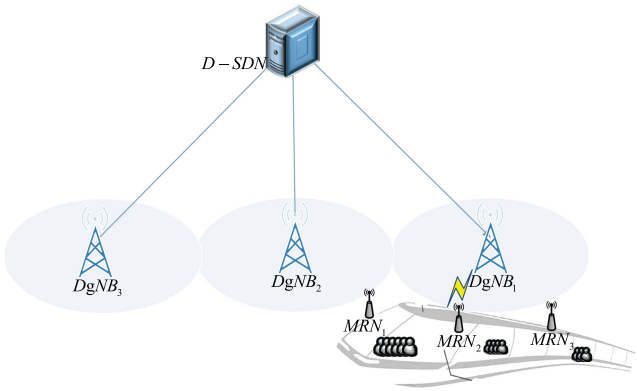


Fig. 1. High-speed rail network architecture.

the robust security properties including mutual authentication, key agreement, PFS/PBS, anonymity, unlinkability, FKS/BKS as well as withstanding several protocol attacks. At the same time, it can achieve the ideal efficiency.

4) The formal verification tool named Tamarin is employed to demonstrate that the two proposed schemes can achieve these security properties.

Outline: The remainder of this paper is organized as follows. In Section II, we firstly present our high-speed rail network architecture and give our design idea. Subsequently, we introduce the proposed FTGPHA1 and FTGPHA2 in Section III and Section IV, respectively. Then, we give the security and performance evaluations in Section V and Section VI, respectively. Finally, we draw a conclusion in Section VII.

II. System Model and Design Idea

A. System Model

Fig. 1 depicts the detailed modules of the proposed high-speed rail network architecture, which mainly consists of four parts: $D-SDN$ [18], Donor New Radio Node B (DgNB), MRN and UE. $D-SDN$ is just a program running on the server and can be placed anywhere in the 5G core network [19]. $D-SDN$ and DgNBs are connected over the wired links, whereas DgNBs and MRNs are connected over wireless links. In this architecture, we explore $D-SDN$ as a platform for user authentication, authorization and mobility management. MRN pre-installed on the train acts as a UE to perform the initial authentication and handover procedures and then acts as a base station to provide uninterrupted connectivity services for the UEs. DgNBs acting as the base stations of 5G Radio Access Network (5G-RAN) are used to realize hop by hop protection between MRNs and the $D-SDN$ [3].

B. Design Idea

The critical design idea of the proposed schemes can be briefly described as follows. All MRN_i s installed on the same train construct a MRN group. Without loss of generality, we assume the number of the MRN group members is n and MRN_1 is supposed to be the group leader. In the high-speed railway running process, MRN_1 with active power supply can continuously monitor the signal strength, the effective coverage of the source DgNB $DgNB_1$, the current geographic location information and the heading and speed of the train. Moreover, MRN_1 judges whether the Handover Trigger Threshold (HTT) is reached based on the monitored data. For example, assume the HTT is that the time for a train to continue to reside at the $DgNB_1$ is less than 3 seconds. Upon reaching the HTT, MRN_1 unites the MRN group members to transmit a user handover request message including the trajectory information of the train to the $D-SDN$ via the $DgNB_1$. Receiving the user handover request message, since the trajectory of the high-speed railway is usually fixed, $D-SDN$ can store/obtain the location information of all DgNBs and further determine the next DgNB $DgNB_2$ that MRNs will visit. Meanwhile, in consideration of the possibility that once entering the range of the $DgNB_2$ the train will quickly leave and enter the range of the next base station $DgNB_3$, the collaborative handover procedure for the MRN group to perform the handover procedure with the $DgNB_2$ and the $DgNB_3$ simultaneously is taken into account. $D-SDN$ judges whether the Collaborative Handover Trigger Threshold (CHTT) is reached from the trajectory information of train and the necessary information of the $DgNB_2$.

III. The First Proposed Scheme: FTGPHA1

A. Brief Overview of This Scheme

In this section, we present a simple group-based pre-handover authentication scheme with low computational overheads. Note that when the MRN_i firstly enters the network, the standard 5G-AKA/EAP-AKA' [6], [20] can be employed to achieve the initial authentication procedure for each MRN_i. As stated in [6], after the successful initial authentication procedure, the MRN_i and the Access and Mobility Management Function (AMF) can obtain the shared secret key K_{AMF_i} and the temporary identity $5G-GUTI_i$. Subsequently, the NH_i shall be derived via the K_{AMF_i}, and the AMF provides the NH_i and the $5G-GUTI_i$ to the source DgNB $DgNB_1$. Finally, the session key K_{gNB_i} will be derived from the NH_i and be employed to protect the communication channel.

When the train is about to leave the current base station $DgNB_1$, the pre-handover authentication procedure with the assistance of the $DgNB_1$ and the $D-SDN$ is initiated. By the procedure, the MRN group members send their valid temporary identities to the MRN group leader MRN_1 and then the MRN_1 transmits all the received identities together with the train's information to the $D-SDN$. The $D-SDN$ verifies the identities, picks a suitable target DgNB $DgNB_2$ and sends a new NH_i^* to the $DgNB_2$. Subsequently, the MRN group members and the $DgNB_2$ employ the new NH_i^* to compute the session key. The brief overview of the first scheme is shown in Fig. 2

B. The Concrete Process

The detailed group-based pre-handover authentication procedure is presented in the following steps.

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

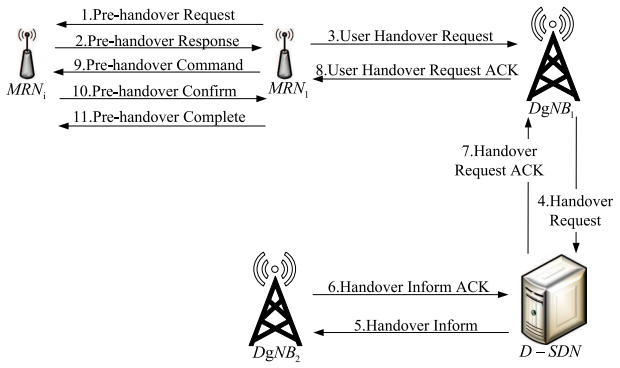


Fig. 2. Overview of the FTGPHA1.

Step 1: $MRN_1 \rightarrow MRN_i$: PRE-HANDOVER REQUEST (r_M)
When HTT is satisfied, the MRN_1 generates a random number r_M and broadcasts it by a PRE-HANDOVER REQUEST message.

Step 2: $MRN_i \rightarrow MRN_1$: PRE-HANDOVER RESPONSE $(5G-GUTI_i, MAC_i)$
Upon the receipt of the message, each MRN_i computes $MAC_i = h(SUPI_i, NH_i, r_M)$ and responds with the PRE-HANDOVER RESPONSE message including its temporary identity $5G-GUTI_i$ and MAC_i, where $SUPI_i$ is the SUbscription Permanent Identifier of the MRN_i corresponding to the $5G-GUTI_i$ and the $h()$ is a secure one-way hash function.

Step 3: $MRN_1 \rightarrow DgNB_1$: USER HANDOVER REQUEST $((5G-GUTI_i)_{i=1,\ldots,n}, MAC, r_M, other)$
On receiving these PRE-HANDOVER RESPONSE messages, the MRN_1 calculates $MAC = MAC_1 \oplus MAC_2 \oplus \ldots \oplus MAC_n$ and transmits a USER HANDOVER REQUEST message containing the MAC, the r_M, all the MRN_i's $5G-GUTI_i$ and other necessary information for the handover such as the position, speed and heading of the train to the source DgNB, where the necessary information of the train shall be encrypted with the session key K_{gNB_1} between the MRN_1 and the $DgNB_1$.

Step 4: $DgNB_1 \rightarrow D-SDN$: HANDOVER REQUEST $((5G-GUTI_i)_{i=1,\ldots,n}, MAC, r_M, other)$
Upon the receipt of the USER HANDOVER REQUEST message, the $DgNB_1$ forwards it to the $D-SDN$.

Step 5: $D-SDN \rightarrow DgNB_2$: HANDOVER INFORM $((5G-GUTI_i{}^*, NH_i{}^*)_{i=1,\ldots,n})$
On receiving the HANDOVER REQUEST message, the $D-SDN$ firstly checks if the r_M is fresh, then searches the $SUPI_i$ and the NH_i corresponding to the $5G-GUTI_i$ values and verifies if the MAC is correct. If both the verifications are successful, the $D-SDN$ selects the suitable next DgNB $DgNB_2$ based on the gathered trajectory information of the train and the base stations, and computes a new $NH_i{}^*$ for each MRN_i as shown in Eq.(1). Besides, the $D-SDN$ calculates a new temporary value $5G-GUTI_i{}^*$ for each MRN_i as shown in Eq.(2). Then, the $D-SDN$ sends a HANDOVER INFORM message including all the $(5G-GUTI_i{}^*, NH_i{}^*)$ and other necessary information for handover to $DgNB_2$.

$$NH_i{}^* = KDF(K_{AMF_i}, NH_i, r_M) \quad (1)$$

$$5G-GUTI_i{}^* = KDF(SUPI_i, NH_i{}^*, r_M) \quad (2)$$

In addition, if detecting that the CHTT is satisfied, the $D-SDN$ shall initiate the collaborative handover procedure. Concretely, the $D-SDN$ computes a new $NH_i{}^{**}$ and a new $5G-GUTI_i{}^{**}$ for each MRN_i. Subsequently, the $D-SDN$ sends a HANDOVER INFORM message including the new $(5G-GUTI_i{}^{**}, NH_i{}^{**})$ to the $DgNB_3$. In this case, the $D-SDN$ sets the value of $ContinousChangeBS$ field to true.

Step 6: $DgNB_2 \rightarrow D-SDN$: HANDOVER INFORM ACK (m_{gNB_2})
Once receiving the HANDOVER INFORM message from the $D-SDN$, the $DgNB_2$ computes the new session key for each MRN_i as shown in Eq.(3) and associates the $K_{gNB_i}{}^*$ with the $5G-GUTI_i{}^*$. The $DgNB_2$ shall directly use the $K_{gNB_i}{}^*$ as the session key with the MRN_i and adopt the $5G-GUTI_i{}^*$ as each MRN_i's temporary identity. Then, the $DgNB_2$'s information m_{gNB_2} containing the $DgNB_2$'s Physical Cell ID (PCI), Frequency ARFCN-DL (FADL) and so on, will be included in the HANDOVER INFORM ACK message and sent back to the $D-SDN$. Finally, each $(5G-GUTI_i{}^*, K_{gNB_i}{}^*)$ will be stored in the $DgNB_2$.

$$K_{gNB_i}{}^* = KDF(NH_i{}^*, PCI, FADL) \quad (3)$$

In addition, if the $DgNB_3$ also receives the HANDOVER INFORM message from the $D-SDN$, it performs the same operations as $DgNB_2$ and sends m_{gNB_3} to the $D-SDN$.

Step 7: $D-SDN \rightarrow DgNB_1$: HANDOVER REQUEST ACK $(m_{gNB_2}, r_D, MAC^*)/(m_{gNB_2}, m_{gNB_3}, r_D, MAC^*, ContinousChangeBS)$
Upon the receipt of the HANDOVER INFORM ACK message, the $D-SDN$ picks a random number r_D and calculates the MAC^* as shown in Eq. 4 or Eq. 5 in case the value of $ContinousChangeBS$ field is true and transmits a HANDOVER REQUEST ACK message including m_{gNB_2}, r_D and MAC^* to the source DgNB. Note that the $h()$ is a secure one-way function. The m_{gNB_3} and the indication $ContinousChangeBS$ shall also be included

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

in the HANDOVER REQUEST ACK message if the value of $ContinousChangeBS$ field is true.

$$MAC^* = h(m_{gNB_2}, NH_1{}^*, SUPI_1, r_D) \oplus \ldots h(m_{gNB_2}, NH_n{}^*, SUPI_n, r_D) \quad (4)$$

$$MAC^* = h(m_{gNB_2}, NH_1{}^*, SUPI_1, r_D) \oplus h(m_{gNB_3}, NH_1{}^{**}, SUPI_1, r_D) \oplus \ldots h(m_{gNB_2}, NH_n{}^*, SUPI_n, r_D) \oplus h(m_{gNB_3}, NH_n{}^{**}, SUPI_n, r_D) \quad (5)$$

Step 8: $DgNB_1 \rightarrow MRN_1$: USER HANDOVER REQUEST ACK (m_{gNB_2}, r_D, MAC^*) / $(m_{gNB_2}, m_{gNB_3}, r_D, MAC^*, ContinousChangeBS)$
On receiving the HANDOVER REQUEST ACK message from the $D-SDN$, the source DgNB $DgNB_1$ transmits them to the MRN_1 in a USER HANDOVER REQUEST ACK message.

Step 9: $MRN_1 \rightarrow MRN_i$: PRE-HANDOVER COMMAND $(m_{gNB_2}, r_D)/(m_{gNB_2}, m_{gNB_3}, r_D, ContinousChangeBS)$
Upon the receipt of the USER HANDOVER REQUEST ACK message, the MRN_1 broadcasts the PRE-HANDOVER COMMAND message including the (m_{gNB_2}, r_D) or $(m_{gNB_2}, m_{gNB_3}, r_D, ContinousChangeBS)$ to the MRN group members.

Step 10: $MRN_i \rightarrow MRN_1$: PRE-HANDOVER CONFIRM $MAC_i{}^*$
On receiving the PRE-HANDOVER COMMAND message, each MRN_i firstly checks if the r_D is fresh. If it is, each MRN_i verifies if the value of $ContinousChangeBS$ field is true. If it is not true, each MRN_i computes a new $NH_i{}^*$ as shown in Eq.(1) and figures out the $MAC_i{}^* = h(m_{gNB_2}, NH_i{}^*, SUPI_i, r_D)$. Otherwise, each MRN_i calculates $NH_i{}^*$ and $NH_i{}^{**}$, and works out the $MAC_i{}^* = h(m_{gNB_2}, NH_i{}^*, SUPI_i, r_D) \oplus h(m_{gNB_3}, NH_i{}^{**}, SUPI_i, r_D)$. Finally, each MRN_i transmits the $MAC_i{}^*$ to the MRN_1.

Step 11: Once the receipt of these PRE-HANDOVER CONFIRM messages, the MRN_1 verifies the validity of the Eq. 6. If the verification is successful, the MRN_1 sends a PRE-HANDOVER COMPLETE message to each MRN_i and a HANDOVER CONFIRM message to the $DgNB_2$.

$$MAC^* = MAC_1{}^* \oplus MAC_2{}^* \ldots \oplus MAC_n{}^* \quad (6)$$

Subsequently, each MRN_i calculates the new session key ${K_{gNB_i}}^*$ to be used with the $DgNB_2$ as shown in Eq.(3) and derives its new temporary identity $5G-GUTI_i^*$ as shown in Eq.(2). If the received value of $ContinousChangeBS$ field is true, each MRN_i calculates two sets of data: $({K_{gNB_i}}^*, 5G-GUTI_i{}^*)$ used between the MRN_i and the $DgNB_2$, and $({K_{gNB_i}}^{**}, 5G-GUTI_i{}^{**})$ used between the MRN_i and the $DgNB_3$. Upon the receipt of the HANDOVER CONFIRM message, the next DgNB prepares the admission control for each MRN_i.

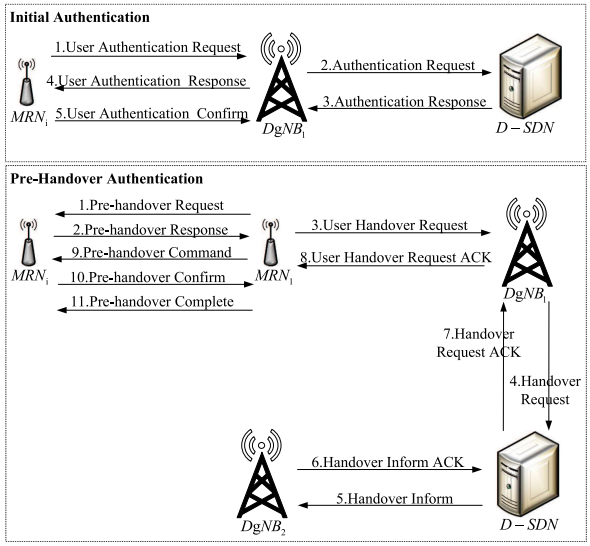


Fig. 3. Overview of the FTGPHA2.

After the pre-handover procedure, once the train enters the range of the next DgNB $DgNB_2$/$DgNB_3$, each MRN_i and the next DgNB can directly use the session key $K_{gNB_i}^*$/$K_{gNB_i}^{**}$ to communicate with each other.

IV. The Second Proposed Scheme: FTGPHA2

A. Brief Overview of This Scheme

In this section, we present a new secure-enhanced group-based pre-handover authentication scheme. Although it costs more overheads than the first one, it can achieve a higher security level than the first one. Note that when each MRN_i enters into the 5G network, it performs the initial authentication procedure. In this procedure, by providing its valid identities, the MRN_i can obtain its private key and public key from the $D-SDN$. At the same time, with the assistance of the $D-SDN$, the MRN_i negotiates the session key with its current DgNB $DgNB_1$. When the MRN group will leave from one base station to another, the MRN group performs the pre-handover authentication procedure. In this procedure, each MRN_i encrypts and signs its privacy information, and then the MRN group leader MRN_1 aggregates all signatures to a single signature and sends it to the $D-SDN$. Subsequently, the $D-SDN$ verifies the signature. If the verification is successful, the $D-SDN$ chooses the suitable next DgNB $DgNB_2$ and assists the $DgNB_2$ and the MRN group members to negotiate the session key. The brief overview of the second scheme is shown in Fig. 3. The notations used in this scheme are given in Table I.

B. The Concrete Process

The detailed process includes the following three phases, which are described as follows.

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

TABLE I
NOTATIONS IN FTGPHA2

Notation	Definition
G	a cycle group on an elliptic curve E
P, q	the generator and the order of the G
sk_{SDN}/pk_{SDN}	the private/public key of $D-SDN$
sk_i/pk_i	the private/public key of node i
$H_1() - H_6()$	$H_1 : G \rightarrow \{0,1\}^*$, $H_2 : G \rightarrow Z_q{}^*$, $H_3 : G \times G \times \{0,1\}^* \rightarrow Z_q{}^*$, $H_4 : G \times \{0,1\}^* \rightarrow \{0,1\}^*$, $H_5 : G \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q{}^*$, $H_6 : G \times \{0,1\}^* \times G \times \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q{}^*$

1) Initialization Phase: In the initialization procedure, the $D-SDN$ chooses a cycle group G on an elliptic curve E. The generator of the G is P and the order of the G is q. Besides, the $D-SDN$ picks a random number $sk_{SDN} \in Z_q{}^*$ as the master secret key and the pk_{SDN} as the raw public key, where $pk_{SDN} = sk_{SDN} * P$ and pk_{SDN} is securely provisioned to the MRN group members. Subsequently, the $D-SDN$ chooses six secure hash functions, H_1, H_2, H_3, H_4, H_5 and H_6. Finally, the $D-SDN$ publishes $(G, P, q, H_1, H_2, H_3, H_4, H_5, H_6)$ as the system public parameters and keeps the sk_{SDN} in secret.

2) Initial Authentication Phase: When each MRN_i firstly connects to the 5G network, it needs to perform the initial authentication process with the $D-SDN$ as follows.

Step 1: $MRN_i \rightarrow DgNB_1$: USER AUTHENTICATION REQUEST (C_i, K_i)
The MRN_i randomly selects a value $k_i \in Z_q{}^*$, and computes U_i, K_i and the ciphertext C_i as shown in Eq.(7), where the MRN_i's identity $SUPI_i/5G-GUTI_i$ is denoted as ID_i. Then, the MRN_i sends a USER AUTHENTICATION REQUEST message including the C_i and K_i to the $DgNB_1$.

$$\begin{aligned} U_i &= k_i * pk_{SDN} \\ K_i &= k_i * P \\ C_i &= H_1(U_i) \oplus ID_i \end{aligned} \tag{7}$$

Step 2: $DgNB_1 \rightarrow D-SDN$: AUTHENTICATION REQUEST (C_i, K_i)
The $DgNB_1$ forwards the received message to the $D-SDN$.

Step 3: $D-SDN \rightarrow DgNB_1$: AUTHENTICATION RESPONSE $(A_i, Y_i, TK_{1-i}, ID_i')$
Upon the receipt of the message from $DgNB_1$, the $D-SDN$ computes U_i' and decrypts the MRN_i's identity ID_i' from C_i as shown in Eq.(8).

$$\begin{aligned} U_i' &= K_i * sk_{SDN} \\ ID_i' &= H_1(U_i') \oplus C_i \end{aligned} \tag{8}$$

Then, the $D-SDN$ picks a random number $y_i \in Z_q{}^*$ and computes Y_i, the MRN_i's public key pk_i, z_i and TK_{1-i} as shown in Eq.(9).

$$\begin{aligned} Y_i &= y_i * P \\ pk_i &= Y_i + K_i \\ z_i &= y_i + sk_{SDN} * H_3(pk_i, pk_{SDN}, ID_i') \\ &\mod q \\ TK_{1-i} &= y_i * K_i \end{aligned} \tag{9}$$

Besides, in order to protect the MRN_i's secret value z_i, we adopt the following operation.

$$A_i = H_2(U_i') \oplus z_i \tag{10}$$

Finally, the $D-SDN$ sends a AUTHENTICATION RESPONSE message including the $(A_i, Y_i, TK_{1-i}, ID_i')$ to the $DgNB_1$ and stores the $(ID_i,' pk_i)$.

Step 4: $DgNB_1 \rightarrow MRN_i$: USER AUTHENTICATION RESPONSE (A_i, Y_i)
The $DgNB_1$ stores the TK_{1-i} as the session key with the MRN_i and makes the ID_i' as the MRN_i's identity. The $DgNB_1$ forwards the (A_i, Y_i) to the MRN_i in the USER AUTHENTICATION RESPONSE message.

Step 5: $MRN_i \rightarrow DgNB_1$: USER AUTHENTICATION CONFIRM
Upon receiving the message, the MRN_i computes z_i' and pk_i, and verifies z_i' as shown in Eq.(11).

$$\begin{aligned} z_i' &= H_2(U_i) \oplus A_i \\ pk_i &= Y_i + K_i \\ z_i' * P &= Y_i + pk_{SDN} * H_3(pk_i, pk_{SDN}, ID_i) \end{aligned} \tag{11}$$

If the verification is successful, the MRN_i computes the session key TK_{1-i} with the $DgNB_1$ as shown in Eq.(12), stores sk_i as its private key and pk_i as its public key and sends a USER AUTHENTICATION CONFIRM message to the $DgNB_1$.

$$\begin{aligned} TK_{1-i} &= k_i * Y_i \\ sk_i &= (z_i' + k_i) \, mod \, q \end{aligned} \tag{12}$$

After the initial authentication procedure, the session key TK_{1-i} can be employed to ensure the security of the communication channel between the $DgNB_1$ and the MRN_i and the key pair (sk_i, pk_i) can be used to accomplish the pre-handover authentication procedure.

3) Pre-Handover Authentication Phase: When detecting that the HTT is reached, the MRN_1 works as follows.

Step 1: $MRN_1 \rightarrow MRN_i$: PRE-HANDOVER REQUEST
The MRN_1 issues a PRE-HANDOVER REQUEST message to inform its group members to prepare the pre-handover authentication procedure.

Step 2: $MRN_i \rightarrow MRN_1$: PRE-HANDOVER RESPONSE (X_i, S_i, C_i)
Upon the receipt of the PRE-HANDOVER REQUEST message, the MRN_i picks a random number $x_i \in Z_q{}^*$ and computes X_i, V_i, the signature S_i and the ciphertext C_i as shown in Eq.(13), where the M_i contains the necessary information for handover

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

authentication, such as the MRN_i's temporary ID (5G-GUTI).

$$X_i = x_i * P$$
$$V_i = x_i * pk_{SDN}$$
$$S_i = x_i + sk_i + H_3(V_i, X_i, M_i)\ mod\ q$$
$$C_i = H_1(V_i) \oplus M_i \tag{13}$$

Finally, the MRN_i sends a PRE-HANDOVER RESPONSE message including the (X_i, S_i, C_i) to the MRN_1.

Step 3: $MRN_1 \rightarrow DgNB_1$: USER HANDOVER REQUEST $((X_i, C_i)_{i=1,\ldots,n}, sumS, other)$
On receiving these PRE-HANDOVER RESPONSE messages, the MRN_1 computes the $sumS$ as shown in Eq.(14). Finally, the MRN_1 sends a USER HANDOVER REQUEST message containing $((X_i, C_i)_{i=1,\ldots,n}, sumS)$ and other necessary information for the handover such as the position, speed and heading of the train to the $DgNB_1$, where the message can be encrypted with the session key TK_{1-1} between the $DgNB_1$ and the MRN_1.

$$sumS = \sum_{i=1}^{n} S_i\ mod\ q \tag{14}$$

Step 4: $DgNB_1 \rightarrow D - SDN$: HANDOVER REQUEST $((X_i, C_i)_{i=1,\ldots,n}, sumS, other)$
Upon receiving the USER HANDOVER REQUEST message, the $DgNB_1$ forwards it to the $D - SDN$ in the HANDOVER REQUEST message.

Step 5: $D - SDN \rightarrow DgNB_2$: HANDOVER INFORM $((X_i, M_i')_{i=1,\ldots,n})$
On receiving the HANDOVER REQUEST message, the $D - SDN$ obtains all the MRN's M_i' as shown in Eq.(15).

$$V_i' = X_i * sk_{SDN}$$
$$M_i' = H_1(V_i') \oplus C_i \tag{15}$$

Then, the $D - SDN$ verifies the MRN group as shown in Eq.(16), where the ID_i' can be parsed from the M_i' and the pk_i can be searched based on the ID_i'. If the verification is successful, the $D - SDN$ determines the suitable next DgNB $DgNB_2$ for the MRN group based on the existing trajectory and the received necessary information of the train, and sends a HANDOVER INFORM message including the $((X_i, M_i')_{i=1,\ldots,n})$ to the $DgNB_2$ in the secure channel, which has been established in advance.

$$sumS * P = \sum_{i=1}^{n} X_i + \sum_{i=1}^{n} pk_i + \left(\sum_{i=1}^{n} H_3(V_i,' X_i, M_i')\ mod\ q\right) * P + \left(\sum_{i=1}^{n} H_3(pk_i, pk_{SDN}, ID_i')\ mod\ q\right) * pk_{SDN} \tag{16}$$

In addition, if the $D - SDN$ detects that the CHTT is satisfied, the collaborative handover process shall be initiated. Concretely, the $D - SDN$ also sends a HANDOVER INFORM message including the $((X_i, M_i')_{i=1,\ldots,n})$ to the $DgNB_3$. In this case, the $D - SDN$ sets the value of $ContinousChangeBS$ field to true.

Step 6: $DgNB_2 \rightarrow D - SDN$: HANDOVER INFORM ACK (R, m_{gNB_2}, HV)
On receiving the HANDOVER INFORM message, the $DgNB_2$ randomly selects a value $r \in {Z_q}^*$ and computes a value R and the session key TK_{2-i} for each MRN_i as shown in Eq.(17).

$$R = r * P$$
$$TK_{2-i} = r * X_i \tag{17}$$

Subsequently, the $DgNB_2$ calculates a hash value HV as shown in Eq.(18).

$$HV = H_4(TK_{2-1}, M_1') \oplus \ldots \oplus H_4(TK_{2-n}, M_n') \tag{18}$$

Finally, the HANDOVER INFORM ACK message including (R, m_{gNB_2}, HV) is sent back to the $D - SDN$.
In addition, if the $DgNB_3$ also receives the HANDOVER INFORM message, it performs the same operations as $DgNB_2$ and transmits (R^*, m_{gNB_3}, HV^*) to the $D - SDN$.

Step 7: $D - SDN \rightarrow DgNB_1$: HANDOVER REQUEST ACK (R, m_{gNB_2}, HV') / $(R, m_{gNB_2}, R^*, m_{gNB_3}, HV,'' ContinousChangeBS)$
Upon the receipt of the HANDOVER INFORM ACK message, the $D - SDN$ forwards the message including the (R, m_{gNB_2}, HV') to the $DgNB_1$, where the hash value HV' is computed as shown in Eq.(19).

$$HV' = H_5(R, m_{gNB_2}, HV) \tag{19}$$

In addition, if the value of $ContinousChangeBS$ field is true, the $D - SDN$ gathers the received two messages into $(R, m_{gNB_2}, R^*, m_{gNB_3}, HV'')$ and transmits a HANDOVER REQUEST ACK message including $(R, m_{gNB_2}, R^*, m_{gNB_3}, HV,'' ContinousChangeBS)$ to the $DgNB_1$, where the hash value HV'' is computed as shown in Eq.(20).

$$HV'' = H_6(R, m_{gNB_2}, R^*, m_{gNB_3}, HV \oplus HV^*) \tag{20}$$

Step 8: $DgNB_1 \rightarrow MRN_1$: USER HANDOVER REQUEST ACK (R, m_{gNB_2}, HV') / $(R, m_{gNB_2}, R^*, m_{gNB_3}, HV'', ContinousChangeBS)$

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

Once obtaining the HANDOVER REQUEST ACK message, the $DgNB_1$ forwards it to the MRN_1 in the USER HANDOVER REQUEST ACK message.

Step 9: $MRN_1 \rightarrow MRN_i$: PRE-HANDOVER COMMAND (R) / $(R, R^*, ContinousChangeBS)$
On receiving the USER HANDOVER REQUEST ACK message, the MRN_1 broadcasts a PRE-HANDOVER COMMAND message including the $(R)/(R, R^*, ContinousChangeBS)$ to the MRN group members.

Step 10: $MRN_i \rightarrow MRN_1$: PRE-HANDOVER CONFIRM (RES_i)
Once the MRN_i obtains the R, the MRN_i computes the session key TK_{2-i} and generates a PRE-HANDOVER CONFIRM message including RES_i as shown in Eq.(21).

$$\begin{aligned} TK_{2-i} &= R * x_i \\ RES_i &= H_4(TK_{2-i}, M_i) \end{aligned} \tag{21}$$

In addition, if the value of $ContinousChangeBS$ field is true, each MRN_i needs to calculate two session keys: $TK_{2-i} = R * x_i$ with the $DgNB_2$ and $TK_{3-i} = R^* * x_i$ with the $DgNB_3$. Besides, the MRN_i generates the PRE-HANDOVER CONFIRM message including RES_i as shown in Eq.(22).

$$RES_i = H_4(TK_{2-i}, M_i) \oplus H_4(TK_{3-i}, M_i) \tag{22}$$

Step 11: On receiving all these RES_i messages, the MRN_1 verifies the hash value HV' as shown in Eq.(23) or the hash value HV'' as shown in Eq.(24) in case the value of $ContinousChangeBS$ field is true.

$$RES = RES_1 \oplus \ldots \oplus RES_n$$

$$HV' = H_5(R, m_{gNB_2}, RES) \tag{23}$$

$$HV'' = H_6(R, m_{gNB_2}, R^*, m_{gNB_3}, RES) \tag{24}$$

If the verification is successful, the MRN_1 issues a PRE-HANDOVER COMPLETE message including the $m_{gNB_2}/(m_{gNB_2}, m_{gNB_3})$ to its group members and a HANDOVER CONFIRM message to the $D-SDN$ to inform that the pre-handover authentication achieves successfully.

After the pre-handover procedure, when the train enters the range of the $DgNB_2/DgNB_3$, each MRN_i and the $DgNB_2/DgNB_3$ can directly use the session key TK_{2-i}/TK_{3-i} to communicate with each other.

V. Security Evaluation

In this section, we adopt the qualitative security analysis and the formal verification by Tamarin tool to demonstrate the security of the two proposed schemes.

A. Security Analysis

In this section, we analyze the security properties of the two proposed schemes: FTGPHA1 and FTGPHA2.

1) **Mutual Authentication:** For the proposed FTGPHA1, only the legitimate MRN_i and $D-SDN$ hold the $SUPI_i$ and NH_i. In the pre-handover procedure, the $SUPI_i$ and the NH_i are employed for each MRN_i to generate the correct MAC_i and the MRN group leader MRN_1 aggregates all MAC_i into a single MAC. The $D-SDN$ authenticates the MRN group by checking the correctness of the MAC. Once there is an invalid one, the verification would fail. Likewise, the MRN group can authenticate the $D-SDN$ by verifying the validity of the MAC^*. For the proposed FTGPHA2, on the one hand, each MRN_i generates the signature S_i with its private key sk_i and then the MRN group leader MRN_1 aggregates all signatures to a single signature $sumS$. Subsequently, the $D-SDN$ verifies the aggregate signature. Once there is an invalid signature, the verification would fail. Only the legitimate MRN_i can generate the valid signature and then obtain the valid aggregate signature. Thus, the $D-SDN$ can authenticate the MRN group by checking the aggregate signature. On the other hand, since each MRN_i encrypts its privacy information M_i with the $D-SDN$'s public key pk_{SDN}, only the designated $D-SDN$ can obtain the M_i and then generate the valid hash value HV'. Therefore, the MRN group can verify the $D-SDN$ by checking the hash value.
2) **Key Agreement:** For the proposed FTGPHA1, each MRN_i and $D-SDN$ employ the secret key K_{AMF_i} and NH parameter NH_i to derive the next NH parameter $NH_i{}^*$. Then, the $D-SDN$ delivers all $NH_i{}^*$ to the $DgNB_2$ through the secure channel which has been established in advance. Subsequently, each MRN_i and the $DgNB_2$ derive the session key $K_{gNB_i}{}^*$ from the $NH_i{}^*$. Without the $NH_i{}^*$, any adversary is unable to work out the session key $K_{gNB_i}{}^*$. For the proposed FTGPHA2, each MRN_i transmits X_i to the $DgNB_2$ and the $DgNB_2$ delivers R to the MRN group. Subsequently, they calculate the session keys TK_{2-i} by the equation $TK_{2-i} = R * x_i = r * X_i$, where the parameters r and x_i are the secret values of the $DgNB_2$ and MRN_i, respectively. The computation of session key from the two parameters X_i and R without knowing x_i or r is equivalent to solving the Elliptic Curve Diffie-Hellman Problem (ECDHP) or Elliptic Curve Discrete Logarithm Problem (ECDLP).
3) **Anonymity and Unlinkability:** For the proposed FTGPHA1, the temporary value $5G-GUTI_i$ is adopted to achieve the anonymity and is updated in each pre-handover authentication procedure. However, since the $5G-GUTI_i$ will not change in a while, it is still likely for an adversary to identify or trace the MRN_i based on the $5G-GUTI_i$. Thus, this scheme cannot fully satisfy the anonymity and unlinkability. For the proposed FTGPHA2, since the MRN_i's privacy information M_i

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

is encrypted with the $D-SDN$'s public key pk_{SDN}, the MRN's privacy information will not be revealed to anyone except for the $D-SDN$. Thus, the scheme can satisfy the anonymity. Besides, with the use of the random number in each message (X_i, S_i, C_i), it is hard to decide whether two messages are computed by the same MRN group members. Thus, this scheme can achieve the anonymity and unlinkability.

4) **Perfect Forward/Backward Secrecy (PFS/PBS):** For the proposed FTGPHA1, the session key ${K_{gNB_i}}^*$ is computed from the secret key K_{AMF_i}. Once the secret key K_{AMF_i} is compromised, it is possible for an adversary to obtain the session key ${K_{gNB_i}}^*$. Thus, this scheme cannot achieve the PFS/PBS. For the proposed FTGPHA2, the session key TK_{2-i} is computed via the equation $TK_{2-i} = R * x_i$ or $TK_{2-i} = r * X_i$. Even if the MRN_i's private key sk_i is obtained, the adversary cannot acquire the parameter x_i from the signing equation $S_i = x_i + sk_i + H_3(V_i, X_i, M_i)\ mod\ q$ since the value V_i is only held by the MRN_i and the $D-SDN$ and thus, it cannot further calculate the session key TK_{2-i}. Similarly, even if the $D-SDN$'s private key sk_{SDN} is derived, the adversary cannot obtain the parameter r from the R or the hash value HV' and cannot further compute the session key TK_{2-i}. Therefore, this scheme can fully achieve the PFS/PBS.
5) **Forward/Backward Key Separation (FKS/BKS) [21]:** For the proposed FTGPHA1, the $D-SDN$ and the MRN_i generate the fresh ${NH_i}^*$ values with their private values K_{AMF_i} in each pre-handover procedure and then the $D-SDN$ transmits the ${NH_i}^*$ to the $DgNB_2$. Subsequently, the MRN_i and the $DgNB_2$ use the fresh ${NH_i}^*$ to compute the session key ${K_{gNB_i}}^*$. Even if the current NH value or the current session key is obtained, any adversary without the K_{AMF_i} is unable to calculate the previous or the next NH value and further compute the corresponding session key. Therefore, this scheme is secure against the FKS/BKS. For the proposed FTGPHA2, since the random numbers x_i and r are adopted for computing the key TK_{2-i} in each session, each key is independent of the other one. Even if the current session key is derived, any adversary cannot acquire the previous or the next session key. Thus, this scheme can satisfy the FKS/BKS.
6) **Resistance against Replay Attacks:** For the proposed FTGPHA1, the random numbers r_M and r_D are employed to generate the one-time hash values in each pre-handover procedure. Thus, this scheme can defend the replay attacks. For the proposed FTGPHA2, the replay attacks can be resisted with the use of the random numbers x_i and r in each message.
7) **Resistance against Impersonation Attacks:** For the proposed FTGPHA1, on the one hand, as each MRN_i and the $D-SDN$ generate the valid hash value with their private values $SUPI_i$ and NH_i, any adversary without the $SUPI_i$ and NH_i cannot generate the valid hash value and further impersonate as a legitimate $DgNB_2$ or the MRN_i. On the other hand, any adversary without the ${NH_i}^*$ cannot acquire the session key $K^*_{gNB_2}$ and thus, cannot impersonate as a legitimate $DgNB_2$ or the MRN_i. Therefore, this scheme is secure against the impersonation attacks. For the proposed FTGPHA2, on the one hand, only the legitimate MRN_i holds the private key sk_i and any adversary without a valid private key is impossible to forge a valid signature S_i. In addition, since the $D-SDN$'s public key pk_{SDN} has been previously provisioned to the MRN_i and each MRN_i encrypts its privacy information M_i with the $D-SDN$'s public key pk_{SDN}, any adversary without a valid private key sk_{SDN} is unable to obtain the MRN_i's privacy information and further generate the correct hash value HV'. On the other hand, as stated above, any adversary cannot obtain the session key TK_{2-i} and thus, cannot impersonate as a legitimate $DgNB_2$ or the MRN_i. Therefore, this scheme is able to resist the impersonation attacks.
8) **Resistance against Man-in-the-Middle (MitM) Attacks:** For the proposed FTGPHA1, any adversary cannot masquerade as a legitimate MRN_i or $D-SDN$ to deceive the $D-SDN$ or MRN_i without the corresponding $SUPI_i$ and NH_i. Thus, this scheme successfully prevents the MitM attacks. For the proposed FTGPHA2, on the one hand, without the private key sk_{SDN} corresponding to the public key pk_{SDN}, the adversary is unable to impersonate as a legitimate $D-SDN$ to communicate with the MRN group members. On the other hand, any adversary without the private keys sk_i is impossible to trick the $D-SDN$. Thus, this scheme is secure against the MitM attacks.

As stated above, the proposed FTGPHA1 does not achieve the anonymity, unlinkability and PFS/PBS, but the proposed FTGPHA2 can fully satisfy all the aforementioned security properties.

Fig. 4. Tamarin result of the first scheme FTGPHA1.

B. Formal Verification: Tamarin

In this section, we formally analyze the proposed schemes by using the automatic verification tool named Tamarin [22], which can precisely analyze the secrecy and complex authentication properties of various protocols. Tamarin tool supports the equational specification of some cryptographic operators, such as Diffie-Hellman exponentiation and bilinear pairings [23]. The Tamarin simulation results of the two proposed schemes are shown as follows.

The execution result of the proposed FTGPHA1 in Tamarin version 2.7.1 on Linux is presented in Fig. 4, where the $Secrecy\_message$ lemma is employed to demonstrate the

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

```
==============================================================================
summary of summaries:

analyzed: FTGPHA2_Scheme.spthy

  ExecutableRequest (exists-trace): verified (13 steps)
  ExecutableConfirm (exists-trace): verified (14 steps)
  SDN_auth_MRN (all-traces): verified (6 steps)
  MRN_auth_SDN_AND_Negotiate_sesskey (all-traces): verified (13 steps)
  Secrecy_message (all-traces): verified (20 steps)
  Secrecy_PFS (all-traces): verified (16 steps)

==============================================================================
```

Fig. 5. Tamarin result of the second scheme FTGPHA2.

secrecy of the identity $SUPI_i$ of the MRN_i. From Fig. 4, it can be seen that the proposed FTGPHA1 can achieve the security properties including the mutual authentication, key agreement and partially anonymity. The execution result of the proposed FTGPHA2 is given in Fig. 5. It demonstrates that the proposed FTGPHA2 could achieve the mutual authentication, key agreement, privacy preservation and PFS. The concrete proof of this Tamarin results is provided in Supplemental Materials.

VI. Performance Evaluation

In this section, we evaluate the performance of the FTGPHA1 and FTGPHA2 by comparing them with these closely related schemes: 5G schemes in [5], [6] and these schemes in [11], [12], [15], [16].

A. Brief Overview of Performance Analysis

Firstly, we analyze the performance in terms of the signaling, communication and computational overheads, respectively. Due to the introduction of the collaborative pre-handover in our proposed schemes, here we consider the following two contrasting scenarios: common handover scenario **Scen1** and collaborative handover scenario **Scen2**. **Scen1** means that the MRN group members will not leave the next base station $DgNB_2$ soon and do not need to perform the collaborative pre-handover procedure. **Scen2** shows that once the MRN group members enter the $DgNB_2$, they will quickly leave and enter the $DgNB_3$ and thus, the collaborative pre-handover shall be performed in our proposed schemes. In **Scen2**, since the MRN group members actually accomplish the pre-handover procedures with two base stations continuously, the overheads divided by 2 represent the average overheads in one pre-handover procedure. Without the consideration of the collaborative handovers, all of the reference schemes have the same overheads in **Scen1** and **Scen2**. Subsequently, we analyze the performance when there are some unknown attacks in the execution of these reference schemes in **Scen1**.

For the sake of fairness, we define that the security levels in these schemes are equivalent to AES 128 bits. Concretely, we suppose that the NH parameter and the key for symmetric encryption/decryption are 128 bits, the key size for algorithms based on Elliptic Curve Cryptography (ECC) is 256 bits, the public key size for algorithms based on the Finite-Field Cryptography (FFC) is 3072 bits and the private key size is 256 bits [24], [25]. In addition, the output length of the hash is 128 bits, the size of the random number is 128 bits and the size of the timestamp is 32 bits, respectively. In addition, since all these contrasting schemes are about the handover authentication, which must transfer the necessary information for handover such as the SUPI, 5G-GUTI, PCI and so on, we assume that the length of these parameters is 128 bits. Without loss of generality, it is supposed that the number of the MRN group members is n.

B. Signaling Overhead

On the signaling overhead, we evaluate our schemes with other related schemes in terms of the number of signaling messages for n MRNs. For the proposed FTGPHA1 and FTGPHA2, there are $(2n + 3)$ messages between the group members and the group leader MRN_1, 3 messages between the group leader MRN_1 and the source base station $DgNB_1$, 3 messages between the source base station $DgNB_1$ and the $D - SDN$ and 3 messages between the $D - SDN$ and the target base station $DgNB_2$/$DgNB_3$ in the group pre-handover authentication procedure. For the 5G schemes in [5], [6], there are 2 messages between the UE and the source base station, 2 messages between the source base station and the MME, 3 messages between the target base station and the MME and 1 message between the UE and the target base station in a full intra-MME handover procedure. For the scheme in [16], there are $(n + 1)$ messages between the group members and the group leader, 3 messages between the group leader and the target base station, $(n + 3)$ messages between the target base station and the MME and n messages between the group members and the target base station in a group roaming authentication procedure. For the scheme in [15], there are $2n$ messages between the group members and the source base station, 2 messages between the source base station and the MME, 2 messages between the MME and the target base station and n messages between the group members and the target base station in a full group handover authentication procedure. For the scheme in [11], there are $(2n + 2)$ messages between the group members and the group leader, 3 messages between the group leader and the target base station and 2 messages between the target base station and the MME in a group handover authentication procedure. For the scheme in [12], there are $(n + 2)$ messages between the group members and the group leader, 2 messages between the group leader and the source base station, 3 messages between the source base station and the target base station, 2 messages between the group leader and the target base station and 2 messages between the target base station and the MME in a group handover authentication procedure. The comparison of the signaling overhead of the related schemes is derived as shown in Table II. Fig. 6 depicts the comparison results of our schemes and other related schemes in terms of the signaling messages with the increasing number of MRNs. From the Fig. 6(a), the signaling overheads incurred in our proposed schemes are slightly larger than those of the scheme in [12], similar to those of the scheme in [11] and less than these of other schemes. In addition, the signaling overheads of our proposed schemes can be largely reduced by performing the collaborative handover procedures according to the Fig. 6(a).

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

TABLE II
SIGNALING OVERHEADS FOR n MRNS

(bytes)	FTGPHA1	FTGPHA2	5G schemes [5], [6]	[16]	[15]	[11]	[12]
Scen1	$2n$+12	$2n$+12	$8n$	$3n$+7	$3n$+4	$2n$+7	n+11
Scen2	($2n$+15)/2	($2n$+15)/2	$8n$	$3n$+7	$3n$+4	$2n$+7	n+11

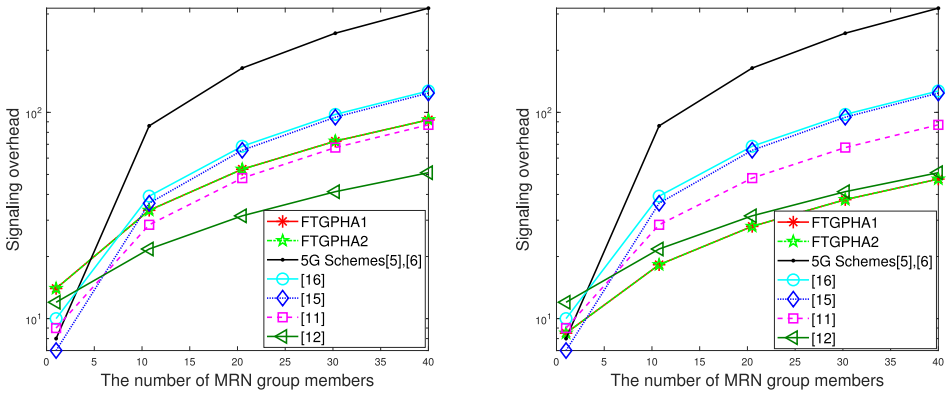


Fig. 6. Comparison of the signaling overhead. (a) In **Scen1**. (b) In **Scen2**.

TABLE III
COMPUTATIONAL OVERHEADS OF THESE CRYPTOGRAPHY OPERATIONS

(us)	T_M	T_E	T_P	T_A	T_H	T_S
MRN	0.96×10^3	1.89×10^3	1.65×10^4	2.53	2.38	2.26
$D-SDN$	0.50×10^3	1.00×10^3	8.36×10^3	1.39	1.21	1.05

C. Computational Overhead

On the computational overhead, we only consider the point addition operation T_A, the point multiplication operation T_M, the modular exponentiation operation T_E, the bilinear pairing operation T_P, the symmetric encryption/decryption operation T_S and the one-way hash operation T_H and omit other operations. We have built a test environment to calculate the computational overheads of these cryptography operations using C/C++ OPENSSL library [26] tested on an Intel(R) Core(TM) m3-6Y30 CPU 0.9 GHz processor as a MRN and an Intel(R) Core(TM) i7-7500 U CPU 2.70 GHz as a DgNB or $D-SDN$. The experiment results are listed in Table III.

We make two comparisons of the computational overheads for n MRNs in the reference schemes, as listed in Table IV. The analysis results of the total computational overheads with the increasing number of MRNs from two different scenarios are shown in Fig. 7. From Fig. 7(a), in **Scen1**, the total computational overheads of the FTGPHA1 are similar to that of the schemes in [11], [15] and 5G schemes in [5], [6], which are much less than that of other schemes. The total computational overheads of the FTGPHA2 are larger than that of the proposed FTGPHA1, the schemes in [11], [15] and 5G schemes in [5], [6], but less than that of other schemes. From Fig. 7(b), in **Scen2**, owing to the introduction of the collaborative handover, the average computational overheads in one pre-handover procedure of the FTGPHA1 and FTGPHA2 are reduced compared with the other related schemes.

D. Communication Overhead

On the communication overhead, we mainly analyze the total size of the messages transmitted by n MRNs in these reference schemes, as listed in Table V. For the proposed FTGPHA1, the 5G schemes in [5], [6] and the schemes in [11], [15], since these transmitted messages mainly include the random numbers, symmetrical encrypted results and the output of hash operations, the communication overheads of those schemes are relatively small. For the proposed FTGPHA2, the scheme in [16] and the scheme in [12], the communication overheads of those schemes are relatively large owing to the use of ECC or FFC, respectively. Fig. 8 depicts the specific comparison results of related schemes in terms of the communication overheads with the increasing number of MRNs. From the Fig. 8(a), the communication overheads of the FTGPHA1 are slightly larger than that of 5G schemes in [5], [6], which are much smaller than that of other related schemes. The proposed FTGPHA2 costs more communication overheads than the proposed FTGPHA1, the schemes in [11], [15] and 5G schemes in [5], [6], but less than the schemes in [12] and [16]. In addition, according to the Fig. 8(b), with the introduction of the collaborative handover, the average communication overheads in one pre-handover procedure of the FTGPHA1 and FTGPHA2 are largely reduced.

E. Performance Under Unknown Attacks

Although we have claimed that the two proposed schemes could resist several known attacks, there still are some unknown attacks which we cannot tell when/where they will happen, and whether our proposed schemes can withstand them if they happen. Thus, in this section, we will analyze the performance under unknown attacks. Here, we only elaborately introduce the communication overhead under unknown attacks and the signaling overhead and computational overhead under unknown

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

TABLE IV
COMPUTATIONAL OVERHEADS FOR n MRNS

Scen1(us)	MRN group	$DgNB_1$, $DgNB_2$ and $D-SDN$	Total
FTGPHA1	$5nT_H+T_S$ = 11.90n+2.26	$5nT_H+T_S$ = 6.05n+1.05	17.95n+3.31
FTGPHA2	$3nT_M+(3n+1)T_H+T_S$=2.89$\times10^3n$+4.64	$(2n+4)T_M+(4n+1)T_H+(2n+1)T_A+T_S$=(1.01$n$+2.00)$\times10^3$	(3.90n+2.00)$\times10^3$
5G schemes [5], [6]	$4nT_H$=9.52n	$4nT_H$=4.84n	14.36n
[16]	$4nT_M+2nT_H+(3n\text{-}1)T_A$=3.85$\times10^3n$-2.53	$(3n+1)T_M+3nT_H+(3n\text{-}2)T_A+3T_P$=(1.51$n$+25.58)$\times10^3$	(5.36n+25.58)$\times10^3$
[15]	$5nT_H$ =11.90n	$5nT_H$=6.05n	17.95n
[11]	$(4n+2)T_H$=9.52n+4.76	$(2n+2)T_H+nT_S$=3.47n+2.42	12.99n+7.18
[12]	$(3n+1)T_P+2nT_E+4nT_H+nT_M$=(5.42$n$+1.65)$\times10^4$	$(n+1)T_P+nT_E+nT_H$=(9.36n+8.36)$\times10^3$	(6.36n+2.49)$\times10^4$
Scen2(us)	MRN group	$DgNB_1$, $DgNB_2$, $DgNB_3$ and $D-SDN$	Total
FTGPHA1	$(9nT_H+T_S)/2$=10.71n+1.13	$(9nT_H+T_S)/2$=5.45n+0.53	16.16n+1.66
FTGPHA2	$(4nT_M+(4n+1)T_H+T_S)/2$=1.92$\times10^3n$+2.32	$((3n+5)T_M+(5n+1)T_H+(2n+1)T_A+T_S)/2$=(0.75$n$+1.25)$\times10^3$	(2.67n+1.25)$\times10^3$
5G schemes [5], [6]	$4nT_H$=9.52n	$4nT_H$=4.84n	14.36n
[16]	$4nT_M+2nT_H+(3n\text{-}1)T_A$=3.85$\times10^3n$-2.53	$(3n+1)T_M+3nT_H+(3n\text{-}2)T_A+3T_P$=(1.51$n$+25.58)$\times10^3$	(5.36n+25.58)$\times10^3$
[15]	$5nT_H$=11.90n	$5nT_H$=6.05n	17.95n
[11]	$(4n+2)T_H$=9.52n+4.76	$(2n+2)T_H+nT_S$=3.47n+2.42	12.99n+7.18
[12]	$(3n+1)T_P+2nT_E+4nT_H+nT_M$=(5.42$n$+1.65)$\times10^4$	$(n+1)T_P+nT_E+nT_H$=(9.36n+8.36)$\times10^3$	(6.36n+2.49)$\times10^4$

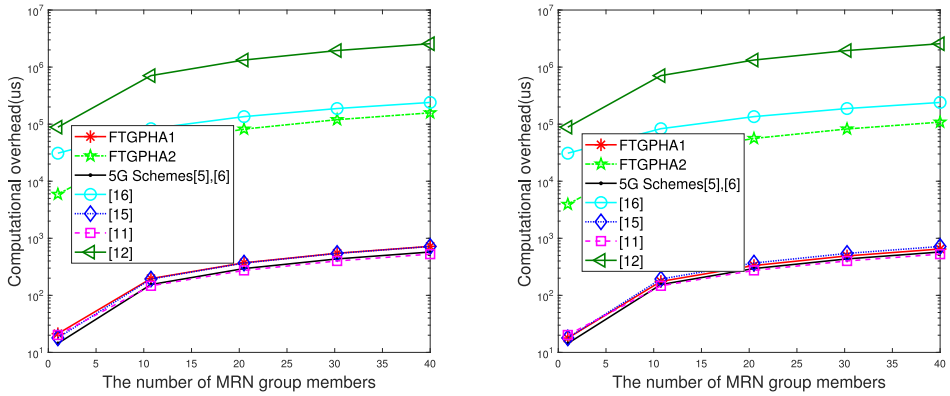


Fig. 7. Comparison of the computational overhead. (a) In **Scen1**. (b) In **Scen2**.

TABLE V
COMMUNICATION OVERHEADS FOR n MRNS

(bytes)	FTGPHA1	FTGPHA2	5G schemes [5], [6]	[16]	[15]	[11]	[12]
Scen1	112n+320	368n+560	80n	496n+128	128n	160n+272	1572n+440
Scen2	72n+224	224n+480	80n	496n+128	128n	160n+272	1572n+440

attacks are similar to the communication overhead under unknown attacks.

$$CO_{avg} = \frac{CO_{fail} * p_{fail} + CO_{succ} * p_{succ}}{p_{succ}} \tag{25}$$

$$CO_{fail} = \sum_{i=1}^{N_{total}} CO_i * q \tag{26}$$

The specific calculation is shown in Eq. 25, where CO_{avg} means the average communication overheads for multiple successful or unsuccessful pre-handover procedures, CO_{fail} represents the communication overhead for an unsuccessful pre-handover procedure under unknown attacks, p_{fail} is the probability of an unknown attack happening in the execution of the protocol, CO_{succ} indicates the communication overhead for a successful pre-handover procedure and $p_{succ} = 1 - p_{fail}$. Besides, we assume that the total number of messages in a pre-handover authentication procedure is N_{total} and the probability of unknown attack occurring in i step is $q = 1/N_{total}$. Thus, the CO_{fail} can be calculated from Eq. 26, where the CO_i represents the total communication overheads before the unknown attack occurs in i step.

Fig. 9 depicts the comparison results of the average signaling, computational and communication overheads with the increasing probability of unknown attacks happened, respectively. In order to simplify analysis, we set $n = 20$ [11]. From Fig. 9(a), the average signaling overheads under unknown attacks by the FTGPHA1 and FTGPHA2 are larger than that by the schemes in [11], [12] and smaller than that by other related schemes. From Fig. 9(b), the average computational overheads under unknown attacks by the FTGPHA1 are similar to that by the schemes in [11], [15] and 5G schemes in [5], [6], but much better than that by other schemes. The average computational overheads under

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

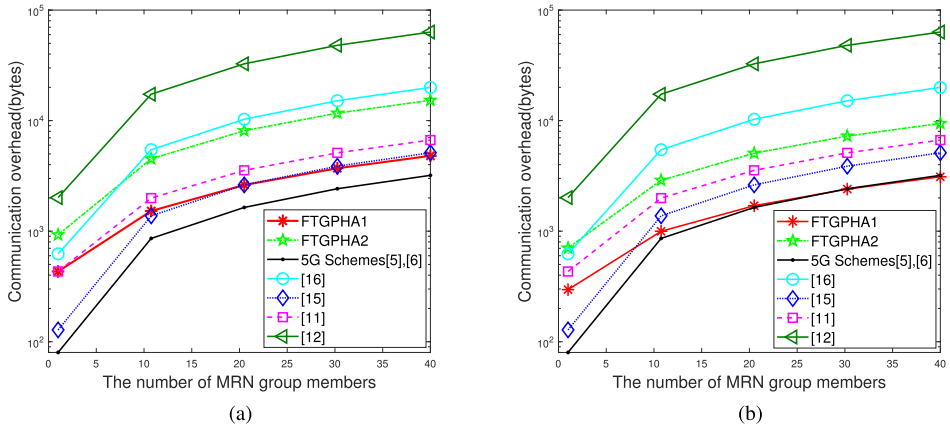


Fig. 8. Comparison of the communication overhead. (a) In **Scen1**. (b) In **Scen2**.

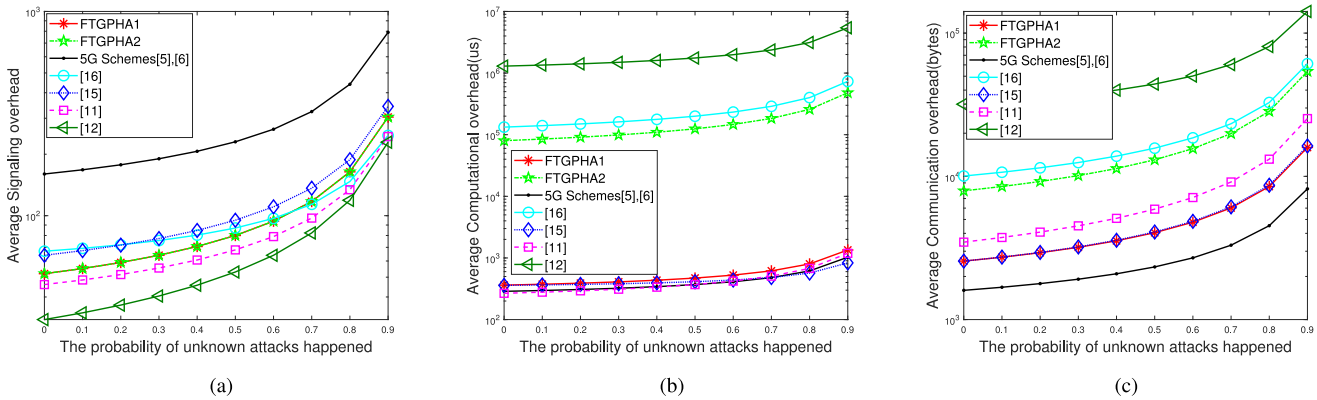


Fig. 9. Comparison of the performance under unknown attacks. (a) Signaling overhead. (b) Computational overhead. (c) Communication overhead.

unknown attacks by the FTGPHA2 are larger than that by the proposed FTGPHA1, the schemes in [11], [15] and 5G schemes in [5], [6], but less than that by other schemes. From Fig. 9(c), the average communication overheads under unknown attacks by the FTGPHA1 are slightly larger than that by the 5G schemes in [5], [6], similar to that by the scheme in [15], but less than that by other schemes. In addition, the average communication overheads under unknown attacks by the FTGPHA2 are larger than that by the FTGPHA1, the schemes in [11], [15] and 5G schemes in [5], [6], but less than that by the schemes in [12], [16].

F. Discussion

We give a comparison of performance and security between our two schemes and other related schemes in Table VI. According to Table VI, the FTGPHA1 has the better performance in security than 5G schemes in [5], [6] and the schemes in [11], [15], [16]. At the same time, it consumes a small amount of computational and communication overheads. The FTGPHA2 can provide much stronger security properties than other schemes except for the scheme in [12], but consumes far less computational and communication overheads than the scheme in [12].

The comparison results of the proposed FTGPHA1 and FTGPHA2 are described as follows. On the signaling overhead, the FTGPHA1 consumes the same signaling overheads as the FTGPHA2. On the communication overhead, since the proposed FTGPHA1 mainly transmits the random numbers, symmetrical encrypted results and the output of hash operations in the group pre-handover authentication process but the proposed FTGPHA2 mainly contains these parameters related to the ECC, the communication overhead of the proposed FTGPHA1 is much less than that of the FTGPHA2. On the computational overhead, since the proposed FTGPHA1 only employs some hash and symmetric encryption/decryption operations similar to the 5G schemes in [5], [6], and the proposed FTGPHA2 mainly employs the ECC and adopts some point multiplication operations to achieve more robust security properties, the computational overhead of the proposed FTGPHA1 is significantly less than that of the proposed FTGPHA2. On the security aspects, the proposed FTGPHA1 can provide these security properties including mutual authentication, key agreement, forward/backward key separation and resisting protocol attacks. However, the proposed FTGPHA1 cannot provide anonymity, unlinkability and perfect forward/backward secrecy, while the proposed FTGPHA2 can provide all these mentioned security properties. As stated, the proposed FTGPHA1 is suitable for the scenario with limited

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

TABLE VI
COMPARISON

	FTGPHA1	FTGPHA2	5G schemes [5], [6]	[16]	[15]	[11]	[12]
Mutual authentication	Y	Y	N	N	N	Y	Y
Key agreement	Y	Y	Y	Y	Y	Y	Y
Anonymity and unlinkability	N	Y	N	N	N	N	Y
Perfect Forward/Backward Secrecy (PFS/PBS)	N	Y	N	Y	N	N	Y
Forward/Backward Key Separation (FKS/BKS)	Y	Y	N	Y	N	N	Y
Resisting protocol attacks	Y	Y	N	N	N	Y	Y
Signaling overhead	M	M	H	M	M	M	L
Computational overhead	L	M	L	M	L	L	H
Communication overhead	L	M	L	M	L	L	H
Signaling overhead under unknown attacks	L	L	H	L	L	L	L
Computational overhead under unknown attacks	L	M	L	M	L	L	H
Communication overhead under unknown attacks	L	M	L	M	L	L	H

Y:Yes, N:No, H:High, M:Midum, L:Low.

communication resources, poor user performance and relatively low security requirements, while the proposed FTGPHA2 is suitable for the scenario with good user performance, high security requirements and relatively abundant communication resources.

VII. CONCLUSION

In this paper, we present two group-based pre-handover authentication schemes: FTGPHA1 and FTGPHA2 for 5G high-speed rail networks. In the FTGPHA1, we draw on the experience of the traditional intra-MME handover procedure to achieve the pre-handover authentication procedure and in the FTGPHA2, we employ the aggregate signcryption to achieve the pre-handover authentication procedure. Additionally, with the assistance of the $D-SDN$, the MRN group and the target base station can accomplish the handover authentication procedure before the MRN arrives in advance and thus, the handover delay in these two schemes could be ignored. The security and performance evaluations demonstrate that the proposed FTGPHA1 is more efficient in terms of communication and computational overheads and the proposed FTGPHA2 outperforms other related schemes in security and achieves ideal efficiency simultaneously.

REFERENCES

[1] Q. Kong, R. Lu, S. Chen, and H. Zhu, "Achieve secure handover session key management via mobile relay in LTE-advanced networks," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 29–39, Feb. 2017.

[2] M. Pan, T. Lin, and W. Chen, "An enhanced handover scheme for mobile relays in LTE-A high-speed rail networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 743–756, Feb. 2015.

[3] 3rd Generation Partnership Project, "Technical specification group services and system aspects; feasibility study on LTE relay node security(Rel 10)," 3GPP, TR 33.816, V10.0.0, Mar. 2011.

[4] 3rd Generation Partnership Project, "Technical specification group radio access network; evolved universal terrestrial radio access (E-UTRA);study on mobile relay(Rel 12)," 3GPP, TR 36.836, V12.0.0, Jun. 2014.

[5] 3rd Generation Partnership Project, "Technical specification group radio access network; NR; NR and NG-RAN overall description; stage 2(Rel 15)," 3GPP, TS 38.300, V15.2.0, Jun. 2018.

[6] 3rd Generation Partnership Project, "Technical specification group services and system aspects; security architecture and procedures for 5G system(Rel 15)," 3GPP, TS 33.501, V15.0.0, Mar. 2018.

[7] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "A formal analysis of 5G authentication," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Jun. 2018, pp. 1383–139.

[8] L. Tian, J. Li, Y. Huang, J. Shi, and J. Zhou, "Seamless dual-link handover scheme in broadband wireless communication systems for high-speed rail," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 4, pp. 708–718, May 2012.

[9] Q. Huang, J. Zhou, C. Tao, S. Yi, and M. Lei, "Mobile relay based fast handover scheme in high-speed mobile environment," in *Proc. IEEE Veh. Technol. Conf.*, 2012, pp. 1–6.

[10] J. Cao, M. Ma, H. Li, Y. Fu, B. Niu, and F. Li, "Trajectory prediction-based handover authentication mechanism for mobile relays in LTE-A high-speed rail networks," in *Proc. IEEE Int. Conf. Commun.*, 2017, pp. 1–6.

[11] J. Cao, M. Ma, and H. Li, "G2RHA: Group-to-route handover authentication scheme for mobile relays in LTE-A high-speed rail networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 9689–9701, Nov. 2017.

[12] Z. Haddad, A. Alsharif, A. Sherif, and M. Mahmoud, "Privacy-preserving intra-MME group handover via MRN in LTE-A networks for repeated trips," in *Proc. IEEE 86th Veh. Technol. Conf.*, Sep. 2017, pp. 1–5.

[13] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, "A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1744–1747, Nov. 2012.

[14] A. Fu, G. Zhang, Y. Zhang, and Z. Zhu, "GHAP: An efficient group-based handover authentication mechanism for IEEE 802.16m networks," *Wireless Pers. Commun.*, vol. 70, no. 4, pp. 1793–1810, Jun. 2013.

[15] J. Cao, H. Li, and M. Ma, "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks," in *Proc. IEEE Int. Conf. Commun.*, 2015, pp. 3020–3025.

[16] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 1011–1016.

[17] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2015, pp. 7246–7251.

[18] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1617–1634, Jul.–Sep. 2014.

[19] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G hetnets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28–35, Apr. 2015.

[20] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA')," RFC 5448, May 2009. [Online]. Available: https://rfc-editor.org/rfc/rfc5448.txt

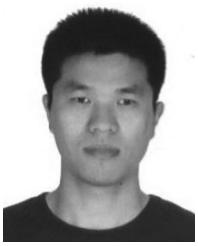
[21] Q. Kong, M. Ma, and R. Lu, "Achieving secure CoMP joint transmission handover in LTE-A vehicular networks," in *Proc. IEEE 86th Veh. Technol. Conf.*, Sep. 2017, pp. 1–5.

[22] *Tamarin*. 2019. [Online]. Available: http://www.infsec.ethz.ch/research/software/tamarin.html

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.

[23] *Tamarin Manual*. 2016. [Online]. Available: https://tamarin-prover.github.io/manual/tex/tamarin-manual.pdf
[24] E. Barker, W. Barker, W. Burr, and T. Polk, "SP 800-57: Recommendation for key management, part 1: General (Revised 4)," National Institute of Standards & Technology, Jan. 2016. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4
[25] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, "SP 800-56A: Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography (Revision 2)," National Institute of Standards & Technology, May 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-56Ar2
[26] OPENSSL. [Online]. Available: http://www.openssl.org/

Ruhui Ma received the B.S. and M.S. degrees in electronics and communications engineering in 2013 and 2016, respectively, from Xidian University, Xi'an, China, where she is currently working toward the Ph.D. degree in cyberspace security. Her research interests include device-to-device communication and LTE/LTE-A/5G networks.



Jin Cao received the B.S. and Ph.D. degrees from Xidian University, Xi'an, China, in 2008 and 2015, respectively. He has been an Associate Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. His research interests include wireless network security and LTE/LTE-A/5G networks.

Dengguo Feng received the B.S. degree from Shaanxi Normal University, Xi'an, China, in 1988, the M.S. and Ph.D. degrees from Xidian University, Xi'an, China, in 1993 and 1995, respectively. He is currently a Professor with the Institute of Software, Chinese Academy of Sciences, Beijing, China. His research interests include trusted computing and information assurance. He has authored or coauthored more than 200 publications in international journals and conferences. He is a recipient of China National Funds for Distinguished Young Scientists. He is the Vice-Chairmen of Chinese Association for Cryptologic Research and a Steering Committee Member of Information Technology in National Hi-Tec R&D Program of China.

Hui Li received the B.Sc. degree from Fudan University, Shanghai, China, in 1990, the M.A.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 1993 and 1998, respectively. Since June 2005, he has been the Professor with the School of Cyber Engineering, Xidian University, Xi'an, China. His research interests include cryptography, wireless network security, information theory, and network coding. He has coauthored two books. He served as a Technique Committee Co-Chair of the International Conference on Information Security Practice and Experience 2009 and International Conference on Information Assurance and Security 2009.

Shiyang He received the B.S. and M.S. degrees in communication and information system, in 2013 and 2016, respectively, from Xidian University, Xi'an, China, where he is currently working toward the Ph.D. degree in cyberspace security. His research interests are mainly in the areas of cryptography.

Authorized licensed use limited to: XIDIAN UNIVERSITY. Downloaded on August 26,2020 at 01:35:36 UTC from IEEE Xplore. Restrictions apply.