Abstract—In Long Term Evolution-Advanced (LTE-A) networks, Mobile Relay Nodes (MRNs) are installed in fast moving buses and trains to connect the passengers’ devices to evolved Node B (eNB). However, since the MRNs and eNBs are installed in open environment, they can be compromised to launch security and privacy attacks. In this paper, we propose a privacy-preserving intra Mobility Management Entity (MME) group handover scheme in LTE-A networks for repeated trips. Comparing to the existing schemes, the proposed scheme is devised to achieve the following requirements. First, the MRNs should be able to authenticate the received messages so that the messages sent from external attackers can be dropped by the MRNs rather than forwarding them to the core of the network. Second, the proposed scheme also aims to reduce the computational and signalling overhead and establish secure session keys. Third, the scheme aims to protect the users’ privacy from singular and colluding MRNs and eNBs. Our analysis demonstrates that the proposed scheme can achieve our security and privacy objectives. Our performance evaluations demonstrate that the proposed scheme requires a few number of messages and low computational overhead.

Index Terms—Privacy preservation, security, group handover, LTE-A networks, and mobile relay nodes.

I. INTRODUCTION

The Long Term Evolution-Advanced (LTE-A) is a packet based cellular network standardized by the Third Generation Partnership Project (3GPP) as a candidate for the fourth-generation (4G) mobile system [1]. The increasing demand for high data rates to support new applications such as multimedia services has motivated the development of the LTE-A cellular wireless technology [2]. The LTE-A network has high capacity and low transmission delay that can provide high data rate and better coverage in a cost efficient manner. The LTE-A architecture is composed of two different domains, called access domain and core domain [3]. The core domain has Home Subscriber Server (HSS) and Mobility Management Entities (MMEs), while the access domain has Mobile Relay Nodes (MRNs) and evolved Nodes B (eNBs).

In fast moving buses and trains, the data transmission suffers from high path loss, and the large number of simultaneous handovers of the passengers’ devices may cause a low handover success rate. To overcome these issues, the concept of MRNs is proposed in the 3GPP in LTE-A [4]. The MRN connects users’ devices to eNBs by using an outer antenna mounted on the top of the buses and trains. It can increase the success rate of the handover by using group handover procedure that can reduce the traffic load [5], [6]. However, since the MRNs and eNBs are installed in an open environment that lacks physical security, they can be compromised.

In LTE-A networks, hiding the users’ sensitive information such as their locations is highly required to preserve their privacy from the MRNs and eNBs. Moreover, the colluding eNBs can track the users’ locations, and the MRN can collude with malicious eNBs to know the session key shared between a legitimate UE and honest eNB.

Various schemes have been proposed to perform secure group handover in LTE-A networks such as [3], [7], [8], but the proposed scheme in [3] is closely related to our paper as it addresses the security and privacy issues of group handover using MRNs. In this scheme, since MRNs can not verify the received messages from UEs before forwarding them to the eNBs, messages sent from external attackers consume a lot of resources before they are dropped. This can be exploited by the attackers to flood the network with fake messages. Moreover, since the eNBs can know the real identities of the users, they can know the locations of the users and track them. In addition, the computational overhead is large and the session key shared between UE and eNB is computed only by the UE, however more secure keys should be computed by contributing the two parties in the key computation.

In this paper, we propose a privacy-preserving intra-MME group handover in LTE-A networks for repeated trips. Each user has a number of public/private key pairs and each key pair is used for only one handover operation to preserve the user’s privacy. All the one-time public keys of the legitimate users are added to a Bloom filter by HSS. Then, the HSS distributes this Bloom filter to all MRNs/eNBs to verify the public keys efficiently because there is no need to distributing certificates or verifying them. The HSS does not need to distribute the Bloom filter to all MRNs and eNBs in the system, but only to the MRNs and eNBs on the repeated trips of the users. In our scheme, the colluding eNBs cannot track the users’ locations as they know only their on-time public keys which change in each handover process and are not linkable. Also, both UE and eNB contribute in the establishment of the session key. Our security and privacy analysis demonstrate that the proposed scheme can satisfy our goals and requirements. Our performance evaluation demonstrate that the proposed handover scheme requires exchanging a few messages and low computational overhead.

The remainder of the paper is organized as follows. The related works are presented in [section II] In [section III] we
describe the system model and the design goals. The preliminaries are presented in section \[\text{IV}\]. The proposed scheme is explained in section \[\text{V}\]. The security/privacy analysis and the performance evaluations are provided in sections \[\text{VI}\] and \[\text{VII}\] respectively. Finally, section \[\text{VIII}\] concludes the paper.

II. RELATED WORK

The security and privacy of the group handover have attracted a great attention in LTE-A networks. In [7], Cao et. al. proposed a secure uniform group-based handover authentication scheme for machine type communication devices based on the multi-signature and aggregate message authentication codes techniques to achieve the authentication process in a simple way to avoid the signaling congestion. In [8], Lai et. al. addressed the security challenges in the access authentication for a group of machine to machine communication devices during roaming by using identity-based aggregated signature technique to accelerate the authentication process. However, these schemes do not consider the privacy issues.

In [3], Kong et. al. propose a secure handover session key management scheme via untrusted MRNs. In the proposed scheme, initially, all the users’ public keys are transferred from the source DeNB (S-DeNB) to the target DeNB (T-DeNB). Then, each user generates the session key, encrypts it with public key of the MME and sends the encrypted key and a signature to the MRN without sending any real or temporary identity to protect users privacy. Then, the MRN re-encrypts the session keys by the T-DeNB re-encryption key so that it can decrypt the ciphertext and get the shared key. For \(n\) users, the T-DeNB received \(n\) public keys from the S-eNB and has \(n\) session keys and \(n\) signatures. To verify every signature, the T-DeNB should perform exhaustive search operation to find which public key can verify each signature which increases the computational cost dramatically. Also, since MRNs can not authenticate the received messages from UEs before forwarding them to DeNBs, messages sent from external attackers can consume a lot of resources before they are dropped at the T-DeNB when no public key could verify them. Moreover, since the DeNBs can know the real identities of the users, they can know the locations of the users and track them. Furthermore, the session key shared between UE and DeNB is computed only by the UE, however more secure keys are usually computed by the contributions of the two associated parties.

Various schemes have been proposed to address the group handover in LTE-A networks. In [9], Pan et. al. used a prediction technique to prepare the handover before occurs and a group aggregation technique to decrease the overhead of the handover. In [10], Balakrishnan et. al. illustrated three different cases that demonstrate the useful deployment options offered by the mobile relays, and propose an enhanced handover mechanism for relay-based group mobility by extending the IEEE 802.16m specification. In [11], Altradt et. al. proposed a dynamic method to trigger the handover in LTE networks. They utilize Doppler frequency estimation in the downlink to adapt to different mobile stations speeds. In [12], Inaba et. al. consider the imprecise of the handover information and proposed a Fuzzy Logic (FL) based approach for handover in wireless cellular networks.

III. SYSTEM MODELS AND DESIGN GOALS

In this section, we describe the considered network and adversary models, and then discuss the design goals.

A. Network Model

LTE-A is a packet-based system, which allows the network entities to exchange data blocks called packets. The LTE-A architecture is composed of two different domains, called access domain and core domain [3]. As illustrated in Fig. 1 the access domain has on-board UEs, MRNs installed on top of trains and buses, and eNBs. The eNBs are connected to each other through x2 link, while MRN can communicate with nearby eNB by using wireless communication. The eNBs are located in fixed locations near the roads or railways. The core domain consists of HSS and MME. The HSS is responsible for certifying the UE’s one-time public/private key pairs and distributing the system’s parameters and keys. The MMEs are responsible for managing the required mobility and switching function with the evolved universal terrestrial radio access network (EUTRAN) entities such as eNBs and MRNs. All the exchanged messages between the UEs and eNBs are forwarded by the MRN.

B. Adversary Model

In our adversary model, we consider that the HSS and MMEs are trusted since they are owned and controlled by the network operators and physically secured. However, MRNs are not trusted since they are owned and operated by a third party instead of the network operators. Moreover, eNBs are also considered untrusted as they are installed in an open environment and the adversaries can access and compromise them. Attackers aim to get sensitive location information about the users. They also aim to obtain the shared keys between the UEs and the eNBs. The attackers can work individually or they can collude to launch stronger attacks. Attackers can also be internal or external.
C. Design Goals

To develop a secure and privacy-preserving intra-MME group handover in LTE-A networks, the following design goals should be achieved in our scheme.

1) Security and Privacy: The following privacy and security requirements should be satisfied in our scheme.

Users’ privacy and routes traceability. Our scheme should be able to hide the users’ identities and routes from MRNs and eNBs. It should also prevent colluding attackers from tracking the users.

Anonymous authentication. Since all the messages between eNBs and UEs are forwarded through the MRN, it should ensure that the incoming messages are from legitimate UEs before forwarding them to the eNBs. Moreover, since the MRNs and eNBs are untrusted, each UE should authenticate itself anonymously to preserve its privacy.

Secure session key agreement. A secure session key between a UE and each eNB should be computed to protect the confidentiality and integrity of the transmitted data. The MRN should not know the session key or even interrupt its generation. The key agreement scheme should also achieve forward and backward secrecy. For forward secrecy, by using the current session key shared between UE and the connected eNB, it is computationally infeasible for the eNB to know the future session keys used for subsequent handovers. For backward secrecy, it is computationally infeasible for any eNB to derive the previous session keys based on the current session key shared with an UE.

Collusion resistance. Our scheme should ensure that the collusion between the malicious eNBs and the malicious MRNs cannot compute the session key shared with honest eNB and cannot identify or track users even if the MRN has a sufficient storage and computation capabilities.

2) Efficiency: The secure and privacy-preserving intra-MME group handover scheme should not introduce heavy computational overhead on the HSS and MMEs. The scheme should not also introduce much computational and communication overheads on the UEs and eNBs.

IV. PRELIMINARIES

A. Bilinear Pairing

Let $G_1$ and $G_2$ be two multiplicative cyclic group of prime order $q$, and $g$ be a generator in $G_1$. Suppose $e$ can map two elements in $G_1$ to an element in $G_2$, i.e., $e: G_1 \times G_1 \rightarrow G_2$ and has the following properties:

- Bilinearity: $e(g^a, h^b) = e(g, h)^{ab} \in G_2$ for all $g, h \in G_1$ and $a, b \in \mathbb{Z}_q^*$.
- Non-degeneracy: $e(g, g) \neq 1_{G_2}$.
- Computability: $e(g, h)$ is efficiently computable for all $g, h \in G_1$.

B. Bloom Filter

Bloom filter is a space-efficient probabilistic data structure that can reduce the overhead of searching a set of items [13]. A Bloom filter building algorithm uses $k$ different hash functions to add an item to a bit vector of length $m$. These $k$ hash functions are defined as $H_i: \{0, 1\}^* \rightarrow b_i$, where $i \in \{1, k\}$ and $b_i \in \{1, m\}$. Initially, a binary vector with size $m$ is created where all the bits’ values are 0. As shown in Figure 2(a), an item $I$ is added to the Bloom filter by hashing it using the $k$ hash functions, and then, the bit locations corresponding to the hash values are set to 1. Figure 2(b) illustrates the process of checking the existence of an item $I$ in the Bloom filter. To check whether a given item $I$ is stored in the Bloom filter, a query algorithm computes the $k$ hash values of $I$ to get $k$ locations in the Bloom filter. If any of these $k$ locations store 0, the item $I$ is definitely not in the set; whereas if all the bits are ones, then $I$ is stored in the filter with high probability.

It is possible that the $k$ locations of an item that is not stored in the filter are accidently set to ones by other items in the set. This case is called false positive probability that can be computed by $(1 - (1-1/m)^k)^N$ [13], where $N$ is the number of items in the filter. Given $k$ and $N$, the size of the Bloom filter $m$ can be chosen such that the false positive probability is a very small value, e.g., below 0.01.

V. PROPOSED SCHEME

In this section, we present our proposed handover procedure. The exchanged messages between the different entities in the system are illustrated in Figure 3, and the main notations used in this paper are listed in Table 1.

A. System Initialization

The HSS generates the parameters $(q, G_1, G_2, g, e)$ and chooses a secure cryptographic hash function $H$, where $H: \{0, 1\}^* \rightarrow G_1$. In addition, it chooses $x_m \in \mathbb{Z}_q^*$ as a private key and computes its public key as $Y_m = g^{x_m}$. Finally, it publishes the system parameters $pubs = \{g, q, G_1, G_2, P, e, H, Y_m\}$. Each user UE has a long-term private key $x_i$ and a corresponding public key $Y_i = g^{x_i}$, and each eNB has a private and public key pair $(x_j, Y_j = g^{x_j})$. 
TABLE I: MAIN NOTATION

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE&lt;sub&gt;i&lt;/sub&gt;</td>
<td>User &lt;sub&gt;i&lt;/sub&gt;</td>
</tr>
<tr>
<td>MRN</td>
<td>Mobile Relay Node</td>
</tr>
<tr>
<td>eNB&lt;sub&gt;j&lt;/sub&gt;</td>
<td>evolved Node B&lt;sub&gt;j&lt;/sub&gt;</td>
</tr>
<tr>
<td>q, G&lt;sub&gt;1&lt;/sub&gt;, G&lt;sub&gt;2&lt;/sub&gt;, g, ê</td>
<td>Parameters of bilinear pairing</td>
</tr>
<tr>
<td>H( )</td>
<td>Cryptographic hash function</td>
</tr>
<tr>
<td>x&lt;sub&gt;j&lt;/sub&gt;, Y&lt;sub&gt;j&lt;/sub&gt;</td>
<td>Private and public keys for eNB&lt;sub&gt;j&lt;/sub&gt;</td>
</tr>
<tr>
<td>x&lt;sub&gt;i&lt;/sub&gt;, Y&lt;sub&gt;i&lt;/sub&gt;</td>
<td>Private and public keys for UE&lt;sub&gt;i&lt;/sub&gt;</td>
</tr>
<tr>
<td>s&lt;sub&gt;î&lt;/sub&gt;, Y&lt;sub&gt;î&lt;/sub&gt;</td>
<td>One-Time private/public keys for UE&lt;sub&gt;i&lt;/sub&gt;</td>
</tr>
<tr>
<td>L</td>
<td>Number of one-time keys given to UEs</td>
</tr>
<tr>
<td>σ&lt;sub&gt;i&lt;/sub&gt;</td>
<td>Signature computed by entity &lt;sub&gt;i&lt;/sub&gt;</td>
</tr>
<tr>
<td>K&lt;sub&gt;ij&lt;/sub&gt;</td>
<td>Session key between UE&lt;sub&gt;i&lt;/sub&gt; and eNB&lt;sub&gt;j&lt;/sub&gt;</td>
</tr>
<tr>
<td>MAC&lt;sub&gt;i&lt;/sub&gt;&lt;sup&gt;MRN&lt;/sup&gt;</td>
<td>MAC value computed by UE&lt;sub&gt;i&lt;/sub&gt; using K&lt;sub&gt;ij&lt;/sub&gt;</td>
</tr>
<tr>
<td>MAC&lt;sub&gt;î&lt;/sub&gt;&lt;sup&gt;agg&lt;/sup&gt;</td>
<td>Aggregated MAC computed by MRN</td>
</tr>
<tr>
<td>MAC&lt;sub&gt;î&lt;/sub&gt;&lt;sup&gt;agg&lt;/sup&gt;</td>
<td>Aggregated MAC computed by eNB&lt;sub&gt;j&lt;/sub&gt;</td>
</tr>
</tbody>
</table>

Each user UE<sub>i</sub> should compute a list of L one-time private/public key pairs (s<sub>î</sub>, Y<sub>î</sub>), where 1 ≤ î ≤ L. Each key pair is used to anonymously authenticate the user to MRN and eNB during the handover procedure. Then, the UE<sub>i</sub> sends the one-time public keys to the HSS. The HSS adds all the one-time keys to the record of UE<sub>i</sub>. It also adds the one-time public keys to a Bloom filter containing the set of all one-time public keys of all users, and then forwards the Bloom filter to the MRNs and all eNBs. We would like to point out that this operation is done offline and each user can generate a new list of public keys every interval of time before he uses all his keys. The HSS should also update the filters and distribute them to the MRNs and eNBs. The HSS does not need to send the filters to every MRNs and eNBs but for only the ones of repeated trips.

B. Group Handover Procedure

The proposed handover procedure can be divided into three phases: Handover Preparation, Handover Execution, and Handover Completion.

1) Handover Preparation:
   Step 1.1 [Measurement Report]. The MRN regularly measures the signal strengths of the serving eNB (S-eNB) and the target eNB (T-eNB). When the signal strengths reach thresholds determined by the network operator, the MRN sends a measurement report to the S-eNB.

   Step 1.2 [Handover Request]. The S-eNB generates a Handover Request message to the T-eNB which in turn broadcasts the message to all on-board UEs.

   Step 1.3 [Handover Request ACK]. The T-eNB reserves the resources needed for the handover if enough resources are available. Then, it chooses a random number r<sub>j</sub>, computes R<sub>j</sub> = g<sup>r</sup> and signature σ<sub>j</sub> = H (R<sub>j</sub>||TS<sub>j</sub>)<sup>T</sup>, where TS<sub>j</sub> is a time stamp. Finally, it sends Handover Request Acknowledge packet having (R<sub>j</sub>, TS<sub>j</sub>, σ<sub>j</sub>, ID<sub>j</sub>) to the S-eNB.

2) Handover Execution:
   Step 2.1 [Handover Command]. The S-eNB sends a Handover Command Message that has (R<sub>j</sub>, TS<sub>j</sub>, σ<sub>j</sub>, ID<sub>j</sub>) to the MRN which in turn broadcasts the message to all on-board UEs.
Step 2.2 [Key Generation and Confirmation]. After receiving the Handover Command message, each UE_i first verifies the received signature by checking $\hat{e}(\sigma_i, g) = \hat{e}(H(R_i || TS_j), Y_i)$. Then, it chooses a random number $r_i \in \mathbb{Z}_q^*$, computes $R_i = g^{r_i} \in \mathbb{G}_1$ and chooses one of his one-time private keys $s_i$ to computes a signature $\sigma_i = H(R_i || TS_j)^{s_i}$. Moreover, it computes the new session key that will be shared with the T-eNB as $K_{ij} = R_i^{s_i} = g^{s_ir_i}$. Finally, it computes $MAC_{ij} = HMAC(K_{ij}, Y_id)$ for key confirmation and transmits a message that has $R_i, TS_j, Y_id, \sigma_i$, and $MAC_{ij}$ to the MRN.

Step 2.3 [Key Generations and Batch Keys Confirmation]. Before signatures verifications, the MRN verifies the received public keys by computing $k$ hash values of $Y_id$ to get $k$ locations in the Bloom filter received from the HSS. Then, it checks the bits at these locations such that if any of the bits at these $k$ locations is 0, then $Y_id$ is invalid and the corresponding message is dropped; whereas if all the bits are 1s, $Y_id$ is valid with high probability. After that, the MRN aggregates the signatures received from users with valid identities as follows

$$\sigma_{agg} = \prod_{i=1}^{n} \sigma_i$$  \hspace{1cm} (1)

The MRN can anonymously authenticate the $n$ users by performing a batch signature verification process by checking

$$\hat{e}(\sigma_{agg}, g) = \prod_{i=1}^{n} \hat{e}(H(R_i || TS_j), Y_i)$$  \hspace{1cm} (2)

In this way, all users can prove to the MRN that they are legitimate members in the repeated-trips group without revealing their real identities. Finally, the MRN aggregates all the received MAC values by

$$MAC_{agg} = \bigoplus_{i=1}^{n} MAC_{ij}$$  \hspace{1cm} (3)

and sends $R_1, \ldots, R_n, TS_j, \sigma_{agg}, MAC_{agg}, Y_id, \ldots, Y_{nd}$ to the T-eNB.

Step 2.4 [Group Handover Confirmation]. The T-eNB executes similar process as the MRN to check the received public keys and perform batch signature verification. Moreover, for each user UE_i, T-eNB computes the new session key as $K_{ij} = R_i^{s_i} = g^{s_i r_i}$, computes $MAC_{ij} = HMAC(K_{ij}, Y_id)$, and computes the aggregated MAC as

$$MAC_{agg} = \bigoplus_{i=1}^{n} MAC_{ij}$$  \hspace{1cm} (4)

Moreover, for each user UE_i, T-eNB computes the new session key as $K_{ij} = R_i^{s_i} = g^{s_i r_i}$, computes $MAC_{ij} = HMAC(K_{ij}, Y_id)$, and the aggregated MAC as

$$MAC_{agg} = \bigoplus_{i=1}^{n} MAC_{ij}$$  \hspace{1cm} (5)

Finally, T-eNB performs a batch key confirmation process by checking that $MAC_{agg}^{MRN} = MAC_{agg}^{T-eNB}$. If the check succeeds, it informs all the users that all keys are confirmed by sending a broadcast message via the MRN.

3) Handover Completion:

In this phase, the T-eNB informs the MME that the UEs have changed cells, and the MME responds to the T-eNB with a PATH SWITCH REQ ACK message to confirm the completion of the handover. Finally, the T-eNB transmits a Release Resources message to the the S-eNB.

VI. SECURITY AND PRIVACY ANALYSIS

In this section, we analyze the security and privacy features of our scheme and discuss how it can satisfy the design goals discussed in subsection III-C.

Anonymous and mutual authentication. Since the MRNs act as gateways for the on-board users, they must ensure that the received messages are coming from legitimate users before forwarding them to the T-eNB. Therefore, users should anonymously authenticate themselves to the MRNs and eNBs. This is achieved in our scheme because each user sends a signature $\sigma_i$ along one-time public key $Y_i$. The MRN and eNB check the existence of $Y_id$ in the Bloom filter received from the HSS to verify the public keys and then verify the signatures to authenticate the users. In this way, the MRNs and eNBs can ensure that the received messages are coming from legitimate users without revealing their real identities. In addition, T-eNB can authenticate itself to the UEs by sending a signature $\sigma_j$.

Unlike the proposed scheme in [3] in which the eNBs are trusted to know the real identities of the users, the eNBs can not identify or track the users in our scheme. Moreover in [3], the MRN re-encrypts all the received handover keys without checking whether they are coming from legitimate users or external attackers. After that, the T-eNB decrypts all the received re-encrypted keys and tries to verify the received signatures by brute-force searching of all the users’ public keys. When no public key can verify the received signature, the T-eNB can learn that this message is coming from an attacker. It is clear that much resources are consumed before identifying and dropping fake messages sent by external attackers. On contrary, in our scheme these messages can be identified and dropped by the MRNs without forwarding them to the eNBs.

Location privacy and routes traceability. In our handover scheme, we aim to hide the user’s location information from the MRNs and eNBs. This is done by hiding the user’s real identity. If the MRN or colluding eNBs learn the user’s identity during the handover procedure, they can easily track his location and route. In our scheme, neither the MRNs nor the colluding eNBs can track the user’s locations from the exchanged handover messages because the user uses different and unlinkable one-time identities during each handover process. Compared to the proposed scheme in [3], colluding eNBs can track the user’s locations while in our scheme the MRNs and eNBs cannot do that.

Secure session key agreement. In our scheme, each UE_i and T-eNB_j can generate the session key $K_{ij} = g^{s_ir_j}$ using the
Diffie-Hellman (DH) algorithm. Based on the discrete logarithmic problem (DLP), attackers can not obtain the random numbers $r_i$ and $r_j$ from $g^{r_i}$ and $g^{r_j}$ respectively. Moreover, based on the computational Diffie-Hellman problem (CDH), it is computationally infeasible to generate the secret key $g^{r_i r_j}$ given $g^{r_i}$ and $g^{r_j}$. Therefore, only UE$_i$ and T-eNB$_j$ can generate the session key $K_{ij}$.

**Perfect forward and backward secrecy (PFS and PBS).** PFS protects past sessions against future compromises of secret keys, i.e., in PFS, a compromised session key should not lead to deriving past session keys. On the contrary, in PBS, a compromised session key should not lead to deriving next session keys. The PFS and PBS are achieved in our scheme because a fresh key is computed in each handover.

**Replay attacks resistance.** Our scheme can resist replay attacks by using signatures and timestamps. During a handover process, an attacker can eavesdrop $R_i = g^{s_i}$, $TS_j$, and $\sigma_i = H(R_i || TS_j)^{s_i}$. In a future handover process, if the attacker tries to reuse the same signature, the attack fails because the signature should be on a different timestamp.

**Impact of false positive probability.** The Bloom filter can be designed to experience a very small false positive probability. Even if and attacker sends a false public key and it is found to be in the filter, the attack fails because the attacker does not have the private key needed to sign his message. Therefore, the false positive probability does not affect the security strength of our scheme.

**VII. PERFORMANCE EVALUATIONS**

In this section we evaluate the performance of our proposed scheme in terms of signaling and computational cost.

**A. Signaling Cost**

The signaling cost is measured by the number of exchanged messages in order to complete the handover process. Figure 4 gives the signaling cost as the number of users ($n$) increases. For the handover scheme proposed in [3], beside the handover preparation messages and the confirmation messages, each user sends an encrypted session key to be shared with the T-eNB and the MRN re-encrypts all the $n$ keys and forwards them individually to the T-eNB. Therefore, the signaling cost in [3] is $2n + 3$. In our scheme, the signaling cost is $n + 6$. The reduction in the signaling cost compared to [3] is achieved because each UE sends only one message for key generation and confirmation and the MRN aggregates the users MAC values for batch MACs verification. As $n$ increases, the signaling cost yields to $2n$ and $n$ in [3] and our scheme, respectively. In this case, our scheme can reduce the signaling cost of [3] by approximately 50%.

**B. Computational Cost**

The computational cost is the time required by UEs, MRNs, and eNBs to run the handover scheme. The total computational cost should be reduced since it affects the handover latency. In our evaluations, all the computations done offline are excluded from the comparison and only the operations computed during the handover procedure are considered. We assume that the times required to compute a modular exponentiation operation, hash operation, point multiplication, and bilinear pairing are denoted by $T_E$, $T_H$, $T_M$, $T_P$, respectively.

During the handover procedure in [3], each user computes a signature which requires the computation of one hashing operation with a cost of $T_H$ and one exponentiation operation with a cost of $T_E$. For the MRN, it computes $n$ pairing operations for $n$ users which costs $nT_P$. For the T-eNB, it decrypts the received ciphertexts and verifies the received signatures. To decrypt the received ciphertext, the T-eNB computes $n$ exponentiation operations and $n$ point multiplications with a total cost of $nT_E + nT_M$. For signatures verifications, the verification process of the first signature requires the computation of one hashing operation, and exhaustive-searching the list of the users’ public keys to find the correct public key that can verify the signature. In the best case, the first signature verification process requires $2$ pairing operations when the first tested public key can verify the signature, while in the worst case, it takes $1 + n$ pairing operations when the last tested public key verifies the signature. We assume that on average, the correct public key will be found after searching half of the public keys’ list which make the verification process costs $1 + \frac{n}{2}$ pairing operations. Similarly, the verification of the second signature requires $1 + \frac{n}{2}$ pairing operations since one public key was excluded from the second exhaustive search. This results in a total cost for signature verification of $nT_H + nT_P + \frac{1}{2} n(n-1)T_P$. It should be noted that from a latency prospective, we will assume the MRN computes only one pairing operation instead of $nT_P$ because the computations in [3] are pipelined, i.e., while the T-eNB verifies the first signature, the MRN is re-encrypting the second ciphertext, and the MRN computations are expected to be faster than the T-eNB computations.

In our scheme, each user verifies the T-eNB signature with a cost $T_H + 2T_P$, computes his own signature with a cost $T_H + T_E$, derives the session key $K_{ij}$ which costs $T_E$ and one MAC computation that costs $T_H$. Therefore the total computation cost for the user is $2T_P + 3T_H + 2T_E$. The MRN computations includes $nkT_H$ to check the existence.
of the public keys in the Bloom filter, \( n \) point multiplication operations to aggregate the signatures, \( n \) hash computation and \( n+1 \) pairing operation to verify the aggregated signature and \( n \) XOR operations to aggregate the MACs which can be ignored because they are very small. Thus, the total computation cost for the MRN becomes \( n(k+1)T_H + nT_M + (n+1)TP \). Finally, the \( T_eNB \) verifies the public keys and the aggregated signature as the MRN. It also computes \( n \) exponentiation operations to compute the session keys and \( n \) HMAC values for key confirmation. Therefore, the total computation cost for the \( T_eNB \) is \( n(k+2)T_H + (n+1)TP + nTP \).

Table III gives the time measurements of primitive cryptographic operations \([14]\). Using these measurements, we compare in Figure 5, the total computation cost of \([3]\) and our scheme versus the number of users. As shown in the figure, as the number of users increases, the total computation cost during the handover procedure in \([3]\) increases at a parabolic rate while our scheme exhibits a linear growth rate. This is because pairing is the most time-consuming operation during the handover process and \([3]\) has a computation complexity of \( O(n^2) \) while it is \( O(n) \) in our scheme. Therefore, our scheme outperforms \([3]\) in terms of the total computation complexity.

### VIII. Conclusion

In this paper, we have proposed a privacy-preserving intra-MME group handover scheme in LTE-A networks for repeated trips. In our scheme, the MRNs and eNBs are not trusted because they are installed in open environment. In order to preserve the privacy of the users and prevent routes traceability, each user uses on-time public/private key pair for each handover process. In order to verify the keys efficiently, they are stored in a Bloom filter and distributed to the MRNs and eNBs of the users’ repeated routes. Our security analysis demonstrated that the singular and colluding MRNs and eNBs cannot identify the users or track them. Moreover, since the MRNs can anonymously authenticate the users, the messages sent from external attackers can be dropped by the MRNs. Our performance evaluations demonstrated that our scheme is more efficient in terms of signalling and computation cost comparing to the most related scheme in the literature.

### References


