Privacy-Preserving Intra-MME Group Handover Via MRN in LTE-A Networks for Repeated Trips

Zaher Haddad*, Ahmad Alsharif**, Ahmed Sherif**, Mohamed Mahmoud**
*Department of Computer Science, Al-Aqsa University, Gaza, Palestine
**Department of Electrical and Computer Engineering, Tennessee Tech. University, TN, USA 38505

***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 network. Second, the proposed scheme also aims to reduce the computational and signaling overhead and establish secure session keys. Third, the scheme aims to prevent MRNs and eNBs from tracking passengers' locations especially if they take same trip regularly. 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 computation 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 3rd Generation Partnership Project (3GPP) [1]. The LTE-A architecture is composed of two different domains, access domain that contains User Equipments (UEs) and evolved Nodes B (eNBs), and core domain which has Home Subscriber Server (HSS) and Mobility Management Entities (MMEs).

In fast moving buses and trains, data transmission suffers from high pathloss, and the large number of simultaneous handovers requests may cause a low handover success rate. To overcome these issues, the concept of Mobile Relay Nodes (MRNs) is proposed for LTE-A [2]. The MRN connects UEs to eNBs by using an outer antenna mounted on the top of buses and trains. It can increase the handover sucess rate by using group handover procedure which reduces the traffic load [3]. However, since the MRNs and eNBs are installed in open environments, they can be compromised.

Hiding users' 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 tries to know the session key shared between UEs and honest eNB. Security and privacy issues have been investigated in different schemes such as [4]–[6] but these schemes cannot be applied to our problem because the network and threat models are different. Other schemes have been proposed to perform secure group handover in LTE-A networks [7], [8]. In [7], Cao et al. proposed a secure group-based handover scheme for machine type communication based on the multi-signature technique 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. Other schemes were proposed in [9], [10], however, these schemes do not consider the privacy issues and/or collusion between MRNs and eNBs.

In [11], Kong et al. proposed a secure handover session key management scheme via untrusted MRNs. In the proposed scheme, initially, all users' public keys are transferred from the serving eNB (S-eNB) to the target eNB (T-eNB). Then, each user generates a session key, encrypts it with the MME's public key and sends the encrypted key with 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-eNB re-encryption key so that it can decrypt the ciphertext and get the shared key. For n users, the T-eNB received n public keys from the S-eNB and has n session keys and n signatures. To verify each signature, the T-eNB should perform exhaustive search to find which public key can verify each signature which increases the computations dramatically. Also, since MRNs can not authenticate the received messages from UEs before forwarding them to eNBs, messages sent from external attackers can consume a lot of resources before they are dropped at the T-eNB when no public key could verify them. Moreover, since the eNBs can know the real identities of users, they can know users' locations and track them.

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 only for one handover process to preserve the user's privacy. All the one-time public keys of legitimate users are added to a Bloom filter by the HSS. Then, the HSS distributes this filter to the MRNs/eNBs to verify the public keys efficiently since there is no need to distribute and verify certificates. The HSS does not need to distribute the filter to all MRNs and eNBs in the system, but only to the MRNs and eNBs on the trips routes of users. Our security/privacy analysis demonstrates that the proposed scheme can preserve users' locations privacy, achieve secure session key agreement and anonymous authentication, and resist collusion between malicious MRNs and eNBs. Our performance evaluation demon-

978-1-5090-5935-5/17/$31.00 ©2017 IEEE

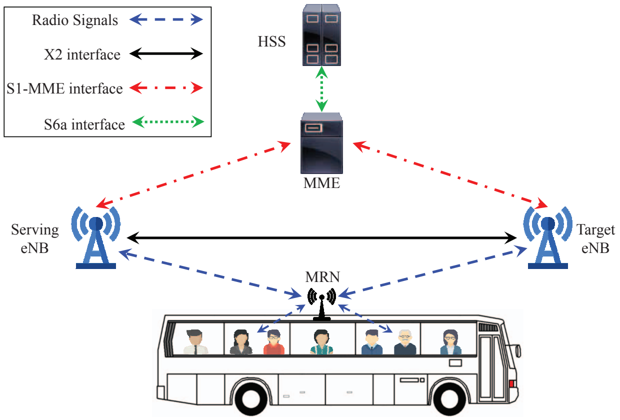

Fig. 1: The network model.

strates that the proposed handover scheme requires exchanging a few messages and low computational overhead.

The remainder of the paper is organized as follows. In Section II, we describe the system model. The proposed scheme is explained in Section III. The security/privacy analysis and the performance evaluations are provided in Sections IV and V respectively. Finally, Section VI concludes the paper.

II. Network and Threat Models

A. Network Model

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 located in fixed locations near the roads or railways and connected to each other through X2 links, while the MRN can communicate with nearby eNB by using wireless communication. The core domain contains 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

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 network operators. Moreover, eNBs are also considered untrusted as they are installed in an open environment and could be compromised. Attackers aim to get sensitive location information about the users or obtain the shared keys between the UEs and the eNBs. Attackers can also be internal or external, they can work individually or they can collude to launch stronger attacks.

III. Proposed Scheme

A. System Initialization

The HSS generates the parameters $(q, \mathbb{G}_1, \mathbb{G}_2, g, \hat{e})$ where $\mathbb{G}_1$ and $\mathbb{G}_2$ are two multiplicative cyclic group of prime order q, g is a generator in $\mathbb{G}_1$ and $\hat{e}$ is a bilinear pairing such that $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. The HSS also chooses a secure cryptographic hash function H, where H: $\{0,1\}^* \to \mathbb{G}_1$. and publishes the system parameters $pubs = \{g, q, \mathbb{G}_1, \mathbb{G}_2, P, \hat{e}, H\}$. Each user UE$_i$ has a long-term private/public key pair $(x_i, Y_i = g^{x_i})$ and each eNB$_j$ has a private and public key pair $(x_j, Y_j = g^{x_j})$.

Each user UE$_i$ should compute a list of L one-time private/public key pairs $(s_{i\ell}, Y_{i\ell})$, where $1 \leq \ell \leq L$. Each key pair will be used to anonymously authenticate the user to MRN and eNB during the handover procedure. Then, UE$_i$ sends the one-time public keys to the HSS. The HSS adds the one-time keys to the record of UE$_i$. It also adds the one-time public keys to a Bloom filter [12] containing the set of all one-time public keys of all users by hashing every one-time public key using k hash functions and the bit locations in the filter corresponding to the hash values are set to 1. Then, the HSS forwards the Bloom filter to the MRNs and eNBs. We would like to point out that this operation is done offline and users can generate new lists of public keys every interval of time before all keys are used. 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

As shown Fig. 2, 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 strengthes of the S-eNB and the 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 sends a *Handover Request* message to the T-eNB with the necessary information to prepare for the handover such as the required resources.

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_j, computes $R_j = g^{r_j}$ and signature $\sigma_j = H\left(R_j || TS_j\right)^{x_j}$, where TS_j is a time stamp. Finally, it sends *Handover Request Acknowledgement* packet having $\langle R_j, TS_j, \sigma_j \rangle$ to the S-eNB.

2) Handover Execution:

Step 2.1 [*Handover Command*]. The S-eNB sends a *Handover Command Message* that has $\langle R_j, TS_j, \sigma_j \rangle$ to the MRN which in turns broadcasts the message to all on-board UEs.

Step 2.2 [*Key Generation and Confirmation*]. After receiving the *Handover Command* message, each UE$_i$ verifies the received signature by checking $\hat{e}\left(\sigma_j, g\right) \overset{?}{=} \hat{e}\left(H\left(R_j || TS_j\right), Y_j\right)$. Then, it chooses a random number r_i, computes $R_i = g^{r_i}$ and chooses one of his one-time private keys $s_{i\ell}$ to computes a signature $\sigma_i = H\left(R_i || TS_j\right)^{s_{i\ell}}$. Moreover, it computes the session key that will be shared with the T-eNB as $K_{ij} = R_j^{r_i} = g^{r_i r_j}$. Finally, it computes a hash-based message authentication code MAC_{ij} = HMAC(K_{ij}, Y_{il}) for key confirmation and transmits a message that has $R_i, TS_j, Y_{i\ell}, \sigma_i$, and MAC_{ij} to the MRN.

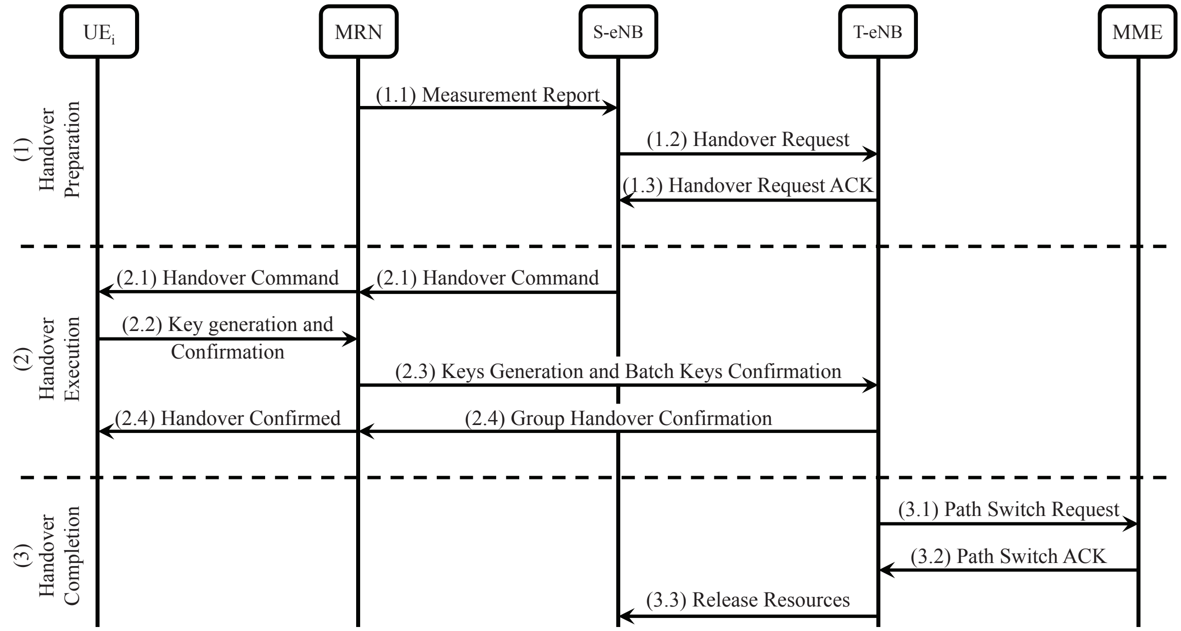

Fig. 2: Detailed intra-MME handover message flow.

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 $Y_{i\ell}$ to get k locations in the Bloom filter received from the HSS. Then, it checks the bits at these k locations such that if any of these bits is 0, then $Y_{i\ell}$ is invalid and the corresponding message is dropped; whereas if all these bits are 1s, $Y_{i\ell}$ is valid with high probability. After that, the MRN aggregates the signatures received from legitimate users as $\sigma_{agg} = \prod_{i=1}^{n} \sigma_i$, then it can anonymously authenticate them by performing a batch signature verification process by checking $\hat{e}\left(\sigma_{agg}, g\right) \overset{?}{=} \prod_{i=1}^{n} \hat{e}\left(H\left(R_i || TS_j\right), Y_i\right)$. In this way, all users prove to the MRN that they are legitimate members in the repeated-trips group without revealing their real identities. Finally, the MRN aggregates the received MAC values as $MAC_{agg} = \bigoplus_{i=1}^{n} MAC_{ij}$ and sends $R_1, \ldots, R_n, TS_j, \sigma_{agg}$, $MAC_{agg}, Y_{1\ell}, \ldots, Y_{n\ell}$ 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 session key as $K_{ij} = R_i^{r_j} = g^{r_i r_j}$, $MAC'_{ij} = HMAC(K_{ij}, Y_{il})$, and the aggregated MAC $MAC'_{agg} = \bigoplus_{i=1}^{n} MAC'_{ij}$. Finally, the T-eNB performs a batch key confirmation process by checking that $MAC'_{agg} \overset{?}{=} MAC_{agg}$. If they are equal, the T-eNB informs all 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 handover completion. Finally, the T-eNB transmits a *Release Resources message* to the S-eNB.

IV. Security and Privacy Analysis

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 can be achieved because each user sends a signature σ_i and one-time public key $Y_{i\ell}$. The MRN and eNB check the existence of $Y_{i\ell}$ 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 σ_j.

Unlike the proposed scheme in [11] in which the eNBs are trusted to know the real identities of users, the eNBs can not identify or track the users in our scheme. Moreover in [11], 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 received re-encrypted keys and tries to verify the received signatures by brute-force searching of all 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 the contrary, in our scheme these messages can be identifies 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 user's real identity. If the MRN or colluding eNBs learn the user's identity during the handover procedure, they can easily track

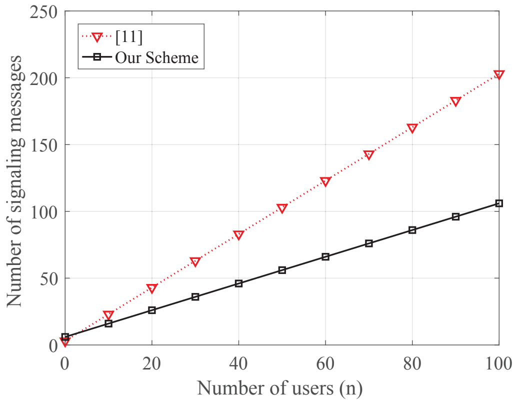

Fig. 3: Signaling cost comparison.

his location and route. In our scheme, neither the MRNs nor the colluding eNBs can track the users' 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 [11], colluding eNBs can track the users' locations while in our scheme the MRNs and eNBs can not do that.

Secure session key agreement. In our scheme, each UE$_i$ and T-eNB$_j$ can generate the session key $K_{ij} = g^{r_i r_j}$ 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). 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 $R_i = g^{r_i}$, TS_j, and $\sigma_i = H(R_i \parallel TS_j)^{s_{i\ell}}$. 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. If an attacker sends a false public key and it is found to be in the filter, the attack fails since he 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.

V. 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. Fig. 3 gives the signaling cost as the number of users (n) increases. For the handover scheme proposed in [11], 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 [11] is $2n + 3$. In our scheme, the signaling cost is $n + 6$. The reduction in the signaling cost compared to [11] 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 [11] and our scheme, respectively. In this case, our scheme can reduce the signaling cost of [11] 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 computations that can be 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 [11], each user computes a signature which requires the computation of one hashing and one exponentiation operations while the MRN 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 multiplication operations with a total cost of $nT_E + nT_M$. For n signatures verifications, the verification of the first signature requires the computation of one hash, and exhaustive-searching the list of users' public keys to find the correct public key that verifies the signature. In the best case, the first verification process requires 2 pairing operations when the first tested public key verifies the signature, while in the worst case it takes $1{+}n$ pairing operations when the last tested public key verifies the signature. We assume on average the correct public key will be found after searching half of the list which make the verification process costs $(1{+}\frac{n}{2})T_P$. Similarly, the verification of the second signature requires $(1 + \frac{n-1}{2})T_P$ since one public key was excluded from the second exhaustive search. This results in a total cost for signature verification of $nT_H + nT_P + \frac{1}{2}\frac{n(n+1)}{2}T_P$. It should be noted that from a latency prospective, we assume the MRN requires T_P instead of nT_P since the computations in [11] 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.

In our scheme, each user verifies the T-eNB signature with a cost $T_H + 2T_P$, computes his signature with a cost $T_H + T_E$, derives the session key with a cost T_E and one MAC computation that costs T_H. Therefore, the total computations for the

TABLE I: Computation Cost Comparison

	[11]	Our Scheme
T_{UE}	$T_H + T_E$	$2T_P + 3T_H + 2T_E$
T_{MRN}	T_P	$n(k+1)T_H + nT_M + (n+1)T_P$
T_{eNB}	$nT_E + nT_M + nT_H + nT_P + \frac{1}{2}\frac{n^2+n}{2}T_P$	$n(k+2)T_H + (n+1)T_P + nT_E$

TABLE II: Time cost of cryptographic operations (ms) [13]

	T_E	T_H	T_M	T_P
UE	1.698	0.0356	1.537	38.376
MRN/eNB	0.525	0.0121	0.475	16.322

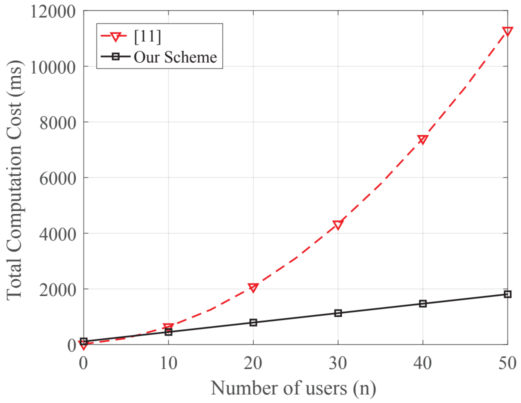

Fig. 4: Total computation cost comparison.

user is $2T_P + 3T_H + 2T_E$. The MRN computations includes nkT_H to check the existence of public keys in the Bloom filter, n point multiplications to aggregate the signatures, n hash computations and $n+1$ paring operations to verify the aggregated signature and n XOR operations to aggregate the MACs which are ignored. Thus, the total computation cost for the MRN is $n(k+1)T_H + nT_M + (n+1)T_P$. Finally, the T-eNB verifies the public keys and the aggregated signature as the MRN. It also computes n exponentiations to compute the session keys and n HMAC values for key confirmation. Therefore, the total computation cost for the T-eNB is $n(k+2)T_H + (n+1)T_P + nT_E$.

Table I summarizes the computations of [11] and our scheme and Table II gives the time measurements of primitive cryptographic operations [13]. Using these measurements, we compare in Fig. 4 the total computation cost of [11] and our scheme. As shown in the figure, as n increases, the total computation during the handover procedure in [11] increases at a parabolic rate while our scheme exhibits a linear rate. This is because pairing is the most time-consuming operation during the handover process and [11] has a computation complexity of $\mathcal{O}(n^2)$ while it is $\mathcal{O}(n)$ in our scheme. Therefore, our scheme outperforms [11] in terms of total computation complexity.

VI. 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 users and prevent routes traceability, each user uses one-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 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 signaling and computation cost comparing to the most related scheme in the literature.

Acknowledgment

This work is supported by US National Science Foundation under the grants numbers 1619250 and 1618549. The statements made herein are solely the responsibility of the authors.

References

[1] S. Parkvall, E. Dahlman, A. Furuskar, Y. Jading, M. Olsson, S. Wanstedt, and K. Zangi, "LTE-Advanced - Evolving LTE towards IMT-Advanced," *Proceedings of 2008 IEEE 68th Vehicular Technology Conference*, pp. 1–5, Septemper 2008.

[2] Y. Sui, I. Guvenc, and T. Svensson, "Interference management for moving networks in ultra-dense urban scenarios," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 111, 2015.

[3] N. Lin, X. Huang, and X. Ma, "Analysis of the Uplink Capacity in the High-Speed Train Wireless Communication with Full-Duplex Mobile Relay," *Proceedings of 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, pp. 1–5, May 2016.

[4] M. Mahmoud, S. Taha, J. Misic, and X. Shen, "Lightweight privacy-preserving and secure communication protocol for hybrid Ad Hoc wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2077–2090, Aug 2014.

[5] M. Mahmoud, X. Lin, and X. Shen, "Secure and reliable routing protocols for heterogeneous multihop wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1140–1153, April 2015.

[6] Z. Haddad, M. Mahmoud, S. Taha, and I. A. Saroit, "Secure and privacy-preserving AMI-utility communications via LTE-A networks," in *IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2015, pp. 748–755.

[7] J. Cao, H. Li, M. Ma, and F. Li, "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks," pp. 7246–7251, June 2015.

[8] 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," *Proceedings of 2014 IEEE International Conference on Communications (ICC)*, pp. 1011–1016, June 2014.

[9] M. S. Pan, T. M. Lin, and W. T. Chen, "An Enhanced Handover Scheme for Mobile Relays in LTE-A High-Speed Rail Networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 743–756, 2015.

[10] Z. Haddad, M. Mahmoud, I. A. Saroit, and S. Taha, "Secure and efficient uniform handover scheme for LTE-A networks," in *IEEE Wireless Communications and Networking Conference*, April 2016, pp. 1–6.

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

[12] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[13] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between HeNB and eNB in LTE networks," *Computer Networks*, vol. 56, no. 8, pp. 2119 – 2131, 2012.