Achieve Secure Handover Session Key Management via Mobile Relay in LTE-Advanced Networks

Qinglei Kong, *Student Member, IEEE*, Rongxing Lu, *Senior Member, IEEE*, Shuo Chen, and Hui Zhu, *Member, IEEE*

***Abstract*—Internet of Things is expanding the network by integrating huge amount of surrounding objects which requires the secure and reliable transmission of the high volume data generation, and the mobile relay technique is one of the efficient ways to meet the on-board data explosion in LTE-Advanced (LTE-A) networks. However, the practice of the mobile relay will pose potential threats to the information security during the handover process. Therefore, to address this challenge, in this paper, we propose a secure handover session key management scheme via mobile relay in LTE-A networks. Specifically, in the proposed scheme, to achieve forward and backward key separations, the session key shared between the on-board user equipment (UE) and the connected donor evolved node B (DeNB) is first generated by the on-board UE and then securely distributed to the DeNB. Furthermore, to reduce the communication overhead and the computational complexity, a novel proxy re-encryption technique is employed, where the session keys initially encrypted with the public key of the mobility management entity (MME) will be re-encrypted by a mobile relay node (MRN), so that other DeNBs can later decrypt the session keys with their own private keys while without the direct involvement of the MME. Detailed security analysis shows that the proposed scheme can successfully establish session keys between the on-board UEs and their connected DeNB, achieving backward and forward key separations, and resisting against the collusion between the MRN and the DeNB as the same time. In addition, performance evaluations via extensive simulations are carried out to demonstrate the efficiency and effectiveness of the proposed scheme.**

***Index Terms*—Handover, Internet of Things (IoT), LTE-Advanced (LTE-A) networks, mobile relay, secure key establishment.**

I. Introduction

With the proliferation of various enabling technologies, many small objects that surround us can be integrated into the Internet in one form or another, which is called the Internet of Things (IoT) paradigm [1]. The third generation partnership project (3GPP) has identified machine type communication (MTC) to be one of the facilitators for IoT in LTE-Advanced (LTE-A) networks [2], [3], and the highly penetrated portable electronic devices (smart phones, tablets, etc.) are regarded as common contact points or gateways for the large-scale deployment of IoT devices [4], [5]. Advanced transportation (high-speed trains, buses, trams, cars, etc.) which are moving along the rails/roads and equipped with various sensors and enough processing power, are perfect candidates for the real-time environmental monitoring and mapping, which is an indispensable part of IoT [6], [7]. For the information and data collected by the on-board sensors, they can be aggregated and processed by the on-board units, and then transmitted to the Internet by on-board mobile devices. In the meanwhile, the mobile devices which belong to the passengers are also responsible for managing the small scale autonomous networks, and the constant wireless broadband network access is mandatory for these on-board mobile devices [8], [9].

However, for public transportation, due to the fast moving well-shielded carriage, data transmission will suffer from high penetration path loss, severe Doppler frequency shift, and low handover success rate caused by a large number of on-board mobile devices performing frequent handovers simultaneously. To circumvent the above problems, the concept of mobile relay is proposed in the 3GPP in LTE-A networks [10]. A mobile relay consists of an outer antenna mounted on the top of the moving transportation providing a wireless backhaul with a donor evolved node B (DeNB) located along the roadside, while the wireless connection to the on-board users is realized by the inner antenna installed inside the carriage [11], [12]. As such, the Doppler effect in this network scenario can be mitigated by referring to the speed and track information [13]. To increase the handover success rate, the mobile relay node (MRN) represents all the user equipments (UEs) to conduct handover, as a result, the heavy traffic loads caused by the handover can be released [14], [15].

From the perspective of mobile operators, the deployment of MRNs may introduce heavy capital expenditure due to the large quantity of public transportation, and bring high operating expenditure owing to their moving characteristics [16]. Meanwhile, the public transportation companies may have a high motivation to install their own MRNs on the top of their public transportation to improve the on-board experiences of their passengers and the quality of the IoT-related services,

Manuscript received April 21, 2016; revised July 25, 2016; accepted September 26, 2016. Date of publication October 4, 2016; date of current version February 8, 2017. This work was supported in part by the Economic Development Board, Singapore, for the "Development of NTU/NXP Smart Mobility Test-bed," project under Grant S15-1105-RF-LLF URBAN, and in part by the National Natural Science Foundation of China under Grant 61303218.

Q. Kong and S. Chen are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: qlkong@ntu.edu.sg; schen@ntu.edu.sg).

R. Lu is with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB E3B 5A3, Canada (e-mail: rxlu@ieee.org).

H. Zhu is with the School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: zhuhui@xidian.edu.cn).

Digital Object Identifier 10.1109/JIOT.2016.2614976

and it can further gain more reputation and economic profits. Despite the countless advantages brought by the MRNs, there still exists many practical challenges in real applications. One crucial challenge is the emerging threats and difficulties in session key establishment between the on-board UE and the DeNB during the handover process [17].

In the 3GPP LTE-A networks, the session key established between one UE and one DeNB, aims to protect the integrity and confidentiality of the control-plane signaling, and the confidentiality of the user-plane data transmission [18], [19]. In the evolved packet system (EPS) of the LTE-A networks, the session key generation is based on the simultaneous key update of both the UE and the DeNB during the handover process according to a key chaining counter [20]. However, there exist many problems related to this key management scheme. One of the potential threats is the desynchronization attack caused by manipulating the key chaining counter, and this type of attack may leave the subsequent session keys vulnerable to be compromised [21]. Especially in our MRN scenario, on the one hand, the on-board UEs may experience frequent handover, and the probability of the desynchronization attack may increase. On the other hand, the untrusted third-party owned MRN can store all the messages it received-and-forwarded, and the corruption of a chain of session keys can potentially lead to the devastating effect of the leakage of all the transmitted messages. Furthermore, the frequent handover may also bring in heavy computational pressure to the MME in the core network, due to the frequent fresh keying material generation.

To protect the secure data transmission between the on-board UEs and the DeNBs, a new handover key management scheme needs to be devised. For the on-board UEs, the proposed scheme should be able to protect the confidentiality and integrity of the data transmission. From the perspective of the DeNBs, if one DeNB is compromised by a rogue base station attack, the corrupted DeNB should be isolated from the network. And the establishment of the large amount of session keys should also not introduce heavy computational load and severe handover latency. From the perspective of the MME, the key establishment process should not introduce heavy computational burden. For the MRN, the ultimate goal of the deployment of the MRN is to bring high quality wireless access service to the on-board UEs, and the MRNs can also be involved in the session key establishment process without revealing the content of the session keys.

Motivated by the above-mentioned analysis, in this paper, we devise a novel secure handover key management scheme in LTE-A networks, when the MRNs are owned by third parties. With the proposed handover key management scheme, each on-board UE can successfully establish its session key with the DeNB during the handover process while guaranteeing the forward and backward session key separations. Specifically, the main contributions of this paper are threefold.

First, instead of updating the session key at both the on-board UE and the DeNB sides, the session key is generated by the on-board UE itself and delivered to the DeNB. Thus, the DeNB can achieve perfect one-hop forward/backward key separation and resist against the desynchronization attack. While in the EPS key management scheme, the forward separation is achieved on a two-hop basis and the key management process is vulnerable to the desynchronization attack [20].

Second, the session key generated by the on-board UE is encrypted by a universal public key, i.e., the public key of the MME, and there requires no public key transmission of the connected DeNB. The location information of the target DeNB is also exploited in the session key encryption to avoid collusion between the mobile relay and the compromised DeNB. Since the target DeNB cannot decrypt the received message encrypted by the public key of the MME, the MRN re-encrypts the received messages into messages that can be decrypted by the target DeNB without revealing the contents of the established session keys. Furthermore, as the MME is not involved during the session key establishment process, the proposed scheme introduces no computational load to the MME.

Finally, to validate the effectiveness of our proposed handover key management scheme, we conduct numerical experiments. We first implement the cryptographical results using Java, then we examine the computational delay with respect to the number of MRNs and the number of UEs, and the communication overhead and storage load are also analyzed.

The remainder of this paper is organized as follows. We introduce the system model and security requirements, and identify the design goals of this paper in Section II. In Section III, we briefly review the LTE EPS handover key management, and recall the bilinear pairing and proxy re-encryption techniques as preliminaries, which will be utilized in subsequent sections. We propose our handover key management in MRN scenario in Section IV, followed by security analysis and performance evaluation in Section V and in Section VI, respectively. We give related work in Section VII, and finally conclude this paper in Section VIII.

II. System Model, Security Requirement, and Design Goal

In this section, we introduce the system model, present the security requirements, and identify our design goals.

A. System Model

The mobile relay network scenario under the 3GPP LTE architecture is composed of the access domain (evolved universal terrestrial radio network) and the core domain [evolved packet core (EPC)] [20]. The access domain consists of on-board UEs, MRNs installed on public transportation, and mobile relay capable DeNBs, as shown in Fig. 1. The DeNBs are connected to each other through the X2 link, while the DeNB and the MME is connected by the S1-C link [20]. When public vehicles or trains are moving forward, the UEs located inside the carriage maintain their connections to the network by communicating with the MRNs which are moving along with the on-board UEs. While at the same time, the MRNs communicate with the fixed DeNBs located near the roads or railways. In the core network domain, we only take the MME into consideration, and the functionalities of an MME includes performing mutual authentication with the UEs on

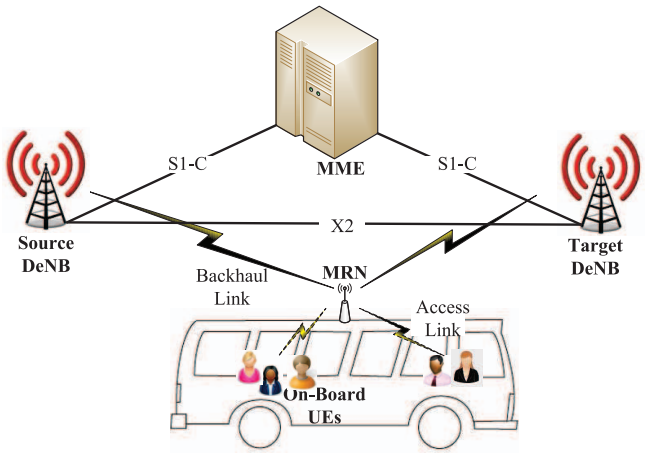

Fig. 1. System model under consideration.

behalf of the EPC and taking control of mobility management of the UEs.

When an on-board UE communicates with one DeNB through the cooperation of an MRN, it may roam out of the coverage area of the current DeNB, and then connect to another DeNB. The 3GPP LTE network supports two types of handover, i.e., inter-MME handover and intra-MME handover. Since the inter-MME handover occurs between the UE and MME by running full EPS authentication key agreement (EPS-AKA) procedure, without the involvement of any signaling transmission between DeNBs, we only consider the intra-MME handover process and focus on the wireless links between the DeNB and the on-board UEs. Under this mobile relay network scenario, the on-board UEs conduct intra-MME handover between two neighboring DeNBs with the help of an MRN which is moving along. When a group of on-board UEs roam to the coverage of a new DeNB, new session keys need to be generated and established to protect the security of the radio access links between the on-board UEs and the new DeNB.

B. Security Requirements

A secure handover key management mechanism is one of the most important processes for the successful practice of an MRN. In our security model, we regard all the entities in the EPC and all the on-board UEs as trustable. Since the MRNs are owned and deployed by the third parties instead of the operators in this network scenario, the MRNs are considered to be untrusted. All the messages transmitted between the DeNBs and the on-board UEs are received-and-forwarded by the MRNs, the MRNs can eavesdrop, modify and replay the received messages. Furthermore, the DeNBs are also viewed as untrusted since they reside in the open environment, and the adversaries can launch some active attacks to corrupt the DeNBs. Therefore, the following security requirements should be satisfied in the secure handover key management.

1) Secure Session Key Establishment [22]: During the handover process, a secure session key between each on-board UE and the DeNB should be derived and established to protect the confidentiality and integrity of the transmission in the radio access link. The MRN should not disrupt the secure session key generation and association or achieve the session keys shared between the on-board UEs and the DeNB, even though it is capable of eavesdropping, modifying or replaying the messages passed through.

2) Backward Key Separation: For any connected DeNB, it is computationally infeasible to derive the previous session keys based on the current session keys shared with the on-board UEs. If one DeNB is corrupted, without the previous session keys, the messages transmitted between the previous DeNBs and the on-board UEs cannot be decrypted, and the attack can only compromise the transmission of the corrupted DeNB.

3) Forward Key Separation: Given the session keys shared between the on-board UEs and the connected DeNB, the DeNB is not computationally feasible to know the future session keys after the subsequent handover. Forward key separation prevents a corrupted DeNB from compromising other future DeNBs, and keeps the security breaches as local as possible.

4) Collusion Resistance [23]: For any compromised DeNB, even though the malicious MRNs owned by third-parties possess sufficient storage and computation capability, it is computationally infeasible for a collusion coalition between a corrupted DeNB and a malicious MRN to recover any of the previous and afterwards transmitted messages.

C. Design Goals

Based on the aforementioned system model and security requirements, our design goal is to develop an efficient and robust key management scheme during the handover process. Specifically, the following objectives should be achieved for the key management scheme during handover.

1) Security: The above-mentioned security requirements should be satisfied in the devised handover key management scheme. According to the previous statement and analysis, without taking the secure handover key management scheme into consideration, the real application of the MRNs is not even possible. Thus, the proposed handover key management scheme should simultaneously guarantee the secure session key derivation and association, achieve forward and backward key separation, at the same time, resist collusion attacks in the mobile relay handover scenario.

2) Efficiency: The security handover mechanism should not introduce heavy computational load to the MME, due to the keying material generation and update caused by the simultaneous frequent handover of the large amount of on-board UEs. For the on-board UEs and the target DeNB, the proposed handover key management scheme should not introduce heavy computational and traffic load, and the latency caused by the session key establishment should not degrade the user experience of the on-board UEs.

III. Preliminaries

In this section, we first make a brief introduction of the EPS handover key management mechanism, which was originally presented in 3GPP release 11 for LTE networks [20]. Then we

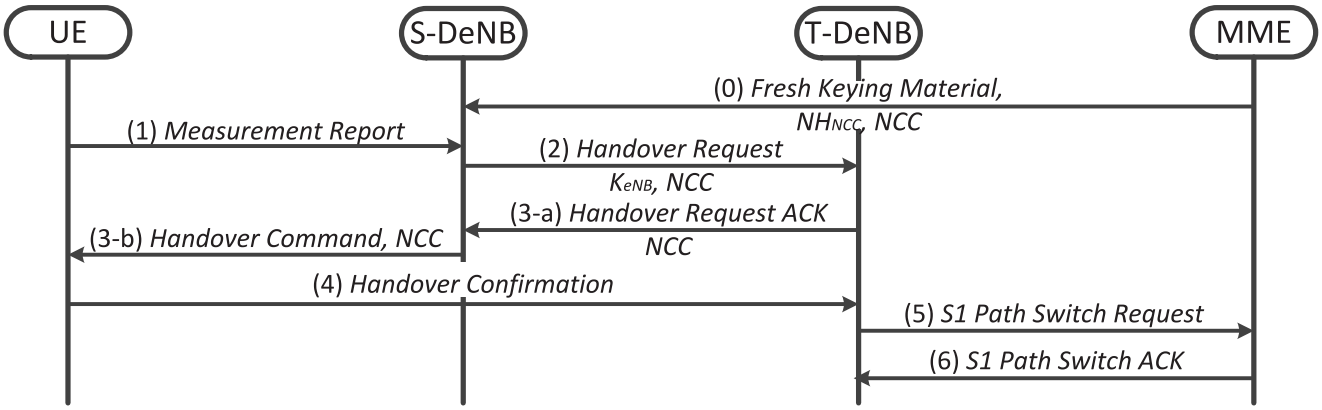

Fig. 2. Message flow during intra-MME handover.

recall the cryptographic techniques: bilinear pairing and proxy re-encryption, which function as the basis of our proposed handover key management mechanism.

A. Review of EPS Handover Key Management

During an intra-MME handover process, it is the task of the current source eNB to provide the next hop (NH) session keys shared between the target eNB and the roaming UEs, and the session key transfer is realized by the secure *X2* link established between eNBs [21]. To ensure backward key separation, the source eNB generates the next-hop session key K^*_{eNB} for the target eNB based on the current session key K_{eNB} by applying a one-way hash function, which is also called the key derivation function (KDF)

$$K^*_{\text{eNB}} = \text{KDF}(K_{\text{eNB}}, \alpha) \tag{1}$$

where α denotes the physical parameter related to the target eNB, and the above key update process is also denoted as the horizontal key derivation. However, after several horizontal key derivations, a set of session keys are linked to each other, which is known as the handover key chaining, and the current session key could be derived from the previous eNBs. To guarantee forward key separation, the vertical key derivation is introduced. After each intra-MME handover process, the MME provides fresh keying material NH_{NCC} to the target eNB for the NH session key generation

$$K^*_{\text{eNB}} = \text{KDF}(\text{NH}_{\text{NCC}}, \alpha) \tag{2}$$

where NH_{NCC} represents that the NH key has been updated next-hop chaining counter (NCC) times, and the current security association between the target eNB and UE is based on the value of NCC value. And the value of NH_{NCC} and the initial value NH_0 are generated as follows:

$$\begin{aligned} \text{NH}_{\text{NCC}} &= \text{KDF}(K_{\text{ASME}}, \text{NH}_{\text{NCC}-1}) \\ \text{NH}_0 &= \text{KDF}(K_{\text{ASME}}, K_{\text{eNB}}) \end{aligned} \tag{3}$$

where K_{ASME} is the first intermediate key used to protect the security of the NAS layer. Thus, a two-hop-based forward key separation is maintained, that is, the source eNB cannot derive the following session keys after two handovers. Fig. 2 depicts the message flow during an intra-MME handover process, by implementing the vertical key derivation.

In the proposed handover key management scheme, a desynchronization attack may happen to disrupt the update of the NCC value in *message* (2) or after *message* (6). To be more specific, if an eNB which is compromised by an adversary through physical, host, and network protocol vulnerabilities, when a UE is connected to the compromised eNB, the compromised eNB can disrupt the update of the NCC value, which results in the desynchronization of the target eNB. The desynchronization attack leads the target eNB to give up the forward key separation, and only able to perform the horizontal key derivation, in which a set of session keys can be linked to each other. To reduce the loss brought by the desynchronization attacks, root key update is an efficient way to prevent further session key exposure [21]. However, the frequent root key update involves the transmission of the UE's identity, and it introduces heavy traffic and computation load to the MME in the core network, especially in this MRN scenario with the involvement of tens of on-board UEs.

B. Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ be two multiplicative groups with the same prime order q. The bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$ has the following properties.

1) *Bilinearity:* $\forall g, h \in \mathbb{G}$, and $\forall a, b \in \mathbb{Z}^*_q$, we can derive the equation $e(g^a, h^b) = e(g, h)^{ab}$.
2) *Nondegeneracy:* There exists at least one g, where $g \in \mathbb{G}$ and one h, where $h \in \mathbb{G}$, which satisfies the condition that $e(g, h) \neq 1_{\mathbb{G}_{\mathbb{T}}}$.
3) *Computable:* $\forall g, h \in \mathbb{G}$, there is an efficient algorithm to compute $e(g, h)$.

In group $\mathbb{G}$, the computational Deffie-Hellman problem is computationally intractable, i.e., given (g, g^a, g^b) for $g \in \mathbb{G}$ and unknown $a, b \in \mathbb{Z}^*_q$, it is computationally infeasible to calculate g^{ab} in polynomial time [24]. While the decisional Diffie-Hellman problem is easy to solve, i.e., given (g, g^a, g^b, g^c) for $g \in \mathbb{G}$ and unknown $a, b, c \in \mathbb{Z}^*_q$, it is easy to determine whether $c = ab \bmod q$ by checking whether $e(g^a, g^b) \stackrel{?}{=} e(g^c, g)$.

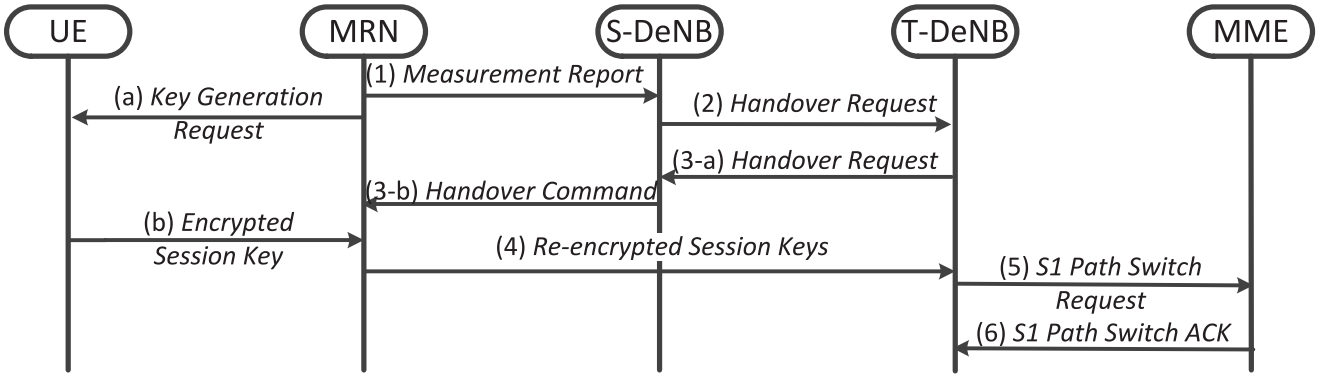

Fig. 3. Message flow in MRN scenario when UE handovers over from the source DeNB to the target DeNB.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ denotes a probabilistic algorithm that takes a parameter related to κ as the input, and gives a 5-tuple $(q, g, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e)$ as the output, where q is κ-bit prime, $\mathbb{G}$, and $\mathbb{G}_{\mathbb{T}}$ are two multiplicative groups with order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ is nondegenerated and computable bilinear map.

C. Proxy Re-Encryption

Proxy re-encryption technique is a cryptographic technique which allows a proxy to alter a ciphertext encrypted for one entity into a new ciphertext which can be decrypted by another entity. Assume *User B* encrypts a message with the public key of *User A*, and it can only be decrypted by the private key of *User A*. If *User A* permits *User C* to reveal the content of the message encrypted by the public key of *User A*, *User A* distributes the corresponding re-encryption key $rk_{A \rightarrow C}$ to the proxy. And the proxy transforms the ciphertext encrypted by the public key of *User A* into a new ciphertext which could be decrypted by the private key of *User C*. Meanwhile, the proxy server is not able to read or reveal the contents of the underlying messages [25].

IV. Proposed Handover Key Management Scheme

In this section, we introduce our proposed secure handover key management scheme in the MRN scenario, as shown in Fig. 3. The session keys are first generated and encrypted by the on-board UEs, and then delivered to the MRNs. The MRNs re-encrypt the received messages, so that the target DeNB can successfully decrypt the received messages to obtain the session keys.

A. System Initialization

Given the security parameter κ, the MME first generates the bilinear parameters $(q, g, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e)$ by running $\mathcal{G}en(\kappa)$, then chooses a symmetric encryption algorithm $\mathcal{E}nc()$ and two secure one-way Hash functions H_1 and H_2, where $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{G}$. In addition, the MME owns a private key x_M, and computes $y_M = g^{x_M}$ as its public key, the notations are shown in Table I. Finally, the MME keeps the private key x_M in confidential, and publishes the system parameter

TABLE I
Notations of Our Proposed Scheme

Notation	Definition
eNB_ID_j	Identifier of the target DeNB
$H_1(L_j)$	Location-based Generator of $DeNB_j$
x_j	Private Key of $DeNB_j$
y_j	Public Key of $DeNB_j$
x_M	Private Key of the MME
y_M	Public Key of the MME
$H_1(L_j)^{x_j/x_M}$	Re-encryption Key of $DeNB_j$
x_i	Private Key of UE_i
y_i	Public Key of UE_i
K_i^j	Session Key Shared between UE_i and $DeNB_j$

$\text{params} = (q, g, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, H_1, H_2, y_M, \mathcal{E}nc())$. For each on-board UE i, it owns a private key x_i, and the corresponding public key y_i, where $y_i = g^{x_i}$. The public key of a UE is stored in the MME during the registration phase, and it can be achieved by the DeNBs under the coverage of the MME.

For DeNB j, it also possesses a pair of private and public keys, which are denoted as $x_j \in \mathbb{Z}_q^*$ and $y_j = H_1(L_j)^{x_j}$. $L_j = (\text{TAC}||\text{eNB\_ID}_j)$ is a unique parameter which is a combination of the location information and its unique identity. The location of DeNB j is indicated by the tracking area code (TAC), which is a unique code that is assigned by the operator to each of its tracking area, including a group of neighboring DeNBs. The unique identity of the DeNB j (eNB_ID_j) is also assigned by the operator during the infrastructure deployment phase. When DeNB j registers itself to the MME, DeNB j delivers the public key $y_j = H_1(L_j)^{x_j}$ to the MME, and proves the authenticity of y_j using the following zero-knowledge proof process [26]. The MME first picks a random number r_z and a random message M_z to form the ciphertext $(a_j = H_1(L_j)^{r_z}, b_j = y_j^{r_z} M_z)$, and then delivers (a_j, b_j) to DeNB j. Then DeNB j decrypts the received ciphertext and replies the random message $M_z = b_j/(a_j)^{x_j}$ to the MME. Thus, the DeNB j can prove that it does deliver its public key to the MME and it does use the unique generator $H_1(L_j)$ in the public key y_j. After the validation of DeNB j, the MME generates a re-encryption key $H_1(L_j)^{x_j/x_M}$ and distributes it to DeNB j. Since the DeNB j periodically broadcasts the pilot signal containing the TAC and eNB_ID_j in its coverage area, the MRN can also produce the generator $H_1(L_j)$ of DeNB j.

Algorithm 1 Session Key Generation and Encryption

Data: A group of n on-board UEs obtain the location-based generator $H_1(L_j)$ of the target DeNB j from the MRN;
Compute:
for $i = 1 : n$ **do**
1. On-board UE i chooses a random number $r_i \in \mathbb{Z}_q^*$;
2. Then on-board UE i generates c_i^1 with public key of the MME y_M:
$c_i^1 = (y_M)^r = (g^{x_M})^r = (g^{r \cdot x_M})$;
3. On-board UE i generates c_i^2 with the session key K_i^j:
$c_i^2 = K_i^j \cdot e(H_1(L_j), g)^r$;
4. On-board UE i generates the signature s_i^j with the current time identifier *Timestamp* and its private key x_i:
$s_i^j = H_2(K_i^j || Timestamp)^{x_i}$
end for
Output: $C_i^j = (c_i^1, c_i^2, s_i^j),\ for\ i = 1, 2, \cdots, n$

Algorithm 2 Session Key Re-Encryption

Data: The MRN obtains the re-encryption key $H_1(L_j)^{x_j/x_M}$ from the target DeNB j;
Compute:
for $i = 1 : n$ **do**
The MRN derives $\hat{c}_i^1$ from c_i^1 and $H_1(L_j)^{x_j/x_M}$:
$\hat{c}_i^1 = e(c_i^1, H_1(L_j)^{x_j/x_M}) = e(g, H_1(L_j))^{r \cdot x_j}$;
Update $\hat{C}_i^j$:
$\hat{C}_i^j = (\hat{c}_i^1, c_i^2, s_i^j)$;
end for
Output: $\hat{C}_i^j,\ for\ i = 1, 2, \cdots, n$

B. Handover Key Management Scheme in MRN Scenario

The message flows between an on-board UE and the target DeNB with the involvement of the source DeNB and MRN in the secure handover key management process is depicted in Fig. 3.

Step 1: Before the handover process, the MRN conducts the communication channel measurement on behalf of the on-board UEs under its coverage area. After conducting the measurement process, the MRN generates and sends a channel measurement report to the source DeNB as a request for handover [*message* (1)].

Step 2: While at the same time, the MRN generates $H_1(L_j) = H_1(\text{TAC}\|\text{eNB\_ID}_j)$ and delivers $H_1(L_j)$ to the on-board UEs under its coverage. The MRN also acknowledges the on-board UEs to prepare for the generation of the session keys that will be utilized during the NH transmission [*message* (a)].

Step 3: According to the channel measurement report, the source DeNB determines whether the MRN representing the on-board UEs under its coverage begins to conduct the handover process or not. If the source DeNB decides to handover to the target DeNB, it initiates a handover request to the target DeNB with the public keys of the on-board UEs attached, which will be further utilized by the target DeNB for signature validation [*message* (2)].

Step 4: After receiving the handover request from the source DeNB, the target DeNB checks its current traffic load. If there is enough spare resource for the on-board UEs, the target DeNB accepts the handover request and replies its re-encryption key $H_1(L_j)^{x_j/x_M}$ back to the source DeNB [*message* (3)]. Then the source DeNB helps to deliver $H_1(L_j)^{x_j/x_M}$ to the MRN and send a handover command to the MRN [*message* (3)].

Step 5: After achieving [*message* (a)], on-board UE i randomly generates a session key, K_i^j, which later will be shared between on-board UE i and the target DeNB j. Then all the on-board UEs begin to compute their encrypted session keys and the corresponding signatures using Algorithm 1, where s_i^j is the signature of the session key K_i^j, aiming to validate the correctness and integrity of the session key sent to the target DeNB after the decryption process. Then the on-board UE transmits C_i^j to the MRN. Regardless of which DeNB it is connected to, all the on-board UEs utilize the universal public key of the MME y_M for the session key encryption instead of exploiting the public key of the target DeNB, which saves the computational and communication resource spent on update of the public key. Furthermore, the generation of c_i^1 and c_i^2 can be done offline in Algorithm 1, which can effectively reduce the computational delay.

Step 6: Since the session key K_i^j shared between the on-board UE i and the target DeNB j is encrypted by the public key of the MME y_M, without the private key x_M, the target DeNB cannot decrypt K_i^j directly. Even though the MRN is owned and deployed by the third party public transportation company, the ultimate goal of the deployment of the MRN is to provide high-quality wireless access services to the on-board UEs. Besides, the MRN possesses certain computational capability. Thus, the MRN has the motivation and ability to join in the key establishment process and functions as a proxy. In this situation, the MRN acts as a delegate to transfer the messages encrypted with the public key of MME into messages, that can be decrypted with the private key of the target DeNB without revealing the contents of the messages. During the re-encryption process, the MRN converts c_i^1 into $\hat{c}_i^1$ by performing Algorithm 2, then the converted message $\hat{C}_i^j = (\hat{c}_i^1, c_i^2, s_i^j)$ is delivered to the target DeNB, as shown in [*message* (4)].

Step 7: When the re-encrypted message $\hat{C}_i^j = (\hat{c}_i^1, c_i^2, s_i^j)$ arrives at the target DeNB, the target DeNB j first decrypts the session key generated by the on-board UE i with its own private key x_j, and validates the accuracy of the session key with the public key y_i of the on-board UE i, as shown in Algorithm 3.

Correctness: We first validate the correctness of the decryption process of K_i^j at the target DeNB j

$$\begin{aligned} K_i^j &= \frac{c_i^2}{\left(\hat{c}_i^1\right)^{x_j^{-1}}} \\ &= \frac{K_i^j \cdot e\left(H_1\left(L_j\right), g\right)^r}{\left(e\left(g, H_1\left(L_j\right)^{r \cdot x_j}\right)\right)^{x_j^{-1}}} \\ &= \frac{K_i^j \cdot e\left(g, H_1\left(L_j\right)\right)^r}{\left(e\left(g, H_1\left(L_j\right)\right)^{r \cdot x_j}\right)^{x_j^{-1}}} = \frac{K_i^j \cdot e\left(g, H_1\left(L_j\right)\right)^r}{e\left(g, H_1\left(L_j\right)\right)^r}. \end{aligned} \tag{4}$$

Then we check the correctness of the signature verification process by exploiting the following mathematical process:

$$e\left(s_i^j, g\right) \stackrel{?}{=} e\left(H_2\left(K_i^j || \text{Timestamp}\right), y_i\right). \tag{5}$$

Algorithm 3 Session Key Decryption and Signature Verification

Data: The DeNB j gets $\hat{C}_i^j, i \in \{1, 2, \cdots, n\}$;
Compute:
for $i = 1 : n$ **do**
1. The DeNB decrypts the session key K_i^j with x_j:
$K_i^j = \frac{c_i^2}{(\hat{c}_i^1)^{x_j^{-1}}} = \frac{K_i^j \cdot e(g, H_1(L_j))^r}{e(g, H_1(L_j))^r}$;
2. The DeNB conducts the following computation:
$e(H_2(K_i^j || Timestamp), y_i)$;
3. The DeNB checks whether:
$e(s_i^j, g) \stackrel{?}{=} e(H_2(K_i^j || Timestamp), y_i)$;
end for
Output: K_i^j, *for* $i = 1, 2, \cdots, n$

Step 8: After the signature verification, the symmetric session key K_i^j is successfully established between the target DeNB j and the on-board UE i, and it is used to protect the control-plane and data-plane transmission.

Thus, we can achieve the objective of the secure key establishment between the target DeNB and the on board UEs under the help of the MRN.

V. Security Analysis

In this section, detailed security analysis of the proposed handover key management scheme is given to demonstrate that it satisfies the requirements of the efficient secure session key establishment, backward and forward key separation, and collusion-resistance.

1) *The Proposed Handover Key Management Scheme Can Efficiently Achieve the Goal of Secure Session Key Establishment Between the On-board UEs and the Target DeNB:* When each on-board UE uses the public key y_M of the MME for the session key encryption, the ciphertext (c_i^1, c_i^2) for the session key K_i^j shared between the on-board UE i and the target DeNB j can only be decrypted by the MME with the private key x_M, which is

$$K_i^j = \frac{c_i^2}{e\left(c_i^1, H_1\left(L_j\right)\right)^{x_M^{-1}}} = \frac{K_i^j \cdot e\left(H_1\left(L_j\right), g\right)^r}{e\left(g^{r \cdot x_M}, H_1\left(L_j\right)\right)^{x_M^{-1}}}. \quad (6)$$

Therefore, no one else can obtain the session key K_i^j at this stage. As the MRN possesses computational capability and has the motivation to conduct the re-encryption, the MRN converts the messages encrypted by the public key y_M of the MME into messages which could be decrypted by the private key x_j of the target DeNB. After the re-encryption, only the target DeNB can decrypt the session key K_i^j with its private key x_j, as indicated in (4). To guarantee the correctness and integrity of the decrypted session key, a signature s_i^j is introduced to further prevent the MRN from distorting the session key. Thus, the goal of the secure session key establishment can be achieved.

2) *The Proposed Handover Key Management Mechanism Can Achieve the Backward and Forward Key Separation of the Session Keys During the Handover Process:* During each handover, the session key K_i^j shared between the target DeNB j and the on-board UE i is generated randomly by the on-board UE i, and transmitted to the target DeNB via the MRN without revealing the content of the session key. Since one session key is randomly generated and can only be utilized once, the compromise of one session key cannot further corrupt the other sessions keys shared between the on-board UE and the other DeNBs. Furthermore, during each session key establishment process, the corresponding re-encryption key $H_1(L_j)^{x_j/x_M}$ for the session key are distinctly different at different L_j, the forward and afterward DeNB cannot decrypt and obtain the session key. As a result, the backward and forward key separation can be achieved during the handover key management in the MRN scenario.

3) *The Proposed Handover Key Management Mechanism Can Resist the Collusion Attack Between the Corrupted DeNB and the MRN:* Suppose DeNB h is corrupted by an attacker and colludes with a malicious MRN, and the goal of collusion is intended to reveal the transmission content of DeNB j. In our scheme, if we do not introduce the location-based generator $H_1(L_j)$ in the re-encryption key, i.e., $H_1(L_j)^{x_j/x_M}$ becomes g^{x_j/x_M}, and c_i^2 will be computed as $c_i^2 = K_i^j \cdot e(g, g)^r$. Therefore, when DeNB h and the malicious MRN intend to reveal the session key K_i^j, the malicious MRN can transform c_i^1 with the re-encryption key g^{x_h/x_M} of DeNB h and obtain the following:

$$\hat{c}_i^{1h} = e\left(g^{x_M r}, g^{x_h/x_M}\right) = e(g, g)^{x_h r}. \quad (7)$$

Then, the session key can be gained by the DeNB h with its private key x_h

$$K_i^j = \frac{c_i^2}{\left(\hat{c}_i^{1h}\right)^{x_h^{-1}}} = \frac{K_i^j \cdot e(g, g)^r}{e(g, g)^r}. \quad (8)$$

Since our proposed scheme introduces $H_1(L_j)$ in the re-encryption key $H_1(L_j)^{x_j/x_M}$, obviously, the above collusion does not work. Therefore, the goal of the collusion attack resistance can be achieved.

VI. Performance Evaluation

In this section, we evaluate the performance of the proposed handover key management scheme in the MRN scenario, in terms of the computational delay of DeNB, MRN, and on-board UE, the communication overhead of the DeNB and on-board UE transmission, and the storage costs of DeNB, MRN, and on-board UE.

A. Computational Cost

T_{UE}, T_{MRN}, and T_{DeNB} denote the average computational cost of an on-board UE, an MRN, and a DeNB, respectively. The experimental environment is a desktop with dual-core 3.10 GHz processor and 8.00 GB installed memory, using the type A pairing in the Java Pairing-Based Cryptography Library [27]. We test the value of T_{UE}, T_{MRN}, and T_{DeNB} 1000 times, and their average values are reported as 13.3, 10.1, and 21.2 ms, respectively.

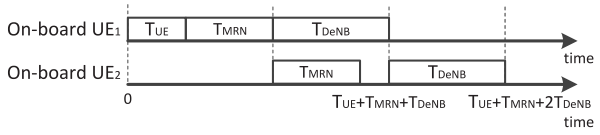

Fig. 4. Computational delay of DeNB, when $T_{\text{MRN}} \leq T_{\text{DeNB}}$.

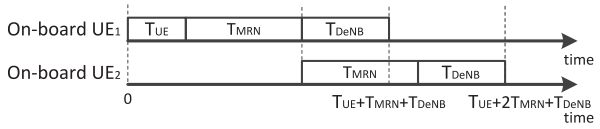

Fig. 5. Computational delay of DeNB, when $T_{\text{MRN}} > T_{\text{DeNB}}$.

Assume there are n on-board UEs and m MRNs installed on a public transportation, and we also assume that the MRNs and the target DeNB have the ability of conducting parallel computation, i.e., four calculations can be carried out simultaneously. Thus, there are $\lfloor (n/4m) \rfloor + 1$ on-board UEs allocated to each MRN.

As shown in Fig. 4, when $T_{\text{MRN}} \leq T_{\text{DeNB}}$, the bottleneck of the computational delay is T_{DeNB}, that is, the second on-board UE needs to wait a short time for the DeNB to conduct decryption and signature verification after the re-encryption of the MRN. In this case, the time consumption for the on-board UE with the maximum computational delay is

$$T_{\text{max-UE}} = T_{\text{UE}} + T_{\text{MRN}} + \left(\left\lfloor \frac{n}{4m} \right\rfloor + 1 \right) T_{\text{DeNB}}. \quad (9)$$

When $T_{\text{MRN}} > T_{\text{DeNB}}$, as shown in Fig. 5, the corresponding time consumption of the on-board UE with the maximum computational delay is denoted as

$$T_{\text{max-UE}} = T_{\text{UE}} + \left(\left\lfloor \frac{n}{4m} \right\rfloor + 1 \right) T_{\text{MRN}} + T_{\text{DeNB}}. \quad (10)$$

Under both cases, the time consumption of the on-board UEs with the minimum delay keeps the same, i.e., the computational delay of the first on-board UE, which is $T_{\text{min-UE}} = T_{\text{UE}} + T_{\text{MRN}} + T_{\text{DeNB}}$. In our proposed handover key management scheme, we use (9) to calculate the maximum delay of the on-board UEs, since $T_{\text{MRN}} \leq T_{\text{DeNB}}$. And the total time consumption of the target DeNB during the session key establishment process is $T_{\text{total-DeNB}} = mT_{\text{max-UE}}$. Since there are m MRNs installed on the public transportation, and the time consumption of the target DeNB with one MRN equals the maximum transmission delay of the on-board UE.

To validate the efficiency of the proposed group handover key management scheme, we compare the proposed scheme with the sequential handover scheme, that is, on-board UEs conduct the handover separately. The time consumption of each on-board UE without exploiting the group handover is $T_{\text{min-UE}}$, and the total time consumption of the target DeNB is $T'_{\text{total-DeNB}} = nT_{\text{min-UE}}$.

In Fig. 6, we compare the computational delay of the target DeNB with and without exploiting the group handover scheme with varying number of the on-board UEs, which is from 20 to 80. As shown in Fig. 6, with more on-board UEs, the computational delay of the target DeNB becomes longer, when the number of the MRN is set to be 1 and 2, respectively. As shown in Figs. 6 and 7, the computational delay of

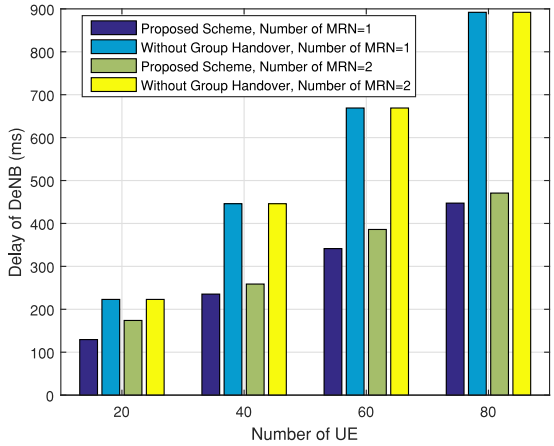

Fig. 6. Comparison of computational delay of DeNB with respect to the number of UE.

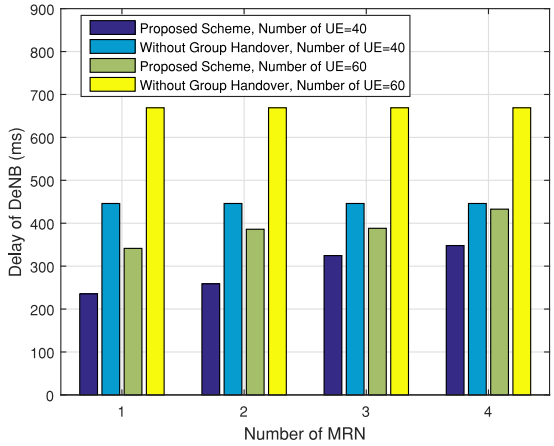

Fig. 7. Comparison of computational delay of DeNB with respect to the number of MRN.

the DeNB in our proposed group handover scheme is always shorter than that in the sequential handover scheme, which shows the efficiency of our proposed scheme in terms of the DeNB's computational delay.

Given the same parameter setup, we simulate and compare the computational delay of the target DeNB with and without exploiting the group handover scheme by choosing different number of MRNs, which ranges from 1 to 4. As shown in Fig. 7, the total computational delay of the target DeNB (with and without exploiting group signature) increases with respect to the increase of the number of MRNs, when the number of the on-board UEs are set to be 40 and 60, respectively. This is explained by the fact that for multiple MRNs, the computational delay of the on-board UE and the MRNs in $T_{\text{total-DeNB}}$ are calculated multiple times. In the sequential handover scheme, the computational delay of the target DeNB $T'_{\text{total-DeNB}}$ almost keep the uniform, this is explained by the fact that each on-board UE calculates the computational delay independently.

Since the proposed group handover key management scheme not only needs to consider the computational delay of the DeNB but also needs to evaluate the computational delay of the on-board UEs, which is related to the quality of service

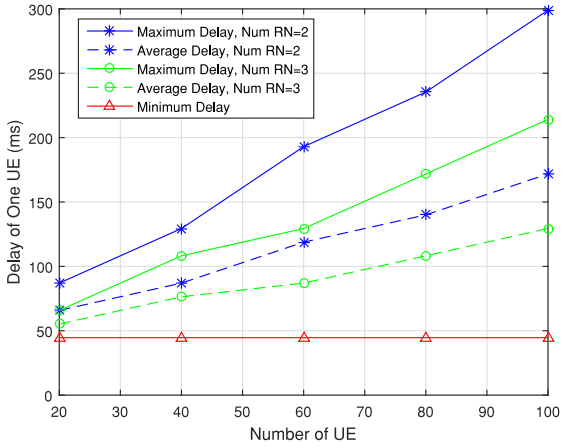

Fig. 8. Computational delay of UE with respect to the number of UE.

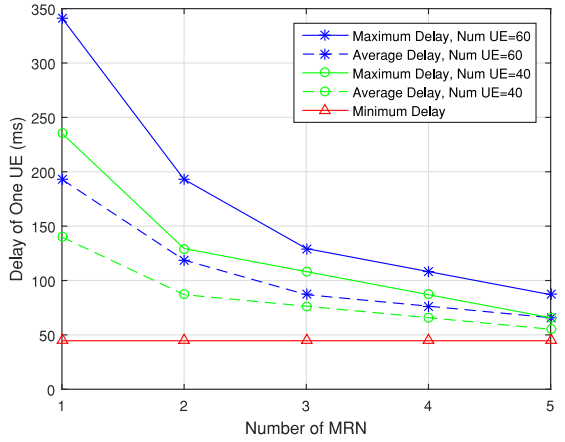

Fig. 9. Computational delay of UE with respect to the number of MRN.

of the on-board UEs. Thus we compare the maximum, average, and minimum computational delay of an on-board UE in the group handover scheme in Fig. 8, when the number of MRN is set to be 2 and 3. With the increase of the number of the on-board UEs, the maximum and average computational delay of the on-board UE increases. This is because with more on-board UEs, the maximum and average waiting time of the on-board UEs are longer.

The computational delay of the on-board UE is also related to the number of the MRN, so we compares the maximum, average, and minimum computational delay of the on-board UEs. We simulate the computational delay of the on-board UEs by choosing different number of MRN, which is from 1 to 5. As shown in Fig. 9, with more MRNs, the maximum and average computational delay of the on-board UE decrease. This is because the increase of the number of the on-board UEs lead to the decrease of the number of the on-board UEs attached to each MRN, the maximum and average waiting time of the on-board UE decrease.

As shown in Fig. 10, we show the maximum computational delay of UE with respect to the increase of number of MRN and UE. The maximum computational delay of UE increases with respect to the increase of the number of UE under the same number of MRN. While with the increase of the number

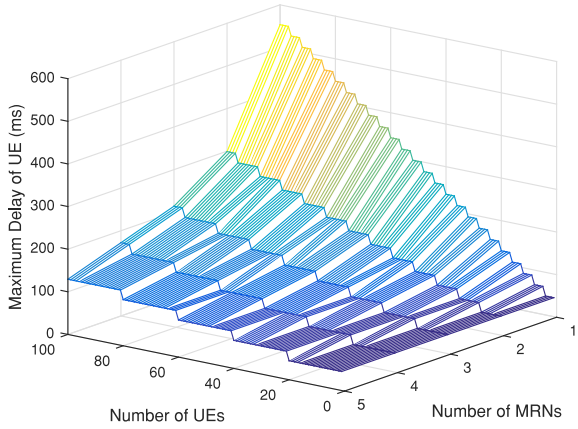

Fig. 10. Maximum computational delay of UE with respect to the number of MRN and UE.

of MRN, the maximum computational delay of UE decreases under the same number of UE.

B. Communication and Storage Overhead

In order to analyze the communication overhead, we assume that both the MRN and the DeNB successfully re-encrypts and decrypts the received messages. For each MRN, since the length of the generator $H_1(L)$ is 1024 bits, the total throughput caused by the location-based generator is calculated as $\text{Throughput}_{\text{LB}} = 1024 * m$ bits. For the on-board UEs under the coverage of one MRN, the introduced throughput is $\text{Throughput}_{\text{UE}} = 3 * 1024 * n$ bits. The overall throughput taking the 1024 bits re-encryption key transmission into consideration is $1024 + 1024 * m + 3072 * n * m$ bits.

We analyze the storage overhead of the handover key management scheme, from the perspective of the three involved entities. For the on-board UEs, the occupied storage space for the public key of the MME is 1024 bits. The storage space of the MRN for the re-encryption key is also 1024 bits. From the perspective of the DeNB, the storage space of the public keys belongs to the on-board UEs is $1024 * m * n$ bits.

VII. Related Works

This paper is related to the secure handover key management scheme via mobile relay in LTE-A networks. In this section, we discuss some related work on the concept and characteristics of mobile relay, and we also review the key management during handover in LTE-A networks.

A. Mobile Relay Networks

The study of the MRN has attracted great attention in LTE-A networks, and we make a brief review on some current directions of the MRN related to this paper [11], [14], [28]. One direction mainly concentrates on the comparison between architectures for the mobile relays. Chen *et al.* [11] investigated the network architecture of the mobile relays, that is, the packet data-gateway and the serving-gateway selection during mobile relay handover processes. The other direction is related to the mobility management scheme, that is, group handover [14], [28]. The group handover is investigated under

the scenario that when on-board UEs are traveling in a public transportation, they will be stay in close distance with each other and perform handovers simultaneously which may lead to the network congestion and blocked handover [29], [30]. The group handover strategy treats the on-broad UEs under the coverage of one MRN as a group, so that the signaling overhead and handover delay can be reduced and it can also decrease the rate of radio link failure. Chae *et al.* [31] proposed a novel eNodeB-to-eNodeB handover scheme for high speed moving vehicular femtocell networks, by utilizing an outside transceiver to perform handover, the connections between outside transceivers and eNodeBs are maintained seamlessly, and the outage probability is reduced compared to conventional handover scheme. However, very limited efforts have been made on the issues of security and key management scheme in mobile relay networks [32].

B. Handover Key Management

There have has been a few research works related to the key management strategies during the handover process in LTE-A networks [18], [19], [21], [33]. Han and Choi [21] identified the possible threats of desynchronization attacks during the handover key management, which may disrupt the forward key separation, and leaving the subsequent keys vulnerable to be compromised. Currently, the most effective way to avoid the desynchronization attack is using the root key update, i.e., the EPS-AKA [33]. The EPS-AKA process involves the mutual authentication between the UE and the core network, and the corresponding key derivation. However, this authentication method requires the transmission of the UE's identity, and the transmission of UE identities through the MRN brings potential threats to the on-board UEs. In this paper, we develop a novel secure key management scheme in mobile relay networks without the transmission of the identities, and it also does not bring computational load to the core network. To the best of our knowledge, this paper is the first key management scheme in mobile relay networks.

VIII. Conclusion

In this paper, we have proposed a secure handover key management scheme in the third-party owned MRN scenario, which mainly concentrates on establishing secure session keys between the on-board UEs and the target DeNB while exploiting the third-party owned MRNs during the key establishment without disclosing the content of the session keys. Detailed analysis shows that the proposed secure handover key management scheme can successfully establish the session keys, achieve the requirements of the backward and forward key separation, and resist the collusion attack. We also conducted the performance evaluation in terms of computational cost, communication overhead, and storage cost to demonstrate the effectiveness and efficiency of our proposed scheme, and the tradeoff between the number of MRNs and the computational latency was deliberately discussed. In our future work, we plan to carry on smart-phone-based and real public transportation scenario-based experiments to verify the effectiveness and efficiency of the proposed handover key management scheme.

References

[1] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach," *Int. J. Commun. Syst.*, vol. 25, no. 9, pp. 1189–1212, 2012.

[2] Z. Zhou, M. Dong, K. Ota, G. Wang, and L. T. Yang, "Energy-efficient resource allocation for D2D communications underlaying cloud-Ran-based LTE-A networks," *IEEE Internet Things J.*, vol. 3, no. 3, pp. 428–438, Jun. 2016.

[3] J. Wu, M. Dong, K. Ota, L. Liang, and Z. Zhou, "Securing distributed storage for social Internet of Things using regenerating code and Blom key agreement," *Peer-To-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1133–1142, 2015.

[4] L. Costantino, N. Buonaccorsi, C. Cicconetti, and R. Mambrini, "Performance analysis of an LTE gateway for the IoT," in *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, San Francisco, CA, USA, 2012, pp. 1–6.

[5] R. W. Heath, Jr., M. Honig, S. Nagata, S. Parkvall, and A. C. K. Soong, "LTE-advanced pro: Part 1," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 74–75, May 2016.

[6] Z. Zhou, M. Dong, K. Ota, and Z. Chang, "Energy-efficient context-aware matching for resource allocation in ultra-dense small cells," *IEEE Access*, vol. 3, pp. 1849–1860, 2015.

[7] M. Peng, Y. Li, Z. Zhao, and C. Wang, "System architecture and key technologies for 5G heterogeneous cloud radio access networks," *IEEE Netw.*, vol. 29, no. 2, pp. 6–14, Mar./Apr. 2015.

[8] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[10] "Technical specification group radio access network; mobile relay for evolved universal terrestrial radio access (E-UTRA)," Tech. Rep. 3GPP TR 36.836, Nov. 2012. [Online]. Available: http://www.3gpp.org/

[11] L. Chen *et al.*, "Mobile relay in LTE-advanced systems," *IEEE Commun. Mag.*, vol. 51, no. 11, pp. 144–151, Nov. 2013.

[12] J. Kokkoniemi *et al.*, "Performance evaluation of vehicular LTE mobile relay nodes," in *Proc. 24th IEEE Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, London, U.K., 2013, pp. 1972–1976.

[13] O. Altrad and S. Muhaidat, "Intra-frequency handover algorithm design in LTE networks using Doppler frequency estimation," in *Proc. Workshops Glob. Commun. Conf. (GLOBECOM)*, Anaheim, CA, USA, 2012, pp. 1172–1177.

[14] Y. Sui *et al.*, "Moving cells: A promising solution to boost performance for vehicular users," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 62–68, Jun. 2013.

[15] N. Lin, X. Huang, and X. Ma, "Analysis of the uplink capacity in the high-speed train wireless communication with full-duplex mobile relay," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, Nanjing, China, 2016, pp. 1–5.

[16] F. Y.-S. Lin, C.-H. Hsiao, K.-C. Chu, and Y.-H. Liu, "Minimum-cost QoS-constrained deployment and routing policies for wireless relay networks," *J. Appl. Math.*, vol. 2013, pp. 1–19, 2013.

[17] 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. (ICC)*, Sydney, NSW, Australia, 2014, pp. 1011–1016.

[18] G. M. Køien, "Mutual entity authentication for LTE," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Istanbul, Turkey, 2011, pp. 689–694.

[19] D. Forsberg, "LTE key management analysis with session keys context," *Comput. Commun.*, vol. 33, no. 16, pp. 1907–1915, 2010.

[20] "Technical specification group service and system aspects; 3GPP system architecture evolution (SAE)," Tech. Rep. 3GPP TS 33.401, Sep. 2012. [Online]. Available: http://www.3gpp.org/

[21] C.-K. Han and H.-K. Choi, "Security analysis of handover key management in 4G LTE/SAE networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457–468, Feb. 2014.

[22] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[23] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 12, no. 1, pp. 98–110, Jan./Feb. 2015.

[24] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.
[25] H. Lin, J. Shao, C. Zhang, and Y. Fang, "CAM: Cloud-assisted privacy preserving mobile health monitoring," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 985–997, Jun. 2013.
[26] M. Bauer, "Proofs of zero knowledge," *CoRR*, vol. cs.CR/0406058, 2004. [Online]. Available: https://arxiv.org/abs/cs/0406058
[27] A. D. Caro and V. Iovino, "jPBC: Java pairing based cryptography," in *Proc. 16th IEEE Symp. Comput. Commun. (ISCC)*, 2011, pp. 850–855.
[28] 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 Trans. Veh. Technol.*, vol. 64, no. 2, pp. 743–756, Feb. 2015.
[29] W. Lee and D.-H. Cho, "Enhanced group handover scheme in multiaccess networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 5, pp. 2389–2395, Jun. 2011.
[30] W. Lee and D.-H. Cho, "Group handover scheme using adjusted delay for multi-access networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Cape Town, South Africa, 2010, pp. 1–5.
[31] S. Chae, T. Nguyen, and Y. M. Jang, "A novel handover scheme in moving vehicular femtocell networks," in *Proc. 5th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Danang, Vietnam, 2013, pp. 144–148.
[32] R. Balakrishnan, X. Yang, M. Venkatachalam, and I. F. Akyildiz, "Mobile relay and group mobility for 4G WiMAX networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Cancún, Mexico, 2011, pp. 1224–1229.
[33] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, 2013.

Rongxing Lu (S'09–M'11–SM'15) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, in 2012.

He has been an Assistant Professor with the Faculty of Computer Science, University of New Brunswick, Fredericton, NB, Canada, since 2016. He was an Assistant Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2012 to 2016. He was a Post-Doctoral Fellow with the University of Waterloo, from 2012 to 2013. His current research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security and privacy. He has been published extensively in his areas of expertise with over 7500 Google Scholar citations.

Dr. Lu was a recipient of the most prestigious Governor Generals Gold Medal, the 8th IEEE Communications Society (ComSoc) Asia–Pacific Outstanding Young Researcher Award in 2013, the Student Best Paper Award (with his students and colleagues), ITS Summit Singapore 2015, the IEEE IES Student Best Paper Award 2014, and the Best Paper Awards of *TSINGHUA Science and Technology Journal* 2014, IEEE ICCC 2015, IEEE WCNC 2013, BodyNets 2010, and IEEE ICCCN 2009. He was/is on the Editorial Boards of several international referred journals, such as, the *IEEE Network*, and currently serves as the Technical Symposium Co-Chair for IEEE GLOBECOM16, and many Technical Program Committees of the IEEE and other international conferences, including IEEE INFOCOM and ICC. In addition, he is currently organizing a special issue on security and privacy issues in fog computing in *Elsevier Future Generation Computer Systems* and a special issue on big security challenges in big data era in the IEEE INTERNET OF THINGS JOURNAL. He currently serves as the Secretary of the IEEE ComSoc Communications and Information Security Technical Committee.

Shuo Chen received the M.E. degree from the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, in 2014.

He is currently a Research Associate with the School of Electrical and Electronic Engineering, Nanyang Technological University. His current research interests include network security and applied cryptography.

Qinglei Kong (S'15) received the B.Eng. degree in communication engineering from the Harbin Institute of Technology, Harbin, China, in 2012, the M.Eng. degree in electronic and information engineering from the Shenzhen Graduate School, Harbin Institute of Technology, Harbin, in 2015. She is currently pursuing the Ph.D. degree at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore.

Her current research interests include wireless communications, VANET, and game theory.

Hui Zhu (M'13) received the M.Sc. degree from Wuhan University, Wuhan, China, in 2005, and the Ph.D. degree from Xidian University, Xi'an, China, in 2009.

From 2010 to 2014, he was an Associate Professor with the School of Telecommunications Engineering, Xidian University, where he has been with the School of Cyber Engineering, as an Associate Professor, since 2015. His current research interests include applied cryptography and cyber security and privacy.