A Secure Relay-Assisted Handover Protocol for Proxy Mobile IPv6 in 3GPP LTE Systems

Yuh-Shyan Chen, Tong-Ying Juang & Yao-Tsu Lin

Wireless Personal Communications
An International Journal

ISSN 0929-6212
Volume 61
Number 4

Wireless Pers Commun (2011)
61:629-656
DOI 10.1007/s11277-011-0424-2

Springer

Wireless Pers Commun (2011) 61:629–656
DOI 10.1007/s11277-011-0424-2

A Secure Relay-Assisted Handover Protocol for Proxy Mobile IPv6 in 3GPP LTE Systems

Yuh-Shyan Chen · Tong-Ying Juang · Yao-Tsu Lin

Published online: 26 October 2011

Abstract The LTE (Long Term Evolution) technologies defined by 3GPP is the last step toward the 4th generation (4G) of radio technologies designed to increase the capacity and speed of mobile telephone networks. Mobility management for supporting seamless handover is the key issue for the next generation wireless communication networks. The evolved packet core (EPC) standard adopts the proxy mobile IPv6 protocol (PMIPv6) to provide the mobility mechanisms. However, the PMIPv6 still suffers the high handoff delay and the large packet lost. Our protocol provides a new secure handover protocol to reduce handoff delay and packet lost with the assistance of relay nodes over LTE networks. In this paper, we consider the security issue when selecting relay nodes during the handoff procedure. During the relay node discovery, we extend the access network discovery and selection function (ANDSF) in 3GPP specifications to help mobile station or UE to obtain the information of relay nodes. With the aid of the relay nodes, the mobile station or UE performs the pre-handover procedure, including the security operation and the proxy binding update to significantly reduce the handover latency and packet loss. The simulation results illustrate that our proposed protocol actually achieves the performance improvements in the handoff delay time and the packet loss rate.

Keywords LTE · Mobility · Handover · Relay-assisted · Security

Contract/grant sponsor: National Science Council of the Republic of China; contract/grant number: NSC-97-2221-E-305-003-MY3 and NSC-98-2219-E-305-001.

Y.-S. Chen (✉) · T.-Y. Juang
Department of Computer Science and Information Engineering,
National Taipei University, San-Shia, Taipei 237, Taiwan, R.O.C.
e-mail: yschen@mail.ntpu.edu.tw

T.-Y. Juang
e-mail: juang@gm.ntpu.edu.tw

Y.-T. Lin
Graduate Institute of Communications Engineering, National Taipei University,
San-Shia, Taipei 237, Taiwan, R.O.C.
e-mail: YaoTsu.Lin@gmail.com

1 Introduction

With the rapid growth of personal mobile communications, a mobile device with the user equipment (UE) connected to the Internet for IP-based multimedia service is significantly increased. The LTE (Long Term Evolution) technologies defined by 3GPP is the last step toward the 4th generation (4G) of radio technologies designed to increase the capacity and speed of mobile telephone networks. The core network (CN) part of the evolution of the LTE system is classified into the system architecture evolution (SAE) and the radio access network (RAN). The main objective of RAN part is to increase the system capacity, the transmission coverage, the throughput, and reduce the handoff latency. The LTE system is the IP based architecture, in which all radio control functions, such as handover control and admission control, are enforcement in eNB. LTE system not need the central control entity. User plane follows the same radio link standards, such as RLC/MAC in eNB.

When a mobile user is roaming between different base stations, called as eNodeB (eNB), of LTE networks, UE needs to perform the handover protocol to keep the data connections. Traditional handover protocol suffers from high handover latency and large packet loss. Our main objective is to develop a new handoff protocol to reduce the handover latency and improve the packet loss rate.

Figure 1 illustrates the 3GPP long term evolution (LTE) architecture, which is defined by 3GPP [1]. The LTE is all-IP network architecture to provide higher bit rate, lower transmission latency, and wider service coverage. The 3GPP LTE becomes a major competitive 3GPP connection technology to deal with the rapid development of IP data traffic. When the UMTS system currently builds in the world, the system performance and cost optimization must take into account two issues [2]. The first issue is to upgrade the existing UMTS performance; for instance, HSDPA standard in 3GPP Release 5 and HSUPA standard in 3GPP Release 6. However, the maximum data rate is 14.4 Mbps in downlink and 5.76 Mbps in uplink. Second issue is to develop the evolved radio interfaces, 3GPP defined evolved UTRA and E-UTRAN, which are packet based network architecture. The main objective of LTE is to achieve 100 Mbps in downlink and 50 Mbps in uplink. The evolution of LTE system is the core network (CN) part. The CN is generally classified into the system architecture evolution (SAE) and the radio access network (RAN). The most important of RAN is the increased capacity, the better coverage, the high throughput, and the reduced latency. The

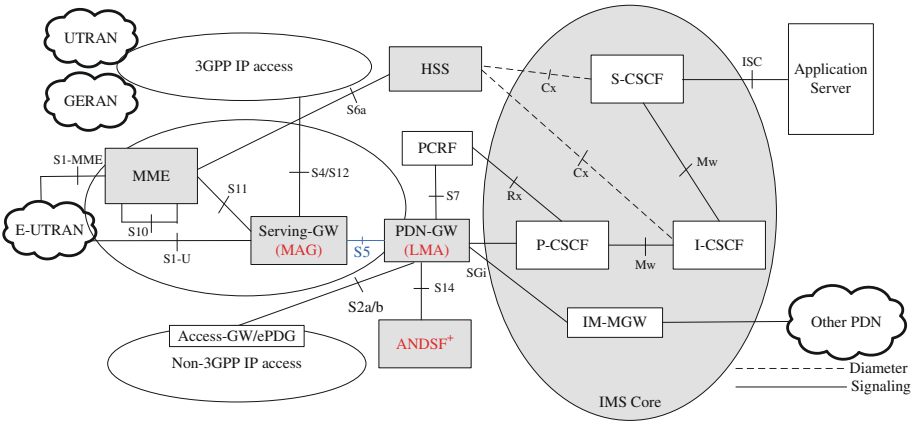

Fig. 1 The LTE architecture

Table 1 The comparison of existing results with our approach

Schemes	P_HMIPv6 in 802.11 [7]	P_HMIPv6 in 802.16e [8]	RN_PMIPv6
Network model	IEEE 802.11 system	IEEE 802.16e system	3GPP LTE system
Mobility protocol	Hierarchical mobile IPv6	Hierarchical mobile IPv6	Proxy mobile IPv6
Mobility management	Client-based	Client-based	Network-based
Pre-handover process	DAD	DAD	Security and PBU
Security	No	No	Yes

LTE has been introduced IP based architecture, all radio control functions, such as handover control and admission control, etc., are enforced in eNB.

The main demand of the Evolved Packet Core (EPC) is to provide the IP-layer seamless mobility, when a UE moves between different eNBs. In the EPC standard, proxy mobile IPv6 based on the network-based mobility mechanism is used to provide mobility issue. Two methods are defined in LTE EPC standard, known as network-based mobility protocol, proxy mobile IPv6 (PMIPv6) [3], and client-based mobility protocol, dual-stack mobile IPv6 (DSMIPv6) [4] and mobile IPv4 (MIPv4) [5]. Therefore, this paper focus on discussed how to improve the PMIPv6 handover in the LTE system. A network-based management protocol, called PMIPv6, is network-based localized mobility management (NetLMM) from the IETF working group. Unlike MIPv6, PMIPv6 allows controlling the network-based mobility management on the behalf of MN. Therefore, PMIPv6 can remove some MN-related signalings. However, network-based mobility management, such as PMIPv6, still suffers from the high packet loss and handover latency.

In this paper, we propose a secure relay-assisted handover, called RN_PMIPv6, protocol for proxy MIPv6 in 3GPP LTE networks. The proxy MIPv6 protocol [6] still suffers from the high handoff delay and the large packet lost. Our protocol provides a new protocol to reduce handoff delay and packet lost with the assistance of relay nodes over LTE networks. The basic idea of the relay node performing the pre-handover procedure is already developed in [7,8] for IEEE 802.11 networks and IEEE 802.16e systems, respectively. The design differences of these protocols are given in Table 1. Unfortunately, none of them have considered the security issue. In this paper, we specifically consider the security issue when selecting relay nodes during handoff. During the relay node discovery, we extend the access network discovery and selection function (ANDSF) in 3GPP specifications to help mobile station or UE to obtain the information of relay nodes. With the aid of the relay nodes, the mobile station or UE performs the pre-handover procedure, including the security operation and the proxy binding update to significantly reduce the handover latency and packet loss. The simulation results illustrate that our proposed protocol actually achieves the performance improvements in the handoff delay time and the packet loss rate.

The rest of this paper is organized as follows. Section 2 describes related works. Section 3 describes the system architecture and basic idea. The proposed protocol is presented in Sect. 4. Performance evaluation is discussed in Sect. 5. Section 6 finally gives a conclusion.

2 Related Works

This section first introduces IPv6-based mobility protocols, including MIPv6, PMIPv6, and SPMIPv6 protocols. The PMIPv6 protocol in LTE system is then described in Sect. 2.2.

2.1 IPv6-based Mobility Protocol

Mobility management is the most important mechanism in the IP-based next generation network environment. The MIPv6 [9] protocol necessary to exchange signaling messages between a UE and the home agent (HA), in order to maintain correspondence between the permanent IP address and temporary IP address. The client functionality of mobility support must be provided to the UE in MIPv6 protocol. However, some results discuss how to improve MIPv6-based handover scheme [10]. The recent advances in network-based localized mobility management (NetLMM) have facilitated the realization of All-IP based wireless networks. In addition, Proxy mobile IPv6 (PMIPv6) [11,12] is a solution to support the NetLMM, the network is utilized to perform the location update signalings.

The MIPv6 protocol [10] allows UE to maintain the communications from a corresponding node (CN) to the UE. Each UE used the home address (HoA) to identify its location. When the connection to the external network, UE may receive the router advertisement to obtain external network prefix and automatically configurations a care-of address (CoA). After CoA configured, UE then performs the DAD procedure to ensure the unique of the CoA. If CoA is available, the UE sends the location information to the CN and HA for the location binding, and then packet tunnels to the new location.

The PMIPv6 protocol [11,12] allows a UE to maintain the original IP address, which means the new network has partially extracted by the address prefix. The UE does not be required to perform the IP address configuration if the network connection changes. The PMIPv6 protocol defined the local mobility anchor (LMA) and the mobile access gateway (MAG) [6]. All PMIPv6 domains of the mobility management functions are used by LMAs and MAGs. When a UE moves and connect to the new MAG, the MAG must detect the connection and initiates the required authentication and authorization procedures to connect with the network for the IP session for UE. The local mobility anchor (LMA) is similar to the home agent. The LMA is the topological anchor point, keeps the current UE location binding information. The mobile access gateway (MAG) acts as a proxy agent and controls the mobility signalings to LMA. MIPv6 protocol has ability to control the IP handover between different based stations, large handover latency makes MIPv6 protocol cannot be fully used in the real-time services; such as voice over IP (VoIP) application. The PMIPv6 protocol uses the network-based mobility management actually reduces the signaling overhead, PMIPv6 protocol still suffers the high handover latency and packet loss.

Lee et al. [12] proposed a fast handover for proxy mobile IPv6 based on 802.11 networks. This scheme uses the conversion scheme by the context information from the previous MAG to the new MAG by IAPP (Inter-Access Point Protocol) (authentication information, profile information of UE). With the advanced conversion of the context information, this scheme can reduce the handoff delay.

Kang et al. [11] proposed a seamless handover scheme for proxy mobile IPv6, illustrated in Fig. 2. This scheme uses the neighbor discovery (ND) messages in IPv6 to reduce the handover latency. The ND message sends the MN-profile to neighboring MAGs before the handover operation. This scheme can eliminate the MAGs obtained from policy store (PS) of the MN-profile procedure when the UE needs handover. To prevent on-the-fly packet loss, this caused by the routing between previous LMA and MAG. A packet buffering is needed on the MAG and LMA to solve the problem of packet loss.

Chen et al. [7,8] recently proposed a cross-layer partner-assisted handover mechanism based on HMIPv6, termed as P-HMIPv6 protocol. P-HMIPv6 protocol is a cross-layer, layer 2 + layer3, solution as show in Fig. 3. The basic idea of the partner node (PN) is to perform the pre-handoff procedure based on [7]. The UE can detect in advance the existence of the nearby

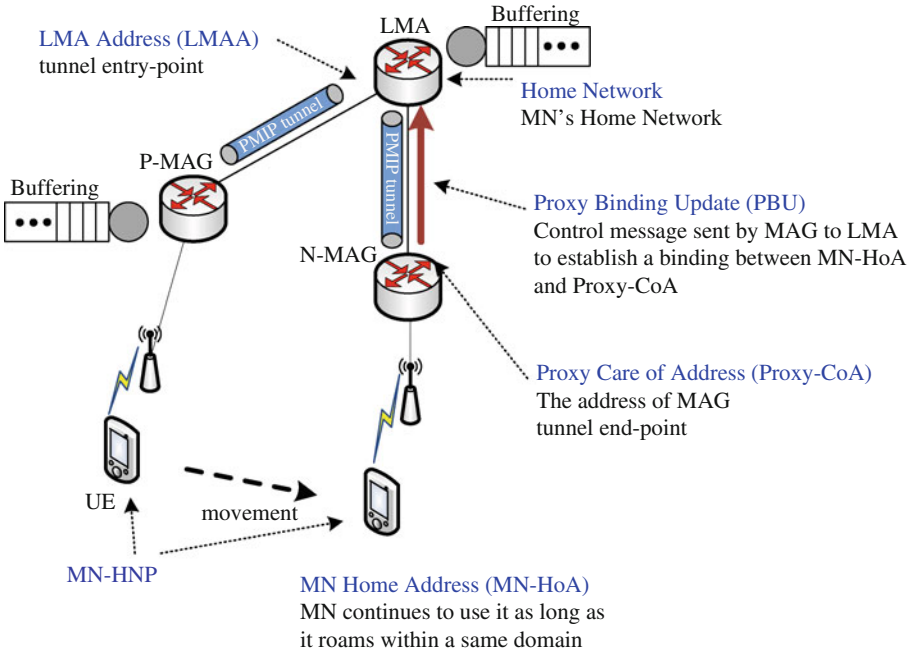

Fig. 2 Seamless proxy mobile IPv6

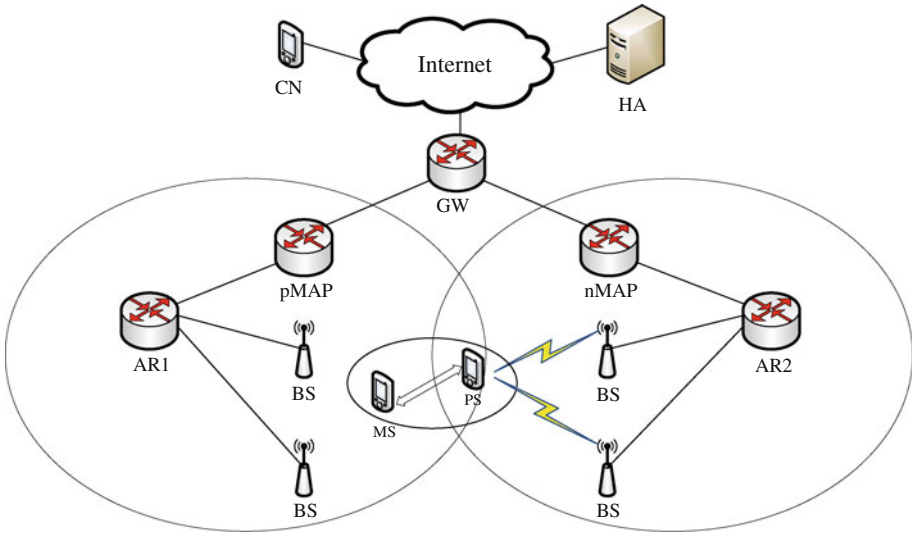

Fig. 3 Partner-assisted mechanism based on HMIPv6

base station, and the layer 2 handover operation tries to invite a number of PNs. Selected PN then pre-perform the duplicate address detection (DAD) procedure of new care-of-address of UE, when the UE is in movement. P-HMIPv6 protocol significantly reduces the handover latency and packet loss.

2.2 Proxy Mobile IPv6 Protocol in LTE System

The 3GPP LTE standard may adopt the network-based and client-based mobility protocols. Example of the network-based and client-based mobility protocols are proxy mobile IPv6 (PMIPv6) and MIPv6 protocols, respectively.

In the network-based mobility management, network detects whether a UE has moved to another point of attachment, and provides the same IP address of the previously point of attachment to the UE. Network components provide IP addresses to the UE, and control the mobility anchor updating. Thus, these packets can successfully reach the new point of attachment. In the client-based mobility management, a UE obtains a new local IP address or care-of-address if the UE moves to a new point of attachment. Then, the UE updates the address information to the home agent. Home agent maintains a binding between the care-of-address and the home address of UE.

The LTE system introduces two functionality entities for supporting the PMIPv6 protocol, there are PDN gateway (P-GW) and Serving Gateway (S-GW). First, the PDN gateway (P-GW) provides the access in different packet data networks (PDN). Through the address space of the PDN, P-GW gives a UE an IP address, which is IPv4 address or IPv6 prefix. The P-GW is a mobility anchor point. The main role of P-GW is the management of IP address and prefix of UE, and also is a role of PMIPv6 LMA. Second, S-GW includes the MAG functionality of PMIPv6 which is used for the IP mobility management. The S-GW is also a role of layer 2 mobility anchor. The main function is to detect and control procedures if a UE moves into the 3GPP access network. The 3GPP standard Release 8 [13] describes the attachment of UE to EPC. The function of MAG is sending a proxy binding update (PBU) to the LMA. Thus, the P-GW uses tunnel technique for the downlink packets of UE to avoid the problem of packet loss. The P-GW provides an IP address/prefixes in the proxy binding agent (PBA) to the UE. The P-GW uses Generic Routing Encapsulation (GRE) key, and the S-GW also uses tunnel technique for the uplink packets of UE.

Traditional client-based mobility protocol suffers the high signaling overhead. Although, the network-based mobility protocol improves problem of the heavy signaling overhead. The network-based mobility protocol, PMIPv6, still suffers the high handover latency and packet loss. Efforts made in this work is to develop a secure relay-assisted handover protocol for PMIPv6 in 3GPP LTE Systems to significantly improve the handover latency and packet loss. One main contribution of this work is to develop a new relay-assisted handover protocol with consideration of the security for PMIPv6 in 3GPP LTE systems.

3 Preliminary

This section initially describes the handover procedure defined in 3GPP LTE [14]. The system architecture and the challenge are then explained. The basic idea is finally introduced.

3.1 Mobility in 3GPP LTE System

The mobility management of the 3GPP LTE standard has been defined in [14]. The control plane handling during the E-UTRAN mobility activity for UEs is done by the handover preparation signaling which is a part of the handover command to the target eNB, as follows.

The preparation work of handover is that source eNB sends all necessary information; for instance, RRC (radio resource control context information; to the target eNB. Source eNB and UE retain some context; for instance, C-RNTI (cell radio network temporary identifier) information. The UE connects to target cell by the random access channel (RACH) by a ded-

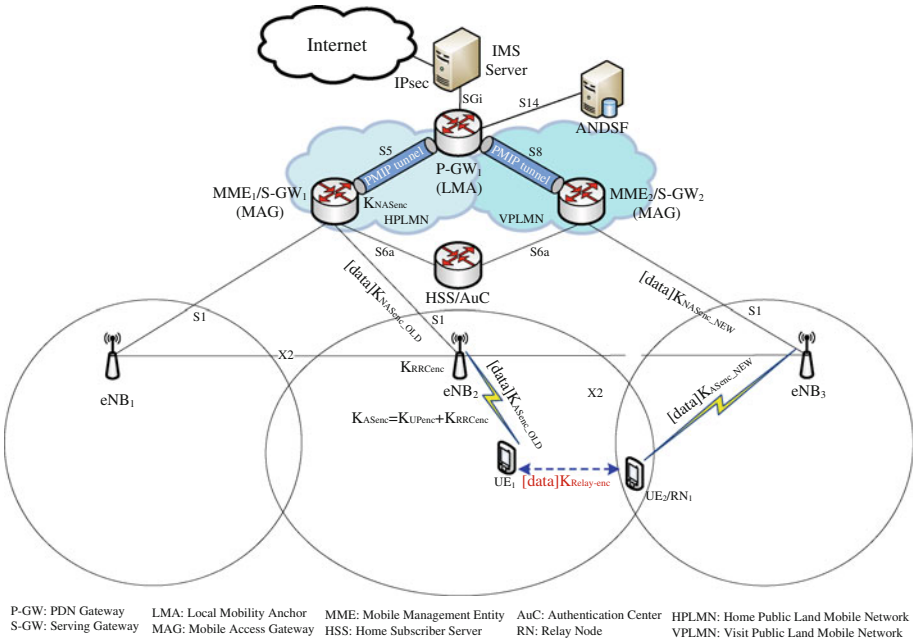

Fig. 4 System architecture

icated contention-free procedure using the RACH preamble or dedicated contention-based procedure if RACH preamble cannot be used. The UE uses the dedicate RACH preamble until the handover procedure is initiated. If the target cell in the RACH procedure is not successful, the UE begins to select the best cell from the radio link recovery. In the handover procedure, the header compression (ROHC) context exchange is not robust. It is noted that handover procedure not negotiate with EPC, and the preparation messages directly exchanged between eNBs.

The user plane handling during the E-UTRAN mobility activity for UEs is to avoid the data loss during handover. When the handover preparation is done, the user plane tunnel is built between the source eNB and the target eNB. The establishment of tunnels is used to transmit uplink and downlink data. When the handover execution, user data is re-forward from the source eNB to the target eNB. When the handover completion, the target eNB sends and informs to the MME a path switch message to perform the path switch. The MME sends a user plane update request message to the serving gateway, thus the path of user-plane from the serving gateway is switched to the target eNB.

3.2 System Architecture

The system architecture of our scheme is illustrated in Fig. 4, where is the 3GPP LTE system environment. In this study, network-based mobility protocol, proxy mobile IPv6, is considered as the mobility management in the 3GPP LTE systems. A little portion of the components of LTE system needs to increase its functionality. When a UE with the weak signal strength received from the serving eNB to enable the handover procedure, but still not reach to the coverage of neighbor eNB. The UE tries to find out some UEs located at the coverage of neighbor eNB. Such UEs is called as relay node (RN). The functionality of the RN is to help the UE to perform the pre-handoff procedure and to reduce the handoff latency. The formal definition of RN is given.

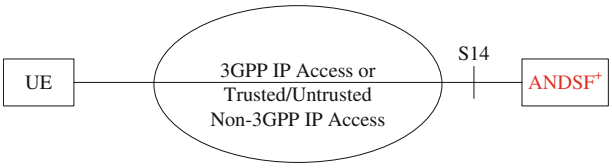

Fig. 5 Access network discovery and selection function^{+}

Definition 1 (*Relay Node (RN)*) Given a UE located at serving eNB, all possible neighbor UEs of the UE located at the coverage of neighboring eNB are called as relay nodes or RNs of the UE, where the UE can directly communicate with all relay nodes (RNs). The main function of the RN is to assist the UE to pre-perform the partial handover procedures which is defined in the 3GPP LTE Intra E-UTRAN mobility.

If a UE needs the assistance from a RN, the first task for the US is to search for useful RNs. This task is called as the RN discovery. The main goal of the RN discovery is to find the best RN for the UE. The 3GPP LTE specifications introduces the access network discovery and selection function (ANDSF) [15], illustrated in Fig. 5. The main function of ANDSF is to search for the suitable neighbor access networks. Our RN discovery is utilized the ANDSF and add additional information table in the ANDSF to be ANDSF^{+}. The formal definition of ANDSF^{+} is given as follow.

Definition 2 (*ANDSF*$^{+}$) Given an access network discovery and selection function (ANDSF) [15]. The ANDSF^{+} is an ANDSF and appended additional information table into the ANDSF. The main function of ANDSF^{+} is used for a UE to execute the relay node discovery.

A UE who wants to become a RN needs to satisfy the following conditions:

- The RSSI of the eNB downlink to the UE must less than $\mathrm{RSSI}_{threshold}$ to ensure that the UE is nearly in boundary of the neighbor eNB's coverage.
- The UE is stable.
- The UE belongs to different eNBs.
- The UE supports the ad hoc communication capability.
- The UE provides the location information.

A RN is near to the edge of the coverage of serving eNB, because the major function of RN is viewed as an extension coverage to the next eNB to assist the UE to pre-perform the handover procedure. The second condition is that the RN must be stable, not moving rapidly. This ensures the selected RN can be stable for a long period of time. The third condition is that the RN is belong to the different eNB domain. The last one is that the RNs must support the ad hoc communication with the UE. In addition, Fig. 6 also gives the protocol stack. This figure shows that our protocol stack is modified from the 3GPP LTE specifications. Ad hoc communication interface between the UE and RN is also illustrated in the protocol stack.

3.3 Motivation and Basic Idea

This work mainly improves the results from [7,8]. There are partner-based handoff protocols in IEEE 802.11 [7] and IEEE 802.16 [8], respectively. In [7], Chen *et al*. proposed a cross-layer partner-based fast handoff mechanism for IEEE 802.11 wireless networks. In [8], Chen *et al*. proposed a cross-layer partner-assisted handoff scheme for hierarchical mobile

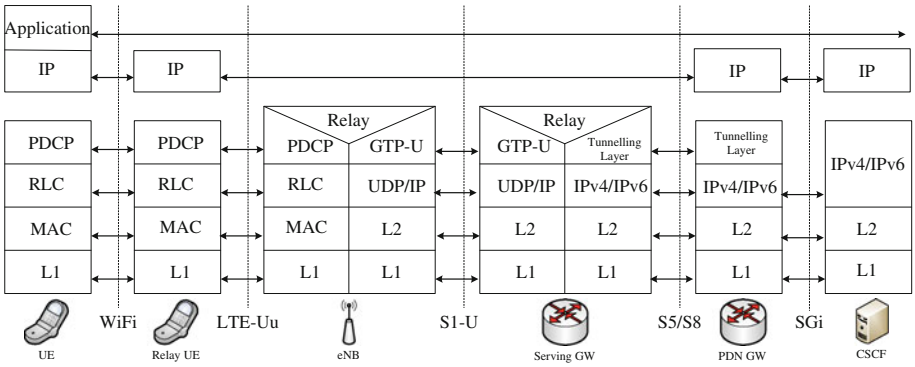

Fig. 6 The LTE protocol stack

IPv6 in IEEE 802.16e systems. Unfortunately, these two partner-based handoff protocols do not consider the security issue. Therefore, it is not guarantee the reliable and safety data transmission if the protocol design not further consider the security issue. This is because that the data transmission is done through possible non-reliable and no-safety relay nodes. The main motivation of this work is to consider the security issue to develop a secure realy-assisted handoff protocol. Two contributions of this work is developed; (1) one is to develop a new network-based mobility protocol with the assistance of relay node in LTE systems, (2) another one is that a security scheme is investigated for the communication between UE and RN. Figure 7 gives the LTE key hierarchy. In this work, Because of add RN in this protocol, we modified specifications to enhance the secure communication between UE and RN. The usage of RN is execute the partial handover procedures for UE before the UE entering the coverage of the target eNB. This idea mainly comes from result from [7,8]. The comparison of existing results with our new approach is given in Table 1.

The basic idea is stated as follows. The goal of RN is to assist UE to pre-execute partial handover procedures before the UE entering the target eNB coverage of a new public land mobile network (PLMN) domain. In the 3GPP LTE standard [16], UE handover procedures is divided into two modes; there are X2-based (intra-domain handover) and S1-based (inter-domain handover) handover procedures. The standard handover process is divided into three phases; (1) handover preparation, (2) handover execution, and (3) handover completion. Initially, the handover execution phase contains some important security operations. The security operation includes that a target eNB not only performs the encryption and decryption algorithms, but also check the new authentication key. The security operation is to ensure the safely handover procedure to the target eNB. The handover completion phase performs the operations of proxy binding update (PBU) and proxy binding acknowledgement (PBA). The PMIPv6 tunnel between eNB and serving gateway (S-GW) achieves the network-based mobility. The handover latency and packet loss caused during the handover procedure. Efforts will be made to develop a security RN-based procedure of the PMIPv6 binding procedure.

4 Secure Relay-assisted Handover Protocol for PMIPv6

The secure relay-assisted handover protocol for PMIPv6 in 3GPP LTE systems is split into *relay node discovery* phase, *secure communication* phase, *secure relay-assisted handover* phase, as follows.

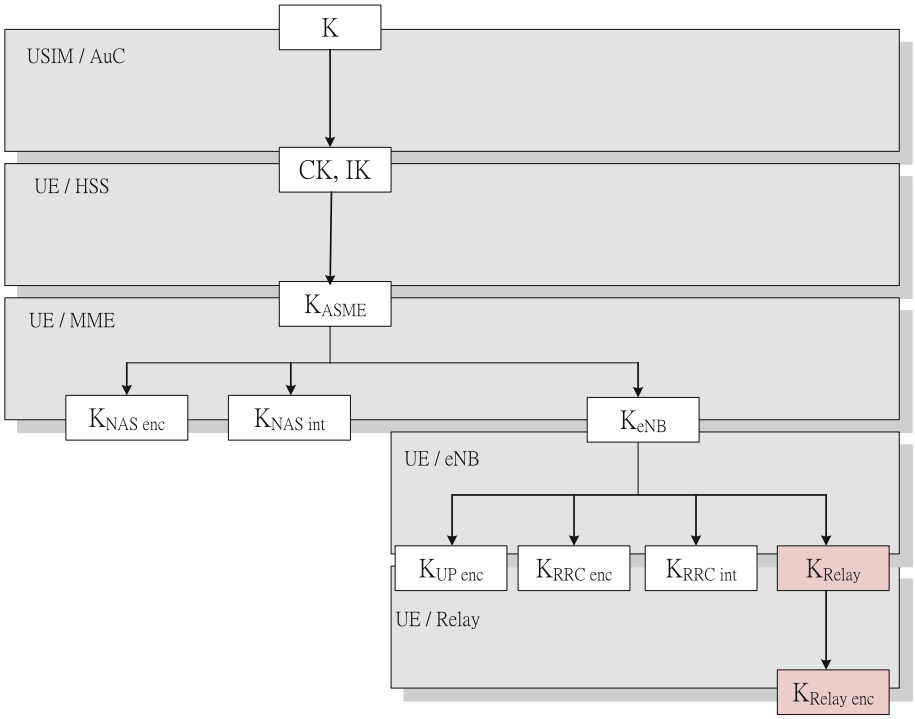

Fig. 7 The LTE key hierarchy

- *Relay node discovery* phase is to discover RNs by the UE. Because of the RN coverage extension of the neighbor eNBs, the UE detects and identifies the existence of all possible RNs located at neighbor eNBs before entering the transmission range of next eNB by negotiating with ANDSF^{+}. With the assistance of the RN, the UE pre-perform partial layer 3 handoff procedures before the UE entering into the transmission range of target eNB.
- *Secure handover* phase establishes a security mechanism to provide the secure communication between UE and RN during the handover.
- *Secure relay-assisted handover* phase provides a complete relay-assisted handover protocol with security for PMIPv6.

To explain the secure operation of the relay-assisted handover protocol, let $X \overset{action}{\Longrightarrow} Y$ denote that X executes a *communication action* to Y, where X and $Y = \{$UE, RN, ANDSF, CN, source eNB, source MME, target eNB, target MME$\}$ and *communication action* $= \{$forward, register, negotiation, request, response$\}$. The detailed operations are described as follows.

4.1 Relay Node Discovery Phase

The main task of this phase is to discover the relay node when UE needs to handover to the target eNB. A relay discovery scenario is given in Fig. 8. The operation of relay node discovery is given.

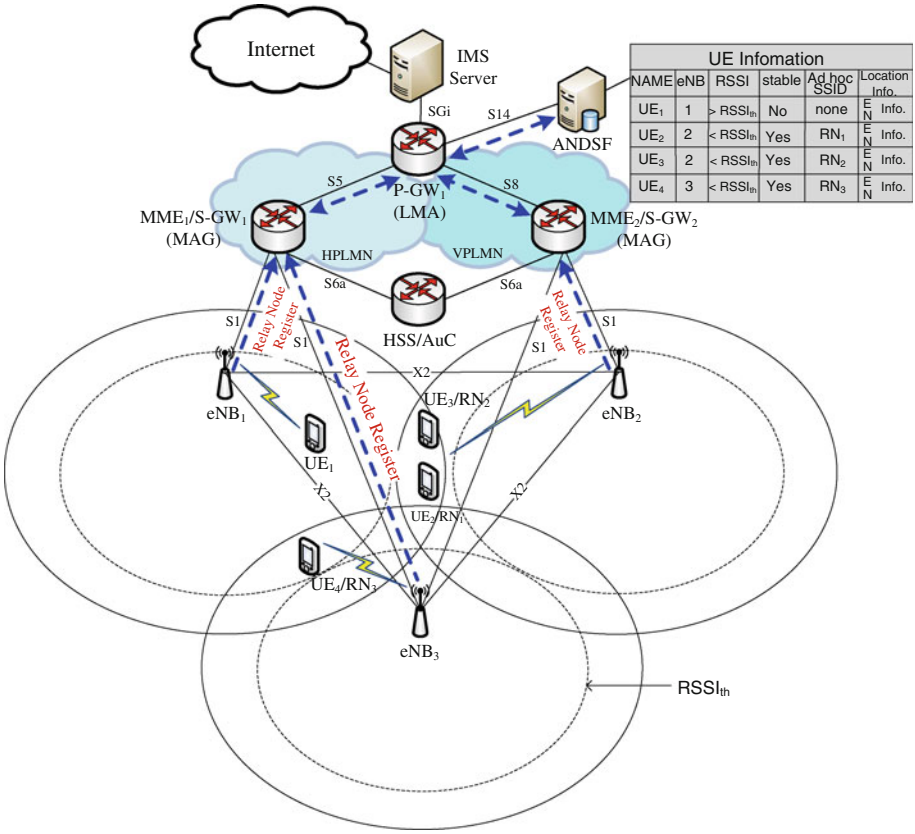

Fig. 8 The relay node registers to ANDSF$^+$

S1: $UE \overset{register}{\Longrightarrow} ANDSF^+$: Before the UE inquiring the RN information from ANDSF$^+$, each UE registers its information to ANDSF$^+$. These information includes UE name, eNB information, RSSI strength, mobility information, ad hoc or infrastructure modes, and the location information. These information stores in the table of the ANDSF$^+$ database, as illustrated in Fig. 8.

S2: $UE \overset{query}{\Longrightarrow}$ ANDSF$^+$: The UE inquiries the RN information from ANDSF$^+$. The UE sends a request message to ANDSF$^+$. When the UE not reach to coverage of all possible target eNB. Observe that, now UE still not determine the final target eNB. Logically, the usage of RN is to extend to the coverage area of target eNB, as illustrated in Fig. 9. The UE sends a request to ANDSF$^+$, and received RN information from ANDSF$^+$. By the location information of RNs, the UE discovers the closest RN as the candidate of RN.

S3: $UE \overset{negotiation}{\Longrightarrow} RN$: When the UE obtained the candidate of RN, the UE has to decide target eNB. After determining the final target eNB, the UE selects one best RN from many RN candidates, by the signal strength, in the final target eNB domain. Then, the authentication mechanism is performed to improve the security of the UE-to-RN connection.

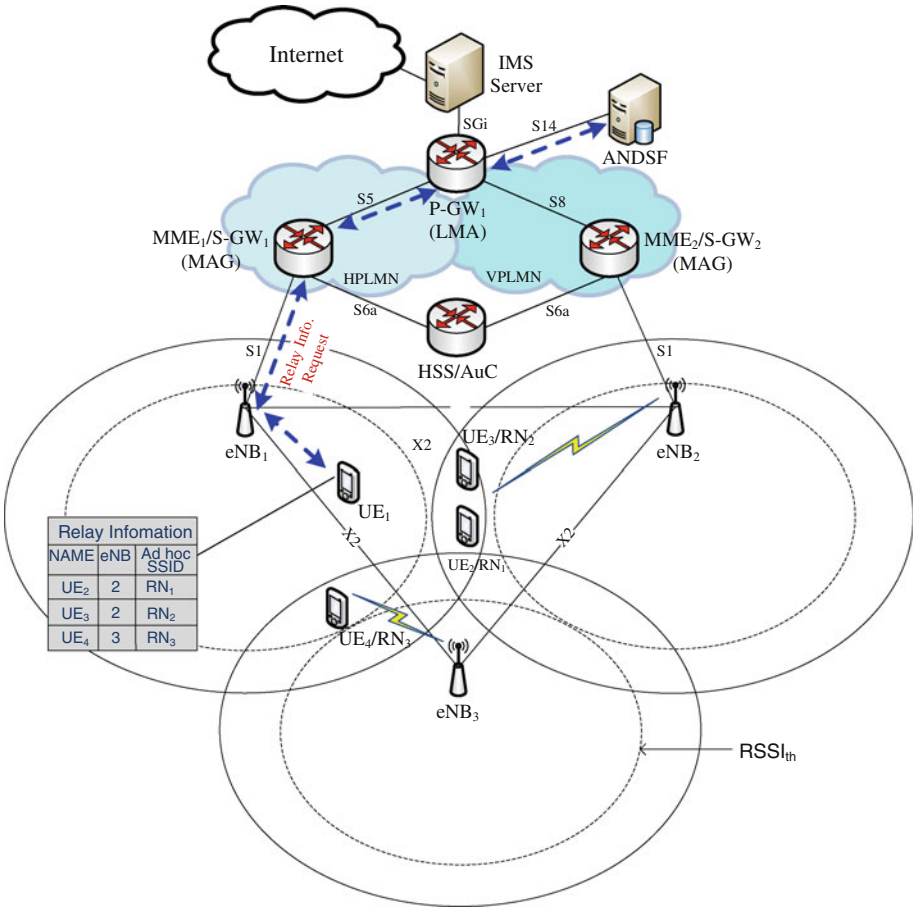

Fig. 9 The UE requests relay node information

Example can be seen in Fig. 10, UE_2 is a RN (RN_1) of UE1 if the target eNB is eNB_2 and UE_4 is a RN (RN_3) of UE1 if the target eNB is eNB_3.

4.2 Secure Handover Phase

This subsection aims to establish a security mechanism to provide the secure communication between UE and RN during the handover.

Before describing the security mechanism with consideration of relay nodes, a secure handover procedure, including authentication key and encryption key, is investigated as follows. Through the key exchange procedure, the authentication operation is done during the handover. With the authentication key and encryption key, the UE can safely transmit data to the target eNB. Figure 11 [1] shows the detailed message flow of the LTE handover procedure with security. The detailed steps are described as follows.

S1: When a source eNB initiates a handover procedure. The source eNB creates an authentication key. Source eNB calculates a hash function over the current K_{eNB} and cell ID of target eNB to have K_{eNB*}.

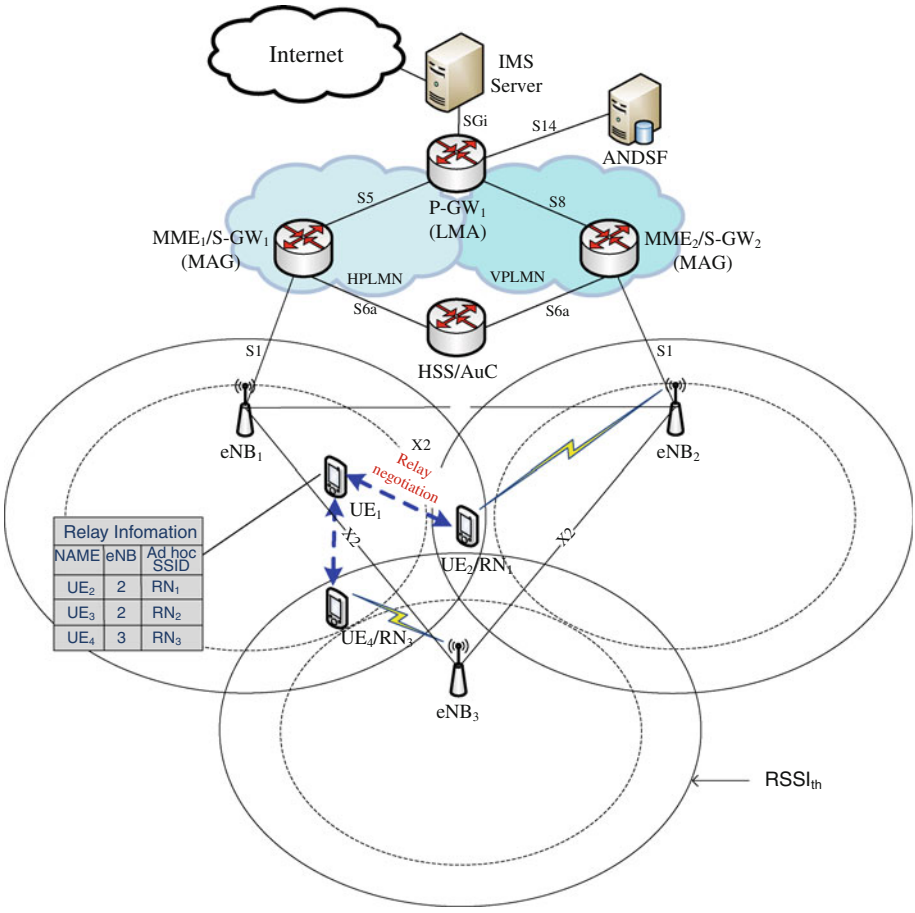

Fig. 10 The UE negotiates with relay nodes

S2: *Source eNB* $\overset{request}{\Longrightarrow}$ *source MME* : The K_{eNB*} is sent by source eNB through the handover request message to the source MME.

S3: *Source MME* $\overset{request}{\Longrightarrow}$ *target MME* : Source MME sends K_{eNB*} and related security information of MME (K_{NAS}, COUNT, K_{ASME}) by the handover request message.

S4: *Target MME* $\overset{request}{\Longrightarrow}$ *target eNB* : Target MME uses K_{eNB*} and K_{ASME} to calculate K_{eNB+}, from the definition of generated key deviation function [17]. Target MME adds K_{eNB+} and the information of RRC/UP algorithm in handover request message and then is transmitted to the target eNB.

S5: *Target eNB* $\overset{response}{\Longrightarrow}$ *target MME* : Target eNB selects a target MME permitted by the selected RRC/UP algorithm. Target eNB returns the handover response to the target MME. The handover response message contains new C-RNTI and selected RRC/UP algorithm. Target eNB uses C-RNTI and K_{eNB+} to compute a new K_{eNB}, by the key deviation function [17].

S6: *Target MME* $\overset{response}{\Longrightarrow}$ *source eNB* : Target MME sends the handover response back to the source MME and the source eNB. The handover response information contains the selected C-RNTI and the MME safety information (NAS-MAC).

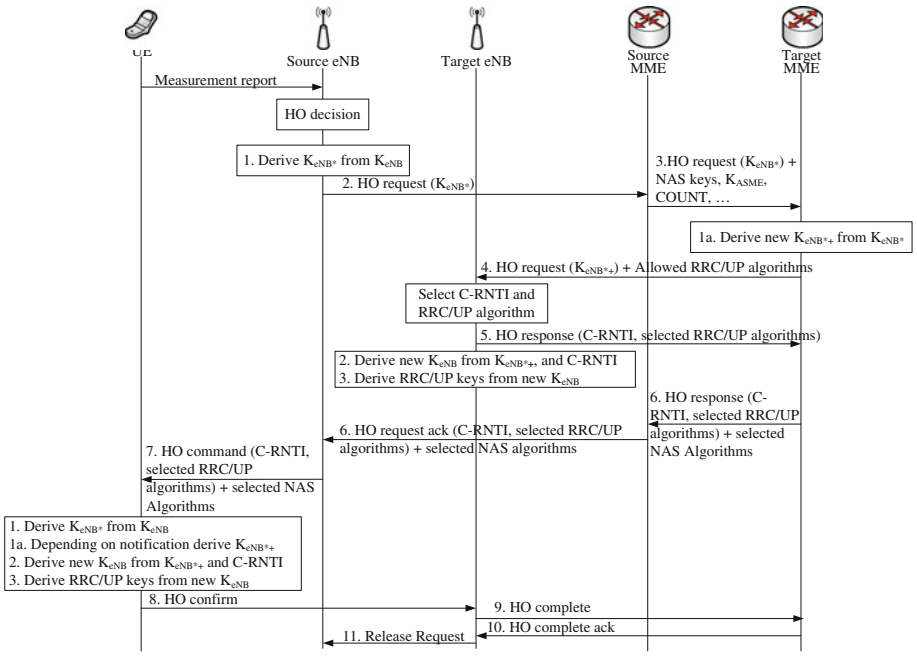

Fig. 11 Message flow of the secure LTE handover protocol

S7: *Source eNB* $\overset{HOcommand}{\Longrightarrow}$ *UE* : Source eNB receives the handover response message, the handover command message then is transmitted to the UE, it contains a C-RNTI, the target domain of the NAS, and AS new safety information. The UE uses the information from handover command message to generate K_{eNB+}. The UE uses K_{eNB+} and C-RNTI to produce the target domain K_{eNB}. After having the target domain K_{eNB}, then we can have K_{RRCenc}, K_{RRCint},and K_{UPenc}.

S8: *UE* $\overset{HOconfirm}{\Longrightarrow}$ *target eNB* : The UE sends the handover confirm message and new RRC key to the target eNB if the handover is completed.

Figure 12 shows an example of the LTE handover procedure with security. The source eNB initially knows the UE into the cell boundary region. The UE initiates the handover procedure. Figure 12 shows the data transmission of encryption key, the usage of encryption between source eNB, source MME, target eNB, and target MME. Figure 12 mainly shows how to have the keys of K_{AS} and K_{NAS}, where K_{AS} is used for many communication protocol, such as the radio resource control (RRC) and the packet data convergence protocol (PDCP). The K_{NAS} is mainly used for the communication service link set up protocol, mobility management (MM), and GPRS mobility management (GMM). The source eNB generates a key K_{eNB*} which is used for the certification.

In the following, the detailed operations of security of handover procedure by adding the relay node (RN) is presented. Figure 13 illustrates the message flow of the security of handover procedure with the relay node (RN). It is observed that two new security keys, K_{Relay} and K_{Relay_enc}, are generated to guarantee the secure communication for the relay nodes.

S1′: The UE generates K_{eNB} and simultaneously performs the relay node discovery to find SSID of RN to obtain an authentication key, K_{Relay}, to verify with the selected RN.

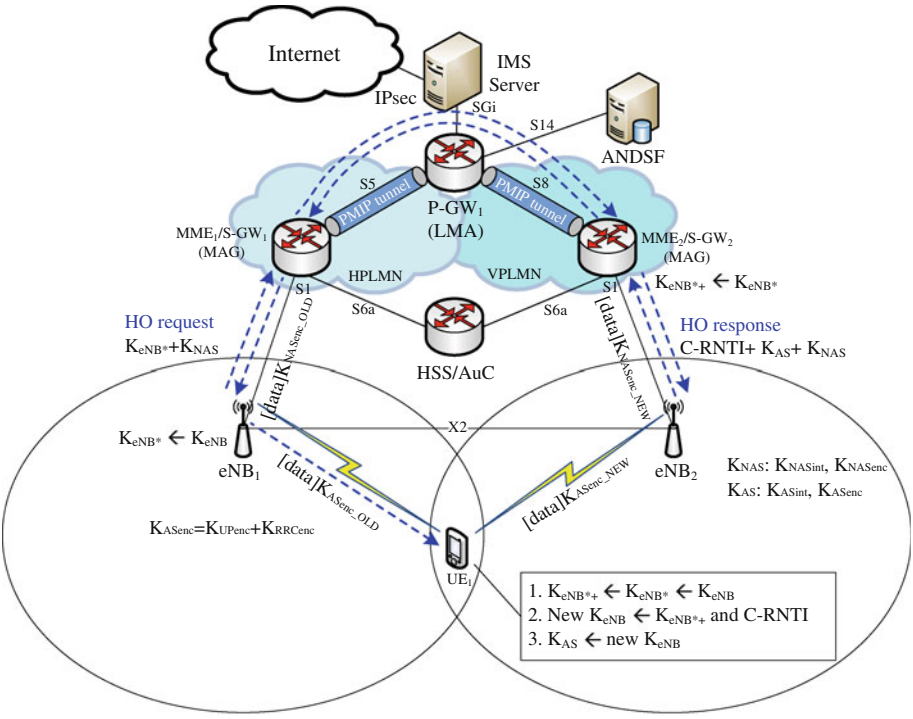

Fig. 12 The LTE handover procedure with security

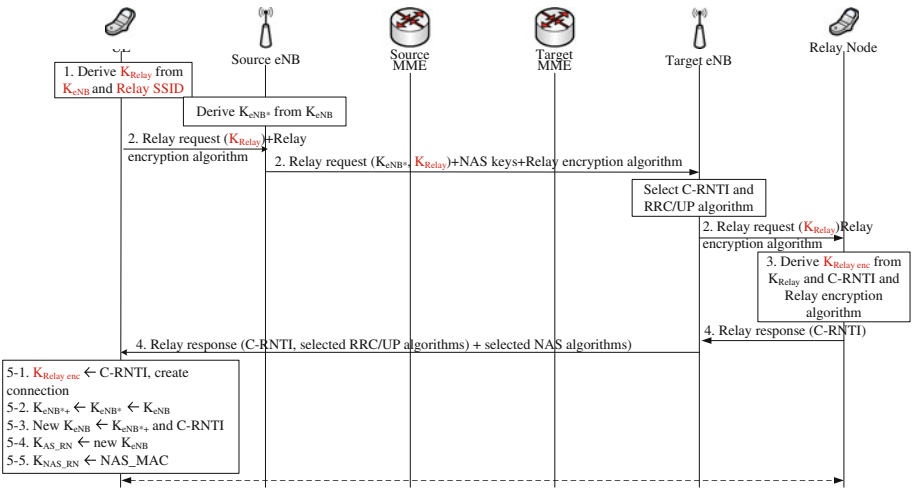

Fig. 13 The message flow of a secure relay-assisted handover protocol

S2′: $UE \overset{request}{\Longrightarrow} RN$: After the UE obtaining K_{Relay}, the information of K_{Relay} and encryption algorithms used by the RN are added into the *relay request* message, and the *relay request* message is sent through the LTE core network to the target eNB. Target MME appends K_{eNB+} and the information of RRC/UP algorithm into the *handover*

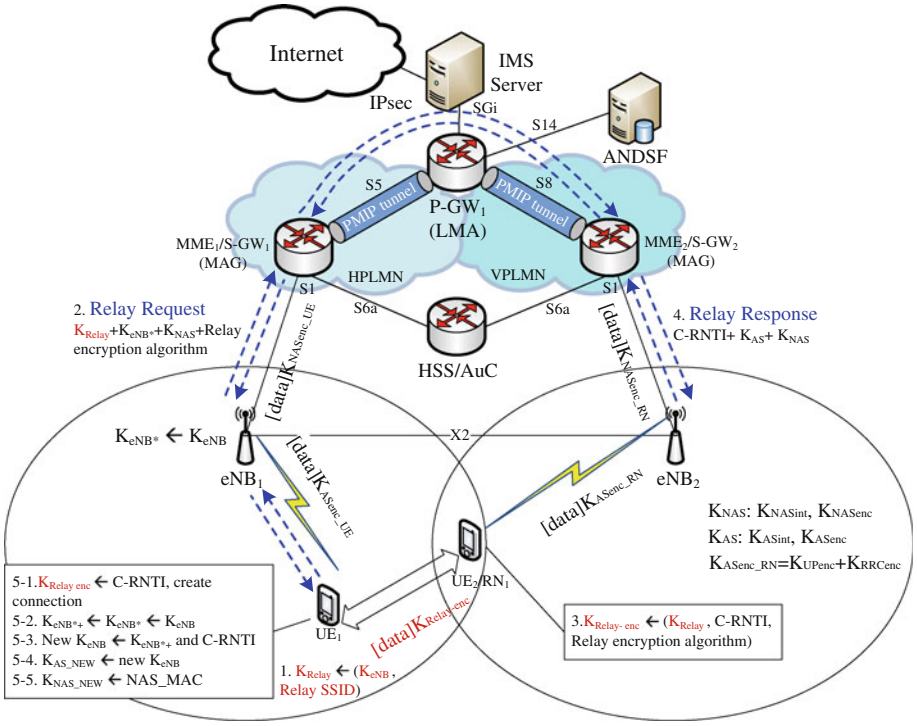

Fig. 14 The relay-assisted handover operation with security

request message, and then sent to the target eNB. The target eNB selects the permitted RRC/UP algorithm from the *handover request* message.

S3′: When a RN receives K_{Relay} and encryption algorithm from the *relay request* message. The RN uses the received information and C-RNTI of target eNB to re-produce K_{Relay_enc}. This is used the data encryption key between the UE and RN.

S4′: $RN \overset{response}{\Longrightarrow} UE$: The RN reply *relay response* message, which contains the C-RNTI of target cell information, to the UE.

S5′: The UE receives the *relay response* message and produced K_{Relay_enc} by the received C-RNTI information. Then, the UE and the RN have two keys, K_{Relay} and K_{Relay_enc}. Establish a connection using these two keys for the secure communication. Then, UE uses the information of *relay response* message to generate K_{eNB+}, and then use K_{eNB+} and C-RNTI to generate K_{eNB}. Finally, the UE keeps K_{eNB}, K_{RRCenc}, K_{RRCint}, and K_{UPenc}.

Example is given in Fig. 14 for a scenario of relay-assisted handover with consideration of security. When a UE obtains relay discovery information by the ANDSF^{+}. The UE generates an authentication key by KDF. The UE determines a key encryption algorithm and adds this information into the *relay request* message. The relay request message sends to the source eNB, MME, target MME, eNB, and RN. When the RN receives the relay request message, it can completes the successful authentication procedure. The RN returns the request response message back to UE. The UE identifies the relay response message to complete the RN authentication process. Thus, the UE can use the security information to establish the safe ad hoc connection with RN. In the handover period, the UE simultaneously obtains the

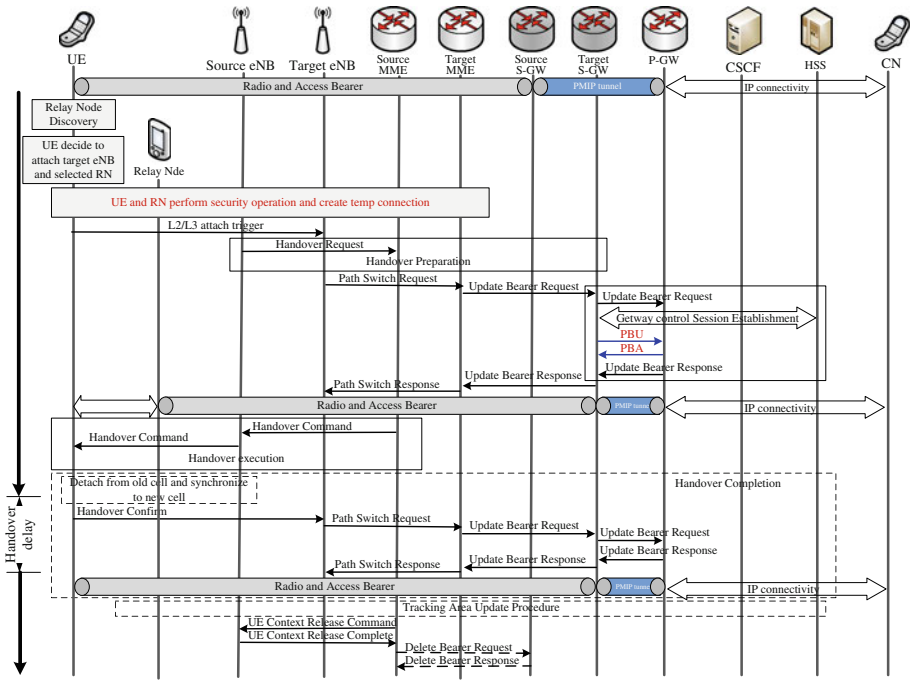

Fig. 15 The message flow of relay-assisted handover with security for PMIPv6

authentication key and information of AS and NAS encryption algorithms. After through the security procedure above mentioned, the UE can obtain security keys and establish of secure connection by adding two security keys, K_{Relay} and K_{Relay_enc}, where K_{Relay} used in the authentication to ensure that the RN is not a malicious node, and K_{Relay_enc} used in verification, ensure between the UE and RN data validity and usability.

4.3 Secure Relay-assisted Handover Phase

This subsection describes the secure relay-assisted handoff protocol for PMIPv6. The main contribution of the proposed scheme is to improve the handoff latency and packet loss with the assistance of RN. If a UE cannot find out any RN, our scheme can automatically switches to default LTE handoff procedure to ensure that the UE can successfully perform the secure handover operation. The message flow of the secure relay-assisted handover procedure is given in Fig. 15. The detailed steps are also given below.

S1: $UE \overset{action}{\Longrightarrow}$ ANDSF^{+}: The relay node discovery phase is performed and described in Sect. 4.1. The UE obtains a list of the RN candidates. The UE chooses a RN belongs to target eNB, and finally selects the best RN from the RN candidates.

S2: $UE \overset{action}{\Longrightarrow} RN$: The secure handover phase is performed and introduced in Sect. 4.2. When a UE selects the RN for the pre-handover, the UE must establish a secure UE-RN connection.

S3: *Source eNB* $\overset{action}{\Longrightarrow}$ *target S-GW* : The step is the handover preparation. The source eNB sends the handover request to source MME. The source eNB sets bearers of data forwarding. The target MME forward the handover request message to target eNB.

This message creates the UE context information by the used target eNB, including information of bearers. Observe that, step 2 pre-executes the secure process to reduce the handover preparation time.

S4: *Target eNB* $\stackrel{PBU}{\Longrightarrow}$ *P-GW* : The step is the pre-handover procedure. The UE has the assistance from RN. The UE performs pre-handover procedure. The target eNB sends *path switch request* message to target MME. The target MME sends *update bearer request* message to serving gateway. Then serving gateway sends *proxy binding update* message to PDN gateway. The PDN gateway prior switches path to target domain. Secure data traffic goes though RN to UE.

S5: *UE* $\stackrel{handover}{\Longrightarrow}$ *target MME* : The step is the handover execution. The source MME sends a *handover command* message to the source eNB. This step ensures that the handover preparation is executed. The source sends a command to inform UE to start layer 2 handover procedure.

S6: *UE* $\stackrel{switch}{\Longrightarrow}$ *PDN Gateway* : The step is the handover completion. With the assistance of RN, the handover procedure is pre-executed. When UE knows that the layer 2 handover procedure is finished, the UE sends *path switch request* message to the serving gateway. The serving gateway switches path to UE.

S7: *UE* $\stackrel{TAU}{\Longrightarrow}$ *HSS* : The step is the tracking area update procedure. The target MME knows that the handover procedure has been executed, the source eNB releases resource of the UE and responds *context release complete* message.

5 Performance Evaluation

In this section, the mathematical analysis and simulation results are described.

5.1 Mathematical Analysis

The handover latency, packet loss, location update cost of our proposed scheme are analyzed. The variables and notations followed the system parameters defined from [7,18], and given in Table 2.

5.1.1 Handover Latency

Let D_{L2} denote as the layer-2 handover latency, let D_{LTE_OP} be the execution delay of the LTE handover preparation procedure, including bearer setup procedure and location update procedure. The handover latency of PMIPv6, $T_{HO,PMIP}$, is derived as follow.

$$\begin{aligned} T_{HO,PMIP} &= D_{L2} + D_{L3} + D_{HO\_Security} \\ &= D_{L2} + t_{PBU} + 4t_{UE\_S\_GW} + D_{HO\_Security}, \end{aligned} \tag{1}$$

where D_{L3} is layer-3 handover delay latency, including the delay time of the proxy binding update and time cost of packet transmissions between UE and serving gateway. In addition, $D_{HO\_Security}$ is the processing time of LTE handing with security procedure during handover. The t_{PBU} is

$$t_{PBU} = 2t_{S\_GW\_P\_GW} + t_{LMA\_OP}, \tag{2}$$

where $t_{S\_GW\_P\_GW}$ is the delay time for packet transmission between serving gateway and PDN gateway, and t_{LMA_OP} is the proxy binding update request time for LMA. The $t_{S\_GW\_P\_GW}$ is

Table 2 System parameters

Variable	Description
BW_{wire_LTE}	Bandwidth of the wire link
L_{wire_LTE}	Latency of the wire link
S_{ctr}	Average size of the control message
D_{L2}	The time of layer 2 handover delay
$D_{HO\_Security}$	The time of perform LTE handover processing with security
t_{RN}	The time of the RN performing the pre-handover procedure
$t_{UE\_S\_GW}$	The time of the delay for transmission between UE and S-GW
$t_{S\_GW\_P\_GW}$	The time of the delay for transmission between P-GW and S-GW
t_{PBU}	The time of proxy binding update delay
$t_{D\_internet}$	The time of average delay of that a packet traveling in the Internet
t_{LMA_OP}	The time of LTE execution request
$t_{acq\_profile}$	The time of acquire MN profile in SPMIPv6
U	The average cost of proxy binding update to LMA
L	The cost for connection between nMAG and pMAG in SPMIPv6
R	The cost for relay node discovery of pre-handover
S	The cost for security operation of EPC

$$t_{S\_GW\_P\_GW} = n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) + t_{D\_internet}, \tag{3}$$

where S_{ctr} is the average size of the control message, BW_{w_LTE} is the bandwidth of wired link, L_{w_LTE} is the latency of wired link, $t_{D\_internet}$ is the average delay of a packet traveling in Internet. The handover of PMIPv6 is

$$\begin{aligned} T_{HO,PMIP} &= D_{L2} + t_{PBU} + 4t_{UE\_S\_GW} + D_{HO\_Security} \\ &= D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) + t_{D\_internet} \\ &\quad + t_{LMA\_OP} + 4t_{UE\_S\_GW} + D_{HO\_Security} \end{aligned} \tag{4}$$

The seamless PMIPv6 handover latency, $T_{HO,SMIP}$, is derived as follow.

$$\begin{aligned} T_{HO,SPMIP} &= D_{L2} + D_{L3} + D_{HO\_Security} \\ &= D_{L2} + t_{PBU} - t_{acq\_profile} + 4t_{UE\_S\_GW} + D_{HO\_Security} \\ &= D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) + t_{D\_internet} \\ &\quad + t_{LMA\_OP} - t_{acq\_profile} + 4t_{UE\_S\_GW} + D_{HO\_Security} \end{aligned} \tag{5}$$

It is observed that the usage of RN to perform the pre-handover procedure to eliminate t_{RN_OP} as follow.

$$\begin{aligned} t_{RN\_OP} &= D_{L2} + t_{PBU} + D_{HO\_Security} \\ &= D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) \\ &\quad + t_{D\_internet} + t_{LMA\_OP} + D_{HO\_Security} \end{aligned} \tag{6}$$

Consequently, the handover latency of proposed protocol, T_{HO,RN_PMIP}, is derived as follow.

$$\begin{aligned} T_{HO,RN\_PMIP} &= D_{L2} + D_{L3} + D_{HO\_Security} - t_{RN\_OP} \\ &= 4t_{UE\_S\_GW} \end{aligned} \tag{7}$$

Let $t_{\Delta 1}$ be the time difference between $T_{HO,PMIP}$ and T_{HO,RN_PMIP}.

$$\begin{aligned} t_{\Delta 1} &= T_{HO,PMIP} - T_{HO,RN\_PMIP} \\ &= D_{L2} + t_{PBU} + D_{HO\_Security} \\ &= D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) \\ &\quad + t_{D\_internet} + t_{LMA\_OP} + D_{HO\_Security} \end{aligned} \tag{8}$$

Observed that $t_{\Delta 1} > 0$ illustrates that the handover latency of RN_PMIPv6 is better than PMIPv6. Let $t_{\Delta 2}$ be the time of difference between $T_{HO,SPMIP}$ and T_{HO,RN_PMIP}.

$$\begin{aligned} t_{\Delta 2} &= T_{HO,SPMIP} - T_{HO,RN\_PMIP} \\ &= D_{L2} + t_{PBU} + D_{HO\_Security} + D_{HO\_Security} - t_{acq\_profile} \\ &= D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) + t_{D\_internet} \\ &\quad + t_{LMA\_OP} + D_{HO\_Security} - t_{acq\_profile} \end{aligned} \tag{9}$$

Observed that $t_{\Delta 2} > 0$ illustrates that the handover latency of the RN_PMIPv6 is better than that of seamless PMIPv6.

5.1.2 Packet Loss

Let λp be the packet arrival rate [18], where λ be the Poisson random variable. The number of packet loss is counted under the packet lost is exponentially distribution. The number of lost packet during handover of is

$$\begin{aligned} L_{HO,PMIP} &= \lambda p \times (T_{HO,PMIP} - t_{UE\_S\_GW}) \\ &= \lambda p \times \left(D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) + t_{D\_internet} \right. \\ &\quad \left. + L_{wire\_LTE} + t_{LMA\_OP} + 4t_{UE\_S\_GW} + D_{HO\_Security} - t_{UE\_S\_GW} \right) \end{aligned} \tag{10}$$

The seamless PMIPv6 protocol utilizes the buffering scheme. Let $Buffer_{MAG,LMA}$ denote the packet buffer size of LMA and MAG. The number of lost packet during handover of seamless PMIPv6 is

$$\begin{aligned} L_{HO,SPMIP} &= \lambda p \times (T_{HO,SPMIP} - t_{UE\_S\_GW}) - Buffer_{MAG,LMA} \\ &= \lambda p \times \left(D_{L2} + 2n \times \left(\frac{S_{ctr}}{BW_{wire\_LTE}} + L_{wire\_LTE} \right) \right. \\ &\quad + t_{D\_internet} + t_{LMA\_OP} - t_{acq\_profile} + 4t_{UE\_S\_GW} \\ &\quad \left. + D_{HO\_Security} - t_{UE\_S\_GW} \right) - Buffer_{MAG,LMA} \end{aligned} \tag{11}$$

Our scheme adopts the RN to perform the pre-handover procedure. The number of lost packet during handover of our scheme is

$$\begin{aligned} L_{HO,RN\_PMIP} &= \lambda p \times (T_{HO,RN\_PMIP} - t_{UE\_S\_GW}) \\ &= \lambda p \times (4t_{UE\_S\_GW} - t_{UE\_S\_GW}) \end{aligned} \tag{12}$$

5.1.3 Location Update Cost

The system parameters are followed the similar definitions from [18]. Let α is the UE call to mobility ratio, $\alpha = \lambda p/t$, where λp denotes the call arrival rate. The mean stay time of UE in a cell is $1/t$ second. Let C_U be the average cost of location update to the LMA. The cost is the delay of the signaling messages, including the transmission and propagation delay. Let C_S be the cost of security procedure during a UE moves from one serving eNB to target eNB. Let C_L be the cost of establishing a direct connection between serving MAG and target MAG in the seamless PMIPv6 protocol. Let $\alpha(i)$ be the probability of a UE moving i steps between two consecutive packet arrivals, where $\alpha(i)$ is the exponential distribution. The probability density function is defined as $f_\alpha(x) = \alpha e^{-\alpha x}$. The location update cost of PMIPv6 is

$$C_{PMIP} = \sum_{i=0}^{\infty} i(C_U + C_S)\alpha(i) = \frac{C_U + C_S}{\alpha}$$

The seamless PMIPv6 protocol reduces the packet lost by forwarding the packets from serving MAG to the target MAG, and from LMA to the target MAG. There is additional signaling cost to establish a direct connection between the serving MAG and the target MAG. The location update cost of seamless PMIPv6 protocol is

$$C_{SPMIP} = \sum_{i=0}^{\infty} i(C_U + C_L + C_S)\alpha(i) = \frac{C_U + C_L + C_S}{\alpha}$$

Our proposed protocol needs more control packets for handling with the RNs to consider the security issue. The location update cost of our proposed protocol is

$$C_{RN\_PMIP} = \sum_{i=0}^{\infty} i(C_U + C_R + 2C_S)\alpha(i) = \frac{C_U + C_R + 2C_S}{\alpha}$$

5.2 Simulation results

To evaluate the relay-assisted PMIPv6 (denoted as RN_PMIPv6) PMIPv6 [3], seamless PMIPv6 (denoted as SPMIPv6) [11] protocols in 3GPP LTE systems, all of these protocols are mainly implemented using the network simulator-2 (ns-2) [19] with PMIPv6 module [20] and eurane module [21]. Observe that the eurane module is the HSDPA module, and we modify eurane module to simulate the 3GPP LTE environment in our simulation. Figure 16

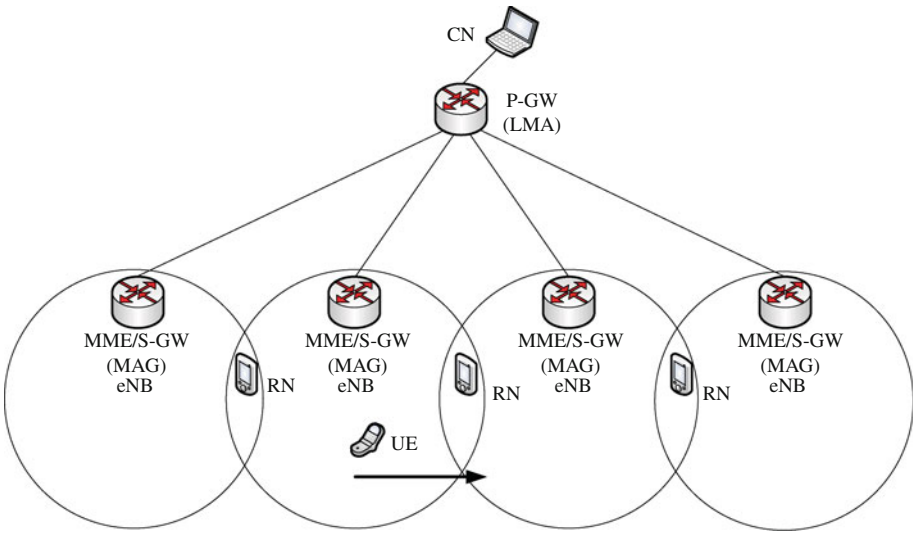

Fig. 16 The simulation scenario for the handover

shows the simulation scenario for the handover. To simplify the scenario, each eNB is also the mobility access gateway. The transmission range and the link bandwidth of all eNB are assumed to be 50 km and 100 Mbps. A cbr (udp) traffic application between CN to UE is 0.01 s intervals in our simulation. In addition, a sniffer program was developed to estimate the handoff delay times for all implemented protocols. The performance metrics to be observed are:

- *Handover latency* (HL)**:** The handover latency is the delay time from a UE disconnects the serving eNB, then re-connects to the target eNB, and to receive data packet from CN through target eNB.
- *Packet loss* (HL)**:** The packet loss counts from the UE disconnecting to serving eNB to receiving new packets from the target eNB.
- *Handover jitter* (HJ)**:** The handover jitter is the jitter that counts during the handover time. Assumed that three consecutive packets, P_{i-2}, P_{i-1} and P_i are received by UE. Let T_{i-2}, T_{i-1} and T_i denote the time to receive packets P_{i-2}, P_{i-1} and P_i. Therefore, handover jitter is $HJ_{j-2} = (T_i - T_{i-1}) - (T_{i-1} - T_{i-2}) = T_i - 2T_{i-1} + T_{i-2}$.
- *Location update cost* (LUC)**:** The location update cost is the total number of signal messages for a UE roaming from the serving eNB to the target eNB.

It is worth mentioning that an efficient secure handoff protocol in LTE networks is achieved with a low *handover latency*, low *packet loss*, low *handover jitter*, and low *location update cost*. In the following, we illustrate our simulation results for *handover latency*, *packet loss*, *handover jitter*, and *location update cost* from several aspects.

5.2.1 Handover Latency (HL)

Before describing the simulation results of handover latency, we give the simulation results of the sequence number below. Figure 17 illustrates the simulation results of the sequence number vs time for PMIPv6, SPMIPv6 and RN_PMIPv6, protocols. Figure 17 shows the simulation results of the sequence number vs time. We observed that from the start handoff time

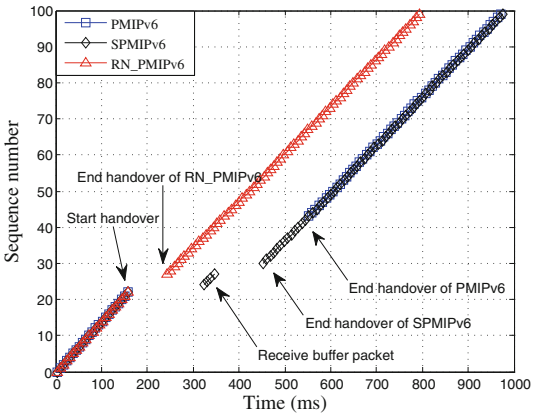

Fig. 17 The performance of sequence number versus time

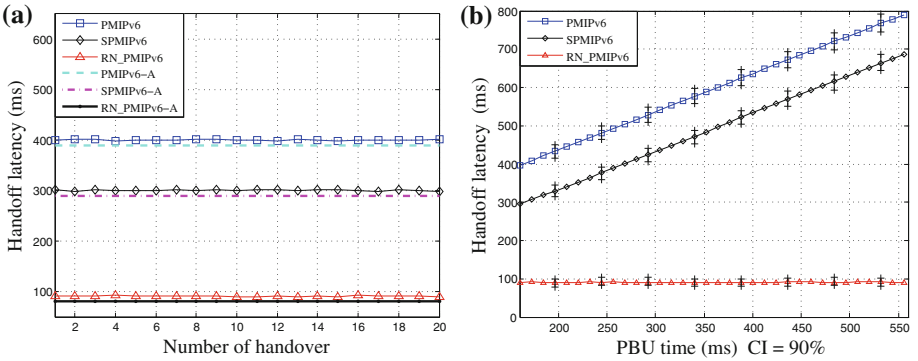

Fig. 18 The performance of handover latency versus **a** number of handover, **b** proxy binding update time

to handoff time of PMIPv6, SPMIPv6 and RN_PMIPv6, the RN_PMIPv6 scheme receives packets from the UE earlier than that of PMIPv6 and SPMIPv6. The curves of PMIPv6, SPMIPv6 and RN_PMIPv6 start the handoff at a time of 180 ms. The RN_PMIPv6 receives the new packets at a time of 250 ms which was lower than the SPMIPv6 at a time of 295 ms and PMIPv6 at a time of 390 ms. This is because that RN_PMIPv6 has the assistance of relay nodes.

Figure 18a, b illustrate the simulation results of handover latency vs. number of handover and proxy binding update time for the PMIPv6, SPMIPv6 and RN_PMIPv6 protocols. Figure 18a shows that the average HL values were in the following order: RN_PMIPv6 < SPMIPv6 < PMIPv6 from the perspective of number of handover. This verifies that the and our RN_PMIPv6 protocol had better HL than the other protocols. Figure 18a also displays the use of mathematical analysis for the PMIPv6-A, SPMIPv6-A, and RN_PMIPv6-A. It was nearly the same as our implementation as illustrated by the curves of PMIPv6 and PMIPv6-A about 400 ms, the curves of SPMIPv6 and SPMIPv6-A about 300 ms, and the curves of RN_PMIPv6 and RN_PMIPv6-A about 100 ms.

Figure 18b shows the handover latency under various proxy binding update (PBU) time. In general, the HL increases as the PBU time increases. We observe that PMIPv6 and SPMIPv6 has the curves of HL between 410˜900 ms and 305˜710 ms, but the curve of RN_PMIPv6

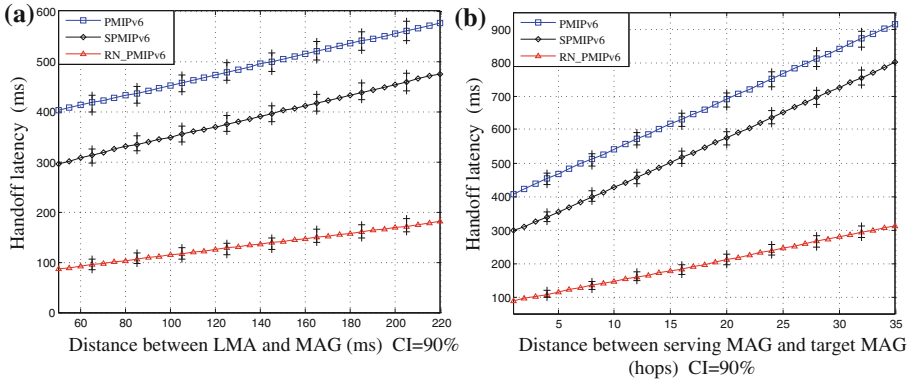

Fig. 19 The performance of handover latency versus **a** distance between LMA and MAG, **b** distance between serving MAG and target MAG (hops)

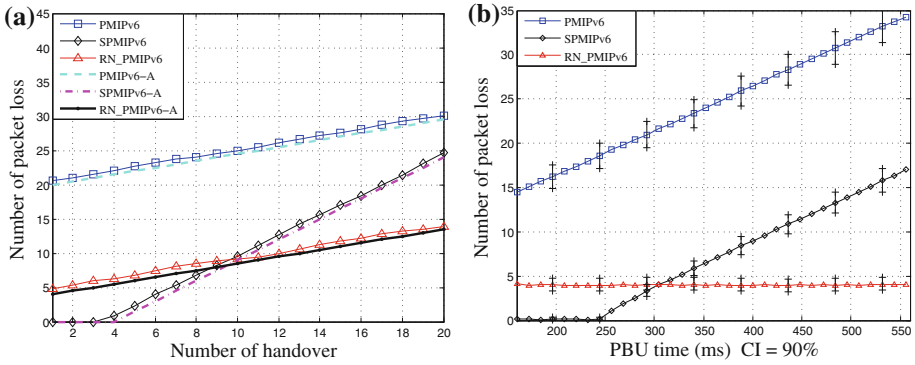

Fig. 20 The performance of packet loss ratio versus **a** distance between LMA and MAG, **b** proxy binding update time

was around 100 ms. This is because that the RN_PMIPv6 can eliminate the partial proxy binding update time due to the assistance of relay node (RN).

Figure 19a illustrates the handover latency vs distance between LMA and MAG, for the PMIPv6, SPMIPv6 and RN_PMIPv6 protocols. For each case, the higher the distance between LMA and MAG, the higher the HL. Figure 19a shows that the average HL values were in the following order: RN_PMIPv6 < SPMIPv6 < PMIPv6 from the perspective of distance between LMA and MAG. Figure 19b illustrates the handover latency vs. distance between serving MAG and target MAG. For each case, the higher the distance between serving MAG and target MAG, the higher the HL. Figure 19a shows that the average HL values were in the following order: RN_PMIPv6 < SPMIPv6 < PMIPv6 from the perspective of distance between serving MAG and target MAG.

5.2.2 Packet Loss (PL)

Figure 20a illustrates the mathematical analysis and simulation result of packet loss vs the number of handover. In general, the PL increased as the number of handover increases. The RN_PMIPv6 has low packet loss that of PMIPv6 and SPMIPv6. Is is observed that SPMIPv6

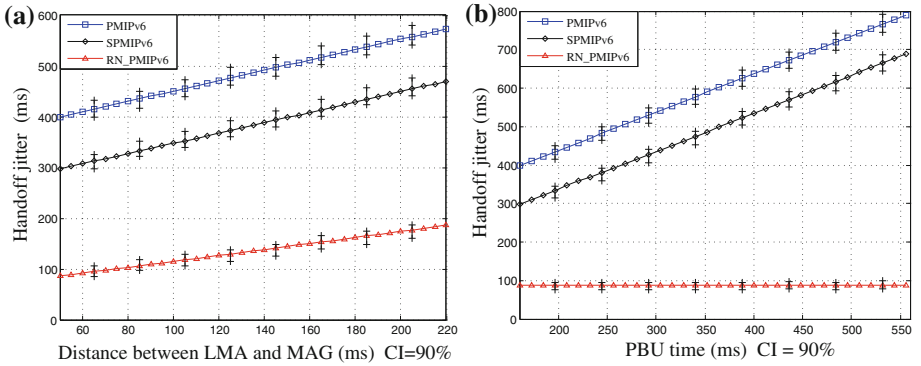

Fig. 21 The performance of handover jitter versus **a** distance between LMA and MAG, **b** proxy binding update time

has lower packet loss if the number of handover is less. This is because that the buffering scheme is used in SPMIPv6 with extra hardware cost. It was nearly the same as our implementation as illustrated by the curves of PMIPv6 and PMIPv6-A , the curves of SPMIPv6 and SPMIPv6-A, and the curves of RN_PMIPv6 and RN_PMIPv6-A.

Figure 20b displays the simulation result of PL vs PBU time. The PL increased as PBU time increases. The RN_PMIPv6 has low packet loss that of PMIPv6 and SPMIPv6. Is is observed that SPMIPv6 has lower packet loss if PBU time is small. This is because that the buffering scheme is used in SPMIPv6 with extra hardware cost.

5.2.3 Handover Jitter (HJ)

Figure 21a, b illustrate the simulation result of handover jitter vs distance between LMA and MAG, and PBU time for PMIPv6, SPMIPv6 and RN_PMIPv6 protocols. The HJ was measured as the time from the serving eNB to the target eNB. Traditional wireless-link delay time between the UE and target eNB is between 10 ms and 50 ms. Figure 21a illustrates that PMIPv6 has the highest jitter compared to SPMIPv6 and RN_PMIPv6. The curve of RN_PMIPv6 was lower than those of SPMIPv6 and PMIPv6. The average handover jitter values were in the following order: RNPMIPv6 < SPMIPv6 < PMIPv6 from perspective of distances between LMA and MAG. Figure 21b also illustrates the handover jitter vs PBU time. The average handover jitter values were in the following order: RNPMIPv6 < SPMIPv6 < PMIPv6 from perspective of PBU time. This is because the overlapping result caused by the relay node for our relay-assisted design can significantly reduce the HJ.

5.2.4 Location Update Cost (LUC)

Figure 22 illustrates mathematical analysis and simulation result of the location update cost (times) vs. the call to mobility ratio for PMIPv6, SPMIPv6 and RN_PMIPv6 protocols, while the x-axes sets to be the logarithmic scale. It is observed that the result is not-linear. The increase in packet arrival to mobility ratio means that the movement of UE becomes slower. In general, the LUC drops as the call to mobility ratio increases. The average LUC were in the following order: RN_PMIPv6 > SPMIPv6 > PMIPv6. The mathematical analysis of LUC were in the following order: RN_PMIPv6-A > SPMIPv6-A > PMIPv6-A. This shows that RN_PMIPv6-A needs more location

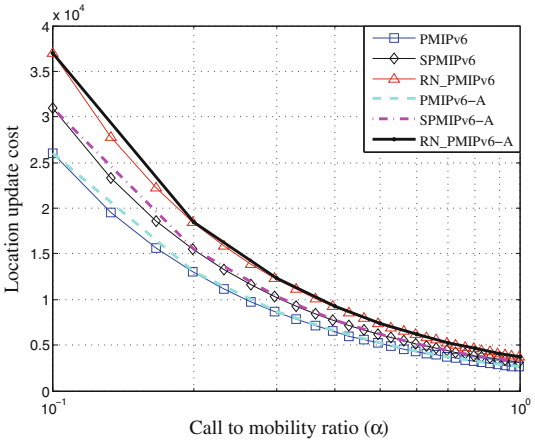

Fig. 22 The performance of location update cost versus call to mobility ratio

update cost than that of SPMIPv6-A and PMIPv6-A due to the relay node managements.

6 Conclusion

In this paper, we presented a new protocol to reduce handoff delay and packet lost with the assistance of relay nodes over LTE networks. We considered the security issue when selecting relay nodes during handoff. During the relay node discovery, we extend the access network discovery and selection function (ANDSF) in 3GPP specifications to help mobile station or UE to obtain the information of relay nodes. With the aid of the relay nodes, the mobile station or UE performs the pre-handover procedure, including the security operation and the proxy binding update to significantly reduce the handover latency and packet loss. The simulation results illustrated that our proposed protocol actually achieves the performance improvements in the handoff delay time and the packet loss rate.

References

1. 3rd Generation Partnership Project TS33.821. (March, 2009). *Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE)*, Release 8, v8.0.0.
2. Lee, J., Kimura, S., & Ebihara, Y. (2008). An approach to mobility management in Cellular IP networks utilising power-save mode of IEEE 802.11. *International Journal of Ad Hoc and Ubiquitous Computing, 3*(3), 191–203.
3. Gundavelli, S. (2008). Proxy Mobile IPv6. *Internet Engineering Task Force (IETF), RFC-5213*.
4. Soliman, H. (May, 2007). Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6). *Internet Engineering Task Force (IETF), draft-ietf-mip6-nemo-v4traversal-06 (work in progress)*.
5. Perkins, C. (2002). IP mobility support for IPv4. *Internet Engineering Task Force (IETF), RFC-3344*.
6. Le, L., & Liebsch, M. (April, 2009). Preliminary binding: An extension to proxy mobile IPv6 for inter-technology handover. *IEEE International Conference on Wireless Communications and Networking Conference,* (WCNC), Budapest, pp. 1–6.
7. Chen, Y.-S., Hsiao, W.-H., & Chiu, K.-L. (2010). Cross-layer partner-based fast Handoff mechanism for IEEE 802.11 Wireless Networks. *International Journal of Communication Systems, 23*(5), 596–632.
8. Chen, Y.-S., Wu, K.-L. (Oct. 2009). A cross-layer partner-assisted handoff scheme for hierarchical mobile IPv6 in IEEE 802.16e systems. *Wireless Communications and Mobile Computing*, Published online: Oct. 2009.

9. Johnson, D. (2004). Mobility support in IPv6. *Internet Engineering Task Force (IETF), RFC-3775*.
10. Oh, H., Yoo, K., Na, J., & Kimi, C. (2009). Seamless handover scheme in IPv6-based mobile networks. *International Journal of Ad Hoc and Ubiquitous Computing, 4*(1), 54–60.
11. Kang, J., Kum, D., Li, Y., & Cho, Y. (October, 2008). Seamless Handover Scheme for Proxy Mobile IPv6. *IEEE International Conference on Wireless and Mobile Computing,* (WIMOB), Washigton, DC, pp. 410–414.
12. Lee, J., & Park, J. (February, 2008). Fast handover for proxy mobile IPv6 based on 802.11 networks. *IEEE International Conference on Advanced Communication Technology,* (ICACT), Phoenix Park, pp. 1051–1054.
13. 3rd Generation Partnership Project TS23.402. (January, 2009). *Architecture enhancements for non-3GPP accesses*, Release 8, v8.4.1.
14. 3rd Generation Partnership Project TS36.300. (March, 2009). *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Overall description*, Release 8, v8.8.0.
15. 3rd Generation Partnership Project TS24.312. (December, 2008). *Access Network Discovery and Selection Function (ANDSF) Management Object (MO)*, Release 8, v8.0.0.
16. 3rd Generation Partnership Project TS23.401. (March, 2009). *General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN)*, Release 8, v8.5.0.
17. 3rd Generation Partnership Project TS33.401. (December, 2008). *3GPP System Architecture Evolution (SAE) Security architecture*, Release 8, v8.3.1.
18. Yeh, J.-H., Chen, J.-C., & Agrawal, P. (2009). Fast intra-network and cross-layer handover (FINCH) for WiMAX and mobile internet. *IEEE Transactions on Mobile Computing, 8*(4), 558–574.
19. The Network Simulator NS-2. http://www.isi.edu/nsnam/ns/.
20. Choi, H. *Proxy Mobile IPv6 for Ns-2*. http://commani.net/pmip6ns/.
21. T. I. for Wireless and M. Communications. *Enhanced UMTS Radio Access Network Extensions for NS-2 (EURANE)*. http://eurane.ti-wmc.nl/eurane/.

Author Biographies

Yuh-Shyan Chen received the B.S. degree in Computer Science from Tamkang University, Taiwan, R.O.C., in June 1988 and the M.S. and Ph.D. degrees in Computer Science and Information Engineering from the National Central University, Taiwan, R.O.C., in June 1991 and January 1996, respectively. He joined the faculty of Department of Computer Science and Information Engineering at Chung-Hua University, Taiwan, R.O.C., as an associate professor in February 1996. He joined the Department of Statistic, National Taipei University in August 2000, and joined the Department of Computer Science and Information Engineering, National Chung Cheng University in August 2002. Since 2006, he has been a Professor at the Department of Computer Science and Information Engineering, National Taipei University, Taiwan. Prof. Chen served as Editor-in-Chief of International Journal of Ad Hoc and Ubiquitous Computing (SCIE), Regional Editor (Asia and Pacific) of IET Communications (SCI), Editorial Board of Telecommunication System Journal (SCIE), EURASIP Journal on Wireless Communications and Networking (SCIE), International Journal of Communication Systems (SCIE), Mobile Information Systems (SCIE), and Journal of Internet Technology (SCIE). He also served as Guest Editor of ACM/Springer Mobile Networks and Applications (MONET), Wireless Communications and Mobile Computing, The Computer Journal, and Wireless Personal Communications. His paper wins the 2001 IEEE 15th ICOIN-15 Best Paper Award. Prof. Chen was a recipient of the 2005 Young Scholar Research Award, National Chung Cheng University, R.O.C. His recent research topics include wireless communications, mobile computing, and next-generation personal communication system. Dr. Chen is a senior member of the IEEE Communication Society and Phi Tau Phi Society.

Tong-Ying Juang is a professor in the Department of Computer Engineering and Information Science, and director of Computer Center at National Taipei University. His research interests include and mobile computing, wireless networks and distributed and parallel computing. He received a B.S. in naval architecture from National Taiwan University, and his M.S. and Ph.D. in computer science from the University of Texas at Dallas. Contact him at the Department of Computer Engineering and Information Science, National Taipei University, Taipei, 10433, Taiwan.

Yao-Tsu Lin received thes B.S. degree in Department of Computer and Communication Engineering from National Kaohsiung First University of Science and Technology, Taiwan, R.O.C., in June 2006 and the M.S. degree in Graduate Institute of Communication Engineering from National Taipei University, Taiwan, R.O.C., in July 2008. His research interest includes secure issues for mobility management.