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

Yuh-Shyan Chen, Yun-Wei Lin, Yao-Tsu Lin, and Tong-Ying Juang
Department of Computer Science and Information Engineering
National Taipei University, Taiwan, ROC.
Email: yschen@mail.ntpu.edu.tw

***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 to provide the mobility mechanisms. However, the PMIPv6 still suffers 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. In this paper, we consider the security issue when selecting relay nodes during 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.**

***Index Terms*—LTE, PMIPv6, Handover, Relay, Security**

I. 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.

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 [8] 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 [2][3] for IEEE 802.11 networks and IEEE 802.16e systems, respectively. The design differences of these protocols are given in Table I. 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 II describes the system architecture and basic ideas. The proposed protocol is presented in section III. Performance evaluation is discussed in section IV. Section V finally gives a conclusion.

II. Preliminary

A. Network architecture

Our approach is developed in the 3GPP LTE networks, and the network architecture is given in Fig. 1. In the investigation, we adopt the proxy mobile IPv6 protocol as the mobility management of LTE system. When the UE received very weak signals from current eNB and not reach to the coverage of the next eNB, the UE tries to find a different UE, called as RN (relay node) defined below, located in coverage of the next eNB. The RN performs the pre-handoff procedure.

Definition 1: Relay Node (RN): Given a UE, any neighbor UEs of the UE located in different base station domain can

Table I: Our approach compares with previous schemes

Schemes	**P_HMIPv6 in 802.11** [2]	**P_HMIPv6 in 802.16e** [3]	**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

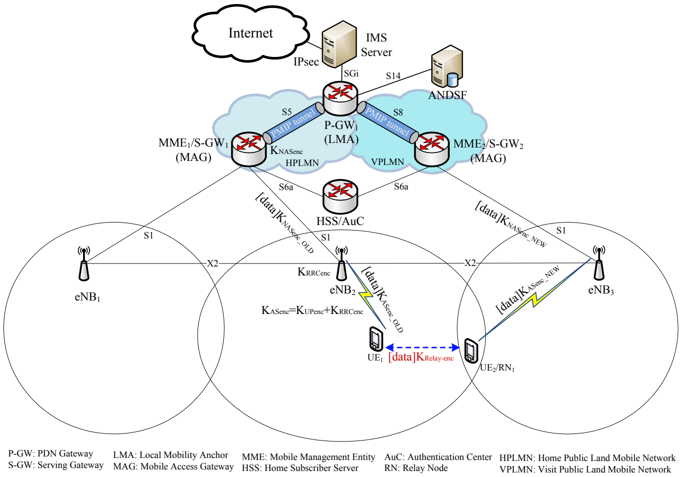


Fig. 1. The network architecture.

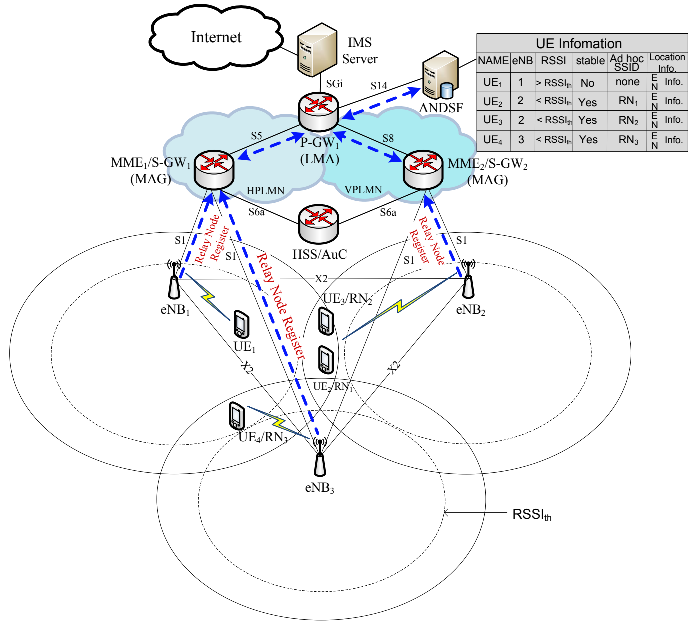


Fig. 2. RN registers to ANDSF$^+$.

become the RNs. Given an UE, the UE is called as a relay node (RN) if the UE satisfies the following assumptions.

- RN located in cell boundary of current eNB and its RSSI is less than RSSI$_{threshold}$.
- RN is stable and located on different eNBs.
- RN and UE support ad hoc mode communication.
- RN and UE provide its location information to ANDSF$^+$.

The function of the RN is to assist the UE to perform the partial work of the handover procedure which is defined in the 3GPP LTE Intra E-UTRAN mobility.

Each UE may enquire the assistance of RNs, a secure relay node discovery is necessary to ensure the authentication of RNs. This work is done by the access network discovery and selection function (ANDSF) of the 3GPP LTE specification. In this work, we add some new components, UE information table, into ANDSF to be ANDSF$^+$ to select the best RN.

Definition 2: ANDSF$^+$: Given an original ANDSF in 3GPPstandard, We add UE information table into ANDS to be ANDS$^+$. The function of ANDSF$^+$ is to assist the UE to easily discover the relay nodes.

B. Basic idea

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, 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.

III. Secure Relay-assisted Handover Protocol for PMIPv6

A. Relay node discovery

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. 2. The operation of relay node discovery is given.

Step 1: $UE \stackrel{register}{\Longrightarrow} ANDSF^+$: 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 store in the table of the ANDSF$^+$ database, as illustrated in Fig. 2.

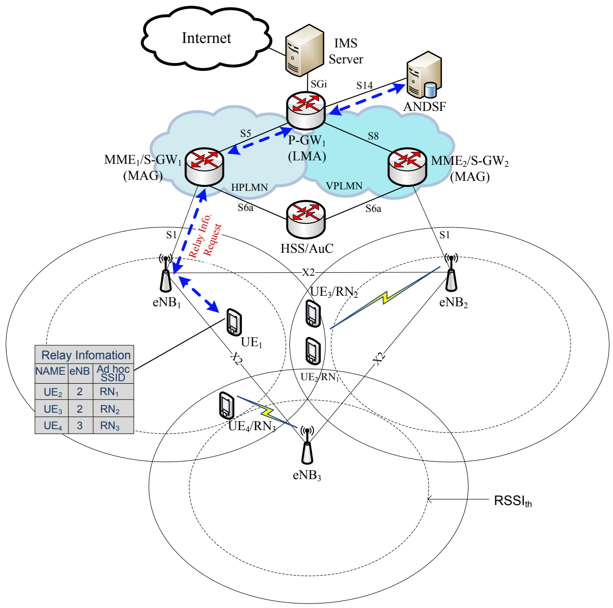


Fig. 3. UE requests the relay information.

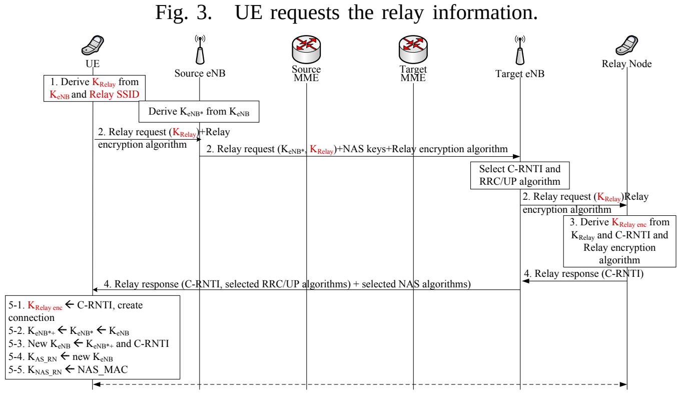


Fig. 4. Message flow of secure handoff procedure.

Step 2: $UE \overset{query}{\Longrightarrow} ANDSF^{+}$: 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 use of RN is to extend to the coverage area of target eNB, as show in Fig. 3. 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.

Step 3: $UE \overset{negotiation}{\Longrightarrow} RN$: 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.

B. Secure handover procedure

The detailed operations of security of handover procedure is presented. Fig 4 illustrates the message flow of the secure relay-assisted LTE handover procedure.

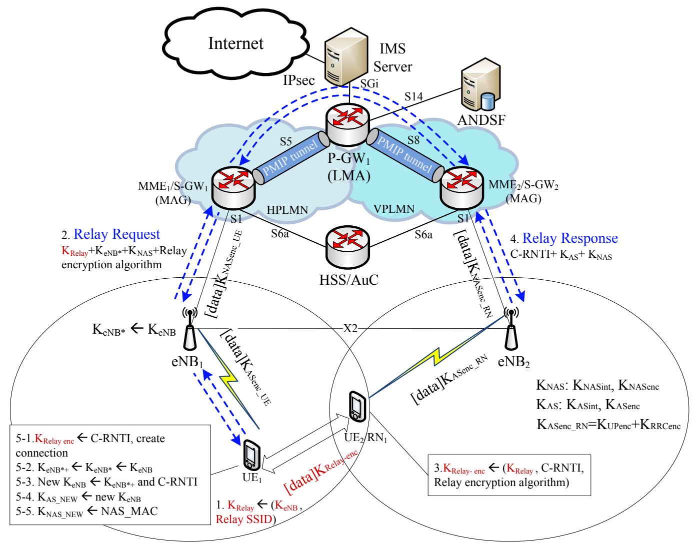


Fig. 5. RN_PMIPv6 protocol.

Step 1: The UE uses K_{eNB} and performs the relay node discovery to find SSID of RN to obtain an authentication key, K_{Relay}, to verify with the RN.

Step 2: $UE \overset{request}{\Longrightarrow} RN$: 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 request* message, and then sent to the target eNB. The target eNB selects the permitted RRC/UP algorithm from the *handover request* message.

Step 3: When a RN receives K_{Relay} and encryption algorithm from the *relay request* message. The RN can use the received information and C-RNTI of target eNB to reproduce K_{Relay_enc}. This is used the data encryption key between the UE and RN.

Step 4: $RN \overset{response}{\Longrightarrow} UE$: The RN reply *relay response* message, which contains the C-RNTI of target cell information, to the UE.

Step 5: 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 5 for a scenario of the secure relay-assisted handover.

C. Secure relay-assisted handover protocol for PMIPv6

This section describes the secure relay-assisted handover protocol for PMIPv6 and the message flow is illustrated in Fig. 6.

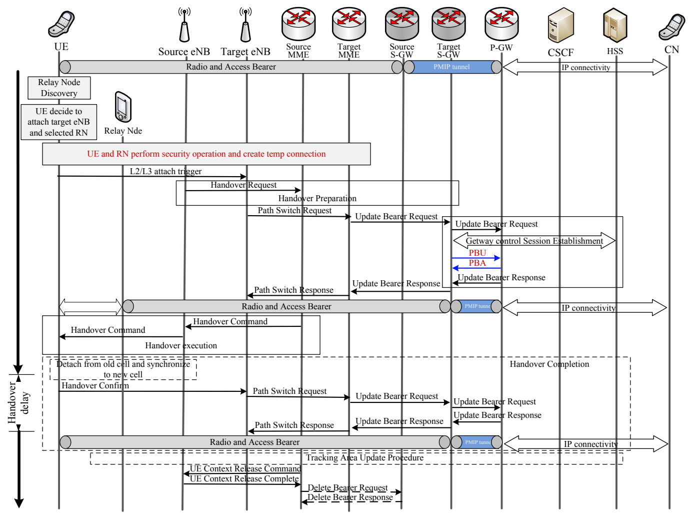


Fig. 6. Message flow of RN_PMIPv6 protocol.

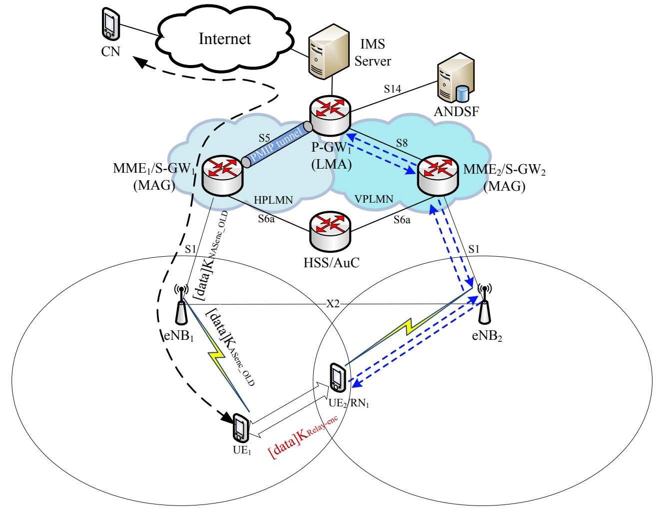


Fig. 7. UE pre-performs the proxy binding update.

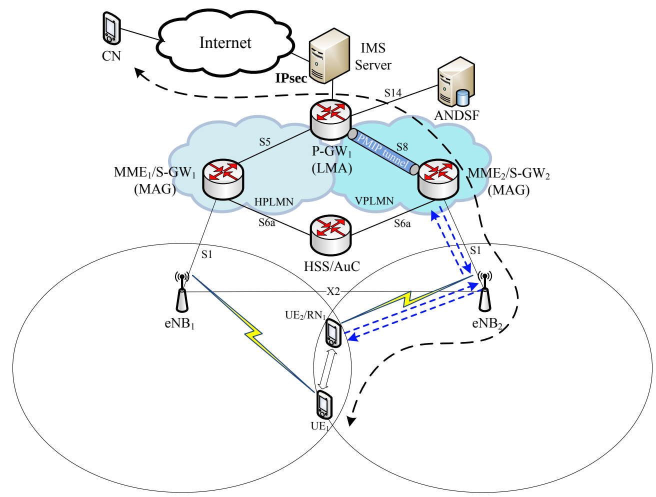


Fig. 8. UE setups a temporary connection with RN.

Step 1: $UE \overset{action}{\Longrightarrow} ANDSF^+$: This relay node discovery operation is performed and described in Section III.A. 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.

Step 2: $UE \overset{action}{\Longrightarrow} RN$: This security handover procedure is performed and introduced in Section III.B. When UE selects the RN for the pre-handover, UE must establish a secure UE-RN connection.

Step 3: $Source\ eNB \overset{action}{\Longrightarrow} target\ S\text{-}GW$: This 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.

Step 4: $Target\ eNB \overset{PBU}{\Longrightarrow} P\text{-}GW$: This 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.

Step 5: $UE \overset{handover}{\Longrightarrow} target\ MME$: This 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.

Step 6: $UE \overset{switch}{\Longrightarrow} PDN\ Gateway$: This 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.

Step 7: $UE \overset{TAU}{\Longrightarrow} HSS$: This 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.

Fig. 7 shows that the UE establishes the secure UE-RN connection. Fig. 8 illustrates that the UE setups a temporary connection with RN.

IV. Performance Evaluation

To evaluate our RN_PMIPv6 protocol, PMIPv6 [6], SP-MIPv6 [7] in 3GPP LTE systems, all of these protocols are mainly implemented using the network simulator-2 (ns-2) [1] with PMIPv6 module [4] and eurane module [5]. Observe that the eurane module is the HSDPA module, and we modify eurane module to simulate the 3GPP LTE environment in our simulation. Fig. 9 shows the mobility scenario for our simulation. To simplify the scenario, each eNB is also the

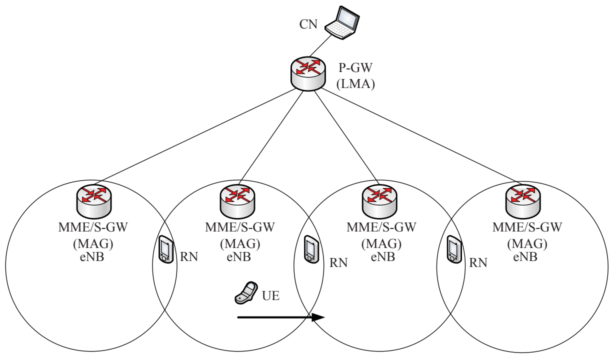


Fig. 9. The handover scenario.

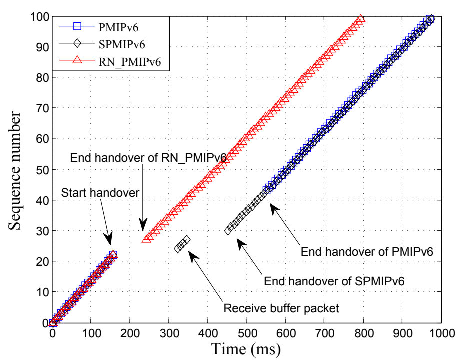
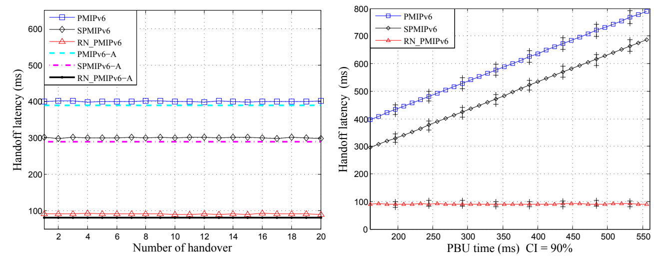


Fig. 10. Performance of sequence number vs. time.

mobility access gateway. The transmission range and the link bandwidth of all eNB are assumed to be 50km and 100 Mbps. A cbr (udp) traffic application between CN to UE is 0.01 second intervals in our simulation. The performance metrics to be observed are:

- *Handover latency***:** 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***:** The packet loss counts from the UE disconnecting to serving eNB to receiving new packets from the target eNB.
- *Handover jitter***:** 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***:** The location update cost is the total number of signal messages for a UE roaming from the serving eNB to the target eNB.

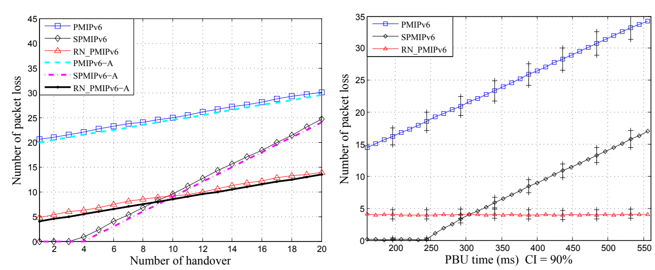
1) Handover latency: Fig. 10 initially illustrates the sequence number vs. time for PMIPv6, seamless PMIPv6 and RN_PMIPv6 protocols, respectively. In our RN_PMIPv6, due to the pre-handover procedure is performed by RN, the UE can ask RN through the target eNB to execute the proxy binding update and security procedure. Obviously, the handoff delay can be significantly reduced. Fig. 10 shows that the UE initiates the handoff procedure is at 160 ms and the handoff completion time of RN_PMIPv6, SPMIPv6, and PMIPv6 protocols are at 250 ms, 295ms, and 390ms, respectively. Therefore, our RN_PMIPv6 protocol outperforms SPMIPv6 and PMIPv6 protocols.



(a) (b)

Fig. 11. Performance of handover latency vs. (a) number of handover and (b) proxy binding update time.

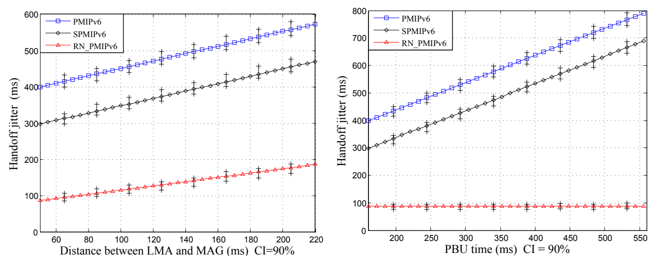
Fig. 11(a) illustrates the handover latency vs. the number of handover. We observed that the handover latency of PMIPv6 $<$ that of SPMIPv6 $<$ that of RN_PMIPv6. Fig. 11(b) illustrates the handover latency vs. the proxy binding update time. In general, the higher the proxy binding update time is, the higher the handover latency will be for PMIPv6 and SPMIPv6. We also observed that the handover latency of PMIPv6 $<$ that of SPMIPv6 $<$ that of RN_PMIPv6. This implies that the handover latency of RN_PMIPv6 is lower than that of PMIPv6 and SPMIPv6.



(a) (b)

Fig. 12. Performance of packet loss ratio vs. (a) distance between LMA and MAG and (b) proxy binding update time.

2) Packet loss: Fig. 12(a) illustrates the number of packet loss vs. the number of handover. The number of packet loss of PMIPv6 is higher than that of RN_PMIPv6 and SPMIPv6. In addition, the number of packet loss of RN_PMIPv6 is higher than that of SPMIPv6 when the number of handover is larger than 9. Fig. 12(b) illustrates the packet loss vs. the proxy binding update time. The number of packet loss of PMIPv6 is higher than that of RN_PMIPv6 and SPMIPv6. In addition, the number of packet loss of RN_PMIPv6 is higher than that of SPMIPv6 when he proxy binding update time is larger than 300. This is because that SPMIPv6 uses the extra hardware cost (memory buffer) to reduce the number of packet loss. This verifies that the number of packet loss of RN_PMIPv6 is better than that of SPMIPv6 and PMIPv6.



(a) (b)

Fig. 13. Performance of handover jitter vs. (a) distance between LMA and MAG and (b) proxy binding update time.

3) Handover jitter: Fig. 13(a) and Fig. 13(b) illustrate the handover jitter vs. the distance between LMA and MAG, and PBU time. In general, the handover jitter increases as the distance between LMA and MAG increases. The curve of the handover jitter of PMIPv6 $>$ that of SPMIPv6 $>$ that of RN_PMIPv6. Our RN_PMIPv6 has the better result of the handover jitter.

4) Location update cost: Fig. 14 illustrates the location update cost vs. call to mobility ratio. The the location update cost drops as the call to mobility ratio increases. The curve of the location update cost of PMIPv6 $<$ that of SPMIPv6 $<$ that of RN_PMIPv6. This shows that our RN_PMIPv6 protocol offers slightly higher the location update cost than SPMIPv6 and PMIPv6.

V. Conclusions

In this paper, we present a new protocol to reduce handoff delay and packet lost with the assistance of relay nodes over LTE networks. We 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 illustrated that our proposed protocol actually achieves the performance improvements in the handoff delay time and the packet loss rate.

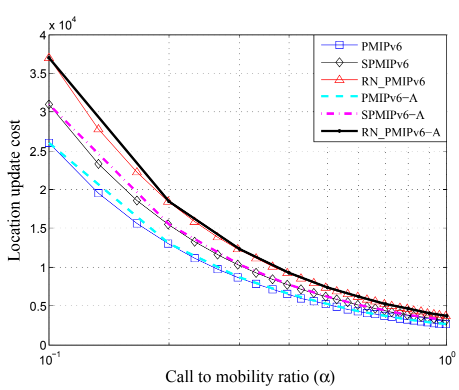


Fig. 14. Performance of location update cost vs. call to mobility ratio.

VI. Acknowledgments

This research was supported by the National Science Council of the R.O.C. under grants NSC-97-2219-E-305-001, NSC-97-2221-E-305-003-MY3, and NSC-98-2219-E-305-001.

References

[1] The Network Simulator NS-2., http://www.isi.edu/nsnam/ns/.

[2] Y.-S. Chen, W.-H. Hsiao, and K.-L. Chiu. ”Cross-Layer Partner-Based Fast Handoff Mechanism for IEEE 802.11 Wireless Networks”. *International Journal of Communication Systems*, 2009.

[3] Y.-S. Chen and K.-L. Wu. ”A Cross-Layer Partner-Assisted Handoff Scheme for Hierarchical Mobile IPv6 in IEEE 802.16e Systems”. *Wireless Communications and Mobile Computing*, 2009.

[4] H. Choi. ”Proxy Mobile IPv6 for Ns-2”. *http://commani.net/pmip6ns/*.

[5] T. I. for Wireless and M. Communications. ”Enhanced UMTS Radio Access Network Extensions for NS-2 (EURANE)”. *http://eurane.ti-wmc.nl/eurane/*.

[6] S. Gundavelli. ”Proxy Mobile IPv6”. *Internet Engineering Task Force* (*IETF*), *RFC-5213*, 2008.

[7] J. Kang, D. Kum, Y. Li, and Y. Cho. ”Seamless Handover Scheme for Proxy Mobile IPv6”. *IEEE International Conference on Wireless and Mobile Computing*, (WIMOB), Washigton, DC, USA, pp. 410-414, October 2008.

[8] L. Le and M. Liebsch. ”Preliminary Binding: An Extension to Proxy Mobile IPv6 for Inter-Technology Handover”. *IEEE International Conference on Wireless Communications and Networking Conference*, (WCNC), Budapest, Hungary, pp. 1-6, April 2009.