A Relay-assisted Handover Pre-authentication Protocol in the LTE Advanced Network

Ling Tie
The Department of Information Science and Technique
The Chengdu University
Chengdu, Sichuan, China
tlcd4579@gmail.com

Di He
The Department of Electronic Engineering
The Shanghai Jiaotong University
Shanghai, China
dihe@sjtu.edu.cn

***Abstract*—With the help of relaying, The Long Term Evolution Advanced network is improved on the coverage and capacity. But relaying concept brings many problems on handover management. In this paper, a relay node is introduced in the system structure. We extend the handover procedure to support relaying and transmit security context. We design a relay assisted handover pre-authentication protocol, which happened before the mobile node handovers to the target cell. This article focuses on formal analysis of our proposed security protocol. Finally, an improved strand space and ideal formal analysis method, which includes message authentication code, is introduced. We use it to prove that our proposed protocol can meet the security and authentication proprieties.**

Keywords- Long Term Evolution; relay; handover; security; strand space; ideal

I. INTRODUCTION

The Long Term Evolution Advanced network (LTE-A) is considered as one of the main standards for the 4th generation broadband wireless network. Recently, due to the increasing demand for high transport rate and capacity, the relaying concept is introduced. The implementation of relay can overcome the restriction of coverage, especially at the cellular boundary. With the help of relay node (RN) located at the overlap between two adjacent cells, the user equipment (UE) being served by a source cell can pre-handover to the target cell. The handover interrupt rate and delay will be reduced significantly.

There are many papers have talked about handover schemes happened in the relay LTE-A network. In [1], five relay handover scenarios are categorized in multi-hop cellular network (MCN). Several handover frameworks for relay enhanced LTE Network are introduced in [2]. Some relay handover procedures supporting centralized and decentralized relaying are illustrates. But，these articles do not discuss security and authentication issues.

In the 3GPP draft 36.300 [3], a Relay Node (RN) is connected to an evolution Node B (eNB) wirelessly. The eNB serving the RN is called Donor eNB (DeNB). The Draft 36.300 gives an end-to-end authentication and key agreement (AKA) procedure when the RN first attaches to the LTE. The 3GPP draft 33.816 [4] proposes many solutions that support LTE relay node security. But，these standards do not discuss pre-handover authentication issue.

In this paper, a relay-assisted handover pre-authentication protocol is provided. The UE, RN and Target DeNB authenticate mutually before handover occurs. This protocol will reduce the handover delay significantly. But, this paper focuses on only formal analysis of our proposed security protocol. The performance of our proposed protocol will be discussed in future works.

The rest of the paper is organized as follows. The system architecture is given in Section II. In Section III, the proposed relay assisted handover authentication protocol is presented. The extended strand space is introduced in Section IV. The security is proved using this strand space model. Section V gives a brief introduction of the performance improvement. Section VI concludes this paper.

II. SYSTEM STRUCTURE

The system architecture of the proposed scheme is illustrated in Figure1. During the UE handovers from cell 1 to cell 2, the signal strength between the UE and the sourcing DeNB decreases. When the signal strength falls below certain threshold, handover will happen. However, the UE still remain in the source cellular. The UE will try to find one RN located at the coverage area between the source DeNB and the target DeNB. The RN helps the UE to pre-authentication to the target DeNB.

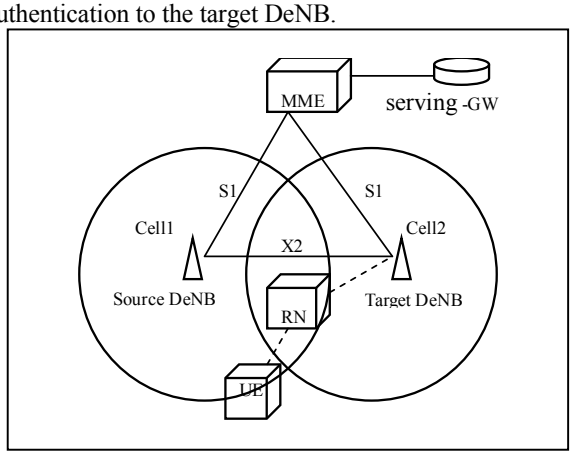

Figure 1. Relay handover structure

The LTE-A consists of the following major components:

- User Equipment (UE): It is mobile host.

 ISBN: 978-1-61208-186-1

- Relay Network (RN): It provides multi-hop Wireless connectivity from the UE to the Target DeNB.
- Donor eNB (DeNB): It is an eNB serving the RN.

III. RELAY ASSISTED HANDVER PRE-AUTHENTCAITON PROTOCOL

A. Notations

Before we describe the relay assisted pre-authentication protocol, we will specify some of notations used in the protocol, as shown in Table I.

TABLE I. NOTATIONS

symbol	Explanation
k_X	The Key known by the X
$MAC(k_X, h)$	Message authentication code produced by k_X
$\{h\}_{k_X}$	The message is encrypted by the key k_X
N_X	The nonce value produced by X
ID_X	The identification of X
$\|\|$	Concatenation
$KDF(k_X, h)$	Security key produce function by k_X

B. Handover Key Hierarchy

According to the 3GPP draft 33.816 [4], the calculation of k^*_{eNB} and $k_{\mathrm{Re}lay}$ is based on the key hierarchy in Figure 2. The k_{eNB} is achieved from traditional AKA authentication method defined in the draft 33.401 [5].The handover key k^*_{eNB} is produced according to the method published in the draft 33.401 .The relay key is calculated as in (1).

$$k_{\mathrm{Re}lay} = \mathrm{KDF}\,(k_{eNB} \,||\, \mathrm{SSID}_{\mathrm{relay}}) \quad (1)$$

C. Relay Assisted Handover Procedure

Figure 3 shows the relay assisted pre-handover procedure. This procedure is based on [2]. We extended this procedure to include the calculation and transmission of security key. All the handover messages are protected by the key in Figure 2.

The Steps are as follows:

Step 1: The RN sends the measurement control message to the UE.

Step 2: The UE sends the measurement report message to the RN and forward it to the Source DeNB.

Step 3: Based on the measurement report, the Source DeNB makes RN handover decision. If RN handover is allowed, the source DeNB initiates the handover process. The source DeNB will calculate k^*_{eNB} as the handover key for the target DeNB[5]. It can also produce the key $k_{\mathrm{Re}lay}$ for the RN.

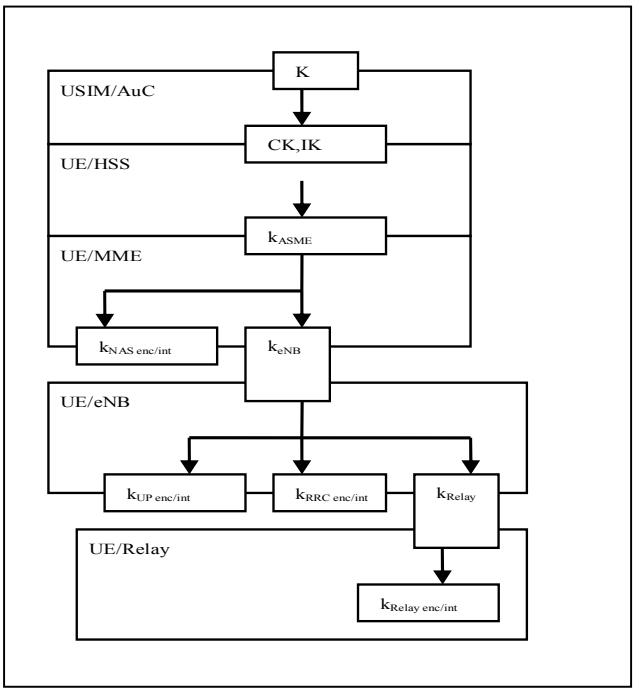

Figure 2. Handover key hierarchy

Step 4: The source DeNB sends the handover request message to the Target DeNB. This message includes k^*_{eNB} and $k_{\mathrm{Re}lay}$, which are protected by the RRC key.

Step 5: The target DeNB accepts the handover request message.

Step 6: After completing admission control, the target DeNB sends the handover request acknowledge message to the source DeNB.

Step 7: The source DeNB sends the handover command message to the RN securely. This message includes $k_{\mathrm{Re}lay}$ for the RN.

Step 8: The RN receives the handover command message and $k_{\mathrm{Re}lay}$ for the RN. It sends the handover command message to the UE, which includes Relay SSID.

Step 9: The UE uses information received from the handover command message to create k^*_{eNB}. It calculates $k_{\mathrm{Re}lay}$ simultaneously. Now，the UE has keys k^*_{eNB} and $k_{\mathrm{Re}lay}$.

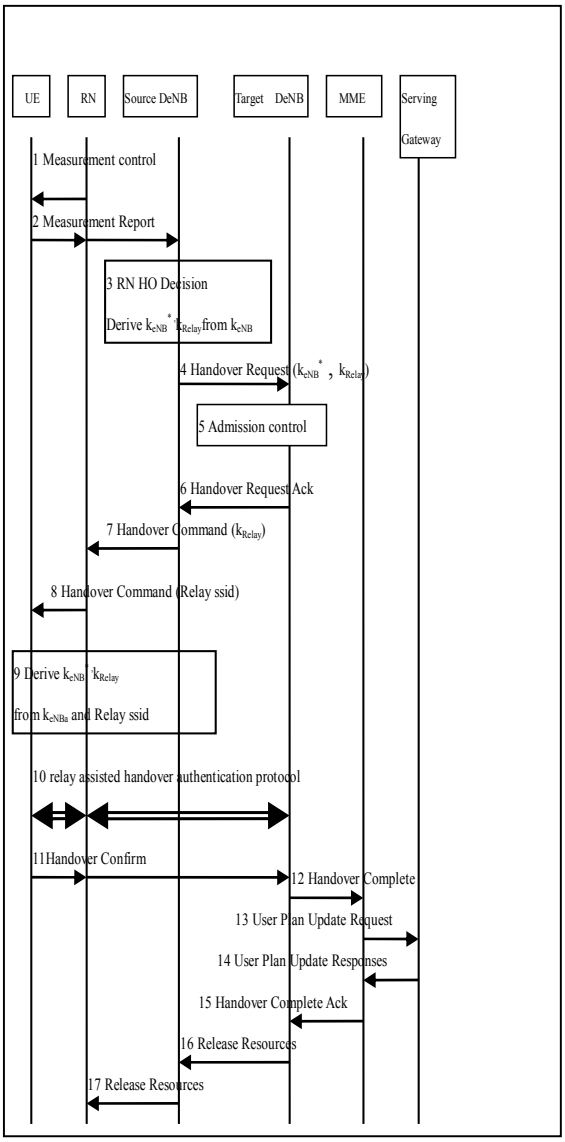

Figure 3. Relay-assisted handover Pre-authentication Sequence

Step 10: The UE achieves relay-assisted handover pre-authentication with the Target DeNB through the RN.

Step 11: The UE sends the handover confirm message to the RN and forward it to the Target DeNB.

Step 12: The Target DeNB sends the handover complete message to the MME.

Step 13: The MME sends the user plan update Request message to the Serving GW.

Step 14: The Serving GW sends the user plan update Response message to The MME.

Step 15: The MME sends the handover complete Ack message to the Target DeNB.

Step 16: The Target DeNB sends the release resource message to the Source DeNB

Step 17: The Source DeNB sends the release resource message to the RN.

D. Relay Assisted Handover Pre-authetication Protocol

In this section, a detailed description of our proposed pre-authentication protocol is given. It is the step 10 in figure 3. The extension of the step 10 sequence in Figure 3 is showed in Figure 4.

Step10. 1: When the UE still remain in the cell 1, it begins the pre-authentication procedure, with the help of RN. The UE sends the relay handover authentication request message to the RN. The UE generates two nonces. $N2_{UE}$ is used for RN, the other $N1_{UE}$ is used for Target DeNB. The nonce is encrypted by the key known only by the RN and the Target DeNB. The UE calculates the message authentication code (MAC) of the RN and the Target DeNB.

Step 10.2: Upon receiving the relay authentication request message, the RN decrypts the message and verifies the MAC using the key k_{Relay}. If the verifications succeed, the RN authenticates the UE.The RN produces a nonce $N1_{RN}$ and generates the MAC using the key k_{Relay} .The nonce and the identification of the relay are encrypted using the key k_{Relay} . Then the RN sends a Target authentication request message to the Target DeNB.

Step 10.3: When this message reaches the Target DeNB, the Target DeNB carries out the same MAC computation. If the verification is correct. The Target DeNB will successfully authenticate the UE and the Relay. The Target DeNB produces two nonces, $N1_T$ and $N2_T$. The Target DeNB constructs Target authentication response messages include the session key k_{U-T} as in (2) share between the UE and Target DeNB and the key k_{R-T} as in (3) share between the RN and Target DeNB. The Target DeNB uses the MAC algorithm to produce two message authentication codes for the RN and the UE.

$$k_{U-T} = \text{KDF}(k_{eNB}^*, N1_T, N1_{UE}+1, ID_T, ID_{UE}) \quad (2)$$

$$k_{R-T} = \text{KDF}(k_{Relay}, N1_{RN}+1, N2_T, ID_{RN}, ID_T) \quad (3)$$

Step 10.4: The RN receives the Target authentication response message and uses the key k_{relay} to decrypt the k_{R-T} as in (3). The RN verifies the MAC and authenticates the Target DeNB. Then, it calculates the key k_{U-R} as in (4) between the UE and RN. Then it adds the MAC of the UE into the

relay authentication response message and sends it to the UE.

k_{U-R} =KDF ($k_{\mathrm{Re}lay}$, N2$_{\mathrm{Relay}}$, N2$_{\mathrm{UE}}$+1, ID$_{\mathrm{RN}}$, D$_{\mathrm{UE}}$) (4)

Step 10.5: The UE receives the relay authentication message and decrypts k_{U-T} and k_{U-R} .The UE uses the same MAC algorithm to authenticate the RN and Target DeNB.

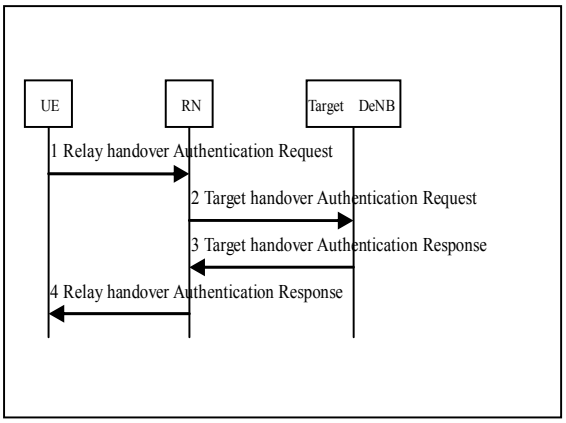

Figure 4. Relay assisted handover pre-authentication protocol

The protocol described in detail below:

UE →RN:

$\{N1_{UE}, ID_{UE}\}_{k^*_{eNB}}, MAC(k^*_{eNB}, N1_{UE} \| ID_{UE})$,

$\{N2_{UE}, ID_{UE}\}_{k_{\mathrm{Re}lay}}, MAC(k_{\mathrm{Re}lay}, N2_{UE} \| ID_{UE})$

RN →Target DeNB:

$\{N1_{UE}, ID_{UE}\}_{k^*_{eNB}}$, $MAC(k^*_{eNB}, N1_{UE} \| ID_{UE})$,

$\{N1_{RN}, N2_{UE}, ID_{UE}, ID_{RN}\}_{k_{\mathrm{Re}lay}}$,

$MAC(k_{\mathrm{Re}lay}, N1_{RN} \| N2_{UE} \| ID_{RN} \| ID_{UE})$

Target DeNB → RN:

$\{k_{U-T}, N1_T, N1_{UE}+1, ID_T, ID_{UE}\}_{k^*_{eNB}}$,

$MAC(k^*_{eNB}, K_{U-T} \| N1_T \| N1_{UE}+1 \| ID_T \| ID_{UE})$

$, \{k_{R-T}, N1_{RN}+1, N2_T, ID_{RN}, ID_T, ID_{UE}\}_{k_{\mathrm{Re}lay}}$,

$MAC(k_{\mathrm{Re}lay}, k_{R-T} \| N1_{RN}+1 \| N2_T$

$\| ID_{RN} \| ID_T \| ID_{UE})$

RN→UE:

$\{k_{U-T}, N1_T, N1_{UE}+1, ID_T, ID_{UE}\}_{k^*_{eNB}}$,

$MAC(k^*_{eNB}, K_{U-T} \| N1_T \| N1_{UE}+1 \| ID_T \| ID_{UE})$,

$\{k_{U-R}, N2_{RN}, N2_{UE}+1, ID_{RN}, ID_{UE}, ID_T\}_{k_{\mathrm{Re}lay}}$,

$MAC(k_{\mathrm{Re}lay}, k_{U-R} \| N2_{RN} \| N2_{UE}+1$

$\| ID_{RN} \| ID_{UE} \| ID_T)$

This protocol happens before the UE handovers to the target cell. Due to space limitations, we do not discuss the performance of the proposed protocol. This paper will pay more attention on security formal analysis.

IV. SECURITY FORMAL ANALYSIS

In this section, we will use strand space formal analysis method to prove that our protocol is secure. Although strand space method [6] is efficient, there are some shortcomings. We extend strand space to include message authentication code (MAC) item.

A. Extend Strand Space

We define the set A of terms. The element in A is the information exchanged among subjects. In particular, we will assume:

- A set T of texts (represent the atomic messages) $T \subset A$.
- A set of cryptographic keys K disjoint from T . $K \subset A$.
- A unary operator $inv : K \to K$.
- Three binary operators

$$encr : K \times A \to A$$
$$join : A \times A \to A$$
$$MAC : K' \times A \to A$$

As usual, we will write $inv(K)$ as K^{-1}, $encr(K, m)$ as $\{m\}_K$, and $join(a, b)$ as ab .

We redefine axioms as follows.

Axiom 1: for $m, m' \in A$ and $k_1, k_2 \in K$, $k_1', k_2' \in K$

If $\{m\}_{k_1} = \{m'\}_{k_2}$ then $m = m'$ and $k_1 = k_2$;

If $MAC(k_1', m) = MAC(k_2', m)$ then $m = m'$ and $k_1' = k_2'$.

Axiom 2: for $m_0, m_0', m_1, m_1' \in A$, and $k, k' \in K$

(1) $m_0 m_1 = m_0' m_1' \Rightarrow m_0 = m_1' \wedge m_1 = m_1'$

(2) $m_0 m_1 \neq \{m_0'\}_{k'}$

(3) $m_0 m_1 \notin K \cup T$

(4) $\{m_0'\}_k \notin K \cup T$

(5) $m_0 m_1 \neq MAC(k', m_0')$

(6) $MAC(k', m_0') \notin K \cup T$

We extend it to include MAC item according to [7].

Definition 1 A strand space is a set $\sum$ with a trace mapping tr : $\sum \to (\pm A)^*$.

Definition 2 A penetrator trace is one of the following:

M. Text message :< +t>, where $t \in T$

F. Flushing :<-g>

T. Tee : <-g,+g,+g>

G. Concatenation : <-g,-h, +gh>

S. Separating into components:<-gh, +g,+h>

K. Key :< +k>, where $k \in K_P$

E. Encryption: <-k,-h, + $\{h\}_k$ >

D. Deception : <-k,-h. - $\{h\}_k$,+h>

MAC . Message authentication code:

<-k',-h, $MAC(k',h)$ >

Definition 3 Let C be a set of edges, and let N_C be the set of nodes incident with any edge in C . C is bundle if :

(1). C is finite.

(2). If $n_1 \in N_C$ and $term(n_1)$ is negative, then there is a unique n_2 such that $n_2 \rightarrow n_1 \in N_C$.

(3). If $n_1 \in N_C$ and $n_2 \Rightarrow n_1$ then $n_2 \Rightarrow n_1 \in N_C$.

(4). C is acyclic.

Definition 4 If C is a bundle and $s \in \sum$, then the C height of s , denoted C- $height(s)$, is the largest $i \le length(tr(s))$, such that $s \in \sum$ and $\langle s, i \in C \rangle$

Definition 5 An infiltrated strand space is a pair $\langle \sum, P \rangle$ with $\sum$ a strand space and $P \in \sum$ such that $tr(p)$ is a penetrator trace for all $p \in P$

Definition 6 The sub-term relation $\sqsubset$ is defined Inductively, so that:

(1) $a \sqsubset t$ for $t \in T$ iff $a = t$

(2) $a \sqsubset k$ for $k \in K$ iff $a = k$

(3) $a \sqsubset \{g\}_k$ iff $a \sqsubset g$ or $a = \{g\}_k$

(4) $a \sqsubset gh$ iff $a \sqsubset h$, $a \sqsubset g$ or $a = gh$

(5) $a \sqsubset MAC(k',g)$ iff $a \sqsubset g$ or $a = MAC(k',g)$

We redefine the ideal and honest idea [8] including the MAC.

Definition 7 If $\kappa \subseteq K$, a κ -ideal of A is a subset I of A such that for all $h \in I$, $g \in A$ and $k \in \kappa$

(1) $gh, hg \in I$

(2) $\{h\}_k \in I$

(3) $MAC(k',h) \in I$

The smallest κ - ideal containing h is denoted $I_\kappa[h]$.

Definition 8 h is a sub-term of g , written $h \sqsubset g$, defined as $g \in I_\kappa[h]$.

Proposition 1 $\sqsubset$ is a transitive ,reflextive relation .

More over ,if $h, g \in A$ and $k, k' \in K$, then

(1) $h \sqsubset h\ g$ and $g \sqsubset g\ h$

(2) $h \sqsubset \{h\}_k$

(3) $h \sqsubset MAC(k',h)$

Definition 9 If $S \subseteq A$ $I_\kappa[S]$ is the smallest κ - ideal containing S .

Definition 10 Support $\kappa \subseteq K$. $s \in A$ is a κ - subterm of $t \in A$, written $s \sqsubset_\kappa t$ iff $t \in I_\kappa[s]$

Proposition 2 if $S \subseteq A$, $I_\kappa[S] = \cup_{x \in S} I_\kappa[x]$

Lemma 1 Let $S_0 = S$,

$$S_{i+1} = \{\{g\}_k, MAC(k',g) : g \in I_\phi[S_i], g \in I_\phi[S_i], k, k' \in \kappa\}$$

then $I_\kappa[S] = \cup_i I_\phi[S_i]$

Proposition 3 Suppose $S \subseteq A$, and every $s \in S$ is simple .If $gh \in I_\kappa[S]$ then either $g \in I_\kappa[S]$ or $h \in I_\kappa[S]$

Proposition 4 Suppose $k, k' \in K$; $S \subseteq A$, and for every $s \in S$, s is simple and is not of the form $\{g\}_k$ or $MAC(k',g)$.

if $\{h\}_k \in I_\kappa[S]$ or $MAC(k',h) \in I_\kappa[S]$,then $h \in I_\kappa[S]$.

Lemma 2 Suppose $k_1' \neq k_2'$, and

$MAC(k_1', h_1) \sqsubset MAC(k_2', h_2)$,

Then $MAC(k_1', h_1) \sqsubset h_2$

Proposition 5 Suppose $k, k' \in K$, $S \subseteq A$,and every $s \in S$ is simple and is not of the form $MAC(k',h)$ or $\{h\}_k$ .If $MAC(k',h) \in I_\kappa[S]$ or $\{h\}_k \in I_\kappa[S]$, then $k \in \kappa$ or $k' \in \kappa$.

Proposition 6 Suppose C is a bundle over A. If m is minimal in $\{m \in C : term(m) \in I\}$, then m is an entry point for I .

Definition 11 A set $I \subseteq A$ is honest relative to a bundle C if and only if whenever a penetrator node p is an entry point for I , p is an M node or a K node.

Theorem 1 Suppose C is a bundle over $A, S \subseteq T \cup K, \kappa \subseteq K, K \subseteq S \cup \kappa^{-1}$, Then $I_\kappa[S]$ is honest.

 ISBN: 978-1-61208-186-1

Corollary 1 Suppose C is a bundle, $\mathrm{K} \subseteq S \cup \kappa^{-1}$, and $S \cap \mathrm{K_P} = \phi$. If $term(m) \in I_\kappa[S]$ for some $m \in C$, then for some regular node $n \in C$, n is an entry point for $I_\kappa[S]$.

Corollary 2 Suppose C is a bundle, $\mathrm{K} \subseteq S \cup \kappa^{-1}$, $S \cap \mathrm{K_P} = \phi$, and no regular node $\in C$ is an entry point for $I_\kappa[S]$. Then any term of the form $\{g\}_k$ and $MAC(k', g)$ for $k, k' \in S$ does not originate on a penetrator strand.

B. The Bundle

We will use extended honest and ideal concept to prove the security of our proposed protocol. The goal of this protocol is to mutually authenticate hop-by-hop. The bundle of our proposal is shown in Figure. 5.

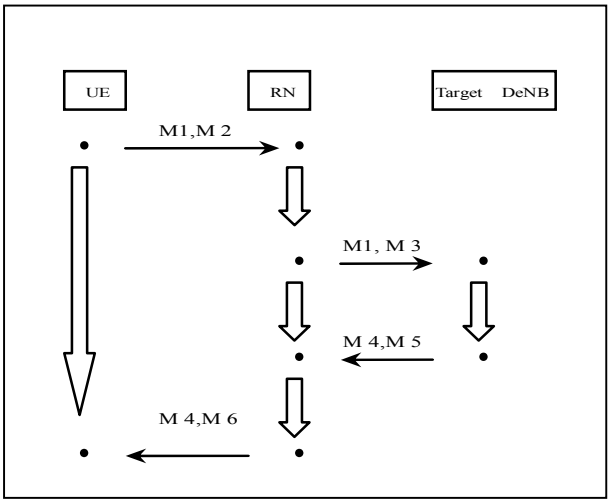

Figure 5. Our propose strand space

M1= $\{N1_{UE}, ID_{UE}\}_{k^*_{eNB}}$ $MAC(k^*_{eNB}, N1_{UE} \| ID_{UE})$

M2= $\{N2_{UE}, ID_{UE}\}_{k_{\mathrm{Re}lay}}$ $MAC(k_{\mathrm{Re}lay}, N2_{UE} \| ID_{UE})$

M3= $\{N1_{RN}, N2_{UE}, ID_{UE}, ID_{RN}\}_{k_{\mathrm{Re}lay}}$,

$MAC(k_{\mathrm{Re}lay}, N1_{RN} \| N2_{UE} \| ID_{RN} \| ID_{UE})$

M4= $\{k_{U-T}, N1_T, N1_{UE}+1, ID_T, ID_{UE}\}_{k^*_{eNB}}$

$MAC(k^*_{eNB}, K_{U-T} \| N1_T \| N1_{UE}+1 \| ID_T \| ID_{UE})$

M5= $\{k_{R-T}, N1_{RN}+1, N2_T, ID_{RN}, ID_T, ID_{UE}\}_{k_{\mathrm{Re}lay}}$

$MAC(k_{\mathrm{Re}lay}, k_{R-T} \| N1_{RN}+1 \| N2_T \|$

$ID_{RN} \| ID_T \| ID_{UE})$

M6= $\{k_{U-R}, N2_{RN}, N2_{UE}+1, ID_{RN}, ID_{UE}, ID_T\}_{k_{\mathrm{Re}lay}}$,

$MAC(k_{\mathrm{Re}lay}, k_{U-R} \| N2_{RN} \| N2_{UE}+1 \|$

$ID_{RN} \| ID_{UE} \| ID_T)$

Definition 12 An infiltrated strand space $(\sum, \mathrm{P})$ is a space if $\sum$ is the union of three kinds of strands:

(1) Penetrator's strand $s \in \mathrm{P}$;

(2) UE 's Strand

$s \in UE[N1_{UE}, N2_{UE}, N1_T, N2_{RN}, ID_{UE}, ID_T, ID_{RN}, k_{U-T}, k_{U-R}]$

with trace, defined to be:

$<+M1, +M2, -M4, -M6>$

(3) Relay's strand

$s \in RN[N2_{UE}, N2_T, N1_{RN}, N2_{RN}, ID_{UE}, ID_{RN}, ID_T, k_{R-T}, k_{U-R}, H, G]$

with trace, defined to be:

$<-H, -M2, +H, +M3, -G, -M5, +G, +M6>$

(4) Target DeNB's Strand

$s \in$ Target DeNB

$[k_{U-T}, k_{R-T}, N1_{UE}, N1_T, N2_T, N1_{RN}, ID_{UE}, ID_{RN}, ID_T, \mathrm{H}]$

with trace defined to be:

$<-H, -M3, +M4, +M5>$

For

$k_{U-T}, K_{R-T}, k_{U-R} \notin \mathrm{K_P}$

$k_{U-T}, K_{R-T}, k_{U-R} \notin \{k_{\mathrm{Re}lay}, k^*_{eNB}\}, k_x = k_x^{-1}$

Proposition 7 The set UE,RN and Target DeNB are disjoint each other.

C. Security Analysis

We first prove that session keys can not be disclosed unless penetrator posses one of the long term keys.

Theorem 2 suppose C is a bundle in strand space $\sum$, $RN \in T_{name}$, session key k_{R-T} are uniquely originating; $k_{R-T} \notin \mathrm{K_P}$; and $s \in \sum_{RN}$ has C - height 3. Let $S = \{k_{\mathrm{Re}lay}, k^*_{eNB}, k_{R-T}\}$ and $\kappa = \mathrm{K} \setminus S$ For every node $m \in C$, $term(m) \notin I_\kappa[k_{R-T}]$.

PROOF: By proposition 2, it suffices to prove that stronger statement that for every node m, $term(m) \notin I_\kappa[S]$. Since $S \cap \mathrm{K_P} = \phi$, $\kappa = \kappa^{-1}$, and $\mathrm{K} = \kappa \cup S$ by Corollary 1**,** It suffices to show that no regular node m is an entry point for $I_\kappa[S]$.

We will argue by contradiction and assume m is a regular node which is an entry point for $I_\kappa[S]$. Since m is an entry point for $I_\kappa[S]$, by the definitions, it follows that $term(m)$ is an element of $I_\kappa[S]$. By proposition 2, this implies that one of the keys $k_{\mathrm{Re}lay}, k^*_{eNB}, k_{R-T}$ is a sub term of $term(m)$. Now, no regular node contains any key $k_{\mathrm{Re}lay}, k^*_{eNB}$ as a sub-term. In fact, the only session keys which occur as sub-terms of $term(m)$ for m regular, are the session keys emanating from the Target DeNB. If m is a positive regular node on a strand s, then $k_{R-T} \sqsubset term(m)$ implies either:

(1) $s \in \sum_{Target\ DeNB}$ and $m = \langle s,2 \rangle$, in which case k_{R-T} is the session key;

(2) $s \in \sum_{RN}$ and $m = \langle s,3 \rangle$ $k_{R-T} \sqsubset H$

In case 2, m is not an entry point for $I_\kappa[S]$, because $H \sqsubset \langle s,1 \rangle$, which is a preceding negative node. So m is not entry point of $I_\kappa[S]$.

So consider case 1. By the unique origination of k_{R-T}, $s = S_{Target\ DeNB}$, so $term(m)$ = M5 or $term(m)$ =M4

By Proposition **3**, either

1) $\{k_{R-T}, N1_{RN}+1, N2_T, ID_{RN}, ID_T, ID_{UE}\}_{k_{\mathrm{Re}lay}} \in I_\kappa[S]$

2) $\{k_{U-T}, N1_T, N1_{UE}+1, ID_T, ID_{UE}\}_{k^*_{eNB}} \in I_\kappa[S]$

3) $MAC(k_{\mathrm{Re}lay}, k_{R-T} \| N1_{RN}+1 \| N2_T \| ID_{RN} \| ID_T \| ID_{UE}) \in I_\kappa[S]$

4) $MAC(k^*_{eNB}, K_{U-T} \| N1_T \| N1_{UE}+1 \| ID_T \| ID_{UE}) \in I_\kappa[S]$

But，the first and the second are impossible. The third and the fourth are impossible by Proposition 5.□

Similarly, we can prove that k_{U-T} and k_{U-R} are secure. So, we can conclude that session keys can not be disposed. Our protocol is secure.

D. Authetication Analysis

In this section we will prove the authentication guarantees to its UE, RN and Target DeNB.

Proposition 8 Consider a bundle C in $\sum$, Suppose $\mathrm{Target\ DeNB} \in T_{name}$ and $k^*_{eNB} \notin \mathrm{K_P}$. Then no term of the form $\{g\}_{k^*_{eNB}}, MAC(k^*_{eNB}, g)$ can originate on a penetrator node in C.

PROOF: Let $S = \{k^*_{eNB}\}$ and $\kappa = \mathrm{K}$. To apply **Corollary 2,** we must check that no regular node is an entry point for $I_\kappa[S]$, or equivalently, the k^*_{eNB} does not originate on any regular node.

A key originates on a regular node only if it is a session key k originating on a Target DeNB strand $s \in \sum_{Target\ DeNB}$. However, by the definition of $\sum_{Target\ DeNB}$, the session key k is never a long term key k^*_{eNB}.

Hence we may apply **Corollary 2** to $I_\kappa[S]$, so any term $\{g\}_{k^*_{eNB}}, MAC(k^*_{eNB}, g)$ can only originate on a regular node. □

Lemma 3 Consider a bundle C in $\sum$, Suppose $RN \in T_{name}$ and $k_{\mathrm{Re}layB} \notin \mathrm{K_P}$. Then no term of the form $\{g\}_{k_{\mathrm{Re}lay}}, MAC(k_{\mathrm{Re}lay}, g)$ can originate on a penetrator node in C.

Proposition 9

1) If $\{H\}_{k^*_{eNB}}$ originates on a regular strand s, then

If $s \in \sum_{Target\ DeNB}$,

then $H = k_{U-T} \| N1_T \| N1_{UE}+1 \| ID_T \| ID_{UE}$

and $k_{U-T} \in \kappa$

2) If $\{H\}_{k_{\mathrm{Re}lay}}$ originates on a regular strand s, then

If $s \in \sum_{Target\ DeNB}$ then

$H = k_{R-T} \| N2_T \| N1_{\mathrm{Re}lay}+1 \| ID_{\mathrm{Re}lay} \| ID_T \| ID_{UE}$

and $k_{R-T} \in \kappa$

If $s \in \sum_{RN}$ then

$H = k_{U-R} \| N2_{RN} \| N2_{UE}+1 \| ID_{RN} \| ID_{UE} \| ID_T$

and $k_{U-R} \in \kappa$

3) If $MAC(k^*_{eNB}, H)$ originates on a regular strand s then If $s \in \sum_{UE}$,then $H = N1_{UE} \| ID_{UE}$

If $s \in \sum_{Target\ DeNB}$,

then $H = k_{U-T} \| N1_T \| N1_{UE}+1 \| ID_{UE} \| ID_T$

4) If $MAC(k_{\mathrm{Re}lay}, H)$ originates on a regular strand s, then If $s \in \sum_{RN}$,

$H = N1_{RN} \| N2_{UE} \| ID_{UE} \| ID_{RN}$

Or

$H = k_{U-R} \| N2_{RN} \| N2_{UE} + 1 \| ID_{RN} \| ID_{UE} \| ID_T$

(5) If $MAC(k_{\mathrm{Re}lay}, H)$ originates on a regular strand s, then If $s \in \sum_{T\arg et\ DeNB}$ then

$H = k_{R-T} \| N2_T \| N1_{\mathrm{Re}lay} + 1 \| N2_{UE} + 1 \| ID_{\mathrm{Re}lay} \| ID_T \| ID_{UE}$

PROOF: By the definition of originating, if the term $\{H\}_k$ originates on m, then m is positive.

If $s \in \sum_{T\arg et\ DeNB}$ then $m = \langle s,2 \rangle$. Thus the encrypted subterm of $term(m)$ $\{k_{U-T}, N1_T, \| N1_{UE} + 1 \| ID_{UE} \| ID_T\}_{k^*_{eNB}}$ is of from (1)

If the term $MAC(k,H)$ originates on m, then m is positive. If $s \in \sum_{UE}$ then $m = \langle s,1 \rangle$. The subterm of this term is of the form (3).

If $s \in \sum_{RN}$, If the term $MAC(k,H)$ originates on m, then m is positive. Then the positive nodes of the s is $m = \langle s,3 \rangle$ and the sub-term of this term is of the form (4). □

Corollary 3 Suppose s is a regular strand of $\sum$

(1) IF $\{k_{U-T}, N1_T, N1_{UE} + 1, ID_{UE}, ID_T\}_{k^*_{eNB}}$ originates on s, then $s \in \sum_{T\arg et\ DeNB}$. The term originates on the node $\langle s,2 \rangle$ and k_{U-T} originates on s.

(2) If $\{k_{R-T}, N1_{RN} + 1, N2_T, ID_{RN}, ID_T, ID_{UE}\}_{k_{\mathrm{Re}lay}}$ originates on s, then $s \in \sum_{T\arg et\ DeNB}$. The term originates on the node $\langle s,2 \rangle$, and k_{R-T} originates on s.

(3) If $\{k_{U-R}, N2_{RN}, N2_{UE} + 1, ID_{RN}, ID_{UE}, ID_T\}_{k_{\mathrm{Re}lay}}$ originates on s, then $s \in \sum_{RN}$, the term originates on the node $\langle s,3 \rangle$ and k_{U-R} originates on s.

(4) If $\{N1_{UE}, ID_{UE}\}_{k^*_{eNB}}$ originates on s, then $s \in \sum_{UE}$, then the term $\{N1_{UE}, ID_{UE}\}_{k^*_{eNB}}$ originates on node $\langle s,1 \rangle$

(5) If $\{N2_{UE}, ID_{UE}\}_{k_{\mathrm{Re}lay}}$ originates on s, then $s \in \sum_{UE}$, $\{N2_{UE}, ID_{UE}\}_{k_{\mathrm{Re}lay}}$ originates on node $\langle s,1 \rangle$

(6) If $MAC(k^*_{eNB}, N1_{UE} \| ID_{UE})$ originates on s, then $s \in \sum_{UE}$, $MAC(k^*_{eNB}, N1_{UE} \| ID_{UE})$ originates on node $\langle s,1 \rangle$

(7) If $MAC(k_{\mathrm{Re}lay}, N2_{UE} \| ID_{UE}\}$ originates on s, then $s \in \sum_{UE}$ $MAC(k_{\mathrm{Re}lay}, N2_{UE} \| ID_{UE}\}$ originates on node $\langle s,1 \rangle$

(8) If $MAC(k_{\mathrm{Re}lay}, N1_{RN} \| N2_{UE} \| ID_{RN} \| ID_{UE})$ originates on s, then $s \in \sum_{RN}$ $MAC(k_{\mathrm{Re}lay}, N1_{RN} \| N2_{UE} \| ID_{RN} \| ID_{UE})$ origin ates on node $\langle s,2 \rangle$

(9) If $MAC(k_{\mathrm{Re}lay}, k_{R-T} \| N1_{RN} + 1 \| N2_T \| ID_{RN} \| ID_T \| ID_{UE})$ originates on s, then $s \in \sum_{T\arg et\ DeNB}$ $MAC(k_{\mathrm{Re}lay}, k_{R-T} \| N1_{RN} + 1 \| N2_T \| ID_{RN} \| ID_T \| ID_{UE})$ originates on $\langle s,2 \rangle$

If $MAC(k_{\mathrm{Re}lay}, k_{U-R} \| N2_{RN} \| N2_{UE} + 1 \| ID_{RN} \| ID_{UE} \| ID_T)$ originates on s, then $s \in \sum_{RN}$, the $MAC(k_{\mathrm{Re}lay}, k_{U-R} \| N2_{RN} \| N2_{UE} + 1 \| ID_{RN} \| ID_{UE} \| ID_T)$ originates on $\langle s,3 \rangle$.

PROOF: Since s is regular, $s \in \sum_{UE} \cup \sum_{RN} \cup \sum_{T\arg et\ DeNB}$ Apply proposition 9. □

The following theorem asserts that if a bundle contains a strand $s \in \sum_{UE}$ then under reasonable assumptions, there are regular strand $s \in \sum_{RN}$, $s \in \sum_{T\arg et\ DeNB}$, Which agrees on the UE, RN, Target DeNB

Theorem 3 Support C is a bundle in $\sum$; $UE \neq T\arg et\ DeNB \neq RN$; $N1_{UE}, N2_{UE}$ is uniquely originating in C; and $k^*_{eNB}, k_{\mathrm{Re}lay} \notin \mathrm{K_P}$ If $s \in \sum_{UE}$ has C - height 2, then there are regular strands :

(1) $s \in \sum_{RN}$ of height 3 at least

(2) $s \in \sum_{Target\ DeNB}$ of height 2

PROOF: According to the trace of $s \in \sum_{UE}$

Since $k^*_{eNB}, k_{Relay} \notin K_P$, by Lemma 3 $-M6$ originates on a regular node in C. By Corollary 3**,** this node belongs to a strand $s \in \sum_{RN}$ which has C - height 3 at least.

Since $k^*_{eNB}, k_{Relay} \notin K_P$, by Lemma 3, $-M4$ originates on a regular node in C. By Corollary 3, this node belongs to a strand $s \in \sum_{Target\ DeNB}$ which C - height 2. □

Theorem 4 Support C is a bundle in $\sum$; $UE \neq Target\ DeNB \neq RN$, $N1_{RN}, N2_{UE}, N1_{UE}$ are uniquely originating in C; and $k^*_{eNB}, k_{Relay} \notin K_P$ If $s \in \sum_{Target\ DeNB}$ has C- height 2, then there are regular strands :

(1) $s \in \sum_{RN}$ of height 2 at least

(2) $s \in \sum_{UE}$ of height 1 at least

PROOF: According to the trace of

$s \in \sum_{Target\ DeNB}$

Since $k^*_{eNB}, k_{Relay} \notin K_P$, by lemma 3, $-M3$ originates on a regular node in C. By Corollary 3 **,** this node belongs to a strand $s \in \sum_{RN}$ which C - height 2 at least.

Since $k^*_{eNB}, k_{Relay} \notin K_P$, by lemma 3 $-M1$ originates on a regular node in C By Corollary 3, this node belongs to a strand $s \in \sum_{UE}$ which C - height 1 at least. □

Theorem 5 Support C is a bundle in $\sum$; $UE \neq Target\ DeNB \neq RN$; $N2_{UE}, N1_{RN}, N1_T$ are uniquely originating in C; and $k_{Relay} \notin K_P$ If $s \in \sum_{RN}$ has C-height 3, then there are regular strands :

(1) $s \in \sum_{Target\ DeNB}$ of height 2

(2) $s \in \sum_{UE}$ of height 1 at least

PROOF: According to the trace of $s \in \sum_{RN}$

Since $k_{Relay} \notin K_P$, by lemma 3, $-M5$ originates on a regular node in C. By Corollary 3 , this node belongs to a strand $s \in \sum_{Target\ DeNB}$ with C - height 2. Since $k_{Relay} \notin K_P$, by lemma 3, $-M1$, originates on a regular node in C. By Corollary 3, this node belongsto a strand $s \in \sum_{UE}$ have height 1 at least. □

So we can conclude that UE, RN and Target deNB can authenticate each other.

V. PERFORMANCE EVALUATION

In this section, we will discuss the performance of our proposal scheme.

In the traditional handover scheme, the UE will tear down the connection with the Source eNB first. When the UE moves into the target cellular, it will establish the connection with the Target eNB. The handover messages are transmitted from the UE to the Source eNB, then to the MME and finally to the serving GW, as in figure 1. UE and Target eNB will finish end-to-end authentication using AKA protocol.

But , in the relay-assisted handover procedure, the handover messages are transmitted among the source DeNB, RN and Target DeNB. With the help of the RN, the handover information does not need to be transmitted on the S1 interface. The handover delay will be reduced significantly.

In our extended relay-assisted handover procedure, security keys are carried on the handover messages. They are protected by the RRC key. Some security keys are transmitted to the target DeNB and RN before the handover happens.

With the help of the RN, wireless connection is established among the UE, RN and the Target DeNB. Before the UE handovers to the target DeNB, Our proposed pre-authentication protocol can be executed among the UE, RN and Traget DeNB hop-by-hop. Because this protocol is happened before handover, the overhead is not calculated on handover delay. When the UE handovers to the target DeNB, it does not need to run the AKA protocol from scratch. The UE only needs to finish local authentication process with the target DeNB. The handover authentication delay will be reduced.

VI. CONCLUSION

Relaying is key technique in future LTE-A network. Relay node is introduced to extend coverage and capacity. In order to enable relaying, handover procedure, architecture and protocol have to be modified. This paper introduced a new relay assisted handover mechanism. Handover messages are exchanged among UE, RN and DeNB. We consider the security issue about the relay-assisted handover procedure. Before the UE moves into the target cellular, security contexts are transferred on the handover messages to the target cellular. With the aid of the relay nodes, the UE performs pre-authentication protocol when the UE still remain in the source cellular. The UE, RN and Target DeNB mutual authenticate using hop-by-hop communications. When the UE handovers to the target cellular, it does not need to perform end-to-end authentication from scratch. Handover authentication delay is reduced significantly. The security formal analysis is our main task. We also extend traditional strand space including message authentication

 ISBN: 978-1-61208-186-1

code. We use the extended ideal and honest idea to prove the security of our pre-authentication protocol. But, in this paper, we do not discuss the handover delay and loss rate. In future work, we will evaluate the overhead of our scheme using simulation and analytical methods.

ACKNOWLEDGMENT

This research work is supported by the National Natural Science Foundation of China (NSFC) under Grant No. 60802058, and the SMC young scholar sponsorship of Shanghai Jiao Tong University.

REFERENCES

[1] C. Sunghyun, E. W. Jang, and J. M. Cloffi, "Handover in multihop Cellular network," IEEE Communication Magzine, Vol. 47, pp. 529–551, July 2009.

[2] O. Teyeb, V. V. Phan, B. Raaf, and D. Redana, "Handover framework for relay enhanced LTE networks," IEEE International Conference on communications workshops, pp. 1–5, June 2009.

[3] The 3GPP draft 36.300, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[4] The 3GPP draft 33.816, "Feasibility Study on LTE Relay Node Security."

[5] The 3GPP draft 33.401 , "3GPP System Architecture Evolution (SAE); Security architecture."

[6] F. J. Thsyer Fabreqa, J. C. Herzog, and J. D. Guttman, "Strand spaces: Why is a Security Protocol Correct," proceedings of IEEE Symposium on security and Privacy, pp. 160-171, May 1998.

[7] Y. Li Li, P. Dai Yuan, and G. Yue Xiang, "Analysis and Improvement of Sensor Networks Security Protocol," Journal on Communications ,Vol . 32, No. 5, pp. 139–145, May 2011.

[8] F. J. Thayer Fabreqa, J. C. Herzog, and J. D. Guttman, "Strand Spaces: Honest Ideals on Strand spaces," Proceedings of the 11th IEEE Computer Security Foundations Workshop, pp. 66–77, June 1998.

,

 ISBN: 978-1-61208-186-1