Secure and Efficient Distributed Relay-Based Rekeying Algorithm for Group Communication in Mobile Multihop Relay Network

A. S. Khan

Network Research Group, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300 UNIMAS, Kota Samarahan, Sarawak, Malaysia.
skadnan@fit.unimas.my

***Abstract*:** In mobile multihop relay (MMR) networks, Relay multicast rekeying algorithm (RMRA) is meant to ensure secure multicast communication and selective updating of keys in MMR networks. However, in RMRA, the rekeying is carried out after a specific interval of time, which cannot ensure the security for multicast communication on joining the member. Secondly, the rekeying scheme generates a huge communication overhead on the serving multihop relay base station (MR-BS) on frequent joining of members. Lastly, there is nothing about when a member left the group communication. Thus, the rekeying scheme of RMRA fails to provide forward and backward secrecy and also is not scalable. To solve this problem, an improved rekeying scheme based on broadcasting a new seed value on joining and leaving of a member for updating the ongoing key management is proposed. The proposed scheme solves the issue of forward and backward secrecy and the scalability in a very simplified way. The forward and backward secrecy of the proposed scheme has been extensively validated by formal method using rank theorem. Furthermore, mathematical derivation showed that the proposed scheme out-performed the RMRA in terms of communication cost and complexity.

***Keywords*:** Relay multicast rekeying algorithm (RMRA), security in WiMAX, Mobile Multihop Relay, 4G networks, SEDRRA, Distributed Algorithms.

1. Introduction

Multicast services in MMR network is an efficient and power saving mechanism which also facilitates the subscribers with strong protection from theft of service by encrypting the broadcast connections within the subscribers, and the serving multihop relay base station (MR-BS). This strong protection is in the shape of confidentiality, authenticity and the integrity of messages delivered within the group members[1-3]. Security of these multicast communications usually depends on secure group communications, which require privacy for participants and access control at the multicast server. In order to ensure secure communication within the group, several secret keys must be shared and updated periodically in that group. MR-BS needs to unicast or broadcast the keys with specific period of time to maintain the key's secrecy and to ensure the secure communication [4]. The group communication can be compromised by any adversary through the compromised group members. The compromised group members may not necessarily be the part of group communication at the time of attack; it may be the member who left the group, and still they have the key with an active lifetime. Thus, security is a critical issue, especially for stock option bidding, pay per view TV broadcasting, and video conferencing kinds of application. Those emerging applications usually depend on secure group communications, which require privacy for participants and access control at the group communicator server [5].

For secure group communication, rekeying mechanism must be efficient enough that the leaving or joining member cannot derive the future and past shared keys i.e. maintain forward secrecy and backward secrecy respectively. However, most of the algorithms by providing these secrecies, they do not care the issue of scalability. Therefore, for a dynamic group in which the membership changes frequently, the rekeying algorithm is a critical factor in overall service efficiency; it should guarantee forward secrecy and backward secrecy; on the other hand, the rekeying algorithm should be scalable to a large group. The challenge of a secure multicast service in MMR networks is to provide an efficient rekeying method for controlling access to a group and its communications that can ensure the issues of secrecies and scalability [6, 7].

Secure group communication is one of the emerging topics in the recent network technologies. During the last ten years, several protocols have been proposed to counter the above challenges. For instance, the initial works for secure multicast and broadcast communication are [8-9]. Later, logical key hierarchy (LKH) [10, 11] and one-way function tree (OFT) [12] were proposed. Several other protocol were proposed based on OFT and LKH [11, 13-15]. However, all these schemes were centralized and have the issues of forward secrecy, backward secrecy and the scalability [15]. Group communication for WiMAX networks recently gained popularity, especially for MMR networks (e.g. smart grid applications) [16-18]. Multicast and broadcast rekeying algorithm (MBRA) is the primary scheme proposed by the standard to ensure the secure group communication in single hop networks [4, 19]. However, several analyses [1, 5, 20-22] showed that the scheme fails to provide the main group communication properties, i.e. forward secrecy, backward secrecy and the scalability. To address the above issues, ELAPSE (Efficient sub-Linear rekeying Algorithm with Perfect Secrecy) has been proposed [1, 5, 23]. ELAPSE

is proposed to counter the weaknesses of MBRA, i.e. forward secrecy, backward secrecy and the scalability. It can be visualized that no doubt the ELAPSE can successfully counter the MBRA issues but still the scheme is not scalable as when the group increases, number of unicast and multicast increases, and even if the member of groups increases, the unicast and multicast messages increases. Secondly, if applied to multihop, the complexity in terms of communication costs will be increased [7]. Thus, the scheme is not suitable for the scenarios where nodes join and leave frequently at multihop networks.

In [24], layered group key management scheme was illustrated; this scheme had the capabilities to counter the forward secrecy and the backward secrecy and has the capabilities to work for mobile multihop WiMAX networks. However, the protocol is complex and less scalable [25]. RMRA is proposed by the standard to ensure the group communication and to enhance the scalability as the scheme works for mobile multihop relay networks [4, 20]. However, analysis shows that the scheme no doubt ensures secure group communication and enhances the network coverage, but the scheme fails to address the issues of forward secrecy and backward secrecy, and also the scheme is centralized, which means still all the joining and leaving members needs to works under the supervision of MR-BS [26]. This scheme is derivative of MBRA for multihop networks. Thus, the scheme is not suitable for dynamic traffic networks, where frequent nodes join or leave the networks [5, 21].

Thus, based on above discussion, it can conclude that literature on secure multicast and broadcast algorithm are very scares for MMR networks having three security features, i.e. forward secrecy, backward secrecy and the scalability under one roof. So, a rekeying algorithm is needed that can fulfill the security requirements of the emerging relay based networks. In this paper, we proposed secure and efficient distributed relay based rekeying algorithm (SEDRRA) to ensure the secrecy properties in a fewer complex and scalable way. In this paper, the comparison is carried out with the baseline protocol i.e. RMRA as up till now there is no other protocol proposed. To the author knowledge, this is the first time very extensive and exhaustive work has been done in this research area.

The rest of the paper is organized as follows. The next section describes the network model and problem formulations. Section 3 demonstrates the proposed SEDRRA rekeying protocol. Section 4 discusses the performance study through formal analysis. Section 5 discusses the performance study through mathematical analysis. In final section, we conclude the paper.

2. Network Model and Problem Formulation

2.1 MMR network model

Figure 1 shows the considered MMR network model for group communication. The network model consists of MR-BS and non-transparent relay stations (N-RS) [27-29]. These N-RS works as decode and forward and has the capabilities to generate the relevant secure group keys. In this model, several N-RSs join together to form a group. These groups can be at single hop or at multihop. For the single and multihop, MR-BS and N-RS is responsible for initiating and managing the group communication respectively. For group communication, two different kinds of keys are used: group key encryption key (GKEK) and group traffic encryption key (GTEK). GTEK is used to encrypt/decrypt the group communication, while, GKEK is used to encrypt/decrypt the GTEK. A Lifetime is specified for both the keys, thus the keys will expire after specific period of time. Normally, N-RS may get the initial GTEK by using key-request and key-response messages.

MR-BS and N-RS updates and distributes these keys using two different key update command messages: GKEK update mode and GTEK update mode. Intermittently, MR-BS unicast the key update command message for GKEK update mode to each N-RS in each group. The message contains the new GKEK encrypted with the key encrypted key (KEK), which is derived from the authorization key (AK) established during authentication procedures. Later, MR-BS multicast the key update command message for GTEK update mode, which contains the recent GTEK encrypted with the corresponding GKEK. The complete protocol can be specified as follow:

MR-BS------- N-RS: $(GKEK)_{KEK}$
MR-BS------- N-RS: $(GTEK)_{GKEK}$

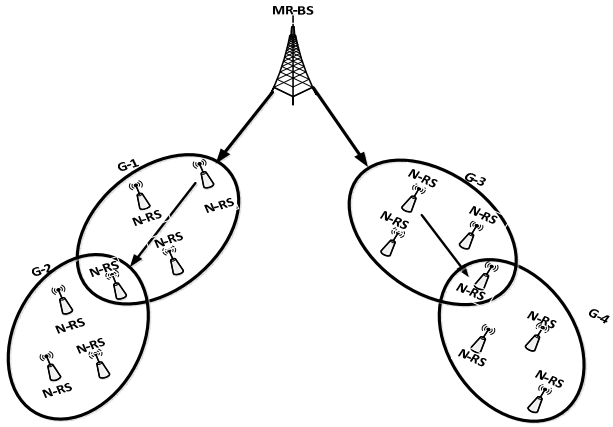


Figure 1. Network model

2.2 Problem formulation

Group communication is carried out using a traditional method of sending the key request and receiving the key response messages. However, critical issues arise once it comes to the matter of rekeying of an algorithm. Rekeying algorithm must be competent enough to deal with the problem of forward secrecy, backward secrecy and the scalability. MBRA, ELAPSE and the RMRA had been proposed to counter the above secrecy issues. MBRA and ELAPSE is for single hop while RMRA is for MMR networks. However, MBRA and RMRA have been proposed by the MMR WiMAX networks standard [4]. If we evaluate MBRA and RMRA, it can be seen that two problems with these protocol exists. Firstly, these protocols are not scalable as they still need to unicast to each

N-RS, and any rekeying algorithm depending on unicast methods is not scalable. Secondly, these protocols do not address the issue of backward and forward secrecy. In the case of member joining, when a new member receives the current GTEK, it can decrypt all previous messages that were multicast during the lifetime of the same GTEK. In the case of member leaving, there is nothing in this protocol that prevents a leaving SS from receiving the next GKEK and decrypting the next GTEK.

In ELAPSE, they use the concept of sub- grouping SS so that the GKEK will not be maintained via unicasting to individual SS, but via broadcasting to sub- groups. During the joining of a member, ELAPSE have the case of multi-joins, and during the multi-joins, the GTEK is not updated immediately, so there is sometimes where the joining member can guess the previous keys thus can limit the capabilities of backward secrecy. The scheme runs in O (log n) message complexity. But this is also not scalable for large value of n, and the scheme cannot be implemented for the multihop networks [7].

In this paper, SEDRRA, an alternative to the MBRA, ELAPSE and the RMRA, is proposed. SEDRRA is more efficient alternatives that ensure forward secrecy and backward secrecy. The proposed scheme had less communication cost thus is scalable. The proposed scheme can be applied to any MMR networks, especially LTE-A, smart grid communication and the MMR WiMAX networks. However, this scheme is validated based on MMR WiMAX networks.

3. Proposed SEDRRA Rekeying Protocol

To countermeasure the above-mentioned flaws, SEDRRA for secure multicast and broadcast services is proposed. This proposed scheme provides backward secrecy and forward secrecy in a very powerful way with a very less complex environment. SEDRRA protocol is illustrated in figure 2.

$$N-RS_i \rightarrow MR-BS : |R_{MR-BS}||R_{N-RS}|AKID|SAID$$

$$MR-BS \rightarrow N-RS_i : |R_{MR-BS}||R_{N-RS}|GKEK|LIFETIME$$

$$N-RS_i \rightarrow MR-BS : [GKEK_{x+i}]^u_{KEK_i}$$

$$MR-BS \rightarrow N-RS_i : [GTEK_{x+j}]^b_{GKEK_{x+i}}$$

$$MR-BS \rightarrow N-RS_i : [S^p]^b_{GTEK_{x+j}}$$

Where 'u' stands for unicast, 'b' stands for broadcast, 'p', 'i' & 'j' are the integer

Figure 2. SEDRRA protocol

According to this protocol, N-RS first send the key request for GKEK and GTEK by transmitting random numbers, AK and SAID. In response, MR-BS transmits with GKEK, GTEK with their lifetimes. Once N-RS receives and installed these keys, it starts updating GKEK by sending Group-Key-Update-Command (GKUC) for GKEK periodically for the expiration of its lifetime. However, to update the refreshed GTEK, MR-BS transmits GKUC for GTEK periodically before the expiration of its lifetime. At a single hop, if any new N-RS joins the group, MR-BS transmit GKEK encrypted by KEK to the requesting N- RS on unicast connection. Secondly, MR-BS broadcast new seed S^p for rekeying the existing rekeying scheme. This seed S^p is encrypted by the updated GTEK. Based on this seed, the entire participating member will update their rekeying scheme.

The detailed conceptual design for SEDRRA schemes in MMR WiMAX is shown in appendix A and the complete pseudo code for SEDRRA rekeying protocol is shown in figure 3. When any N-RS needs to initiate the multicast and broadcast services, it will send the key request for GKEK and GTEK from MR-BS. MR-BS will respond with the keys and their lifetimes using key response message.

Once N-RS achieved the traffic keying parameters from MR-BS, it needs to update GKEK. This updating is one-way, i.e. the client N-RS need to update the GKEK periodically as they previously shared the valid AK.

```
Algorithm 1: SEDRRA rekeying Algorithm

1  SEDRRA Protocol ( )
2  {
3   Snd key-request (GKEK & GTEK)
4   GET key-response (GKEK [KEK] & GTEK [GKEK])
5   If
6            GKEK or GTEK is near to expire
7            {
8            Snd GKUC-GKEK
9            GET GKUC-GTEK
10           }
11  Else if
12          GKEK or GTEK is expired
13           Resnd key-request (GKEK & GTEK)
14  }
```

Figure 3. Pseudo code for SEDRRA rekeying algorithm

Once GTEK life time approaches its maximum limit, GTEK Grace Time starts and causes MR-BS to transmit GKUC message for GTEK. This new GTEK is encrypted with the latest updated GKEK that was previously transmitted by the requesting N-RS. However, both updating is done through (GKUC) message using unicast connection. During these updating, if at any time, either N-RS cannot send the GKUC to update GKEK or received any GKUC to update GTEK from MR-BS, N-RS needs to send the key request again. This is due to the reason that, if MR-BS does not receive any GKUC message for GKEK from N-RS after specific period of time, it will remove N-RS from the list and consider as left the Group. At the Multihop level, any N-RS joins the group; it will follow the same procedure to attain the GKEK and GTEK with their lifetimes from the existing N-RS on unicast connection. Existing N-RS is now responsible to transmit GKUC message for GTEK on behalf of MR-BS. Existing N-RS will broadcast the seed S^{pi} for the participating member to rekey their existing

rekeying scheme. Later, all the members will update their keying table. Like above, at any time, if both entities N-RS_2 and N-RS_1 cannot send the GKUC to update their respective keys, N-RS_1 will remove all the credentials of N-RS_2 after the expiration of lifetimes from the list and consider as left the Group. N-RS_2 needs to send the key request again to make the service available.

3.1 Secrecy management

The detailed forward and backward secrecy management procedures for SEDRRA protocols are discussed in the following sub-sections.

3.1.1 Backward Secrecy Management

The figure 4 shows the complete pseudo code for backward secrecy-SEDRRA rekeying protocol. In the backward secrecy (BS) management, if any new member wants to avail the multicast services, it needs to follow the SEDRRA protocol to obtain the keying parameters.

```
Algorithm 2: BS-SEDRRA rekeying Algorithm
1    Backward Secrecy
2    {
3            //N-RS joins the Group
4    NewJoin ()
5    {
6    //single hop level
7    If (Hop==1)
8      {
9           Snd key-request (GKEK & GTEK)
10          Rec key-response ((GKEK [KEK] & GTEK
11   [GKEK])
12          Rec Seed
13          Update rekeying scheme
14          Initiate updating key
15     }
16   //Multihop Level
17   Else if
18   If (Hop > 1)
19     {
20          GET key-request (GKEK & GTEK)
21          Generate (GKEK [KEK (NRSx)] & GTEK
22   [GKEK])
23          Snd key-response with their lifetimes
24          Rec/Snd Seed
25          Update (rekeying)
26          updating keys
       }
     }
```

Figure 4. Pseudo code for BS-SEDRRA rekeying algorithm

Once it received keying parameters from the MR-BS, it needs to update GKEK periodically before the lifetime approaches maximum limits. Joining member intermittently transmits GKUC message to update GKEK. As long as joining member update GKEK periodically, both entities necessarily update their tables. Once the Grace Timeout value for GTEK approaches its maximum limits, the MR-BS will transmit GKUC message to update GTEK. This GTEK will be encrypted by the latest updated GKEK sent by the joining member. Thus joining member will decrypt GTEK with the latest GKEK from its table to continue availing the multicast and broadcast services. At a single hop, if any new N-RS joins the group, MR-BS transmit GKEK encrypted by KEK to the requesting N-RS on unicast connection. Secondly, MR-BS broadcast new seed S^p for rekeying the existing rekeying scheme. This seed S^p is encrypted by the updated GTEK. Based on this seed, the entire participating member will update their rekeying scheme. At the Multihop level, any N-RS joins the group; it will follow the same procedure to attain the GKEK and GTEK with their lifetimes from the existing N-RS on unicast connection. Existing N-RS is now responsible to transmit GKUC message for GTEK on behalf of MR-BS. Existing N-RS will broadcast the seed S^{pi} for the participating member to rekey their existing rekeying scheme. Later, all the members will update their keying table. Thus joining member cannot guess the past communication which shows that the SEDRRA protocol support backward secrecy.

3.1.2 Forward Secrecy Management

The figure 5 shows the complete pseudo code for forward secrecy-SEDRRA rekeying protocol.

```
Algorithm 3: FS-SEDRRA rekeying algorithm
1  Forward Secrecy
2  {
3     Relay Leave (N-RSy)
4     {
5     If
6       GKEK lifetime approaches its max. Limit
7       {
8         N-RS is expecting GKUC for GKEK
9       }
10   Else if
11     GKEK lifetime expired
12      {
13        Considered as Leave the Group
14         Removal of credential from the table
15        Rec/Snd Seed
16        Update (rekeying)
17        Updates table ( )
18                }
19          }
20   }
```

Figure 5. Pseudo code for FS-SEDRRA rekeying algorithm

In the forward secrecy (BS) management, it is assumed that any N-RS_y is already joined to the existing N-RS, and now it wants to leave the group. The reasons for leaving the group may be due to non-updating the keying parameters from either sides or intentionally leaving the group. Suppose, N-RS_y is leaving the group due to non-updating of keying parameters, at this moment, existing N-RS is expecting GKUC message for GKEK from N-RS_y. If there is no GKUC message within the GKEK lifetime, existing N-RS will wait until the GKEK

lifetime is expired. Once GKEK lifetime is expired and existing N-RS hasn't received any GKUC message, Group will remove all of its credential from the table and considered as left the group. Existing N-RS will broadcast the seed S^{pi} for the participating members to rekey their existing rekeying scheme. Later, all the members will update their keying table. Thus leaving member cannot guess the future communication which shows that the SEDRRA protocol support forward secrecy.

4. Formal Analysis

No doubt that group communication protocol intuitively claims the immunity against forward secrecy and backward secrecy, but the formal analysis and verification is one of the competent methods to analyze either the protocols really possess such secrecy properties. Normally, the formal analysis is meant to express the protocol as an algebraic theorem to verify the secrecy properties i.e. forward secrecy and backward secrecy of group communication in MMR WiMAX network. In order to utilize the theorem proving technique, the group communication protocols need to be modeled in the logical and formal way. In this paper, formal analysis based on rank theorem is carried out to analyze the possessiveness of secrecy properties in the proposed SEDRRA protocol as compared to the baseline RMRA group key protocol [30]. Both protocols are modeled and verified with respect to forward and backward secrecy.

4.1 Formal analysis of SEDRRA protocol

In this section, rank theorem based on formal technique is carried out to verify the secrecy properties of group key protocol. Rank theorem utilizes the rank function to map facts related to given protocol into ranks. This rank has positive, negative or zero value. The complete description can be found in [30].The initial step is to introduce the basic conceptual notations, which will be used to model and proof the proposed protocols. In the second step, proposed protocols will be precisely defined as well as modeled in a formal way with respect to the rank theorem and their secrecy property. The key purpose is to map the rank function between the set of facts with the sets of integers. The set of facts includes; the protocol events, protocol execution traces and the secrecy property.

4.2 Basic notations

Basic notations are given in Table 1.

Table 1. Basic notations

M	Sets of all possible messages that transmit and receive during the execution of group key protocols
U	a legitimate user
S	Sets of all secret messages, S ⊂ M. These messages are hidden from the adversary.
A	Adversary or intruder
E	Set of all possible events, (join or leave)
K_{Gt}	Group key generated for the current session. A ∉ Gt ⇒ $K_{Gt} \in$ S
K_{Gt+i}	Group key generated for the group G_{t+i} and is utilized at any time in the future, A ∉ G_{t+i} ⇒ $K_{Gt+i} \in$ S.
K_{Gt-i}	Group key generated and is utilized in past. A ∉ G_{t-i} ⇒ $K_{Gt-i} \in$ S.
T	Set of all possible traces,
K_0	Set of initial knowledge of the adversary, such that $K_0 \subset$ M. Thus there is no secret in this knowledge. Or it can be said that $\nexists_m \in$ M : $m \in$ S ⇒ $m = \notin K_0$
K	Set of knowledge of the adversary. The adversary upgrades this set by executing E. It starts with K_0 and E, and then by executing sequences of E, it upgrades this knowledge. $K_0 \subseteq$ K and K ⊆ M.
K_f	Set of knowledge of a user who was the member of the group in the past but currently neither he is not a member nor can he access to the secret keys of current group. Kf ∩ K = ∅.
K_b	Set of knowledge of a user who may be the prospective user in future. But currently he is neither a member not can access to the secret keys of current group. Kb ∩ K = ∅.
G_t	Current group,

4.3 Forward secrecy

Definition: For any current group G_t, and an adversary A, where A ∈ G_t and A knows K_{Gt}. If A compromised the $K_{GKEKx-i}$ of P_{Gt}, such that it follows the condition of current group session key, there will be not a single trace T that A can perform to attain the $K_{GKEKx-i}$ to decrypt $K_{GTEKxn-i}$ for G_t to access the future communication.

$$A \in G_t \Rightarrow \neg\exists\tau \in T: K_{GKEKx-i} = \tau(E, M) \quad \text{where } i > 0$$

This can be expressed as

$$\oint_{f\,(SEDRRA)} = \forall_m \in S, A \in G_t \Rightarrow \neg\exists\tau \in T: \tau\,(E, M) \rightarrow m$$

$$\oint_{f\,(SEDRRA)} \equiv (K \cup K_f) \cap S = \emptyset$$

Theorem: $\forall_m \in K, \rho_{\oint(m)} > 0 \Rightarrow Gt| = \oint_{f\,(SEDRRA),}$ Where $m = \tau(E, M)$ and $\tau \in T$

Assumption: $m \in K, \rho_{\oint}(m) = 0$

Proof:

$m \in K$ and $m \notin K_0$ (a)

$\forall_m \in M, m \in S \Rightarrow m \notin K_0$ (b)

$\forall_m \in M, m \notin K_0 \Rightarrow m \in S$ (c)

$m \in K_0 \Rightarrow \rho_{\oint}(m) > 0$ (d)

$m \notin K_0, m \in S \Rightarrow \rho_{\oint}(m) = 0$ (e)

$m \in S$ and $m \notin K_0 \Rightarrow \exists\tau \in T: \tau\,(E, M) \rightarrow m$ (f)

$\exists\tau \in T: \tau\,(E, M) \rightarrow m \Rightarrow \rho_{\oint}(m) = 0$ (g)

$\exists\tau \in T: \tau\,(E, M) \rightarrow m \Rightarrow m \in S$ (h)

By substituting the equation (h) in $\oint_{f(SEDRRA)}$

$\neg\,(\exists\tau \in T: \tau\,(E, M) \rightarrow m) \Rightarrow m \in S$

$\neg\,(m \in S) \Rightarrow m \in S$

$m \notin S \Rightarrow m \in S$

$\rho_{\oint}(m) = 0 \Rightarrow \neg\oint_{f(SEDRRA)}$

$\rho_{\oint}(m) = 0 \Rightarrow Gt| \neq \oint_{f(SEDRRA)}$

According to the theorem, for all the messages that belong to the set of knowledge of adversary, adversary upgrades this knowledge by executing events. The adversary initiates the updates by the primary set of knowledge K_0 and the events. By executing a series of events, adversary updates its knowledge. It can be said that ($K_0 \subseteq$ K and K ⊆ M). For the protocol to satisfy a forward secrecy property $\oint_f$, $Gt| = \oint_f$ protocol needs to maintain a positive rank for the messages generated by the adversary. This is due to the reason that according to the rank function rule, adversary primary knowledge must belong to positive rank. Secondly, only positive rank can be generated from positive ranks. It needs to be ensured that none of the legitimate participant should generate anything non-positive

rank to the system. To proof the theorem, it is assumed that there exist some messages that belong to the set of knowledge of adversary. Adversary sequentially upgrades this knowledge. Secondly, it is assumed that these messages belong to a zero rank. Zero rank messages belong to the set of secret messages that shared between the members and the servers. It also belongs to the set of all group keys that were generated from the previous group. If the forward secrecy property $\oint_{f(SEDRRA)}$ is correct for the SEDRRA protocol with these assumptions, which shows that Gt|= $\oint_f$ in this theorem. Thus for the SEDRRA protocol to hold the forward secrecy property $\oint_f$, need to be invalid with this assumptions so that Gt|= $\oint_f$.

According to equation (a) it is clear that zero rank cannot be generated by the primary knowledge of adversary. If a message belongs to an updated set of knowledge of adversary, then it is for sure not from the initial knowledge of the adversary. Based on equation (a), equation (b) can be deduced. It states that for all the messages that belong to the sets of all messages, if these messages belong to secret messages then for sure, it does not belong to the set of primary knowledge of adversary. Equation (d) shows that if the message belongs to primary knowledge of adversary, it must have positive rank. From equations (a-d) it can be deduced that if a message doesn't belongs to a primary knowledge of adversary, it must not have positive rank. Thus it has either zero rank or negative rank. According to the rank rule, a system cannot generate negative rank, which means that it is definitely zero rank as illustrated in equation (e). Thus from the equation (f) it can be seen that if the message belongs to the set of secret messages, which indicates that there are at least some traces exist, which basically belongs to all possible traces. Such that the message m is derived by the trace by executing the sets of events E on the sets of all possible messages M. By comparing equations (e) and (f) equation (g) can be obtained. If equation (h) is substituted in forward secrecy property $\oint_f$, it can be seen that with this assumption, forward secrecy is invalid for SEDRRA protocol. Hence, it is proved that SEDRRA protocol holds forward secrecy property $\oint_f$, Gt|= $\oint_f$.

4.4 Backward secrecy

Definition: for any current group G_t, and an adversary A, where A ∈ G_t and A knows K_{Gt}. If A compromised the $K_{GKEKx+i}$ of P_{Gt}, such that it follows the condition of current group session key, there will be not a single traces T that A can perform to attain the $K_{GKEKx+i}$ to decrypt $K_{GTEKxn+i}$ for G_t to access the future communication.

A ∈ G_t ⇒¬∃τ ∈ T: $K_{GKEKx+i}$ = τ(E, M) where i > 0

This can be expressed as

$\oint_f$ = ∀m ∈ S, A ∈ G_t ⇒¬∃τ ∈ T: τ (E, M) → m

$\oint_b$≡ (K∪ K_b) ∩ S = ∅

Theorem:

∀m ∈ K, $\rho_{\oint(m)} > 0$ ⇒ Gt|= $\oint_f$,

Where m = τ(E, M) and τ ∈T

Assumption:

m ∈ K, $\rho_{\oint}$ (m) = 0

The proof of the theorem is same as discussed in forward secrecy. Thus from the above analysis, it can be seen that the proposed SEDRRA protocol exhibits both secrecy properties, whereas the current RMRA scheme lacks these properties.

5. Mathematical Analysis

In this mathematical analysis, comparison of communication cost for both SEDRRA and RMRA rekeying schemes is derived. The communication cost of a single hop in MMR WiMAX network involves three types of communication procedures within the joining/leaving N-RS and MR-BS. The processes include key request and key response to and from MR-BS, GKUC for GKEK and GKUC for GTEK. To calculate the statistics of total messages, MR-BS will be taken as the point of reference i.e. the total of messages sent from MR-BS is used to gauge the efficiency.

During this mathematical analysis, it is assumed that

1. The total communication will be calculated during one group key session. One group session key will lasts until the key used to decrypt the multicast communication remains alive.
2. The lifetime of GKEK have six (6) iteration of update command or in case of RMRA it is six (6) iterations for GTEK. After this iteration, group session key will be updated and GKUC is distributed for the new group key session. This "6" iterations is taken as random.
3. Once relays are joined to any hop, it will remain joined for multihop and the messages are summed up for all hops.
4. At least six (6) relays join to each hop to calculate the communication cost at multihop level.

The number six (6) is taken as random

The total communication cost (c) can be defined by equation 1 discussed in [31]. The communication cost is calculated in terms of unicast and multicast messages when any member joins the group on per hop basis.

$$C = H\sum_{A=1}^{K} S_A \quad (1)$$

The total communication cost for single hop for proposed SEDRRA scheme is calculated using equation 2, where 'RJ' illustrates the relay join and '1' shows the number of relays join at a time. According to the protocol, if any member wants to join the group, one unicast message i.e. $GKEK_{[KEK]}$ and two broadcast messages as per the assumptions i.e. GKUC-$GTEK_{[GKEK]}$ and $S^p_{[GTEK]}$ are transmitted from MR-BS to joining member and group session respectively. Equations 3 and 4 shows the message required for the joining of two and n members respectively.

$$C_{Rj-1} = H(\sum_{A=1}^{K=1} S_{UNICAST} + \sum_{A=1}^{K=2} S_{MULTICAST}) \quad (2)$$

$$C_{Rj-2} = H(\sum_{A=1}^{K=1} S_{UNICAST} + \sum_{A=1}^{K=2} S_{MULTICAST}) \quad (3)$$

$$C_{Rj-n} = H(\sum_{A=1}^{K=n} S_{UNICAST} + \sum_{A=1}^{K=2} S_{MULTICAST}) \quad (4)$$

This is due to the reason that the GKEK is refreshed and updated by N-RS itself and GTEK is updated by MR-BS periodically. From equation 4, it can be seen that if 'n' number of members join the group, n numbers of unicast and two multicast message is required.

The total communication cost for two hops for proposed scheme is calculated using equations 5 to 7. As per the assumption, if any new member joins the groups at this hop, there will be no unicast while only one multicast message i.e. GKUC-GTEK $_{[GKEK]}$ is transmitted from the MR-BS. The reason for no unicast is the authentication protocol. As all the keys are managed by N-RS and according to SEDRRA protocol, GKUC for GKEK is transmitted by the joining members and GKUC for GTEK will be managed by the first joined N-RS.

$$C_{Rj-1} = H(\sum_{A=1}^{K=0} S_{UNICAST} + \sum_{A=1}^{K=1} S_{MULTICAST}) \quad (5)$$

$$C_{Rj-2} = H(\sum_{A=1}^{K=0} S_{UNICAST} + \sum_{A=1}^{K=1} S_{MULTICAST}) \quad (6)$$

$$C_{Rj-n} = H(\sum_{A=1}^{K=0} S_{UNICAST} + \sum_{A=1}^{K=1} S_{MULTICAST}) \quad (7)$$

Thus from equation 7, it can be concluded that if n number of member joins the group at two hop level, there will be no unicast while one multicast message will be transmitted from MR-BS as per cost calculation assumptions.

The total communication cost for three hops for proposed scheme is calculated using equation 8. Here if any new member joins the group, as per the assumption, there will be no unicast while only one multicast message i.e. GKUC-GTEK $_{[GKEK]}$ is transmitted from the MR-BS. Thus total message will remain the same i.e. one.

$$C_{Rj-1} = H(\sum_{A=1}^{K=0} S_{UNICAST} + \sum_{A=1}^{K=1} S_{MULTICAST}) \quad (8)$$

Thus from the above discussion, it can be conclude that the total message transmitted by MR-BS is given by equation 9

$$= \sum_{i=1}^{i=n} \left[(nj_{i(h(1))} + 2) + h \right] \quad (9)$$

where *nj*= node joins, Subscript *i* = number of nodes, Subscript (h) = number of hops. However, the communication cost for RMRA based on the same assumptions can be calculated using the equation 10 & 11. From equations, it can be analyzed that the total communication cost for the RMRA scheme depends on the total number of relays joining the group and the product of number of hops with the multicast messages in one hop. The proposed scheme depends on the number of relays joining the group in first hop only and the number of hops.

$$= [(nj_{i(1)} + 6)] + [(nj_{i(2)} + 6)] + [(nj_{i(3)} + 6)] + \ldots [(nj_{i(n)} + 6)] \quad (10)$$

$$= \sum_{i=1}^{i=n} (nj_{i(h)} + 6(h)) \quad (11)$$

Figure 6 illustrates the mathematical analysis of communication cost between the proposed and the existing group communication protocols.

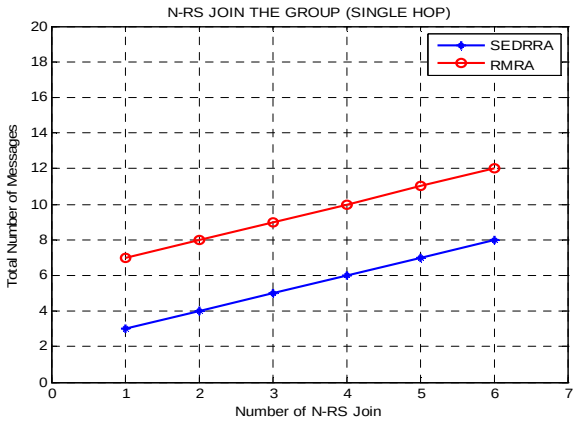


Figure 6. Messages required for N-RS joins (single hop)

It shows the effect of number of N-RS joins the group on message counts in a single hop. It is evident from the figure that if one N-RS joins the group, three and seven messages are required for SEDRRA and RMRA protocol respectively.

If six N-RS joins, it is eight and twelve messages respectively for SEDRRA and RMRA protocols. Thus, it can be concluded that for a single hop, the proposed scheme shows better performance by 33% as compared to RMRA.

Figure 7 depicts the communication cost for two hops. In this figure, if one N-RS joins the group, one and seven messages are required for SEDRRA and RMRA rekeying protocols respectively.

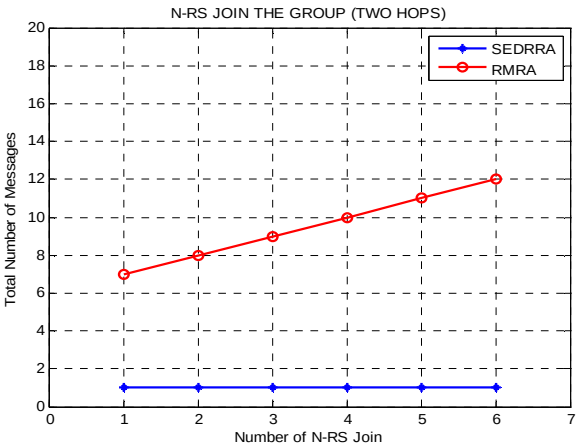


Figure 7. Messages required for N-RS joins (two hops)

However, as 6th N-RS joins, the total number of messages required for RMRA rose up to twelve but the message required by SEDRRA protocol remains stagnant. Thus from the above discussion, it can be concluded that SEDRRA scheme out-performed the RMRA by almost 90% in the second hop.

The same goes to Figure 8 when the communication cost for three hops is considered. According to the figure, SEDRRA performed 90% better then the RMRA scheme.

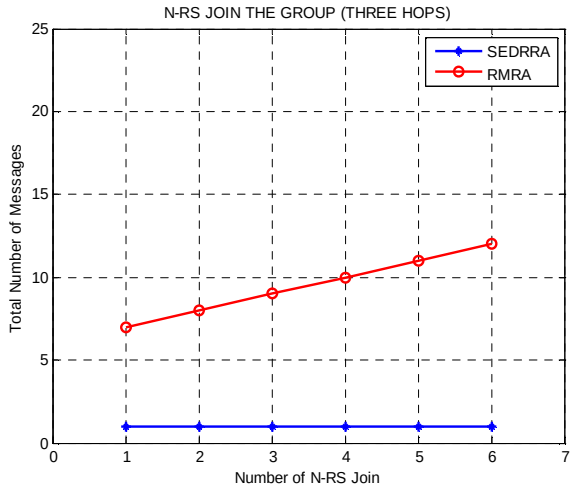


Figure 8. Messages required for N-RS joins (three hops)

Figure 9 shows the effect of N-RS joining in multihop level on the total message count. It can be seen that if one N-RS joins at a single hop, eight and twelve messages are required. However, it will remain stagnant at multihop level. As far as RMRA protocol is considered, in the second hop, there is a great slump and the total messages required decreased to one message and remain stagnant at multihop level.

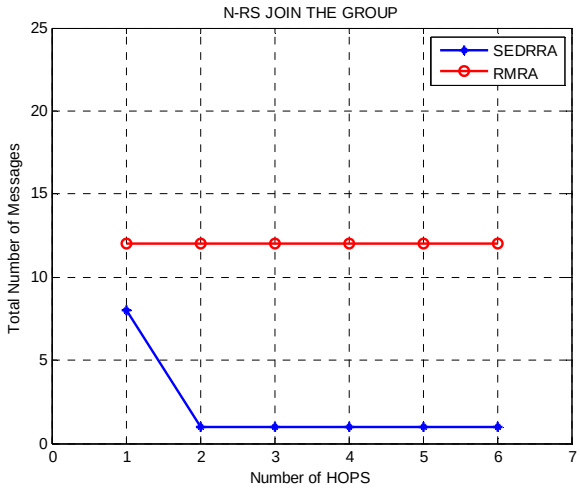


Figure 9. Messages required for multihop

If unicast and multicast messages are evaluated separately for SEDRRA and RMRA protocols, figure 10 shows a clear picture for both schemes. For the first hop, six unicast and two multicasts are required for SEDRRA scheme, when six N-RS joins the group. Later, these messages decrease to zero unicast and one multicast for the multihop.

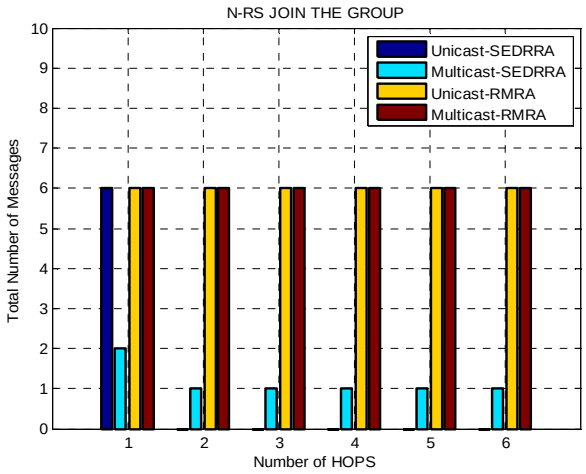


Figure 10. Unicast & multicast messages required for multihop

For RMRA scheme, in the first hop, six unicast and six multicast messages are required and it remains the same for the multihop level. Thus it is clear from the above discussion that the proposed scheme is better performed in terms of communication cost when compared to RMRA scheme.

From the mathematical analysis, it can be analyzed that for the proposed SEDRRA protocol in multihop environment constant number of unicast and one multicast is required for the rekeying group communication. On the other hand, the existing RMRA protocol, for the node join in multihop environment, linear unicast and multicast is needed for the rekeying of the group communication. Thus it can be seen that the proposed SEDRRA protocol performs well in terms of complexity when node joins in multihop environment. Table 2 illustrates the comparison of complexity of both protocols.

Table 2. Comparative analysis of MBS protocols

SCHEME	Node Join		F/S	B/S
	Unicast	Multicast		
RMRA	O(n)	O(n)	NO	NO
SEDRRA	O(1)	0	YES	YES

6. Conclusion

This paper presents the performance analysis of SEDRRA group communication protocol with the comparison of existing RMRA protocol. The performance analysis is carried out with the help of mathematical and formal analysis. Mathematical analysis is used to analyze the communication costs and the complexity of the protocols while formal analysis using rank theorem is used to analyze the possessiveness of the forward and backward secrecy property of the protocols. SEDRRA protocol enhances the previous work by [2] in order to achieve

minimum communication cost in terms of unicast and multicast messages when N-RS joins or leave the Group. In general finding concludes that SEDRRA protocol utilizes less number of messages when relays join the group communication in multihop environment. When comparing to RMRA, SEDRRA protocol out-performed by 33% for single hop and 90% for the second and third hop respectively. In terms of unicast and multicast messages, SEDRRA requires O (1) unicast and one multicast in multihop environment when relays joins the MBS group communication. While, RMRA requires linear O(n) unicast and multicast in the same environment. Formal analysis using rank theorem proved that SEDRRA protocols holds forward and backward secrecy while existing RMRA protocol lacks these secrecy property. Thus, from the three different aspects, the proposed SEDRRA protocol out-performed the existing RMRA protocols. The proposed scheme can be used in LTE-Advanced and smart grid communication applications.

7. Acknowledgement

Special Thanks to MIMOS CoE Universiti Teknologi Malaysia and RIMC Universiti Malaysia Sarawak for their Support.

References

[1] X. Sen, H. C. Tser, and M. Matthews, "Secure multicast in various scenarios of WirelessMAN," in Proceedings of IEEE SoutheastCon, Richmond, VA, pp. 709-714, 2007.

[2] J. Sen, "A Survey on Wireless Sensor Network Security, International Journal of Communication Networks and Information Security (IJCNIS)," Vol. 1, No. 2, pp.55-78, 2009

[3] J. Akpojaro, P. Aigbe and D. Oyemade, "Cost-Based Approach for Analysing the Overheads of Multicast Protocols in Non-Strictly Hierarchical Networks," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, pp. 67-73, 2011.

[4] M. Okuda, C. Zhu and D. Viorel, "Multihop Relay Extension for Wimax Networks Overview and Benefits of IEEE 802.16j Standard," FUJITSU Sci.Tech.J.," Vol. 44, No.3, pp. 292-302, 2008.

[5] S. Xu, C. T. Huang and M. M. Matthews, "Secure Multicast in Wimax," Journal of Networks, Vol. 3, N0. 2, pp. 48-57, 2008.

[6] G. Dini and M. Tiloca, "HISS: A highly scalable scheme for group rekeying," The Computer Journal, Vol. 56, No. 4, pp. 508-525, 2013.

[7] N. Meghanathan, B. Kaushik, D. Nagamalai, S. Chakraborty, S. Majumder, F. Barbhuiya, and S. Nandi, "A Scalable Rekeying Scheme for Secure Multicast in IEEE 802.16 Network," Advances in Networks and Communications, Vol. 132, Springer Berlin Heidelberg, pp. 472-481, 2011.

[8] S. Rafaeli and D. Hutchison, “A survey of key management for secure group communication,” ACM Computing Surveys, Vo. 35, No. 3, pp. 309-329, 2003.

[9] O. Pereira and J. Quisquater, "Some Attacks upon Authenticated Group Key Agreement Protocols," Journal of Computer Security, Vo. 11, No. 4, pp.555–580, 2004.

[10] C.T. Huang, M. Matthews, M. Ginley, X. Zheng, C. Chen and M. Chang, "Efficient and Secure Multicast in Wireless MAN: A Cross- Layer Design", Journal of Communications Software and Systems, Vol. 3, No. 3, pp. 199-206, 2007.

[11] H. Li, Z. G. Liu, L. J. Cheng, and Y. Hu, "A survey of group key management based on logical key hierarchy," Beijing Ligong Daxue Xuebao/Transaction of Beijing Institute of Technology, Vol. 31, pp. 547-551, 2011.

[12] Y. Zhang and W. Wang, "New group key management scheme based on keys tree, XOR operation and one-way function," Journal of Southeast University (English Edition), Vol. 22, No.1, pp. 54-58, 2006.

[13] S. Kumar, N. M. Purusothaman and S. Lavanya, "Design and performance analysis of scalable and efficient group key Management scheme [SEGKMS] for group communication in multicast networks," Life Science Journal, Vol. 10, pp. 1740-1749, 2013.

[14] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Transactions on Software Engineering, Vol. 29, No.5, pp. 444-458, 2003.

[15] M. Y. Malik, "Efficient Group Key Management Schemes for Multicast Dynamic Communication Systems," IACR Cryptology ePrint Archive, DOI: arXiv:1211.3502, p. 628, 2012.

[16] B. E. W. Abdollahpouri, "Multicast Gain for IPTV Transmission in WiMAX Multi-hop Relay Networks," Journal of Networks, Vol. 7, No.11, pp. 760-1772, 2012.

[17] L. Sun-Hwa, K. Young-il, and R. Won, "Dynamic MBS zone configuration mechanism for MCBCS over Mobile WiMAX," in the proceedings of 14th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang, Korea (South), pp. 287-290, 2012.

[18] P. Daegeun, K. Hanna, K. Youngil, and R. Won, "Performance analysis of multicast service using MBS region in mobile WiMAX system," in the proceedings of 15th International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Pyeong Chang, Korea (South), pp. 949-952, 2013.

[19] I. A. Gomaa, H. M. El-Badawy, and E. S. M. Saad, "Adoption of Delayed Feedback Rekeying Algorithm for secure multicast services during handover in mobile WiMAX networks," in the proceedings of IEEE International Conference on Information Theory and Information Security (ICITIS), High-Tech Mansion of BUPT Beijing, China, pp. 474-480, 2010.

[20] A.S.Khan, N. Fisal, S.Kamilah, R. A. Rashid, and M. Abbas, "Secure and Efficient Multicast Rekeying Approach For Non-Transparent Relay-Based IEEE 802.16 Networks," International Journal of Computer Applications, Vol. 16. No.4, pp. 1-7, 2011.

[21] C. Kolias, G. Kambourakis, and S. Gritzalis, "Attacks and Countermeasures on 802.16: Analysis and Assessment," IEEE Communications Surveys & Tutorials, Vol. 15, No.7, pp. 487-514, 2012.

[22] S. H. Min, C. S. Ying, C. S. Min, and C. C. Chien, "An Efficient Rekeying Scheme for Multicast and Broadcast in Mobile WiMAX," in the proceedings of IEEE Asia-Pacific Services Computing Conference (IEEE APSCC), Yilan, Taiwan, pp. 199-204, 2008.

[23] M. Ginley, X. Sen, H. C. Tser, and M. Matthews, "Efficient and Secure Multicast in WirelessMAN," in the proceedings of 2nd International Symposium on Wireless Pervasive Computing held at San Juan, Puerto Rico, pp-407-412, 2007.

[24] Y. W. Chen, J.T. Wang, K.H. Chi, and C. C. Tseng, "Group-Based Authentication and Key Agreement," Wireless Personal Communications, Vol. 62, No.4, pp. 965-979, 2012.

[25] S. H. Fengcai and Y. YANG, "Improved Multicast Security Mechanism in Multi-Hop WiMax Network," Journal of Computational Information Systems, Vol. 7, No.7, pp. 2496- 2503, 2011.

[26] J. H. Serrano, J. V. Campo and J. Pegueroles," Low-cost group rekeying for unattended wireless sensor networks," Wireless Networks, Vol. 19, pp. 47-67, 2013.

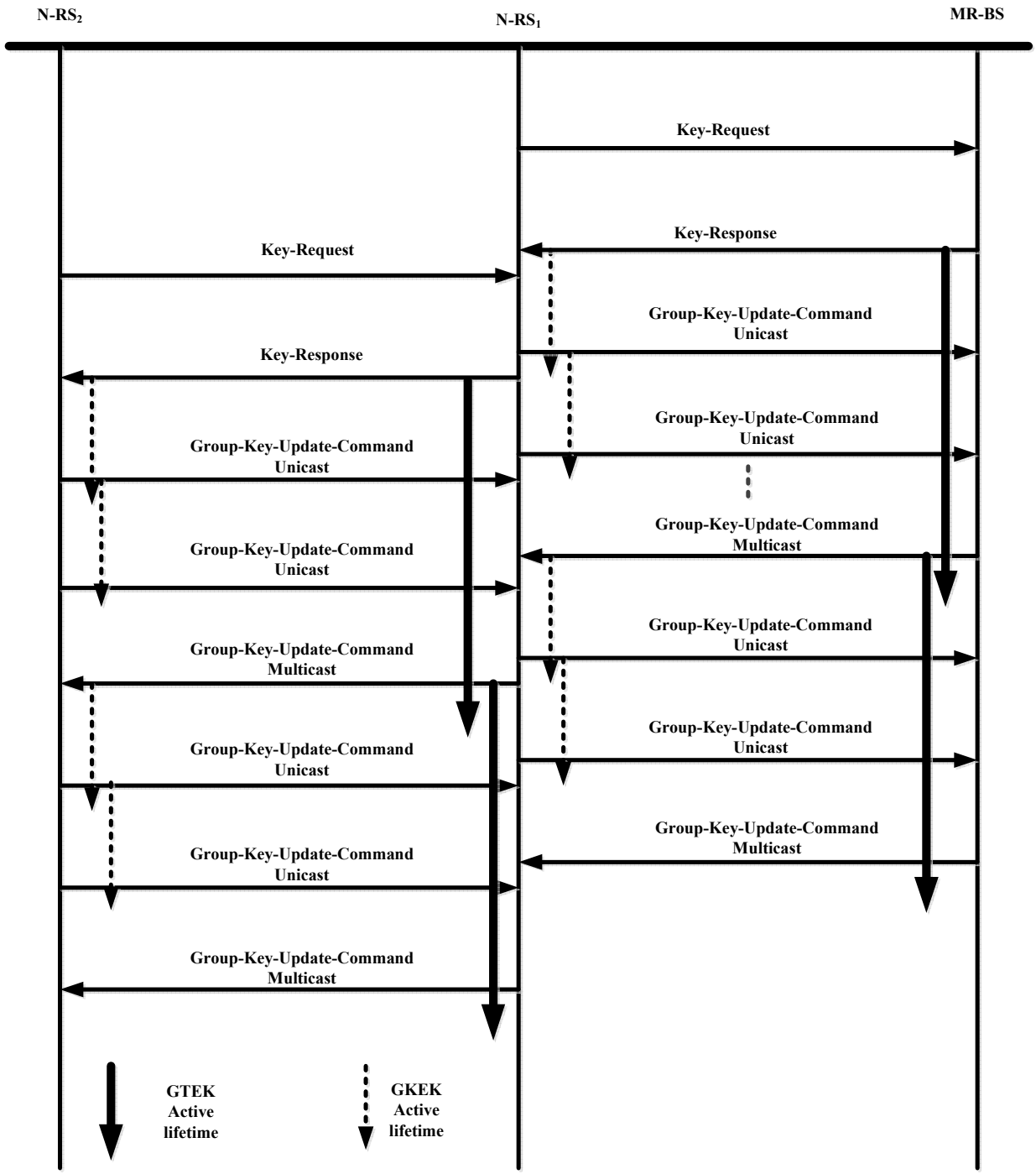
[27] A. S. Khan , N. Fisal , N.N.M.I. Maarof , F.E.I. Khalifa ,M. Abbas, "Security Issues and Modified Version of PKM Protocol in Non-transparent Multihop Relay in IEEE 802.16j Networks," International Review on Computers and Software, Vol. 6, No. 1, pp. 104-109, 2011.

[28] A. S. Khan**,** N. Fisal, M. Esa, S. Kamilah, S. Hafizah, M. Abbas "An Improved Authentication Key Management Scheme for Multihop Relay in IEEE 802.16m Networks," In Proceedings of 2010 IEEE Conference on Applied Electromagnetic, Port Dickson, Malaysia, pp. 11-12, 2010.

[29] A. S. Khan, N Fisal, Z. A. Bakar, N. Salawu, W. Maqbool, R Ullah, H. Safdar,"Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks," Indian Journal of Science and Technology, Vol. 7, No.3, pp. 282–295, 2014.

[30] A. Gawanmeh, A. Bouhoula, and S. Tahar, "Rank Functions Based Inference System for Group Key Management Protocols Verification," International Journal of Network Security, Vol. 8, No.2, pp. 207-218, 2009.

[31] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," IEEE Transactions on Mobile Computing, Vol. 2, No.1, pp. 52-64, 2003.



Appendix A: Conceptual design for SEDRRA schemes in MMR WIMAX