# Secure and Efficient Multicast Rekeying Approach For Non-Transparent Relay-based IEEE 802.16 Networks

Adnan Shahid Khan, Norsheila Fisal, Sharifah Kamilah, Rozeha A. Rashid
UTM-MIMOS Center of Excellence in Telecommunication Technology
Faculty of Electrical Engineering, Universiti Teknologi Malaysia 81310 Skudai, Johor, Malaysia,

M. Abbas
Wireless Communication Cluster
MIMOS Berhad, Technology Park Malaysia
57000 Kuala Lumpur, Malaysia

## ABSTRACT
Many emerging applications that depend on secure group communications demand the privacy of participants and access control at the multicast server. The multicast and broadcast services in IEEE 802.16 are efficient and power saving mechanisms, which no doubt also provide subscribers with strong and powerful security protection from the theft of service by encrypting broadcast connections between subscriber station (SS), relay station (RS), non-transparent relay station (NRS) and Multihop relay base station (MR-BS). However, the existing multicast and broadcast rekeying algorithm (MBRA) not only facing forward secrecy, backward secrecy and scalability problems for IEEE 802.16e but also for multi-hop relay based networks both in centralized as well as distributed zone. Although many researches try to give solutions for the above problems, all of them focus mainly on IEEE 802.16e networks and none of paper is published on distributed relay-based Wimax networks. This paper illustrates the main security problem of MBRA in general which is scalability, backward and forward secrecy and proposes a new Secure and efficient distributed Relay-based Rekeying Algorithm **(**SEDRRA) scheme for non-transparent Multihop IEEE 802.16 networks. The proposed scheme uses non-transparent decode and forward relays. Both analysis and performance evaluation show that our scheme can significantly reduce the complexity and solve all of the above problems in an efficient way.

## Keywords
Multicast and Broadcast Rekeying Algorithm (MBRA), Secure and efficient distributed Relay-based Rekeying Algorithm (SEDRRA), Security Issues in Wimax.

## 1. INTRODUCTION
Wireless networks have become more and more persistent due to their many advantages. The IEEE 802.16 standard aims to provide broadband wireless access (BWA) for metropolitan area network (MAN), and as an alternative to cable and DSL for the delivery of last mile. To support BWA, high data transmission is necessary. In March 2006, a new task group IEEE 802.16j was introduced, which attempted to amend current IEEE 802.16e standard just by injections of RSs in between BS and SSs in order to support multi-hop relay operation in wireless broadband networks. One popular class of applications that will be widely deployed in future wireless networks is the group oriented multimedia applications such as stock option bidding, pay per view TV broadcasting, video conferencing, etc for both fixed and mobile subscribers[1]. This is because service providers can efficiently distribute the same contents to the users within a multicast and broadcast (M&B) group with low bandwidth consumption. Most multicast applications require secure mechanisms to protect communication within a group. Three requirements needed for securing group communication are listed as follows [2]. First is group confidentiality. The messages exchanged within a group cannot be sniffed by attackers. Only authorized group members can obtain multicast and broadcast messages. Second is forward secrecy. If an attacker compromises any subset of old group keys, he still cannot obtain any subsequent group keys. This property means that a leaving user cannot know any group key that will be used in later sessions. Third is backward secrecy. If an attacker compromises a set of group keys, he cannot obtain preceding group keys. This property means that a new joining user cannot know the group key used in previous sessions. Similarly, the group key used in current session should be updated when a user joins the group. For convenience, we call the updating operations for forward secrecy and backward secrecy as rekeying [3]. To enable the multicast service into commercial wireless applications, well designed access admission to multicast data is needed. That deals with scalability and the current scheme is inefficient when the MBS group size becomes larger. In this paper we present SEDRRA, which is an entirely new multicast and broadcast scheme for Multihop Wimax networks. The rest of the paper is as follows. Related works are discussed in sections 2. SEDRRA scheme is discussed in section 3 while section 4 discusses the analysis of the proposed scheme. Simulation results and conclusions are presented in section 5 and 6 respectively.

## 2. RELATED WORKS
In 2006, the IEEE 802.16 working group (WG) approved a project Authorization Request (PAR) focused on the Relay Tasks Group (TG). The main task of this Relay TG was to develop an amendment to the IEEE Std 802.16 enabling the operation of RSs in centralized and distributed scheme defined by 802.16 [2]. Relay stations concept as discussed in [5][6]

introduces four types of RSs from the perspectives of physical and MAC layers. After successful comparison, the main focus is on the non-transparent RS operating in distributed scheduling and security mode [5][14][15][17] due to its throughput improvement, coverage extension and high bandwidth efficiency nature. Secure Multicast and broadcast over insecure channels has been an active research topic for the last ten years and many protocols have been proposed. For secure multicast communication as designed in IEEE 802.16 standard [7][18], the MBRA uses a Group Key Encryption Key (GKEK) and Group Trafficc Encryption Key(GTEK). The GKEK is used to encrypt GTEK and the GTEK is used to encrypt multicast traffic. Both keys are used to ensure the forward and backward secrecy based on their lifetime. But in [3], [8] and [9], the authors have shown that the MBRA fails to ensure forward and backward secrecy. Also the MBRA is not scalable for large group as the message complexity is O(n), which means that it increases proportionally with the number of group members, n. Scalable multicast key distribution and group key management protocols specification are amongst few works in secure multicast and broadcast [3][8]. Kronos [10] takes a unique periodical rekeying approach that rekeys the group only at specified time intervals. Customary rekeying upon member changes are delayed until the next rekeying interval, therefore the number of rekeying is reduced. For distributed method, Lolus approach [11] is a hierarchy of agents used as subgroup controller. Using Lolus scalability is ensured because member changes in one group do not affect other subgroups. For centralized approach, Logic Key Hierarchy (LKH) and one way function tree (OFT) which are based on the efficiency of key tree structure and hash function can be used. LKH are proposed in [11] and [12] which provides O(log n) communication complexity. In LKH, each leaf node corresponds to a group member and the root node is a Group Key Controller (GKC), which is a TTP. Members share a pair wise key with the root node as well as a set of intermediate keys from it to the root. In the event of member change, a rekey message is generated containing each of the new sets of keys encrypted with its respective node's children keys. In [4] and [8], the authors identify the lack of forward and backward secrecy in MBRA architecture. They also discuss the scalability issues in MBRA. MBRA requires O(n) message transmissions. In [9], Huang et al. introduces an approach that handles backward and forward secrecy, Efficient sub-Linear rekeying Algorithm with Perfect Secrecy (ELAPSE), and a cross-layer approach for an improved version of ELAPSE, namely ELAPSE+. Both ELAPSE and ELAPSE+ are based on Logical Key Hierarchy(LKH), as described in [4] and [9], that works in O(log n) message complexity. The ELAPSE and ELAPSE+ can handle forward and backward secrecy with a set of KEKs and Sub Group Key Encryption Keys (SGKEK), and works in O(log n) like LKH. But this is still a problem with large number of n. Typically, applications like pay-TV uses a large value of n for one-to-many group communication. In [9], Sun et al. introduces a new rekeying algorithm for multicast and broadcast in IEEE 802.16 network, that works in O(1) constant time complexity. Their scheme is based on LORE, as proposed in [9], a linear ordering key distribution algorithm that can handle forward and backward secrecy.

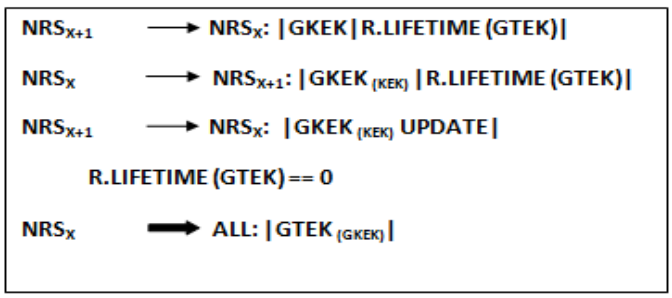
The proposed scheme SEDRRA is not only less complex, but also solves all the above mentioned critical concerns like forward/backward secrecy as well as scalability in a very efficient manner.

## 3. SEDRRA

In our proposed scheme as shown in Figure 2, we use hybrid architecture, centralized as well as distributed security control. In the centralized security control [16], the initial security zone key (SZK) and security zone key encryption key (SZKEK) distribution is performed by using the PKMv2 SA-TEK 3-way handshake. Once an RS shares the traffic keying material with the MR-BS, the MR-BS updates and distributes the traffic keying material periodically by sending PKMv2 Group-Key-Update-Command messages. The MR-BS manages the SZK Grace Time. Length of a SZK Grace Time shall be shorter than the time required for complete exhaustion of relevant packet number space. This parameter means time interval (in seconds) before the estimated expiration of an old distributed SZKEK. The MR-BS distributes updated group key material by sending PKMv2 Group-Key-Update-Command messages before old distributed key is expired. Two message types are distinguished according to the included Key Push Modes. The MR-BS transmits the PKMv2 Group-Key-Update-Command message for the SZKEK update mode in order to distribute the new SZKEK. Moreover, the MR-BS transmits the PKMv2 Group-Key-Update-Command message for the SZK update mode in order to distribute the new SZK. In general, the SZKEK lifetime corresponds to the n (integer being bigger than 1) times of the SZK updates (i.e. the SZKEK shall be updated once while the SZK is updated n times). The MR-BS intermittently transmits the PKMv2 Group-Key-Update-Command message for the SZKEK update mode to each RS in order to reduce the MR-BS's load in refreshing group key material. The SZKEK is needed to encrypt the new SZK. The process is just like the same as in the official IEEE draft.

In the distributed security control, we assume that AK has already been established and now all the NRS have AK and they can easily get KEK. KEK is utilized to encrypt and decrypt GKEK. The overall protocol is shown in Figure 1. In the above scenario, MR-BS transmits GKEK encrypted by KEK to all participating members and once all the members receive GKEK, MR-BS broadcast GTEK encrypted by GKEK. In our scheme, all the NRS maintains corresponding GKEK rekeying tables. As a matter of fact,

**Fig 1**: SEDRRA PROTCOL



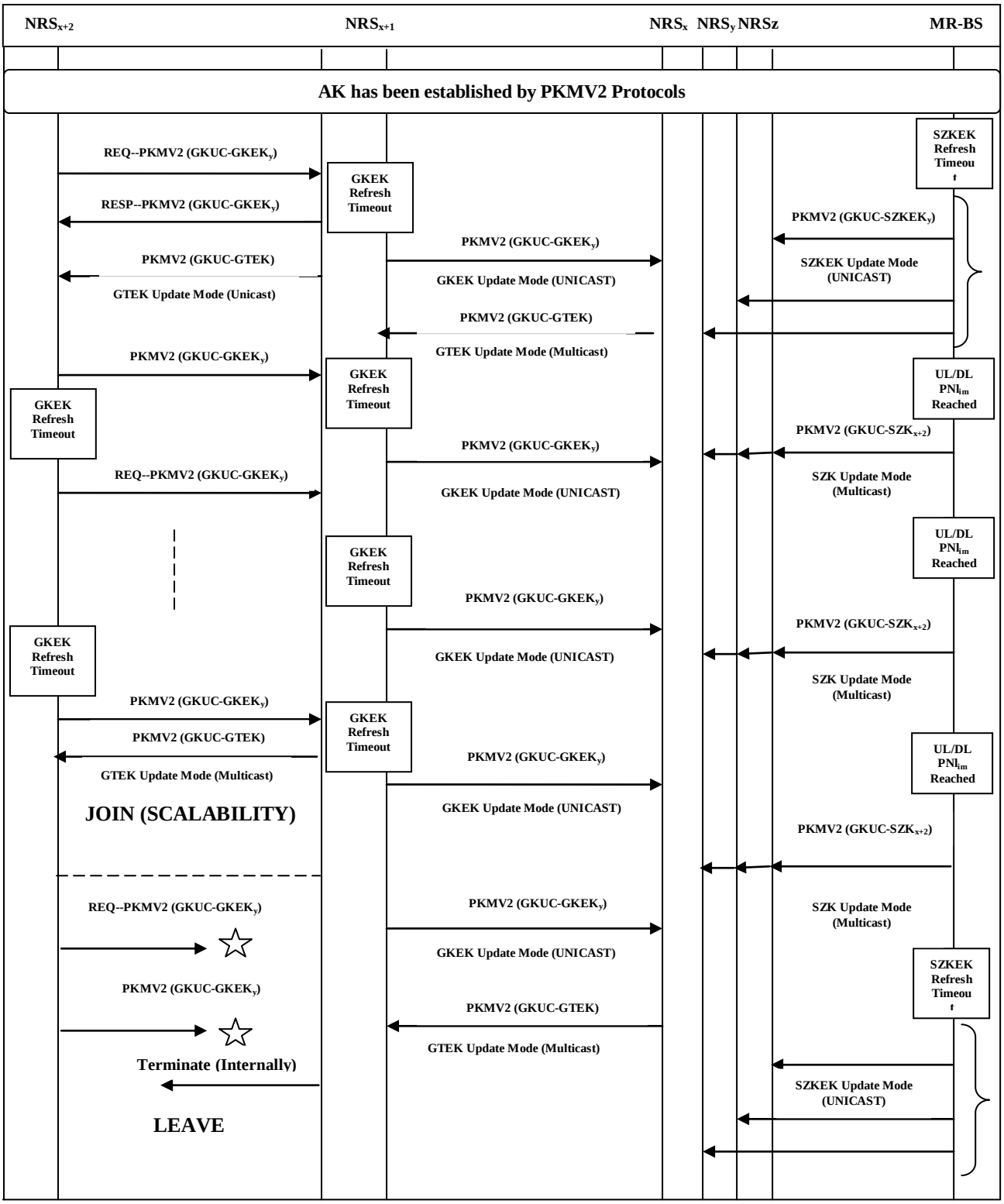



**Fig 2**: Proposed SEDRRA scheme for Multihop relay networks

NRS are basically decode and forward relay and can easily generates keys on behalf of MR-BS stations. Thus these keys are generated by using the same algorithm which was settled during SBC negotiations. In our scheme, $NRS_{X+1}$ send the REQ message for GKEK and get RESP message with GKEK. After specific interval, $NRS_{X+1}$ will send GTEK encrypted by GKEK. Before GTEK is broadcast to all the members of the network, MR-BS send the remaining lifetime of GTEK to NRSx+1, and once the GTEK lifetime reaches the limit, MR-BS broadcast the GTEK encrypted by KEK to all the newly joined NRS as well as the previous one who are continuously updating their keys. The focus of the approach presented here will be entirely different from the sub-grouping of SS. NRS are limited in numbers as compared to SS, and so grouping of NRS is not a healthy solution here. The main aim of our scheme is to provide not only scalability but also furnish with proper solutions that can maintain backward secrecy and forward secrecy. To ensure of the above solutions, $NRS_{X+1}$ send GKEK periodically at specific interval of time. In our proposed scheme, the GTEK life time corresponds to the n(integers being bigger then 1) times of GKEK life time. That is the GTEK shall be updated once while the GKEK is updated n-times. And GKEK's updating is not from NRSX but from $NRS_{X+1}$. After specific interval of time, $NRS_X$ will check the updated key in its GKEK tables and tallies the keys. If both keys are the same, then $NRS_X$ will continue to wait for the next update. After n times of updates, it will broadcast GTEK to all the participating members. Here we can also use grouping techniques to group the subscribers and not the relay stations as the low number of NRS does not require the need for grouping.

In the simple case of rekeying, if there is no member joining or leaving, then GKEK will be updated periodically and both keys are maintained by $NRS_X$ in their key tables. NRSX will periodically broadcast the GTEK to all the members. Note that the life time of GTEKs as specified by IEEE 802.16 standard is an important security consideration. Currently, the range is specified to be 0.5 hours minimum, 12 hours by default, and 7 days maximum. This life time have great leverage on the relationship

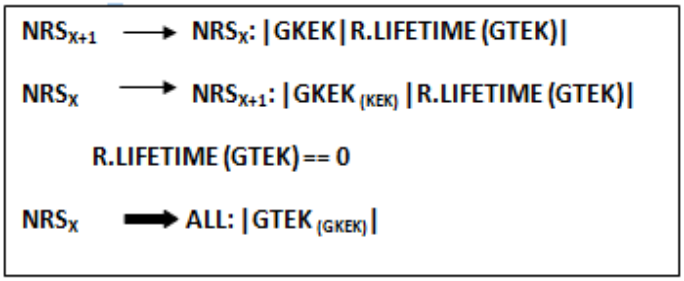



**Fig 3**: NRS joins the networks in SEDRRA

between scalability and forward/backward secrecy provided by the standard. A long enough lifetimes need to be maintained to allow MR-BS enough time individually to update the GKEK so that the new GTEK can be broadcast. However, longer GTEK lifetimes imply much greater lapses in backward/forward secrecy on member joining/leaving the events respectively.

In the case of when any new member wants to join the network, as shown in Figure 3, rekeying due to a member joining in is a little bit different than all others schemes. The member joining in starts off as it does in the original specification with the key request sent from $NRS_{X+1}$ to $NRS_X$ and key reply sent from $NRS_X$ to $NRS_{X+1}$. Once $NRS_{X+1}$ get the RESP message with GKEK encrypted by KEK, it will start sending unicast messages to update the tables residing inside both $NRS_X$ and $NRS_{X+1}$. In our scheme to avoid delay, $NRS_{X+1}$ immediately sends the GTEK message to only $NRS_{X+1}$ in a unicast form. At this stage, we assume that some lifetime is going on to broadcast the GTEK to all of the participating members. If $NRS_{X+1}$ wait for that particular period then this will cause delay. Otherwise, if $NRS_{X+1}$ eventually broadcast GTEK to all the participating members, then they have to maintain again GKEK and this might change the timings to

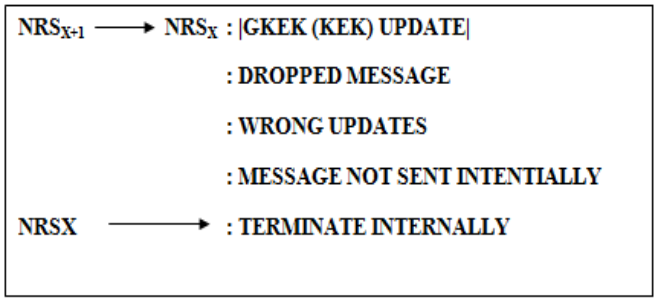



**Fig 4**: NRS leaves networks in SEDRRA

unicast. Some may send this message a few seconds ago and again this message needs to be sent again. This causes high complexity, so in our case, we only unicast this message to a particular $NRS_{X+2}$ immediately. The rest of the procedures are the same as the case of simply rekeying.

On the member leaving the multicast service as shown in Figure 4, first we need to sort out the case when a member can leave the multicast service. First is whether they cannot update the GKEK, which means that they cannot maintain the AK with $NRS_{X+1}$ or they intentionally leave the multicast service. In either case, $NRS_{X+2}$ supposed to leave the group, then $NRS_{X+1}$ will see in the table which member has not send the updating of the key, and will immediate sort it out. If the $NRS_{X+1}$ have not updated the key at a specific period of time, the table will be terminated immediately. Thus, there is no unicast or multicast message needed when any of the NRS left the networks.

## 4. ANALYSIS OF PROPOSED SCHEME

In the previous sections, we have overview the basic MBRA in 802.16 networks and its problems of forward/backward secrecy and scalability and introduce our SEDRRA scheme that aims to address these problems. Next we use theoretical analysis and empirical simulations to evaluate the security properties and efficiency performances of SEDRRA.

### 4.1 Security Analysis

There are three main security requirements for secure communications that are forward secrecy, backward secrecy and scalability. Here in this section, we review all these requirements and how much they are applicable in our proposed approach.

Forward secrecy— In this section, we illustrate that SEDRRA provides backward and forward secrecy because at a join or multi-join event, the group key is updated and at a leave event, the group key and all the sub-group key are updated on the leaving NRS. Forward secrecy is actually a prevention of a leaving member from accessing future communications.

According to SEDRRA, there are certain reasons that NRS leave the multicast services, and intentially terminate and non-updating of keys are amongst them. SEDRRA illustrates, if any NRS leave the communication, which means it cannot update the rekeying tables at both ends. After specific interval of time, serving NRS, or according to Figure 1, $NRS_{X+1}$ could not update its latest key, then $NRS_{X+1}$ will wait till next time out. After 2 time out intervals, $NRS_{X+1}$ terminate its services internally and delete the rekeying table. However, if the GTEK update message have not yet been broadcast as there is no such benefit to announce specially for that updated GTEK, $NRS_{X+2}$ cannot access services and once time out is reached for GTEK , $NRS_{X+1}$ will broadcast the GTEK as normal. Thus our scheme SEDRRA is very much powerful as far as forward secrecy is concerned.

Backward secrecy— This mechanism prevents a joining member from accessing former communications. Suppose if an attacker compromises a set of group keys, he cannot obtain proceeding group keys. This property means that a new joining user cannot know the group key used in the previous sessions. According to SEDRRA, when an NRS wants to join a network, it will send the REQ message. The MR-BS will send the RESP message to NRS with the queue timing for the next broadcast of GTEK. Let's assume GTEK's lifetime is about 30 minutes and NRS send the REQ just after 10 minutes of GTEK's broadcast. So MR-BS RESP message will include 20 minutes wait time to send GTEK. Once lifetime of GTEK reaches its maximum time, MR-BS broadcast the latest GTEK encrypted by GKEK which it already unicast to the joining NRS. So in this case, NRS cannot decrypt any of the previous messages. Thus our scheme helps in backward secrecy in a very powerful way.

Scalability—scalability is another critical concern for the multicast service underlying these applications due to the possible large number of group members. In MBRA, the main problem was scalability as its BS still need to unicast to each SS. As in a potentially large network such as a Wireless MAN, any rekeying scheme depending on unicast methods is not scalable. But according to SEDRRA, unicast is not from MR-BS. Every NRS needs to maintain its REQ lifetime by itself just like in key management schemes where every SS needs to maintain its AK as well as TEK state machines by itself. Similarly, every NRS needs to maintain their GKEK by itself and MR-BS needs to unicast only once during the whole procedure of NRS joining till the particular NRS leaving the multicast service. This approach, thus, provides scalable environment.

## 4.2 Efficiency Analysis

For MBRA in 802.16, since the server should send rekeying messages to each group member respectively with the new group key, the communication complexity is O(n), server space complexity is O(1) and member space complexity is O(1). In the LKH scheme, the communication complexity is O(log n) for the rekeying procedure; the server space complexity is O(n) and member space complexity is O(log n). For ELAPSE, the exact complexity is determined by the number of subgroups, and the ranges of these complexities illustrate the tradeoffs associated with the choice of the number of subgroups. When the number of subgroups increases (from 1 to N, $N = 2k$, $1 \leq N \leq n$), it can be generalized that the communication complexity decreases from O(n) to log N + m, where m is the number of current members in the subgroup to be updated. It is easy to see that when N increases, m will decrease, and when N = n, it becomes equivalent to the LKH scheme. As for the space complexity, the server space complexity increases from O(1) to 2N – 1, and the member space complexity also increases from O(1) to log N + 1 (every key on the path from the subgroup to the root in the key hierarchy). All of the above approaches are only for IEEE 802.16e networks, but SEDRRA works only for IEEE 802.16 distributed relay-based networks. However, we can still make the comparisions with the above approaches by using one hop rekeying managements. In addition, SEDRRA also provides Hop-by-Hop rekeying approach to stregthen the security. In SEDRRA, when any NRS wants to join the network, only one unicast carrying GKEK material is sent to NRS. While for any NRS that wants to leave the network, it is not possible to send a single message either in unicast or multicast. Thus, we can say that overall complexicity remains at O(1).

## 5. SIMULATION RESULTS

To compare the performance, we simulate both MBRA and SEDRRA using NCTUNS 6.0. Due to lack of wide diversity of standard in Multihop relaying-based network in distributed environment, many execution parameters such as key request time out, life time of GTEK, lifetime of GKEK sent from NRS unicast, are not completely defined and were chosen subjectively. However, all of the chosen values are within reasonable ranges. Two simulations were executed from MBRA and SEDRRA. The first simulation was for NRS joining in and runs about 100 seconds while the second simulation was for NRS leaving and runs about 1000 seconds. 8 NRSs were simulated with only one MR-BS delivering one multicast service.

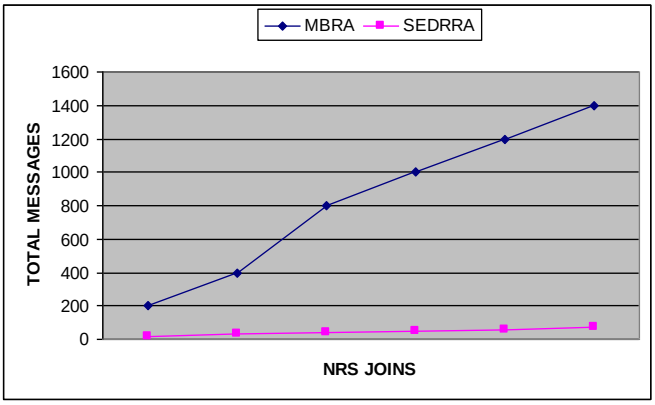



**Fig 5**: NRS joins the networks

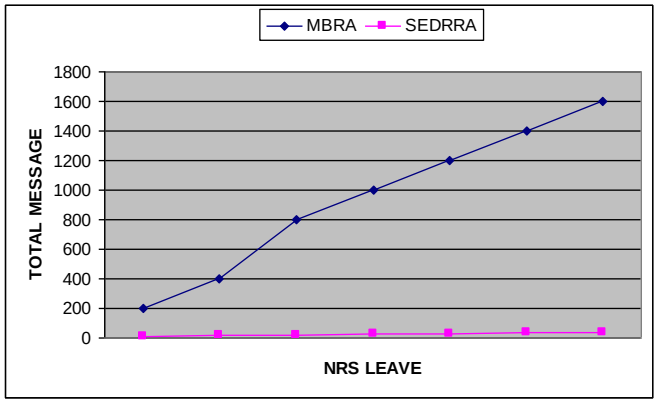



**Fig 6**: NRS leaves the network

In the first simulation, all of the NRSs joined the network at different time periods as shown in Figure 2. As compared to 1400 messages sent by MR-BS to NRS during MBRA approach, only less than 100 messages sent by MR-BS to NRS using SEDRRA approach. In the second simulation, for the NRSs leaving the network randomly, Figure 4 shows almost 1600 messages were sent by MR-BS to NRS during MBRA approach and less than 30 messages sent from MR-BS to NRS using SEDRRA. Mostly, these messages are the broadcast messages in the shape of GTEK. In both simulation runs, we assumed that GTEK broadcast at specific interval of time and GKEK is unicast on joining the networks. However, our simulation does not differentiate between unicast and broadcast messages separately.

## 6. CONCLUSION

In this paper, we have revised the security challenges of multicast and broadcast services in IEEE 802.16 distributed relay-based networks. We have also analyzed MBRA and found some incomplete solutions by not providing backward secrecy and forward secrecy. We also illustrate the scalability concerns for large networks. The approach presented in this paper, SEDRRA, provides backward/forward secrecy in a very powerful way with a very less complex environment. Using SEDRRA, when the NRS wants to join a network, concept of wait and serve is utilized while when the NRS wants to leave the network, concept of one way termination is preferred where not a single message is used for this purpose. Security, efficiency and simulation performance shows that SEDRRA not only supports backward/forward secrecy but also solves the critical concern of scalability for the large network in a very efficient way. In our future work, we will continue to implement a prototype of SEDRRA and extend the scale of the experiments and to allow the usage of other techniques like ELAPSE, LORE and LKH to find out better solutions for the scalability as well as message secrecy.

## 7. ACKNOWLEDGMENT

The author would like to thanks to all Wimax research group specially, FATEH, DAHRU, and Abeda Muhammad Iqbal for their constant help in this topic. This work is fully funded By Ministry of Higher Education under Malaysian Technical Cooperation Programme (MTCP) award and partially by MIMOS BERHAD.

## 8. REFERENCES

[1] IEEE Std 802.16-2009: Air Interface for Broadband Wireless Access Systems, 2009

[2] Steven W.Peters and Robert W.Heath, Jr, The Future of Wimax: Multihop Relaying with IEEE 802.16j, *IEEE communication Magazine*, January 2009.

[3] Sen Xu,Chin-Tser Huang and Manton M. Matthews, Secure Multicast in WiMAX", in Journal of Networks, Vol 3., No 2, February 2008.

[4] Chin-Tser Huang, Manton Matthews, Mathew Ginley, Xinliang Zheng, Chuming Chen and Morris Chang, \Efficient and Secure Multicast in WirelessMAN: A Cross-Layer Design", Journal of Communications Software and Systems, Vol. 3, No. 3, 2007, pp. 199-206.

[5] Adnan Shahid Khan et. al., Efficient Distributed Authentication Key Scheme for Multi-hop Relay In IEEE 802.16j Networks, *International Journal of Engineering Science and Technology (IJEST)*, Vol. 2(6), 2010, 2192-2199.

[6] Adnan Shahid Khan, Prof.Dr.Norsheila Fisal, Abdelhamid, Security Sublayer : A Required Evolution of Wireless Security IEEE 802.16j, *In proceedings of IEEE international Conference on Antenna Propagation and System (INAS 2009)*, Grand paragon Hotel, Johor Bahru, 3-5 December 2009.

[7] IEEE Std 802.16j-2009, Amendment to IEEE STD 802.16-2009

[8] Sen Xu, Chin-Tser Huang and M. Matthews, Secure Multicast in Various Scenarios of WirelessMAN", in the proccedings of IEEE SoutheastCon., March 2007

[9] Hung-Min Sun, Shih-Ying Chang, Shuai-Min Chen, Chien-Chien Chiu, \An Efficient Re keying Scheme for Multicast and Broadcast (M&B) in Mobile WiMAX", in the proccedings of Asia-Pacific Services Computing Conference, December 2008

[10] S. Setia, S. Koussih, S. Jajodia, and E. Harder, "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast", Proc. of IEEE Symposium on Security and Privacy, 2000S. Mittra, "Iolus: A Framework for Scalable Secure Multicasting", in Proc. ACM SIGCOMM'97, 1997.

[11] C. K. Wong, M. G. Gouda and S. S. Lam, Secure Group Communication using Key Graphs." IEEE/ACM Transaction on Networking, Vol. 8, No. 1(Feb), 2000, Pages 16-30.

[12] Adnan Shahid Khan, N. Fisal , N.N.M.I. Ma`arof , F.E.I. Khalifa, M. Abbas. Security Zone and Key Derivation Management in Centralized Security Control in Wimax Multihop Relay System. *In Proceedings 3rd International Graduate Conference Of Engineering Science, and Humanity*, 2010, (IGCESH2010), UTM, Johor Bahru, Malaysia, 2-4 November 2010

[13] Sen Xu, Manton Matthews and Chin-Tser Huang, Security Issues in Privacy and Key Management Protocols of IEEE 802.16, *In ACM SE'06*, Florida USA, March 2006.

[14] Adnan Shahid Khan, Norsheila Fisal, Mazlina Esa, Sharifa Kamilah, Sharifa 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 Electromagnetics (APACE 2010), Port Dickson, Malaysia, 11-12 November 2010.

[15] T. Hardjono, B. Cain, and I. Monga. Intra-domain group key management for multicast security. IETF Internet Draft, November 1998.

[16] A. S. Khan, N. Fisal, S. K. S. Yusof, S. H. S. Ariffin, N. N. Maarof, M. Abbas , Security Issues of Relay-Based IEEE 802.16m Network, *4th International Conference on Post Graduate Education (ICPE- 4 2010), 26th-28th November 2010, Mid Velly Cititel Hotel, Kula Lumpur, Malaysia*

[17] J. Y. Kuo. Analysis of 802.16e multicast/broadcast group privacy rekeying protocol. CS 259 Final Project Report, Stanford University, 2006.

[18] Miss Laiha Mat Kiah, Keith M. Martin, Host Mobility Protocol for Secure Group Communication in Wireless Mobile Environments, International Journal of Security and its Applications, Vol. 2, No. 1, January, 2008

[19] Adnan Shahid Khan, Norsheila Fisal, Abdelhamid, Security Sublayer : A Required Evolution of Wireless Security IEEE 802.16j, *In proceedings of IEEE international Conference on Antenna Propagation and System (INAS 2009)*, Grand paragon Hotel, Johor Bahru, 3-5 December 2009.

**ADNAN SHAHID KHAN** received his degree of B.Sc (Hons) in Computer Science from University of the Punjab, Lahore, Pakistan in 2005. Master of Engineering degree in Electrical (Electronics & Telecommunication) from Universiti Teknologi Malaysia, Skudai, Malaysia in 2008. Currently, he is pursuing his PhD in Electrical Engineering at the Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Skudai, 81310, Johor Bahru, under the supervision of Prof. Dr. Norsheila Fisal. His current Research interests are in the area of Security Issues in IEEE 802.16 Protocol and Cognitive Radio Networks.

**NORSHEILA FISAL** received her B.Sc. in Electronic Communication from the University of Salford, Manchester, U.K. in 1984. M.Sc. degree in Telecommunication Technology, and PhD degree in Data Communication from the University of Aston, Birmingham, U.K. in 1986 and 1993, respectively. Currently, she is the Professor with the Faculty of Electrical Engineering, University Technology Malaysia and Director of Telematic Research Group (TRG) Laboratory. Her current research interests are in **Wireless Sensor Networks, Wireless Mesh Networks, And Cognitive Radio Networks**

**MAZLAN ABBAS** received his B.Eng. in Electrical from Universiti Teknologi Malaysia in 1984, M.Sc. In Telematics from Essex University in 1986, and PhD degree in Telecommunications from Universiti Teknologi Malaysia in 1992. Currently, he is the Chief Research Director of Wireless Communications Cluster of MIMOS Berhad and also the Adjunct Professor with the Faculty of Electrical Engineering, Universiti Teknologi Malaysia. His current research interests are in **WiMAX, LTE, IMS and IPv6.**

**SHARIFAH KAMILAH BNT SYED YUSOF** received BSc (cum laude) in Electrical Engineering from Geoge Washington University USA in 1988 and obtained her MEE and Ph.D in 1994 and 2006 respectively from universiti Tecknologi Malaysia. She is currently Associate Professor with the department of Radio Communication, Faculty of Electrical Engineering Universiti Teknologi Malaysia. Her research interest includes OFDMA based system, Software define Radio and Cognitive radio.

**ROZEHA A. RASHID** received her B.Sc. in Electrical Engineering from University of Michigan, Ann Arbor, USA in 1989 and M.E.E from Universiti Teknologi Malaysia, Skudai, Malaysia in 1993. Currently, she is pursuing her PhD in Electrical Engineering at the Faculty of Electrical Engineering, Universiti Teknologi Malaysia, Skudai, 81310, Johor, Malaysia. Her current research interests are in the area of Cognitive Radio, Ultra Wideband System and Wireless Sensor Networks (WSNs).