An Efficient and Secure Group Key Management for IEEE 802.16j Architecture

Hung-Min Sun[1], Shuai-Min Chen[1], Ying-Chu Hsiao[1], Yue-Hsun Lin[1], Frank Chee-Da Tsai[2]
[1]Dept. of Computer Science, National Tsing Hua University, Taiwan, R.O.C
[2]Networks & Multimedia Institute, Institute for Information Industry, Taiwan, R.O.C
hmsun@cs.nthu.edu.tw

Abstract

The Relay Task Group of IEEE 802.16 has developed IEEE 802.16j which supports mobile multi-hop relay (MMR). MMR utilizes relay stations (RS) to extend network capability. Since attacks are easy to mount in wireless interface between RSs and BS, security issues seem to be more important.

This paper proposes a group key management scheme that agrees with the Security Zone Key (SZK) specified in IEEE 802.16j. The scheme has two features. First, the re-keying mechanism is efficient lightweight. Second, the scheme is flexible to allow new RSs to join the group.

Keywords：CAS, Group Key Management, IEEE 802.16ｊ／WiMAX, MMR, Relay Station

1 Introduction

Wireless technology has become more popular in daily life. IEEE 802.11[1] [2] [3] wireless LAN (WLAN) uses hot-spot to provide wireless connection service. However, WLAN is not sufficient to support Metropolitan Area Network (MAN). Hence, next generation wireless systems are expected to provide fast data transmission rate and high service coverage. Therefore, IEEE 802.16 Standard [4] becomes an oncoming technology for wireless broadband access system. With the different purposes of IEEE 802.16 Standard, there are various versions of IEEE 802.16 Standard. The main versions are 802.16d and 802.16e. IEEE 802.16d Standard [4] is proposed for fixed subscriber station (SS). In 2006 February, the IEEE 802.16 Task Group published IEEE 802.16e Standard [5] for mobility which supports mobile stations (MS). For the growing demand and requirement, the Relay Task Group of IEEE 802.16 has developing IEEE 802.16j Standard which supports mobile multi-hop relay (MMR) operation in order to gain coverage extension and throughput enhancement.

The basic components of MMR network architecture are relay stations (RS). RSs are deployed in a cell for the purpose of relaying information bi-directionally between the MS and the base station (BS). A comparison of RSs with BS [6] shown that, RSs have no direct backhaul connection to the network and are simple and easy to implement. Many research have been shown that BS which cooperates with RSs can improve cell coverage, user throughput, system capacity and decrease cost overhead.

Since there are many RSs work together within one BS in a cell, the BS and RSs would form a group. In order to securely communicate with each other in the group, they should share a group key. IEEE 802.16j defined the Security Zone Key (SZK) [6] is a group key shared by the

MR-BS and a set of RS within the same security zone. The SZK is randomly generated by the BS and is distributed to a RS after the RS got authenticated during initial network entry [6] . However, re-keying seems to be weak and prone to suffer attacks when an adversary gains secrets or useful information through one or more compromised RSs. For example, the compromised RSs can replay the relayed messages to interfere the traffic in the network or they can just discard the message which should be relayed to BS that disrupts the connection between MS and BS. If there are compromised RSs in the group, it is important for the BS to make sure that the group key which held by the compromised RS should not be used any longer. The BS will notify the remaining RSs that they have to perform re-keying operation to avoid disclosing any information of the group in the successive communication.

This paper proposes an efficient key updating scheme adopted for WiMAX relay machine. The proposed scheme uses the Conditional Access System (CAS) mechanism which is designed for large scale environment with lots of subscribers and channels in pay-TV system. The proposed scheme can fast generate a new key for the remaining members in the group. Specifically, the compromised RSs have no ability to generate the newly group key. Furthermore, this scheme provides the mechanism for new RS to join the group.

The rests of this paper are organized as follows. Section 2 describes the background knowledge of 802.16j and the group key management scheme proposed for CAS system. Section 3 describes the proposed scheme. Section 4 gives the security and performance analysis. Finally, the conclusion and future works are given.

2 Related Works

IEEE 802.16j

In the progress of IEEE 802.16, the first Standard is 802.16d [7] , proposed in 2004. IEEE 802.16d Standard defines the physical layer and control layers of broadband wireless communication from fixed Subscriber Stations (SS) to the base stations (BS). Since mobility is another important factor in designing wireless architecture, the working group released IEEE 802.16e Standard [8] in 2005. In IEEE 802.16e Standard, not only the fixed SS but also MS are supported. However, the radio resource or performance is low when extinct spots occurred in the deployed environment. In order to save the deployment cost, the Multihop Relay mechanism (MR), IEEE 802.16j Standard [6] , is proposed to solve this problem.

In IEEE 802.16j Standard, Multihop Relay (MR) is an optional deployment in which a BS (in 802.16e) may be replaced by a Multihop Relay BS (MR-BS) and one or more Relay Stations (RS). The MR mechanism provides several advantages, such as providing additional coverage for the serving BS, increasing transmission speed in an access network, providing mobility without MS handover, decreasing power consumption when transmitting and receiving packets, and enhancing the quality of services (QoS). In addition, the cost of constructing RSs is cheaper than BSs. Besides, the MR is not a mesh, and all the data paths include MR-BS.

In (1) of Figure 1, a RS improves the radio coverage of the MR-BS [9] . In (2), when there is a RS nearby the MS, it can save the power for transmitting and

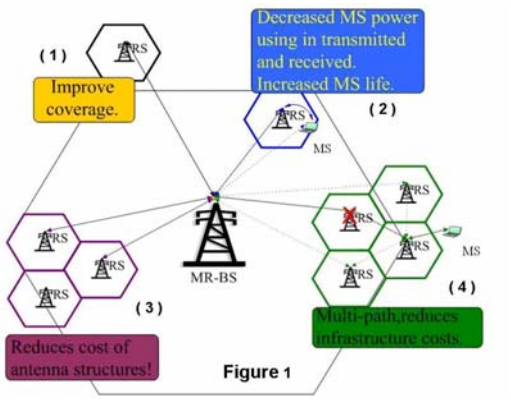

Figure 1. MR architecture in WiMAX environment

receiving by directly linking to RS. In (3), building an antenna structure is more expensive than building a RS. In (4), a path in the 802.16j has been chosen by MR-BS, when some RSs failed, the MR-BS may have another choice to build a path to MS. This mechanism reduces infrastructure costs.

In centralized controls multihop relay (MR) network, MR-BS control the handover (HO) process between an MS and the MR-BS.

RS HO process is occurred when an RS migrates from the air-interface provided by one access station to the air-interface provided by another access station. The HO process is depicted in Figure 2.

The MS HO process is similar to RS HO process, but some stages are omitted. These four stages are path selection, the RS operational parameter configuration, transport/tunnel connection re-establishment, and MS CID update.

In the HO of mobile relay system, there are two modes: moving RS mode and moving BS mode. When a RS enters a new air-interface, it can know which mode the MRS is by negotiating basic capabilities.

For the moving RS mode, the privacy of the MS is established and maintained by this MS and the serving MR-BS. For all the MSs attached to the mobile RS, this RS may need to initiate handover procedure. In the moving BS mode, the mobile RS is also a serving station for MS. When the RS moving into a new IP subnet, those IP addresses of the MSs originally attached to this RS need to be re-established. A dedicated connection may be established between the mobile RS and its serving MR-BS to relay the IP address re-establishment related signaling between the MS and MR-BS.

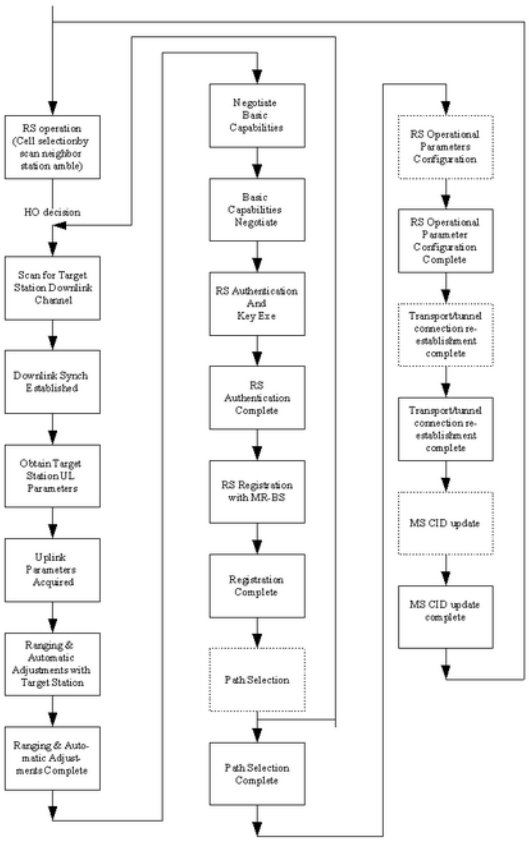

Figure 2. RS Handover Process

Key Refreshing Management

For most of application environments, there are great amounts of users involved in the system. Users may join or leave the system arbitrarily. Hence, the system manager should adopt an efficient key management scheme to maintain system security. In 2006, we proposed an efficient and flexible key distribution scheme for Conditional Access System [7] . This scheme provides the pay-TV system to control the group key refreshing immediately when members leaving or joining. It can prevent invalid users from accessing the system. The original purpose of the key refreshment scheme is to maintain an existing common group key while members leaving [7] [10] [12] , it is suitable to adopt for the group key management of SZK in IEEE 802.16j Standard. For the WiMAX architecture, there are great amounts of MSs joining or leaving the system. Therefore, BS has to maintain the access right of each MS. In this paper, the authors adopt the key refreshment scheme to IEEE 802.16j Standard that provides efficient and flexible key refreshment.

3 The Proposed Scheme

In this section, we propose an efficient key updating scheme used for WiMAX Relay Machine. The proposed scheme adopts the CAS mechanism to maintain the group key refreshment. Since the proposed scheme mainly focus on the relation between BSs, RSs and MSs, note that we will not mention the upper layer of BS in this paper, i.e. CSN, ASN, AAA, etc. All the steps executed beyond CSN, ASN and AAA are the same with IEEE 802.16 Standard [5].

In the WiMAX environment, there are many BSs and RSs deployed arbitrarily. Originally, the BS has a pair-wise key with each of the RS. Assume a BS chooses a certain amount of RSs to be its relay group, e.g. RS_1, RS_2, …, RS_n. Then BS can adopt the CAS mechanism to construct a virtual binary tree graph with the height of the binary tree T is $Log(n)$ and arrange the corresponding leaf nodes to RSs, i.e. RS_1 corresponds to leaf node 1, RS_2 corresponds to leaf node 2, etc. Once BS had deployed the RSs to the virtual binary tree T, BS can randomly choose a key K to be the first group key and then share this group key to all the RSs located in this binry tree by encrypting K with pairwise keys respectively. For the time being, all the RSs and BS shared a common group key.

When a new MS roams to the coverage of the BS, it will execute the authentication process — PKM_{v2} [6]. After executing the PKM_{v2} process, the MS will share a secret key with BS. Hereafter, all the information transmitted between the BS and the MS are encrypted with the group key K established before and are relayed by the specific RSs.

BS Deploy

TABLE I shows the notation used in group key refreshment scheme under WiMAX architecture. The BS has to maintain a structure of a binary tree T which will be used for constructing the new group key. The leaf node of the binary tree T represents an authorized Relay Station RS_i in the relay group. Every node (either an internal node v_i or a leaf node RS_i) in the binary tree T has a corresponding secret number R_{V_i} or R_{RS_i}. Every authorized relay station RS_i (leaf node) will obtain a set of secret numbers I_{RS_i} from the BS by the pair-wise key shared with BS. I_{RS_i} contains all the secret numbers of the binary tree T except those nodes on the path from RS_i to the root node in the tree T. Initially, K is a random chose number by the BS. When a member RS_i leaves the group, the existing group key K must be updated to prevent unauthorized access. The BS will utilize R_{RS_i} to update the group key K. That is, the BS broadcasts a message $\{LEAVE, RS_i\}$ to notify all members that member RS_i has left the group, the BS and all members except RS_i will calculate the new group key K' by $K' = K \oplus R_{RS_i}$. Since the left member RS_i lacks of the secret number R_{RS_i} which is on the path from RS_i to root node, it can not calculate the new group key

TABLE I. NOTATAION

Notation	Definition
M	The number of group members.
T	The binary tree
v_i	Internal node i in T
RS_i	Leaf node that represents an authorized relay station i
I_{RS_i}	The set of all corresponding secret numbers
R_{RS_i}	The secret number corresponding to node RS_i.
$Log(n)$	Logarithmic Operation on n
R_{V_i}	The secret number corresponding to node v_i.
K	The group key
$\oplus$	Exclusive-or operation

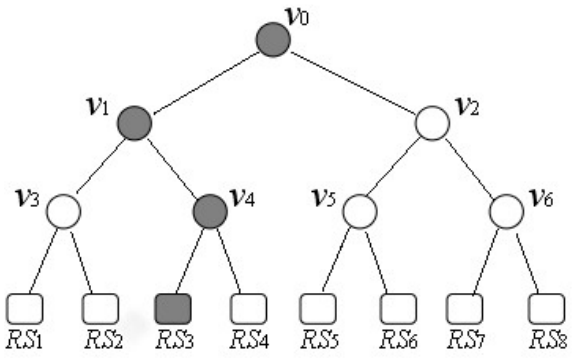

Figure 4. The Binary Tree T

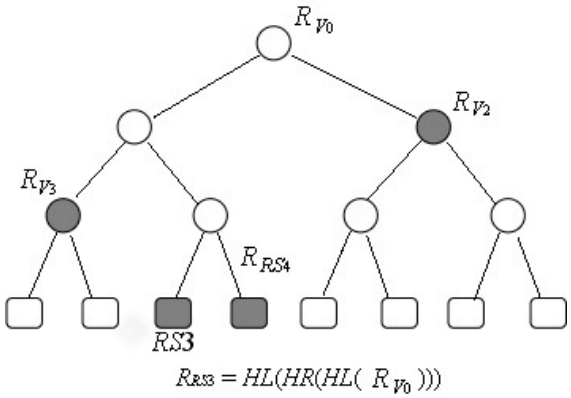

Figure 3. An Example of Tree Using Hash Function

K'.

For example, Figure 4 shows the structure of a binary tree T. The relay station RS_3 is assigned I_{RS_3} which contains the relative node's secret number (R_{V_2}, R_{V_3}, R_{V_5}, R_{V_6}, R_{RS_1}, R_{RS_2}, R_{RS_4}, R_{RS_5}, R_{RS_6}, R_{RS_7}, R_{RS_8}) transmitted from BS. When RS_3 leaves the group, the BS broadcasts {*LEAVE*, RS_3 }. Then all relay stations except RS_3 can calculate the new group key *K'* by $K' = K \oplus R_{RS_3}$.

The above scenario provides an efficient group key refreshment mechanism. However, with the number of member increasing, the binary tree T becomes large and each leaf node has to expense more storage space to save the secret numbers I_{RS_i}. To reduce the storage overhead of I_{RS_i}, the BS can utilize two Hash functions *HL* and *HR* to overcome this problem. Assume there are a parent node v_0, a left child node v_1 of v_0 and a right child node v_2 of v_0, in which v_0 was assigned a secret number R_{v_0}. Then the BS can easily assign the secret number $HL(v_0)$ to v_1 and $HR(v_0)$ to v_2, respectively. As an example shown in Figure 3, the secret number of root node is R_{v_0} and the secret number of RS_3 can be computed as $R_{RS_3} = HL(HR(HL(R_{v_0})))$. Hence, in the view of RS_3, the storage overhead of I_{RS_3} is reduced to { R_{V_2}, R_{V_3}, R_{RS_4} } and then RS_3 can still derive all the secret numbers it should know.

In order to be more flexible, the binary tree T must be extendable to join a new member into the group. Originally, assume the BS constructs an *n*-level tree for key management scheme and all relay stations *M* are the leaf nodes in the binary tree T, note that $2^{n-1} < M \le 2^n$. Consider the case that a new relay station RS_{new} is invited to join the group. If *M* is less than 2^n, the BS can assign the new relay station RS_{new} to a vacant leaf node directly. The new member RS_{new} can obtain the corresponding $I_{RS_{new}}$ from the BS. However, if *M* equals to 2^n, the BS should perform an extension process. The extension process first appends two child nodes to every leaf nodes. Hence, the level of the binary tree becomes *n*+1 and the user capacity of the tree rises to 2^{n+1}. Consequently, the BS assigns the corresponding secret numbers to the new joined member according to the position of the leaf node, and all existed relay stations are moved to the left child node of the original leaf nodes. Thus, there are still $2^n - 1$ vacant leaf nodes and could be assigned the new relay station to one of them. Besides, every original member RS_i will also obtain a new I_{RS_i}' from the BS. It means the group key is updated. In fact, only one additional

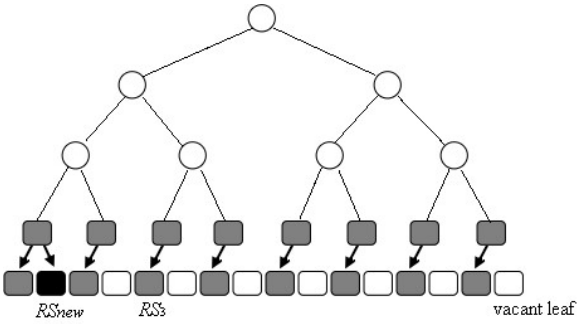

Figure 5. An example of extension process

secret number is added to origin I_{RS_i}. As an example in Figure 5, originally, there are 8 relay stations in the 3-level binary tree in which $M = 2^n$. When the binary tree T is extended to 4-level, and the origin relay stations are moved to the new leaf node as shown in Figure 5. After assigning RS_{new} to a vacant leaf node, the new I_{RS_3}' of the original member RS_3 becomes $I_{RS_3} \cup \{R_{sibling\_of\_RS_3}\}$. Therefore, the server only needs to transmit the $R_{sibling\_of\_RS_3}$ to RS_3.

RS Compromised

Although RSs are constructed by the WiMAX system provider, RS may be compromised by a malicious attacker. The meaning of an attacker's compromising of a RS is equal that an attacker obtains the access right of a RS. Consequently, the attacker also obtains the group key *K* of the tree and could decrypt the relayed information by *K*. Therefore, once a RS was compromised, all the information relayed through this RS will retrieve by the attacker. It may cause great unknowable damages to the WiMAX system.

Nevertheless, the proposed scheme can conquer this problem. When the BS is conscious of a RS being compromised, BS will alert to all the other RSs. BS will transmit the LEAVE message as mentioned in paragraph 3 and calculate the new group key $K' = K \oplus R$. After receiving the LEAVE message, all the RSs will calculate the new group key by formula $K' = K \oplus R$. Since the compromised RS lacks of the key *R*, it can not calculate the new group key *K*'. Hereafter, the transmitted information between the BS and RSs will be encrypted by the new group key *K*'. Although the compromised RS are still situated at the same location, it can no longer decrypt the eavesdropped information.

4 Analysis and performance evaluation

In this paragraph, we analyze the proposed scheme into two aspects, security and performance.

Security analysis

In the proposed scheme, we design a flexible and efficient key distribution scheme for group key architecture. The proposed scheme describes how to distribute necessary keys into the RSs in the initial stage, and key updating when a new RS joining or leaving. To verify the security of the proposed scheme, some attacking methods are listed below. The proposed scheme is still secure under these attacks.

1. Denial of Service attack: an adversary can lunch flooding packets to the serving RS or BS. Since these packets can be attached with some signatures through hashing.
2. Eavesdropping: an adversary can get information from sniffing packets on the air. This can be prevented from encryption with the group key.
3. Forward Security: an adversary cannot decrypt or gain some information in those ciphers which were encrypted with previous secret when he compromises the new secret. In the other words, previous conversations can be protected even if the secret (key) is compromised right now. Forward Security is provided in the proposed scheme.
4. Malicious RS: an adversary might inject some malicious RSs into the deployed network to gain some useful information. Since a new RS should be authenticated before it joins in the group. This cannot be happen in the proposed scheme.

Performance Evaluation

Performance is an import quantity in the practical issue. In the proposed scheme, we use two factors in measuring performance, one is storage cost and the other is message cost. For simplicity, we divide the proposed scheme into three stages, including initialization, registration, and updating (new RS joining or leaving). Assuming there are *n* RSs communicating with the serving BS, we list the average cost in TABLE II. In TABLE II, the Auth is the cost when the BS authenticates the serving RS mutually. In the Initialization stage, the BS should be authenticated with *n* RSs with each other. In addition, the BS should deliver each key material to each RS through the unicast secure communication. In the second stage, when a new RS joins into the existing group, the RS should be authenticated by the BS first. And then the BS delivers its key to the authenticated node. Therefore, the message cost is O(1). When an old RS left, the group key should be re-computed. The BS first delivers the key update command to the remainder RSs. The message cost is constant, O(1). Moreover, the remainder RSs should re-compute the group key through hash functions. In the proposed scheme, the computation cost is approximately O(log*n*). The network contains *n*-1 RSs. Therefore, the computation cost is O(log*n*)*(*n*-1) totally.

TABLE II. The Cost Evaluation

	Message Cost	Computation Cost
Initialization	O(*n*)	O(*n*log*n*)+*n**Auth
New RS joining	O(1)	Auth
Old RS leaving	O(1)	O(log*n*)*(*n*-1)

5 Conclusions

802.16/WiMAX is the next generation of wireless architecture. Since IEEE 802.16j Standard is an ongoing technology for supporting WiMAX framework, relay stations not only provide more and more radio coverage, but eliminate extinct spots in real environment. To maintain the basic security requirements in IEEE 802.16j Standard, SZK (secure zone key) is provided to construct a secure tunnel between RSs. However, the design of SZK does not consider the practical issues, such as RS joining or leaving.

In the proposed scheme, we design a flexible and efficient key distribution scheme for group key architecture. The proposed scheme describe how to distribute keys into RSs in the initial stage, and key updating when new RS joining or leaving. In group key scheme, some secure flaws during key updating will be eliminated. Moreover, the maintaining and setup cost is efficient and the key hierarchy is flexible. Moreover, the proposed scheme is suitable for mobile WiMAX environment.

6 Future Works

In the nearly future, we will extend our scheme to pair-wise key architecture since any two RSs share one unique key between both. The pair-wise key can be used for the highly secure level data communication and the group key can be used for control message transmission. Therefore, combing pair-wise key and group key management can make the communication more secure and flexible.

Reference

[1] IEEE 802.11 Standard, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”, 1999.

[2] IEEE 802.11b Standard, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications”,

1999.

[3] IEEE 802.11g Standard, “Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications”, 2003

[4] IEEE Standard 802.16-2004: Air Interface for Fixed Broadband Wireless Access Systems, Oct 2004.

[5] The IEEE 802.16 Working Group on Broadband Wireless Access Standards, http://grouper.ieee.org/groups/802/16/

[6] IEEE 802.16j Standard, “Draft IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Multihop Relay Specification,” Aug 2007.

[7] H. M. Sun, C. Z. Shieh, C. M. Chen, “An Efficient and Flexible Key Distribution Scheme for Conditional Access System in Pay-TV Systems” *Proceedings of the 16th Information Security Conference*, Taiwan, 2006.

[8] IEEE 802.16d Standard, “IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems” 2004.

[9] IEEE 802.16e Standard, “IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.” 2005.

[10] Intel Communications Technology Lab, “IEEE 802.16 Standard Development” Oct 2006.

[11] A. Fiat and M. Naor, "Broadcast Encryption," *Advances in Cryptology - CRYPTO* '93, Lecture Notes in Computer Science 733, Springer, pp. 480–491, 1994.

[12] D. Naor, M. Naor, J. Lotspiech, "*Revocation and Tracing Schemes for Stateless Receivers*," in Proc. Crypto 2001, Lecture Notes in Computer Science, pp. 41–62, Aug. 2001.