An Overview of Group Key Management Issues in IEEE 802.16e Networks

Mohammad Mehdi Gilanian Sadeghi

Faculty of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran

Received 10 December 2015; accepted 8 January 2016

Abstract

The computer industry has defined the IEEE 802.16 family of standards that will enable mobile devices to access a broadband network as an alternative to digital subscriber line technology. As the mobile devices join and leave a network, security measures must be taken to ensure the safety of the network against unauthorized usage by encryption and group key management. IEEE 802.16e uses Multicast and Broadcast Service (MBS) as an efficient mechanism to distribute the same data concurrently to Multiple mobile Stations (MSs) through one Base Station (BS). To generate, update and distribute the group keys, the MBS applies Multicast and Broadcast Rekeying Algorithm (MBRA). The main performance parameters of group key management schemes are typically communications, computation and storage cost as well as scalability. The purpose of this paper is to review and investigate the challenges and security issues of performance parameters in different group key managements in IEEE 802.16e.

Keywords: Group key management, IEEE 802.16e, Mobile WiMAX, Group key, Rekeying, IEEE802.16.

1. Introduction

Wireless networks have become the principal technology for deployment of communications infrastructure due to their many benefits and advantages in comparison with the wired ones. In future the wireless networks will become the primary interface for network communication and main platform of applications and services [1].

Worldwide Interoperability for Microwave Access (WiMAX) [2] is a heterogeneous wireless network technology. WiMAX is designed to serve as the Metropolitan Area Networks (MANs), and it is an easier and cheaper alternative to wired networks such as backhauling cables, digital subscriber line (DSL) and T1 for various types of networks. WiMAX, which is an industry branding for IEEE 802.16 based networks [3], is derived from the IEEE 802.16 working group [4] is used to identify the air interface for Broadband Wireless Access (BWA) over a metropolitan area. IEEE 802.16e is by far the most popular version, even though newer versions i.e. IEEE 802.16m [5], have also been formulated.

As for the security model of IEEE 802.16, it has been designed to guarantee authentication, confidentiality, integrity, privacy and access control. The main aspect of security is to transfer the security keys between Base Stations (BS) and Mobile Stations (MSs), in a secure way. Hence, in The IEEE 802.16e, an enhanced key management scheme called Privacy Key Management

* Corresponding author. Email: msadeghi@ieee.org

Version 2 (PKMv2) [6] was introduced to define, manage and distribute the keys. IEEE 802.16 supports multicast applications such as pay-per-view, teleconferencing, online auction through Multicast and Broadcast Service (MBS) [6]. MBS, which is a new application feature for broadband wireless standards, constitutes an integral part of the IEEE 802.16e. In order to generate, update and distribute the security keys for secure communication over IEEE 802.16e, the MBS applies Multicast and Broadcast Rekeying Algorithm (MBRA) [6] as a basic rekeying algorithm. In this paper, we review and evaluate the challenges and security issues in existing group key management protocols in IEEE 802.16e networks.

The rest of the paper is organized as follows: Section 2 describes the performance parameters of group key management protocols. In Section 3, the review and analysis on group key management performance parameters are presented. In Section 4, we conclude the paper.

2. Group Key Managements

Typically, group key management scheme has an important role for implementing secure group communications and ensures that only legitimate members can have access to the data. A group key management scheme establishes a set of group keys for its members [7]. Group key management scheme enables a server to distribute a message to all members, such that all members can decrypt that message correctly. When a member joins or leaves, the server needs to update the group keys in order to prevent the joining members from receiving the former messages and the leaving member from getting the latter messages [8]. The procedure of key management scheme scan is divided into three tasks as follows [9]:

- **Key generation:** this refers to the process of group keys generation which will help key distribution manager to transmit keys to all authorized members.
- **Key distribution:** this relates to the delivery of keys to the members in an efficient and secure way, since members may move from one position to another in wireless networks, and the efficient-deliver of the keys to all authorized members is very important.
- **Key updating:** this refers to the update of group keys and sending them to the members, called rekeying algorithm [10]. The aim of updating the keys is to provide backward and forward secrecy.

The group key management schemes have to face many challenges, but the most important among them is on performance and security, as shown in Figure 1. Under the subject of performance, there are issues such as the operational efficiency, scalability and 1-affect-n phenomenon [11]. Operational efficiency is measured typically by storage, communications and computation costs.

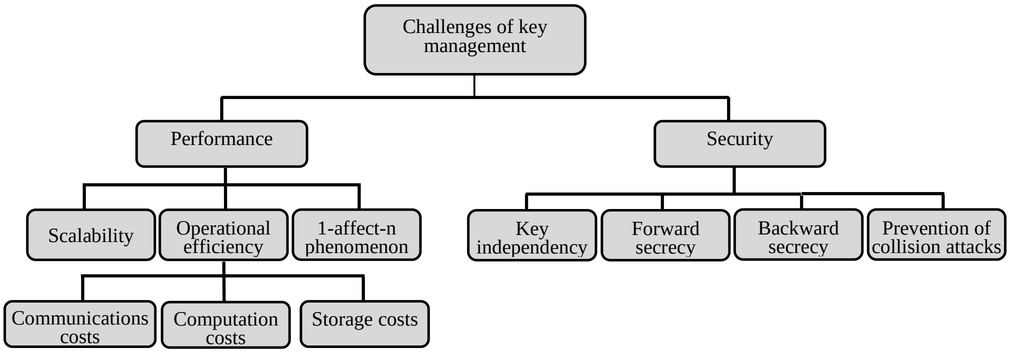

Fig. 1. Challenges in group key management

Storage costs refer to the number of number of keys stored by the server and members; communications costs refer to the number of transmitted group keys upon a rekeying algorithm, and computation costs refer to the time required of ciphering operations in order to get the updated group keys. Scalability means the capability of group key management scheme to handle large groups of members, and also its ability to manage highly dynamic membership changes. The 1-affect-n phenomenon [11] is estimated from the number of members affected by rekeying operations [12].

Generally, group key management protocols can be classified into three types of architectures, namely, Centralized, Decentralized and Distributed [13] as shown in Figure 2.

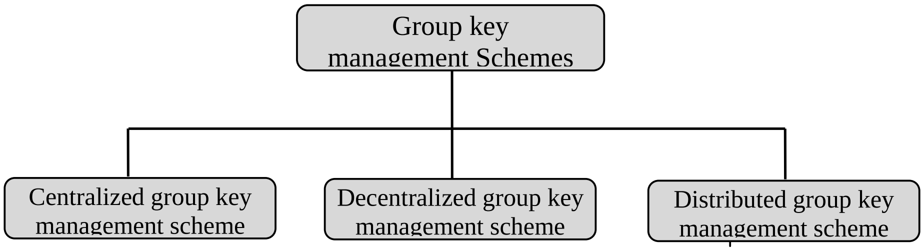
Group key management Schemes
Centralized group key management scheme
Decentralized group key management scheme
Distributed group key management scheme

Fig. 2. Group key management classification

- Centralized Group Key Managements Schemes: In centralized key management, one trusted manager controls the group keys for all groups. In the simplest centralized key management, the manager makes a unique key for each member and then encrypts the group keys with the unique key of each member, separately upon rekeying process.

- Decentralized Group Key Managements Schemes: In decentralized key management, a large group is divided in to small subgroups, and each sub group is controlled by its own manager.

- Distributed Group Key Managements Schemes: In distributed group key management schemes, there is no single manager, and the members need to contribute in order to generate the group keys.

3. IEEE 802.16 Standard Architecture

The IEEE802.16standard is a next generation communication technology. It defines a protocol architecture that is similar to other protocol stacks consisting of various layers [6]. In the following sections we discuss these protocol architectures in further details.

- Protocol Layers within IEEE 802.16

As shown in Figure 3, the protocol stack of IEEE 802.16 standard consists of two main layers: Medium Access Control (MAC) layer and Physical (PHY) layer [14]. The MAC layer is further subdivided into three sub-layers, namely Service Specific Convergence Sub-layer (CS), Common Part Sub-layer (CPS) and Security Sub-layer (SeS) [15, 16]. Each layer of the protocol stack does data processing, and then forwards them to the upper or lower layer.

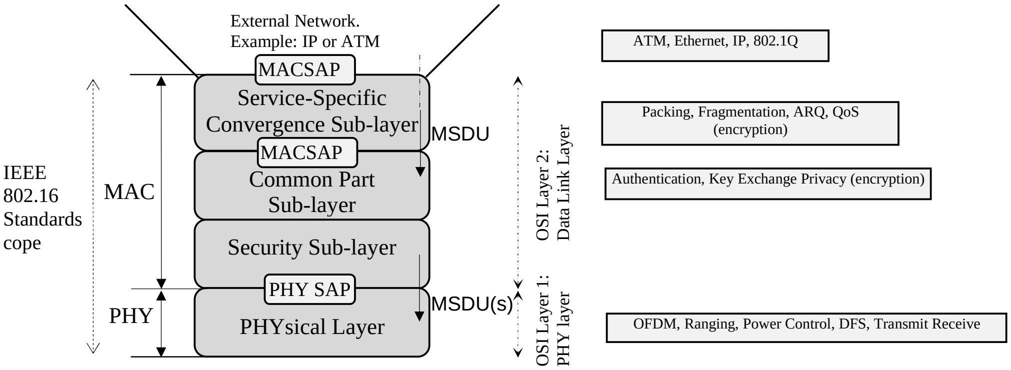
External Network.
Example: IP or ATM
MACSAP
Service-Specific Convergence Sub-layer
MACSAP
Common Part Sub-layer
Security Sub-layer
PHY SAP
PHYsical Layer
MSDU
MSDU(s)
IEEE 802.16 Standards cope
MAC
PHY
OSI Layer 2: Data Link Layer
OSI Layer 1: PHY layer
ATM, Ethernet, IP, 802.1Q
Packing, Fragmentation, ARQ, QoS (encryption)
Authentication, Key Exchange Privacy (encryption)
OFDM, Ranging, Power Control, DFS, Transmit Receive

Fig. 3. Protocol stack of IEEE 802.16 [6]

The security sub-layer lies between common part sub-layer and physical layer. It is responsible for providing authentication, authorization and secured key exchange. It is also used for encryption and decryption of data from the MAC layer to PHY layer and vice versa. It supports 3-DES for changing the keys and 56-bit DES for data traffic.

- Security Sub-layer

The architecture of security sub-layer is shown in Figure 4. As mentioned previously, the security sub-layer provides security services for the standard IEEE 802.16, and it has been made based on two main components an encapsulation protocol and a key management protocol [6].The security sub-layer is the layer where all the essential cryptographic transformations are applied to the MAC PDUs. The elementary security mechanism in IEEE 802.16 is the PKM protocol.

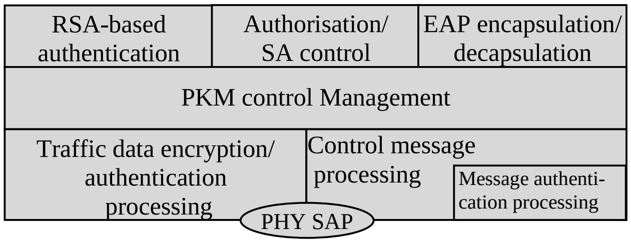
RSA-based authentication
Authorisation/ SA control
EAP encapsulation/ decapsulation
PKM control Management
Traffic data encryption/ authentication processing
Control message processing
Message authenti-cation processing
PHY SAP

Fig. 4. Security sub-layer architecture [6]

Initially, WiMAX security was introduced in the security sub-layer of IEEE 802.16 standard[17],After releasing the initial versions of the IEEE 802.16 standard, a number of articles such as[18-20]criticized the security weaknesses of the standard, and after which some security improvements were made in IEEE 802.16e[6] and IEEE 802.16m[5, 21]. The security functions regarding key managements have been addressed by PKM protocol. In IEEE 802.16d [22], the key management is based on PKMv1 protocol while IEEE 802.16e [6] uses PKMv2, which is an enhanced version of PKMv1.

Generally, PKM protocol is responsible for authorization, authentication, key exchange and data encryption in the networks between the MSs and BS. In the key exchange step, the IEEE 802.16 makes a hierarchy of keys. In fact, a key of a higher level generates the key of lower levels.

3.1. Key Management in IEEE 802.16e: Privacy Key Management Version2

The IEEE 802.16-2004 standard introduced the PKMv1 protocol as a key management protocol. Later, IEEE 802.16e introduced PKMv2 protocol with some improvements on PKMv1 protocol. The PKMv2 protocol is used by MSs to get authorization and security keys from the BS, and also to guarantee continuous and uninterrupted reauthorization/re-authentication and refreshing of the security keys. The PKMv2 applies EAP protocol together with RSA algorithm or a mixed function starting with RSA, followed by EAP. As shown in Figure 5, in EAP of PKMv2, the root of the security keys is Master Session Key (MSK), and the other keys such as Key Encryption Key (KEK) are obtained from the MSK [6].

The procedure of security keys generation using EAP is shown in Figure 5. In this figure, the output of EAP authentication protocol is MSK. Then both the MS and BS generate a Pair wise Master Key (PMK) by removing some bits of the MSK using a number of functions such as Dot16KDF, and also they generate an Authorization Key (AK) from the PMK. After generating the AK, the BS and MS will establish the Key Encryption Key (KEK) from the AK. They use a 3-way handshake to drive Traffic Key Encryption (TEK) which is used to encrypt data in the networks between the BS and MS [6].

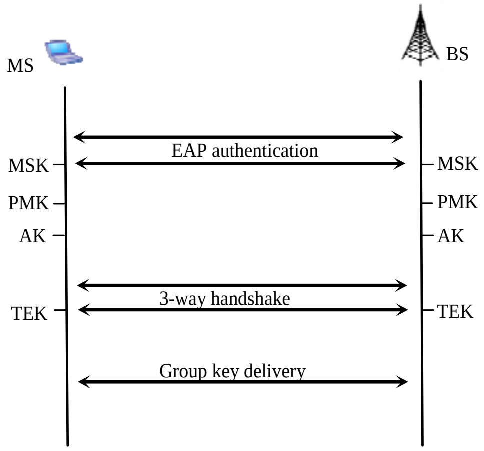

Fig. 5. Key generation at initial network entry [6]

3.1.1. *Multicast Broadcast Service (MBS)*

IEEE 802.16 supports multicast applications such as pay-TV and videoconferencing. In order to establish a secure multicast over IEEE 802.16, the IEEE 802.16e standard introduced Multicast and Broadcast Services (MBS) [6]. The MBS enables a BS as a centralized server to distribute data to many MSs in the network. In this way, only BS is able to send messages to the MSs.

The MBS of IEEE 802.16e is a new feature for broadband wireless standards [6]. It is a mechanism that allows a BS to distribute the same set of data to several MSs concurrently. As highlighted before, first the MSs need to be authenticated by the BS using PKMv2 [6]. After that, the Group Key Encryption Key (GKEK) and the Group Traffic Encryption Key (GTEK) are established, whereby the multicast service is used to send the messages by them.

The BS generates the GKEK randomly, and then sends it to MSs encrypted with the KEK of each MS. The GKEK is used to encapsulate the GTEK which is delivered by the BS to all MSs. The GTEKs are common for all MSs in a group, hence the maintenance and key updating is important.

3.1.2. *Multi cast Broadcast Rekeying Algorithm (MBRA)*

The algorithm for updating of the keys is Multicast Broadcast Rekeying Algorithm (MBRA) [6].The MBS of IEEE 802.16e introduced the MBRA as a basic rekeying algorithm to generate, update and distribute the GKEKs and GTEKs upon member changes. The MBRA uses the GTEK which is shared among all MSs to encapsulate the data traffic. The BS generates the GKEK and the key is used to encapsulate the GTEK. The GKEK is also encapsulated by a KEK of each MS.

Although the MBRA of MBS is quite well designed, it still suffers from efficiency and scalability problem, and does not address backward and forward secrecy [23]. To explain this point, in the MBRA algorithm, the BS should unicast n messages, where n is the number of MS in order to update the group keys. Unfortunately, this would cause weak scalability due to the increased number of unicast messages. Moreover, when there are high numbers of MSs, the effect of sending high volume of unicast as well as broadcast messages would increase communication costs, and accordingly results in poor efficiency. Moreover, there could be insider attacks in the MBRA, meaning that the owner of a common GKEK can cause security breach for the rest of the members [24, 25]. Rekeying algorithms in WiMAX networks need to be executed in the case of any one of three events:

1) When a new MS joins the BS,

2) When the life time of both GTEK and GKEK expire,

3) When an MS leaves the BS.

The event 2 above can be considered as two separate events, because the lifetime of GTEK is not equal to that of GKEK [6]. In fact, the life time of GKEK is several times longer than GTEK, in order to encrypt and distribute more than one GTEK. This part of the calculation involving the lifetimes of GTEK and GKEK has been assumed equal in some papers such as [23]. In general, Event 3 is the most critical event.

In IEEE 802.16e, the role of MBRA is to send and refresh GTEKs and GKEKs. Among all three types of events as mentioned above, the MBRA rekeying algorithm only happen at the expiration time of GTEK or GKEK. As shown in Figure 6, from time to time, the BS broadcasts message (1) encrypted by GKEK to all MSs in order to update the GTEK as well as sending a unicast message (2) to all MSs which has been encapsulated by the KEK of each MS. This is represented by the equations below, and the nomenclatures are listed in Table 1.

$$BS \Rightarrow all\ MS : \{GTEK\}_{GKEK} \tag{1}$$

$$BS \rightarrow each\ MS : \{GKEK\}_{KEK} \tag{2}$$

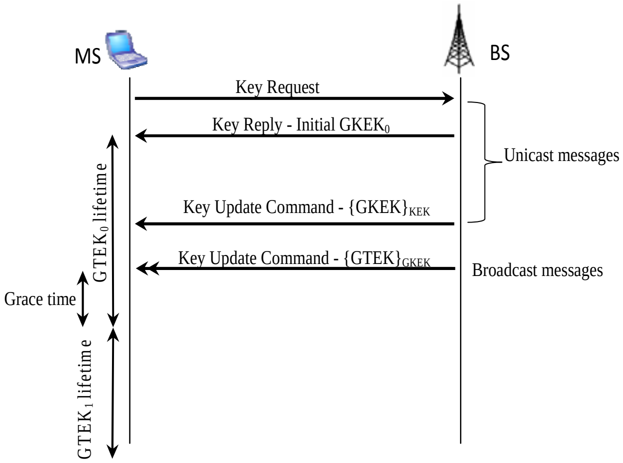

Fig. 6. MBRA messages [6]

Table 1

Nomenclature of key management

N	The number of subgroups
n	The number of MSs
s	The number of MSs per subgroup
$X \Rightarrow Y$	X broadcasts a message to Y
$X \rightarrow Y$	X unicasts a message to Y
$[X]_Y$	X encrypted by using key Y
MS_{SGi}	The collection of all MSs within sub group$_i$

3.2. Related Works on Key Management in IEEE 802.16

As highlighted earlier, in MBRA the number of unicast messages upon rekeying increase with the number of MSs, and hence this method is neither scalable nor efficient. In addition, it does not support forward and backward secrecy, which consequently makes this method vulnerable to attacks [18, 19]. In the literature, researchers have proposed new key management protocols to address the shortcomings of MBRA. In the following we discuss and evaluate the existing key management schemes in IEEE 802.16e.

3.2.1. Enhancement of the MBRA algorithm

The authors in [26] proposed a new improved method for the MBRA. Here, the GTEK, which is encrypted with KEK (not GKEK), is unicast to each MS directly. This method does not have issues with insider attacks, because an attacker needs to get the knowledge of KEK. Also, since this method uses fewer keys, and therefore it would require less storage. However, this method has a poor scalability, because of sending n unicast messages upon key updating, where, n is the number of MSs. In addition, the other issue is the lack of forward and backward secrecy.

3.2.2. Secure Multicast Protocols

Researchers in [23] performed a detailed analysis of the MBRA algorithm and identified its deficiencies. They proposed an improved scheme, which is secure multicast protocol, to address the deficiencies identified. Their scheme also considered that the being of GKEKs is not necessary. In the initial step of key updating in the proposed method, the BS sends n (n being the number of MSs) unicast messages to deliver GTEK, plus one broadcast message to send a notification message. However, in this method, unlike the method in [26], in member join and leave events, key updating is done by broadcasting a key update notification message. With broadcasting this notification message, the MSs generate a new GTEK by themselves by using old GTEK through a hash function.

Even though their method showed some improvements on the MBRA, they suffer a downside in that; the BS needs to send n unicast messages upon every membership changes. This consequently results in the drastic drop in network efficiency for a large number of MSs. In addition, the proposed algorithm also sends some plaintexts for message broadcasting which could cause critical security breaches [24]. In fact, despite some improvements to the MBRA rekeying, the proposed method suffers from security issues such as Denial of Service (DoS) [24] as well as poor scalability and efficiency. In addition, it does not address 1-affect-n phenomenon very well.

3.2.3. Group-Based Key Distribution Algorithm

The authors in [27] proposed a new group key management protocol called Group-Based Key Distribution Algorithm (GKDA) in which the security keys are distributed in to subgroups. In this method, the MBS group is first divided into N subgroups; hence, N GKEKs for the subgroups are used instead of one GKEK being shared among all MSs. By doing so, only that GKEK which is used for a certain subgroup needs to be updated whenever any membership change (e.g. leave event) occurs in that subgroup. The GKEK is encapsulated by each of the MS's KEK in the subgroup, and then unicast to each MS. Although the GKDA provides forward and backward secrecy, it is not scalable and efficient enough, because when the number of MSs in each subgroup grows bigger, the number of unicast messages to update the GKEKs grows likewise. Never the less, the GKDA is still better than MBRA in terms of reducing the number of unicast messages needed to perform updates of the group keys. In GKDA, the GTEK update mode is more lengthy because it consists of N GTEKs which are encapsulated by N GKEK, and thus it consumes more energy to send the messages. Moreover, the proposed method does not address the 1-affect-n phenomenon very well.

3.2.4. Efficient sub-Linear rekeying Algorithm with Perfect Secrecy

In [28, 29], the authors proposed an algorithm called Efficient sub-Linear rekeying Algorithm with Perfect Secrecy (ELAPSE). This is based on key hierarchy, where a fixed binary tree [30] depth is used to partition the MSs into subgroups in order to overcome the deficiencies of MBRA algorithm. However, such a scheme is not suitable in dynamically changing membership environment, since scalability as well as efficiency may be seriously jeopardized. The problem with this algorithm is that it pre-assigns a permanent number of subgroups, N, which is independent of the number of current MSs and may not fit for too large or too small groups. The number of subgroups is manually defined by the administrator in advance, i.e. the number of subgroups is permanent. The result is weak performance in terms of efficiency and scalability; especially when the members join or leave events happen frequently within a large group. Here, all MSs have common GTEK but each MS in a particular subgroup keeps a set of Sub Group Key Encryption Keys (SGKEKs) instead of one GKEK.

As mentioned earlier, the ELAPSE identified that the value of N must be defined at the outset by the administrator in advance. However, in the face of a high changing rate of dynamic members, the number of MSs instantaneously increases and decreases following the changing rate of members. With this scheme, which uses constant tree depth, this high changing rate will cause high rekeying operations. Hence, the results are performance degradation in terms of communications, computation and storage overheads. In the case of IEEE 802.16e, because of the random nature of members joining or leaving the network, as well as how long they stay within the BS's cell, it would not be optimal to assign a fixed number of subgroups (e.g. 4), since when there is a high number of MSs for a period of time, a high volume of key updating messages would be generated within the cells by means of broadcasts and unicasts messages. On the other hand, in cases when the number of MSs is low for the other period of time, a high level of storage and computation costs are expended for both BS and MSs. Hence, there is a dire need for a dynamic and flexible key management scheme that can adjust itself according to the existing number of MSs in order to perform the rekeying algorithm efficiently.

The ELAPSE basically establishes subgroups by employing a binary tree. As such, GKEK is not delivered to each MS via a unicast message; instead, it is distributed among the subgroups through broadcast messages. Here, the MSs are divided into subgroups where each subgroup keeps and stores a hierarchical key set instead of a single one (GKEK).Figure 7 illustrates a schematic diagram of a binary tree with four subgroups, where SGKEK is an abbreviation for "Sub-Group Key Encryption Key". All MSs maintain same GTEK, and each MS in each subgroup saves a set of SGKEKs, for example, the MSs in subgroup1 store three group keys SGKEK1, SGKEK2 and SGKEK1234. The SGKEK1234 acts as the traditional GKEK in the MBRA.

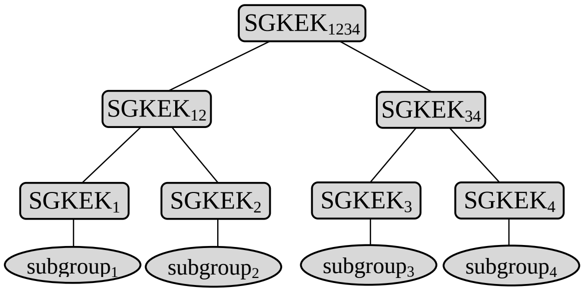

Fig. 7. Key hierarchy with four subgroups [29]

When there is no new member joining or leaving, and the life time of GTEK expires, the BS broadcasts a new GTEK encrypted by SGKEK1234to all MSs represented as message (2.3) below.

$$BS \Rightarrow all\ MSs : \{GTEK\}_{SGKEK_{1234}} \quad (3)$$

Upon a member join event, and subgroup2 happens to be the subgroup with the lowest membership, then the BS assigns the new MS to subgroup2.The BS unicasts message (4) below to the new MS and all existing MSs in the subgroup2in order to update the group keys. Message (4) is encapsulated by KEK of each MS, and contains all new group keys from subgroup2 to the root of binary tree.

$$BS \rightarrow MS_{SG2}\ \&\ new\ MS : \{GTEK, SGKEK_{1234}, SGKEK_{12}, SGKEK_2\}_{KEK} \quad (4)$$

To provide backward secrecy as well as to update the group keys, the BS needs to send two broadcasts i.e. messages (5) and (6), to all MSs excluding subgroup2.

$$BS \Rightarrow MS_{SG3}, MS_{SG4} : \{GTEK, SGKEK_{1234}\}_{SGKEK_{34}} \quad (5)$$

$$BS \Rightarrow MS_{SG1} : \{GTEK, SGKEK_{1234}, SGKEK_{12}\}_{SGKEK_1} \quad (6)$$

Upon member leave event, the procedure of the rekeying algorithm is similar to that of the member join event. For instance, when one MS of subgroup2leaves a BS, then the BS should unicast message (7) to all the remaining MSs in subgroup2. It also needs to broadcast two messages, i.e. messages (8) and (9), to all MSs except subgroup 2.

$$BS \rightarrow MS_{SG2} : \{GTEK, SGKEK_{1234}, SGKEK_{12}, SGKEK_2\}_{KEK} \quad (7)$$

$$BS \Rightarrow MS_{SG3}, MS_{SG4} : \{GTEK, SGKEK_{1234}\}_{SGKEK_{34}} \quad (8)$$

$$BS \Rightarrow MS_{SG1} : \{GTEK, SGKEK_{1234}, SGKEK_{12}\}_{SG\,KEK_1} \quad (9)$$

3.2.5. Hybrid Group Key Management

The authors in [31] proposed a hybrid group key management scheme to improve the performance of ELAPSE upon rekeying by reducing message passing. This scheme uses the architecture of LORE [32] within a subgroup of ELAPSE. In this way, when an MS enters a BS coverage area, the BS assigns it to a subgroup and also provides a Subgroup Forward Key Set (SGFSet) and Subgroup Backward Key Set (SGBSet). These key sets are created by simple Pseudo-Random Number Generator (PRNG) and keep the ordering of nodes inside a subgroup similar to LORE. Hence, if there is k MSs in a subgroup, then there are k numbers of Subgroup Forward Key (SGFK) and k numbers of Subgroup Backward Key (SGBK). In this way, for each MS i there are two set as follows:

$$SGFSet = \{SGFK_m \mid 1 \le m \le i\} \quad (10)$$

$$SGBSet = \{SGBK_m \mid i \le m \le k\} \quad (11)$$

Figure 8 shows the revised version of ELAPSE. Here, a node i in subgroup2has three keys SGKEK1234, SGKEK12 and SGKEK2 as well as two keys set SGFSeti2 and SGBSeti2. Upon member join or leave event, the rekeying algorithm updates SGKEKs and GTEK, but there is no change in SGFSet and SGBSet sets. After a predefined time T, both SGFSet and SGBSet will be renewed.

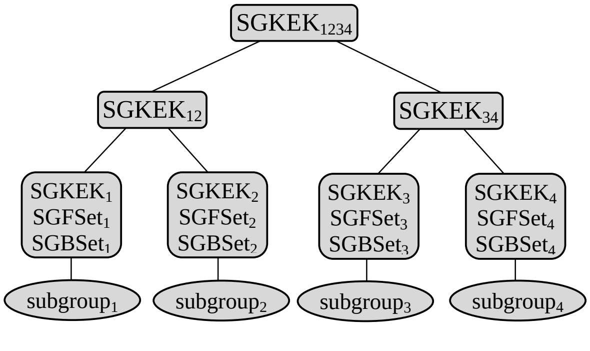

Fig. 8. A revised version of ELAPSE [31]

It should be noted here that this improvement in communication costs over ELAPSE, comes at high computation and storage costs in the revision version of

ELAPSE. Moreover, this method gives rise to security issues like collusion resistance [31] which means two or more MSs must not get secret keys that they are not allowed to know, and this is done by exchanging their respective secret keys.

3.2.6. n-ary Group Key Management

The authors in [33, 34] improved ELAPSE method by using a n-ary tree (where n>2) to improve the efficiency of group key management. Even though the proposed method shows some improvements on the efficiency of ELAPSE, the method still suffers from the limitations associated with fixed number of subgroups. In this method, the tree depth becomes large when the number of MS increases and this is the main issue with a binary tree. Therefore, they suggested that by using n-ary (n>2), the efficiency of group key updating algorithm will improve. Figure 9 shows a 3-ary tree with 9 subgroups.

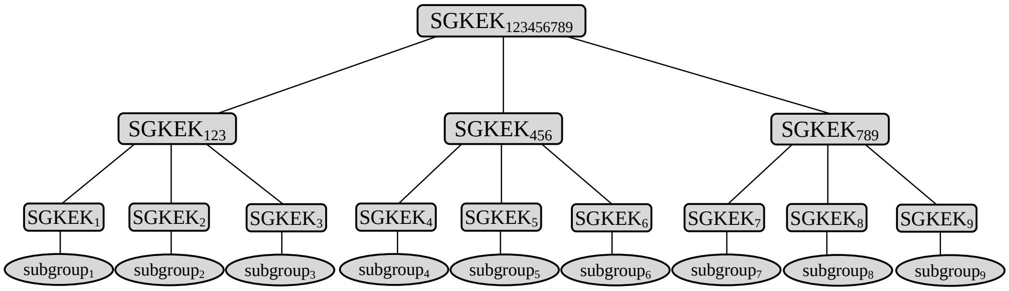

Fig. 9. A 3-ary tree [33]

The number of group keys in n-ary tree and the tree depth are given by equation $k=\sum_{i=0}^{d} n^{i}$ and $d=\left\lceil \log_{n} N \right\rceil$, respectively[33].

By using n-ary tree, the BS needs to keep more group keys compared with ELAPSE method. So, in terms of storage costs, n-ary tree does not perform very well, even though the communication costs is considerably decreased due to the reduction in communication overheads upon group keys updating. The authors made detailed analysis to find the optimal value of n in order to minimize the total energy consumption of the rekeying algorithm. They assumed that transmission and reception energy are equal to total energy consumption of the networks whereby, the energy consumption is represented by the length of broadcast or unicast messages. Finally, they came out with an optimal value of n=4, meaning that 4-ary tree give the best performance in terms of energy consumption.

Moreover, the proposed method used a hash function to enable MSs to generate their keys by themselves. Here, the BS does not unicast or broadcast messages for rekeying process. The method improves the efficiency of the rekeying algorithm because unicasting of the messages happens in the initial phase of rekeying process only. In addition, in this method all MSs share a common GTEK, hence it is vulnerable to insider attacks, and from a security point of view it should be considered very weak.

3.2.7. Asymmetric Group Key Management

The authors in [24] proposed a new method of improving MBRA using asymmetric algorithms such as bilinear maps and ECC. The idea of this method is to establish a common encryption key which is shared among all MSs and even attackers, but every MS has different decryption key. That means, the BS can encrypt the messages including the group keys, and only the valid MS can decrypt the messages. In this way, the proposed method provides backward and forward secrecy, and this is not vulnerable against insider attacks. In terms of operational efficiency, this method needs to perform more computations because of the use of asymmetric cryptography, and hence it consumes more energy in the MSs, which is not good for mobile devices.

However, one advantage of the proposed method is that it sends less unicast or broadcast messages, and hence the overall communication cost is low. In this way, upon member changing, the BS sends a broadcast messages, but on normal key refresh, it needs to send n unicast messages, where n is the number of MSs and also the BS should send two broadcast messages. This method managed to address the backward and forward secrecy issue of the MBRA algorithm. However, it has poor response to scalability, since upon group key updating after the expiration time; it has to send n unicast messages. Moreover, the method needs to make numerous modifications to the standard, which is not practical for implementation in real environment.

Finally, Table 2 summarizes the main characteristics of the rekeying algorithms which have been highlighted in this paper.

Table 2

Summary of the main performance parameters of rekeying algorithms

Scheme	Forward/ Backward Secrecy	Scalability &1-affect-n	Operational efficiency	Comparison
MBRA [6]	not supported	Very weak	non optimal	It does not group the MSs, and hence new group keys need to send to all MSs by unicast messages.
Xu et al. [23]	supported	weak	non optimal	It sends unicast messages to all MS to update the group keys. It suffers from security issues such as DoS. It does not group the MSs.
GKDA [27]	supported	weak	low optimal	It divides the MSs into N subgroups, and upon rekeying; only the group keys in that particular subgroup will be updated by sending unicast message. It does not use tree structures.
ELAPSE [29]	supported	good	optimal	It establishes a fixed Binary tree depth in order to subgroup the MSs. Hence with dynamic member changing, it is not a good enough scalable and efficient.
Chakraborty et al. [31]	supported	good	low optimal	It uses the special architecture within a subgroup of ELAPSE to improve the communication costs, however, computation and storage costs is high.
Brown et al. [33, 34]	supported	good	optimal	It uses n-ary tree to to group the MSs. The scheme suffers from predetermined number of subgroups similar to ELAPSE.
Kambourakis et al. [24]	supported	good	low optimal	It does not use tree strucute. It apply asysmetric algorithm which is not practical for implementation in real environment.

4. Summary

For next generation wireless networks, group key management is very important in providing access control for a group of applications in the wireless environment; for example, a service provider like a TV station can offer several applications for the subscribers, such as channel for news, movie, sport etc. Considering limited resources on both wireless and mobile devices, to manage and control users through an efficient group key management in critical.

In this paper, we explained the IEEE 802.16 networks and the MBRA rekeying algorithm, and investigated and reviewed the literature related to the group key management performance parameters. In the literature performance parameters are very important in rekeying; hence we analyzed the previous works in terms of performance challenges.

References

[1] R. Prasad and F. J. Velez, WiMAX Networks: Springer, 2010.

[2] J. G. Andrews, et al., Fundamentals of WiMAX: Understanding Broadband Wireless Networking: Pearson Education, 2007.

[3] C. Eklund, et al., "IEEE standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access," 2002.

[4] IEEE 802.16 Working Group website. Available: http://WirelessMAN.org, August 2014.

[5] "IEEE 802.16 Work Group: IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment 3: Advanced Air Interface," Ed, 2011.

[6] "IEEE 802.16 Work Group. IEEE Std 802.16e: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Amendment and Corrigendum to IEEE Std 802.16-2004," ed: IEEE, 2006.

[7] C. Guo and C.-C. Chang, "An Authenticated Group Key Distribution Protocol Based on the Generalized Chinese Remainder Theorem," International Journal of Communication Systems, Vol. 27, pp 126-134, 2014.

[8] Q. Xie, "A New Authenticated Key Agreement for Session Initiation Protocol," International Journal of Communication Systems, vol. 25, pp. 47-54, 2012.

[9] X. He, et al., "Dynamic Key Management in Wireless Sensor Networks: A survey," Journal of Network and Computer Applications, vol. 36, pp. 611-622, 2013.

[10] E. E. Mohamed and E. Barka, "OMAC: A New Access Control Architecture for Overlay Multicast Communications," International Journal of Communication Systems, vol. 24, pp. 761-775, 2011.

[11] S. Gharout, et al., "Key Management With Host Mobility in Dynamic Groups," in International conference on Security of information and networks New York, USA, pp. 186-193, 2010,

[12] H. Lee, et al., "User-Oriented Key Management Scheme for Content Protection in OPMD Environment," IEEE Transactions on Consumer Electronics, vol. 58, pp. 484-490, 2012.

[13] J.-S. Li, et al., "Distributed key management scheme for peer-to-peer live streaming services," International Journal of Communication Systems, 2012, Vol. 26, pp 1259-1272. 2013.

[14] "IEEE 802.16 Work Group. IEEE Std 802.16: Air Interface for Broadband Wireless Access Systems and Revision of IEEE Std 802.16-2004," ed: IEEE, 2009.

[15] S. Ahson and M. Ilyas, WiMAX: Standards and Security. CRC Press, Inc. Boca Raton, FL, USA, 2008.

[16] K.-C. Chen and J. R. B. d. Marca, Mobile WiMAX: John Wiley & Sons, Ltd., 2008.

[17] "IEEE 802.16 Work Group. IEEE std 802.16: Air Interface for Fixed Broadband Wireless Access System," ed: IEEE, 2002.

[18] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," IEEE Security and Privacy, vol. 2, pp. 40-48, 2004.

[19] A. Deininger, et al., "Security Vulnerabilities and Solutions in Mobile WiMAX” IJCSNS International Journal of Computer Science and Network Security vol. 7, pp. 7-15, 2007.

[20] T. Shon, et al., "Novel Approaches to Enhance Mobile WiMAX Security," EURASIP Journal on Wireless Communications and Networking, vol. 2010, pp. 11 pages, 2010.

[21] "P802.16m/D6, IEEE Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Broadband Wireless Access Systems - Advanced Air Interface," May 2010

[22] "IEEE 802.16 Work Group. IEEE std 802.16: Air Interface for Fixed Broadband Wireless Access System," ed: IEEE, 2004.

[23] S. Xu, et al., "Secure Multicast in WiMAX," Journal of Networks, vol. 3, pp. 48-57, 2008.

[24] G. Kambourakis, et al., "Revisiting WiMAX MBS security," Computers and Mathematics with Applications, vol. 60, pp. 217-223, 2010.

[25] C. Kolias, et al., "Attacks and Countermeasures on 802.16: Analysis and Assessment," IEEE Communications Surveys and Tutorials, vol. 15, pp. 487-514, 2013.

[26] S. Naseer, et al., "Vulnerabilities Exposing IEEE 802.16e Networks to DoS Attacks: A Survey," in Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD '08), Thailand, pp. 344-349, 2008.

[27] H. Li, et al., "GKDA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security," Advances in Multimedia Information Processing, LNCS, Springer Verlag, vol. 4261, pp. 310-318, 2006.

[28] C.-T. Huang, et al., "Efficient and Secure Multicast in Wireless MAN: A Cross-layer Design," Journal of Communications Software and Systems, vol. 3, pp. 199-206, 2007.

[29] C. T. Huang and J. M. Chang, "Responding to Security Issues in WiMAX Networks," IEEE IT Professional vol. 10, pp. 15-21, 2008.

[30] J. A. Store, An Introduction to Data Structures and Algorithms. Waltham, USA: Birkhauser, Springer, 2011.

[31] S. Chakraborty, et al., "A Scalable Rekeying Scheme for Secure Multicast in IEEE 802.16 Network," Communications in Computer and Information Science, Springer, vol. 132, pp. 471-481, 2011.

[32] J. Fan, et al., "HySOR: Group Key Management With Collusion-Scalability Tradeoffs Using a Hybrid Structuring of Receivers," in Eleventh International Conference on Computer Communications and Networks, pp. 196-201, 2002.

[33] J. Brown, et al., "Efficient Rekeying Algorithms for WiMAX Networks," Security and Communication Networks, vol. 2, pp. 392–400, 2009.

[34] J. Brown and X. Du, "Towards Efficient and Secure Rekeying for IEEE 802.16 e WiMAX Networks," presented at the IEEE Global Telecommunications Conference (GLOBECOM) 2009, Honolulu, HI, 2009.