Safe Multicast approach in Wireless MAN

Zohaib Hasan Khan[1] Mohd Tabrej Alam[2] Piyush Charan[3] Mohd Amir Ansari[4]
[1,2,3,4]Department of Electronics & Communication Engineering
[1,2,3,4]Integral University, Lucknow

Abstract— Multicast delivery of information is an intense component that has solid potential. The favourable effectiveness over unicast is a positive position, however the utilization of multicast postures numerous security dangers. Adequately adding efforts to establish safety to a multicast administration is a fascinating issue, particularly when the administration is conveyed in a remote setting. Next era IEEE 802.16 standard Wireless MAN systems are a flawless case of this issue, and the most recent draft particular of the standard incorporates a protected convention arrangement called Multicast and Broadcast Rekeying Calculation (MBRA). In this paper, we uncover the security issues of MBRA, including non-adaptability and exclusion of in reverse and forward secrecy, and propose a new approach, ELAPSE, to address these issues. We break down the security property of ELAPSE and utilization Qualnet recreations to demonstrate its productivity.

Key words: Wireless MAN, Safe Multicast

I. INTRODUCTION

There are numerous rising applications that rely on upon secure gathering correspondences, which require the protection of members and access control at the multicast server. On the other hand, adaptability is another basic sympathy toward the multicast administration hidden these applications because of the conceivable vast number of gathering individuals. In the area of wired systems, proficient and secure multicast is a generally mulled over issue and a few mainstream conventions have been proposed. This is not so much valid for the area of remote systems, where consideration has been less critical.

Wireless systems have turned out to be more pervasive because of their numerous points of interest. The IEEE 802.16 standard [1] means to give broadband remote access to Metropolitan Territory Networks (MAN) and the as of late discharged IEEE 802.16e [2] includes versatility elements and some different capacities counting multicast. Multicast in Wireless Metropolitan Area Systems (Wireless MAN) is a promising administration, suitable for numerous applications, for example, investment opportunity offering, pay per view Television TV, feature conferencing, and so forth for both settled and portable supporter stations (SS).

The test of a safe multicast administration, for example, the one in IEEE 802.16, is to give a proficient system to controlling access to the gathering and its interchanges. Encryption of gathering messages and particular delivery of the keys utilized for encryption is the essential technique for guaranteeing the security. For a dynamic gathering in which enrollment changes much of the time, the rekeying calculation utilized by the administration is a discriminating element of the general administration effectiveness. This calculation ought to ensure forward secrecy, which keeps a leaving part from getting to future correspondences; and in reverse secrecy, which keeps a joining part from getting to previous correspondences. On the other hand, a rekeying calculation ought to be effective as well. That implies it ought to be adaptable to a substantial gathering and display great execution amid key circulation; execution being measured by correspondence multifaceted nature, focus (server) space multifaceted nature, and client (part) space multifaceted nature. This paper surveys the Privacy and Key Management (PKM) convention (regarding the multicast setting) and the Multicast and Broadcast Rekeying Algorithm (MBRA) in IEEE 802.16e. The shortcomings of these conventions are definite and ELAPSE (Efficient sub-Linear rekeying Calculation with Perfect Secrecy), a subordinate of the Logical Key Hierarchy is proposed. Slip by beats the absence of in reverse and forward secrecy of the 802.16 MBRA and works all the more effectively generally. Whatever is left of the paper is composed as takes after. In Section II, we audit the IEEE 802.16e answer for secure multicast rekeying, with its shortcomings underlined. In Section III, related takes a shot at different ways to deal with secure multicast are depicted, and a complete portrayal of our methodology, ELAPSE, follows in Segment IV. In Section V, ELAPSE is assessed for its effectiveness utilizing the system test system Qualnet, and after that conclusions are made in Section VI.

II. CURRENT 802.16E STANDARD

The Multicast and Broadcast Service in IEEE 802.16 is an proficient and force sparing component, which likewise gives supporters with solid security from robbery of administration by scrambling show associations between a SS and BS. The Multicast and Broadcast Rekeying Algorithm (MBRA) is used to invigorate movement keying material for the multicast administration of IEEE 802.16. Before getting multicast administration, a SS must regsiter and validate with a base station (BS), amid which the BS chooses the level of administration to be approved. By utilization of the extending method on the Initial Ranging or Fundamental Connection, a SS builds up a Primary Management Connection with a BS that is utilized to trade MAC administration messages. On the off chance that the SS is to be dealt with, a Optional Management Connection is set up between the SS and BS. A Secondary Management Connection is used to exchange delay-tolerant, benchmarks based messages inside IP datagrams, for example, DHCP, TFTP, and SNMP.The Privacy Key Management messages are traded through the Primary Management Connection, with the special case that PKMv2 Group-Key-Update-Command is exchanged over the Broadcast Connection. The Privacy and Key Management (PKM) convention is connected in the IEEE 802.16 security sublayer inside of the 802.16 MAC layer and performs two capacities. To begin with, the PKM convention gives secure circulation of keying material from a BS to SS, and second, the convention empowers a BS to authorize access control over system administrations. A brief synopsis of a PKM convention keep running between a SS and BS is as per the following. The SS starts the convention and first confirms with a BS

(PKMv2 moreover gives common confirmation), setting up a mutual secrecy — an Authentication Key (AK). The BS will likewise send a Secure Association Identifier (SAID) list, which shows the administrations expressly approved to the SS. At that point by a Key-REQ message from SS to BS and Key-RSP message from BS to SS, the SS gets the keying material that is suitable for a determined SAID. Before continuing with the subtle elements of the current standard, let us quickly talk about a paltry answer for securing multicast activity

A. Trivial Solution

In this trivial solution, multicast movement is sent from the BS to all SS encoded utilizing a solitary gathering wide session key, on the other hand Group Traffic Encryption Key (GTEK). It is expected that all SS have the present key prepared to decode the multicast information. At the point when another SS wishes to join the gathering, a person solicitation is sent to the BS for the GTEK. The BS reacts to the new SS with another GTEK, and after that additionally sends the overhauled GTEK to all current SS independently (all person trades are encoded with keys set up through a past validation instrument). At the point when a part wishes to leave the gathering, the BS should again send another GTEK to all different SS independently. Albeit offering solid in reverse furthermore, forward secrecy, this minor arrangementhas numerous issues, in particular not being versatile because of the numerous unicast key trades.

B. 802.16 Standard

The IEEE 802.16 standard offers some change to this trifling arrangement. A lifetime is determined for the GTEK and in this way the GTEK will lapse after a certain measure of time. To guarantee convenient delivery of new GTEKs before close of the current one, the utilization of a Group Key Encryption Key (GKEK) is determined. The GKEK has a lifetime that parallels the lifetime of the comparing GTEK. By utilizing this GKEK to scramble the GTEK, new GTEKs can be show to all SS. A SS may get the starting Group Traffic Encryption Key (GTEK), which is utilized to scramble the multicast movement, by Key Request and Key Reply messages over the Primary Administration Connection. A BS redesigns and disseminates the activity sending so as to key material occasionally two Group Key Update Command messages: for the GKEK upgrade mode what's more, for the GTEK overhaul mode. The Group Key Encryption Key (GKEK) is utilized to encode the GTEK in GTEK overhaul mode. Irregularly, a BS transmits the (1) Key Update Charge message for GKEK overhaul mode to each SS through its Primary Management Connection. This message contains the new GKEK scrambled with the Key Encryption Key (KEK), which is gotten from the Authorization Key (AK) built up amid validation. At that point, the BS transmits the (2) Key Update Command message for GTEK overhaul mode through the Broadcast Connection, which contains the new GTEK scrambled with the relating GKEK. The convention can be determined as takes after.

$$BS \rightarrow SS: \{GKEK\}_{KEK} \quad (1)$$

$$BS \rightarrow \text{all SS}: \{GTEK\}_{GKEK} \quad (2)$$

Where (1) stands for a unicast message and (2) remains for a broadcast message. There are still two issues with this convention. Firstly, this convention is not adaptable as regardless it needs to unicast to each SS. It can be summed up, particularly in a possibly expansive system, for example, a Wireless MAN, that any rekeying plan contingent upon unicast techniques is not adaptable. Besides, this convention does not address the issue of in reverse and forward secrecy. On account of part joining, when another part gets the current GTEK, it can decode all past messages that were multicast amid the lifetime of the same GTEK. On account of part leaving, there is nothing in this convention that keeps a leaving SS from accepting the following GKEK and unscrambling the following GTEK. Note that the lifetimes of GTEKs as determined by the IEEE 802.16 standard are an imperative security thought. At present, the extent is determined to be 0.5 hours least, 12 hours as a matter of course, and 7 days most extreme [2]. This lifetime has awesome influence on the relationship in the middle of versatility and forward/in reverse secrecy gave by the standard. A long enough lifetime should be kept up to permit a BS enough time to exclusively redesign the GKEK so the new GTEK can be show. Then again, more GTEK lifetimes suggest much more noteworthy failures in reverse/forward secrecy on part join/leave occasions, separately, as there will be more messages encoded utilizing the given GTEK.

III. RELATED WORKS

Since the first form of the IEEE 802.16 standard [3] was discharged in 2002, a couple articles and books have been distributed. In [4], the seat of the standard gives a specialized review of IEEE 802.16. In the range of 802.16 gathering individuals moreover distributed a book [5] in 2006, which gives a definite review of the standard and clarifies the method of reasoning behind improvement choices. The creators of [6] audit the standard, dissect the security gave by the standard, and talk about the prerequisite of common validation between SS what's more, BS. In [7] the PKM convention is talked about in subtle element, more assaults on the variants of the PKM conventions recorded in [3] and [5] are found, and updates of PKM conventions are proposed. In [8], another assault on PKM variant 2 in [2] is nitty gritty. On the other hand, none of these distributions cover the MBRA variant discharged in before 2006 [2].

There is a report [9] which examines the IEEE 802.16 MBRA, which particularly concentrates on replay assaults against the MBRA, like the assaults recorded in [6], [7] and [8]. Then again, it doesn't cover the regressive and forward secrecy stood to correspondences before/in the wake of rekeying, or the effectiveness of the MBRA, both of which are vital to a alluring, secure rekeying calculation.

All the more for the most part, secure multicast has been a mainstream point in the previous ten years, and numerous conventions have been proposed. [10] and [11] are the initial few works managing secure multicast, in which direct, yet not versatile routines, are portrayed. The Iolus methodology definite in [12] is a disseminated technique in which a progressive system of specialists is utilized as subgroup controllers. Utilizing Iolus, versatility is guaranteed since part changes in one subgroup don't influence other subgroups. It likewise gives other promising components, for example, adaptation to non-critical failure. On the other hand, Iolus may not be straightforwardly material to the 802.16 environment in which there is just one

server (BS) and various customers (SS), and may not make the best utilization of the property of 802.16 that each SS inside of the radio scope of BS can get the multicast messages in one bounce. Kronos [17], takes an interesting periodical rekeying approach that rekeys the gathering just at determined time interims. Standard rekeying upon part changes are postponed until the following rekeying interim, along these lines the number of rekeying is decreased.

Logical Key Hierarchy (LKH) tree calculations are proposed in [13] and [14], which give O(log n) correspondence intricacy, where n is the quantity of gathering individuals. There are three patterns in the Versa-key structure [15], one of which is a brought together tree-based administration plan. It applies a restricted capacity to redesign a key tree upon individuals joining, and along these lines is additionally alluded to as LKH+. In [16] a half breed framework is suggested that incorporates LKH with a basic level pattern, giving a group of key administration calculations as indicated by the quantity of individuals in every subgroup. Every subgroup is then sorted out as a leaf in the LKH tree. By partitioning the gathering into subgroups with O(log n) individuals, the calculation shows just O(n/log n) focus space many-sided quality. The creators of [16] case it is the to begin with rekeying calculation to require just sublinear space at the server.

In this paper, ELAPSE, a different option for the IEEE802.16 MBRA is proposed. Slip by is a more effective option that gives finish in reverse and forward secrecy to interchanges, and coordinates the upsides of the methodologies displayed in [16] and [17] to accomplish better proficiency.

IV. ELAPSE

We have built up that MBRA distributed in the most recent 802.16 standard is inadequate. As specified, the MBRA offers just unobtrusive upgrades over a unimportant arrangement. A fitting arrangement ought to keep up in reverse secrecy and forward secrecy. From these objectives, an enhanced MBRA must re-key on part joins, on part leaves, and intermittently we have built up that MBRA distributed in the most recent 802.16 standard is inadequate. As specified, the MBRA offers just unobtrusive changes over a trifling arrangement. A legitimate arrangement ought to keep up in reverse secrecy and forward secrecy. From these objectives, an enhanced MBRA must re-key on part joins, on part leaves, and intermittently if there is no part join or part take off.

The center of the methodology displayed here will be subgrouping SS so that the GKEK won't be looked after by means of unicasting to individual SS, yet by means of TV to subgroups. For each cell of a BS and numerous SS in a multicast application, the SS will be sub-gathered into N = 2k subgroups, with every sub-gathering keeping up k keys. The precise estimation of N is to be dictated by the implementer to offer the best execution for a given application. Case in point, an application that midpoints 600 SS may pick an estimation of N = 8 sub-aggregates, every sub-gathering averaging 75 individuals and keeping up k = 3 keys. At the point when another SS solicitations keying material, it will be assembled into the sub-bunch with the most minimal part check. This is done to keep the sub-gatherings adjusted in size. Something else, one sub-gathering may turn out to be substantial regarding the others and the productivity of re-keying drops fundamentally.

Each sub-group maintains a hierarchy of sub-group KEKs (SGKEK) instead of a single GKEK. According to a binary tree hierarchy, each SS within a sub-group will store KSGKEKs. The following figure shows the case for N = 4. In the figure, note that sub-group 1 stores SGKEK1, SGKEK12, and SGKEK1234, and that SGKEK1234 will function as the traditional GKEK did. Also, all future examples will be made with reference to Fig. 1.

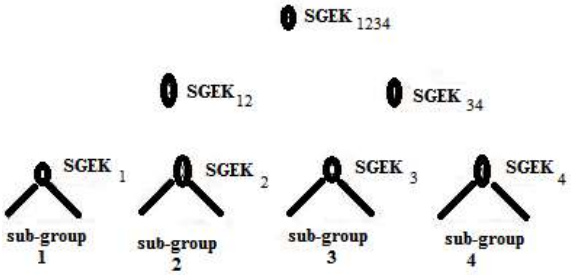

Fig. 1: Basic Hierarchy with 4 sub- groups

In the least complex instance of re-keying, there are no part joins or clears out. For reference, each GTEK lifetime might characterize a multicast session. For this situation the GTEK, or session, lapses because of time with no participation changes. The lifetime of the GTEK continues as before as it is in the 802.16 standard. For this situation one and only message should be sent.

$$BS \rightarrow \text{all SS: } \{GTEK\}_{SGKEK1234} \quad (3)$$

The following case might be re-keying because of a part join. The part join begins off as it does in the first determination with a key solicitation sent from SS to BS, and a key answer sent from BS to SS. On the other hand, the key answer is altered to incorporate another pecking order of SGKEKs. So for instance when another SS joins and sub-gather 2 is right now the sub-bunch with the most reduced number of individuals, the key answer is similar to message (4), with all keys being not present, but rather overhauled renditions.

$$BS \rightarrow SS: \{SGKEK_{1234}, SGKEK_{12}, SGKEK_{2}\}_{KEK} \quad (4)$$

Message (4) is conveyed to all current SS inside subgroup 2 through unicast also. While (4) is being conveyed, the BS re-keys all current SS with new forms of proper keys in parallel. Proceeding with the same circumstance of a SS joining sub-groups 2, (5) and (6) future conveyed to re-key all SS not in sub-groups 2.

$$BS \rightarrow SS_{SG3}, SS_{SG4}: \{SGKEK_{1234}\}_{SGKEK34} \quad (5)$$

$$BS \rightarrow SS_{SG1}: \{SGKEK_{1234}, SGKEK_{12}\}_{SGKEK1} \quad (6)$$

Where; SS_{SGi} means the collection of SS within sub-group i.

The upgraded GTEK is excluded in these messages for an execution reason. In the case of amid the redesigns, more SS endeavor to join, the circumstance has not changed. We will allude to this circumstance as a multi-join. To look after effectiveness, all joining SS in a multi-join occasion will be put into the same subgroup, which was the sub-bunch with least number of individuals toward the begin of the occasion, in any case if including all the joining SS results in the sub-gather not being the littlest any longer. The main expansion on account of a multi-join of a solitary join would be another message (4) to each extra SS joining the administration. At the finish of all SGKEK overhauls amid a

join or multi-join, the new GTEK is show to all SS with message (7).

$$BS \rightarrow \text{all SS} : \{GTEK\}_{SGKEK1234} \quad (7)$$

On a part leaving the multicast administration, re-keying continues precisely as a complete re-keying accomplishes for a join circumstance. In the event that a part from gathering 2 was to leave, (4b) would be unicast to all remaining SS in sub-gather 2. Next, (5b) and (6b) eventual telecast to the individual individuals not in sub-gather 2. The contrast in the middle of join and leaves is that with a leave there is no advantage of postponing the new GTEK show until the end of the whole re-keying procedure. When a SS gets overhauled SGKEK material, it will without a doubt have the capacity to decode the following GTEK. Hence, if an SS that has effectively gotten new SGKEK material in the center of another leave procedure chooses to leave too, no re-keying can be joined and another re-keying procedure must begin. In this occasion messages (4b), (5b), and (6b) are sent by the BS; they are indistinguishable to their partners aside from the incorporation of the freshest GTEK.

$$BS \rightarrow SS: \{SGKEK_{1234}, SGKEK_{12}, SGKEK_{2}, GTEK\}_{KEK} \quad (4b)$$

$$BS \rightarrow SS_{SG3}, SS_{SG4} : \{SGKEK_{1234}, GTEK\}_{SGKEK34} \quad (5b)$$

$$BS \rightarrow SS_{SG1}:\{SGKEK_{1234},SGKEK_{12},GTEK\}_{SGEK1} \quad (6b)$$

V. EVALUATION

In the past areas, we have demonstrated that the MBRA in 802.16e does not give in reverse or forward secrecy, and examined how our ELAPSE methodology guarantees complete in reverse and forward secrecy by rekeying on part joins furthermore, part takes off. Next, we utilize hypothetical investigation and observational recreations to assess the execution of Pass contrasted with MBRA.

A. Efficiency Analysis

To assess the effectiveness of ELAPSE, its correspondence what's more, space many-sided quality will be contrasted with other mulitcast approaches. In the basic level mapping, for example, the MBRA in 802.16, the server (bunch director) ought to send rekeying messages to every gathering part individually, with the new gathering key (GTEK in 802.16) scrambled with its emit key (AK) imparted to server (BS). In this way the correspondence unpredictability is O(n), server space many-sided quality is O(1) (ignoring the individual AKs, which are made amid validation), and part space intricacy is O(1). In the LKH pattern the correspondence intricacy is O(log n) for the rekeying methodology; the server space intricacy is O(n) furthermore, part space is O(log n). For the cross breed diagram, the correspondence intricacy falls in the middle of the basic pattern and LKH mapping, i.e., in the middle of O(n) and O(log n); the server space falls in the middle of O(1) and O(n) and the part space falls in the middle of O(1) and O(log n). The careful intricacy is controlled by the quantity of subgroups, and the scopes of these complexities represent the tradeoffs connected with this decision.

At the point when the quantity of subgroups increments (from 1 to n), it can be summed up that the correspondence intricacy diminishes (from O(n) to O(log n)), while the server space intricacy increments (from O(1) to O(n)) and the part space multifaceted nature additionally increments (from O(1) to O(log n)). The creators in [16] discover a (maybe) ideal offset among these tradeoffs by separating the gathering into subgroups with O(log n) individuals each. With this numerous sub-amasses the correspondence many-sided quality is still O(log n), the same degree as in LKH diagram, while the server space many-sided quality is down to O(n/log n), and the part space is O(log n). Slip by, because of its comparative utilization of sub-gathering, shows the same correspondence and space complexities.

B. Simulation Results

To analyze the execution, we reproduce both ELAPSE also, the 802.16 MBRA utilizing Qualnet. Because of the unfinished nature of the 802.16 standard, numerous execution parameters for example, a key solicitation time out, GTEK lifetime, and so forth are most certainly not totally characterized and were picked self-assertively by the creators. The qualities picked were inside sensible range such that no sweeping statement is lost. Two simulation runs were executed for the MBRA and three variations of ELAPSE, utilizing 2, 4, or 8 sub-bunches individually. The main recreation run was 100 seconds in length, what's more, the second was 1000 seconds. 16 SS hubs were recreated with 1 BS conveying one multicast session, and the SS haphazardly joined and left the session over the whole course of a simulation run. To guarantee decency, the same arbitrary number seed, inferring the same join and leave design for the SS, was utilized for every one of the calculations on the same run. Utilizing the BS as perspective for gathering insights, the aggregate number of messages sent from the BS was utilized to gage proficiency. Messages were tallied as unicast or multicast. Show messages, for example, show GTEK redesign mode messages were considered multicast. Tallying messages with the 802.16 was clear, as key reaction messages sent on join and leave, and GKEK overhaul mode messages were considered unicast. The show GTEK overhaul mode message was considered multicast. For ELAPSE, all key reaction messages inside of the sub-gathering of the joining/clearing out hub were considered unicast. Alternate messages, SGKEK what's more, GTEK overhauls, were considered multicast.

A point about the usage of the 802.16 MBRA must be made as for SS join and leave occasions. In the current standard, there is no unequivocal conduct characterized, so we will expect the BS rekeys the whole gathering each join and clear out. On the off chance that it is to be accepted that no rekeying is performed on part join and leaves and just on GTEK termination, the number of messages sent would be radically lower (equivalent to the quantity of join occasions that happened amid recreation). Be that as it may, there would be passes in secrecy on each join (and leave) equal to the measure of information sent before (and after). Hence, rekeying on SS joining and leaving was included with the 802.16 MBRA simulations so that all calculations could be looked at entirely as far as productivity, with the prerequisite that the calculation guarantees great in reverse and forward secrecy.

Figure 2 demonstrates the consequences of the 100 second long simulation keeps running of the diverse calculations. To successfully look at the variations of ELAPSE, the quantity of unicast and multicast messages were totaled together. Utilizing this aggregate, Slip by and

the 802.16 MBRA can be thought about just as. For the MBRA simulation, the BS conveyed 930 messages. The three variations of ELAPSE utilizing 2, 4, and 8 sub-bunches conveyed 580, 494, and 424 messages, separately.

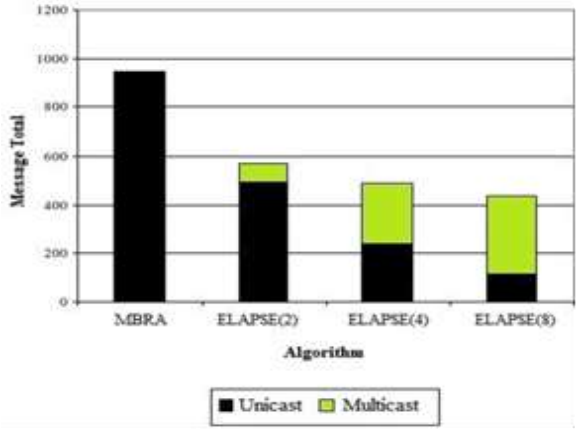

Fig. 2: Messages sent from BS - 100 second simulation

For the 1000 second simulation, whose outcomes are demonstrated in Figure 3, a more extended GTEK lifetime and less forceful join/take off conduct was picked contrasted with the 100 second simulation. The BS running ELAPSE variations in the test system sent 676, 567, and 465 messages, individually. The BS running 802.16 MBRA sent 1020 messages.

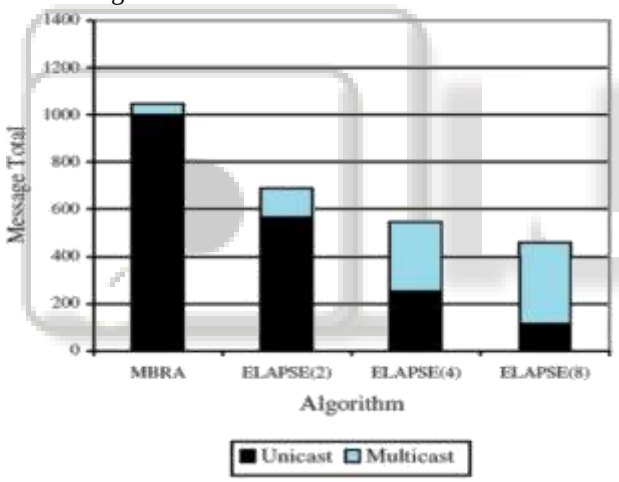

Fig. 3: Messages sent from BS - 1000 second simulation

From the above simulation results, it is clear that the ELAPSE variants outperformed the 802.16 MBRA. However, as stated earlier there is increased state required with such a hierarchical approach. When using ELAPSE with 2 sub-groups, each SS must maintain 1 extra key, and the BS must maintain 2 extra keys. For 4 sub-groups, it becomes 2 extra keys and 6 extra keys, and when using 8 sub-groups the total are 3 extra keys and 14 extra keys at the SS and BS respectively. It is well known that the increased communication efficiency comes at a cost of increased state, so based on the theoretical efficiency discussed above, when there are at most 16 SS, using ELAPSE with 4 sub-groups is the optimal choice. This is because the optimal number of sub-groups is achieved when each sub-group contains O (log n) members. With a maximum of 16 SS at a time, we have $\log_2(16) = 4$, which is the optimal choice. Similarly, the server space requirement increases by 6 keys to O(n) = 7 keys (excluding the GTEK and AK), and the member space requirement becomes O(log n) =3 keys.

VI. Conclusion

In this paper we have checked on the difficulties of secure multicast, and dissected the MBRA of IEEE 802.16e, as it is a imperative case of these difficulties rising in next era systems. While the calculation at present is in the draft stage, it has eminent shortcomings. As far as security, it is a fragmented arrangement by not ensuring secrecy of messages previously, then after the fact part joins and leaves, individually. With respect to dispersing keying material, it is wasteful, and does not exploit the late research showing the viability of progressive methodologies. The methodology exhibited in this paper, ELAPSE, gives in reverse and forward secrecy and beats the 802.16 MBRA in reproduction. This does take a swing at an expense of expanded server and part space prerequisite, yet this trade-off is a matter of uplifted necessities on the equipment that is to really execute the 802.16 standard. Given the quickly diminishing expense of customer side equipment and the considerable prerequisites as of now set up on the server equipment, we trust the expanded space prerequisite is sensible and adequate. Later on work, we will keep on executing a model of ELAPSE and broaden the size of the tests keeping in mind the end goal to assess the execution and focus the fitting estimations of different parameters of ELAPSE in an extensive system. Additionally, we will examine an element subgrouping methodology in which the quantity of subgroups will alterably change as per the late most extreme number of individuals in the multicast administration.

References

[1] IEEE Std 802.16-2004: Air Interface for Fixed Broadband Wireless Access Systems, 2004.
[2] IEEE Std 802.16e: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, 2005.
[3] IEEE Std 802.16-2001: Air Interface for Fixed Broadband Wireless Access Systems, 2002.
[4] Roger Marks: A technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access, IEEE C802.16-02/05, 2002.
[5] C. Eklund, R. B. Marks, S. Ponnuswamy, K. L. Stanwood, N. J. M. V. Waes, "WirelessMAN: inside the IEEE 802.16 Standard for Wireless Metropolitan Networks", Standards Informatin Network, IEEE Press, 2006.
[6] D. Johnston, and J. Walker, "Overview of IEEE 802.16 Security", IEEE Security & Privacy, 2004.
[7] Z. H. Khan, R Paulus, P Charan, M. Kumar Increasing the Performance of IEEE 802.11n in Multi Channel Multi Radio Mobile Ad hoc Networks, International Journal of Applied Science & Technology Research Excellence, Vol.2 Issue 2, 2012
[8] S. Xu, and C. T. Huang, "Attacks on PKM protocols in IEEE 802.16 and its later versions", ISWC06, September 2006.
[9] J. Y. Kuo, "Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol", CS 259 Final Project Report, Stanford University.
[10] A. Ballardie, "Scalable Multicst Key disribution", RFC 1949, 1996.

[11] H. Harney, and C. Muckenhirn, "Group Key Management Protocol Specification", RFC 2093, 1997.
[12] P. Charan, R. Paulus, M Kumar, AK Jaiswal, "A Cross Layer approach for Performance Optimization in Wireless Sensor Networks using Cooperative Diversity", International Journal of Computer Science And Technology, Vol. 3 Issue 2, 2012
[13] D. M. Wallner, E. J. Harder, and R. C. Agee, "Key Management for Multicast: Issues and Architectures", RFC 2627, June 1999.
[14] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group CommunicationsUsing Key Graphs", IEEE/ACM Transaction on Networking, Vol. 8, No. 1, Feb 2000.
[15] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The VersaKey framework: Versatile Group Key Management", IEEE Journal on Selected Areas in Communications Vol. 17, No. 9, 1999.
[16] R. Canetti, T. Malkin, and K. Nissim, "Efficient communication-storage tradeoffs for multicast encryption," in Advances in Cryptology-EUROCRYPT'99, 1999.
[17] 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, 2000.

