PERFORMANCE AND REKEYING ANALYSIS OF MULTICAST SECURITY IN LTE

Mohsen M. Tantawy [1], Adly S. Tag ELdien [2], Esraa Mosleh Eid [3]
[1] National Telecommunication Institute Cairo, Egypt
mohsen@nti.sci.eg
[2, 3] Elec. Eng. Dept. faculty of engineering, Benha university, Shoubra, Cairo, Egypt
[2]adlymerg@yahoo.com
[3]emesunset@yahoo.com

ABSTRACT

Multimedia Broadcast Multicast Services (MBMS) is a point-to-multipoint interface specification for existing and upcoming 3GPP cellular networks, which is designed to provide efficient delivery of broadcast and multicast services, within a cell or within the core network. Target applications include mobile TV and radio broadcasting, file delivery and emergency alerts.The main goal of this paper is to assess the performance of the Secure Multicast Overlay (SMO) and the Group Security Association (GSA). We functionally compare GSA with SMO, in terms of Keys management procedures and look up policies showing that GSA solution is appropriate in certain circumstances and SMO solution is appropriate in others. The comparison will be for different parameters and different services. Also the computational cost and storage cost for Logical Key Hierarchy (LKH) tree with and without dynamic rekeying will be calculated.

KEYWORDS

Multimedia Broadcast Multicast Services, GSA, SMO, LKH, Dynamic Rekeying.

1. INTRODUCTION

The 3GPP has introduced the Multimedia Broadcast Multicast Service (MBMS) as a mean to broadcast and multicast information to 3G users. In MBMS multiple subscribers can receive the same data, sent only once on each downlink. MBMS in real provides two different services Broadcast and Multicast. The Broadcast service can be received by any subscriber located in the area where the service is offered and multicast services can be received by users who have only subscribed to the service and having joined the multicast group associated with the service. The evolved MBMS (e-MBMS) architecture is shown in Figure 1. Some of the entities functions are described below.

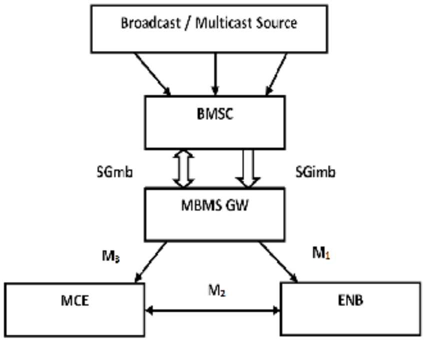

Figure 1. e-MBMS architecture

DOI : 10.5121/ijcnc.2013.5409

The evolved Broadcast Multicast Service Center (e-BM-SC) is the entity that is responsible for providing authorization for terminals that are requesting to activate an MBMS service. The e-BMSC is used as well for scheduling of broadcast and multicast sessions [1-3], Integrity and confidentiality protection of MBMS data and finally MBMS session announcement.

The e-MBMS GW is the root of the distribution tree for the multimedia content that is used to broadcast/multicast the information towards 3G users through the UMTS Terrestrial Radio Access Network (e-UTRAN). The e-MBMS GW performs MBMS Session Control Signaling (session start/stop) toward the e-UTRAN via Mobile Management Entity (MME) [4-6]. It is logically split into two parts, one related to control plane and the other related to user plane. Two interfaces have been defined between e-MBMS GW and e-UTRAN, M1 for user plane and M3 for control plane.

The e-NB is the collectors of the information that has to be distributed to users on the air-interface.
The Multi-cell/multicast Coordination Entity (MCE) is needed to coordinate the transmission of synchronized signals from different cells (e-NBs) and can be implemented inside or outside e-NBs. Multicasting is the optimum technique for such group oriented applications with effective network resource utilization. But maintaining security is critical with frequent membership changes. Confidentiality can be achieved through changing the key material, known as rekeying every time a new member joins the group or existing member leaves from the group. In this paper we introduce two different solutions for MBMS, which are GSA and SMO.
The computational cost and the storage cost for rekeying with and without dynamic rekeying will be investigated.
The rest of the paper is organized as follows: The security solutions with the traffic model with the definition of overlay topology for SMO and GSA is described in section II. The assumptions for LTE multicast services analysis and the key performance indeces is proposed in section III and section IV, respectively. Section V shows the result and result analysis. Finally, we conclude this paper in section VI

2. SECURITY SOLUTIONS

There are two solutions to secure MBMS sessions which are Group Security Association (GSA) and Secure Multicast Overlay (SMO).

2.1. GROUP SECURITY ASSOCIATION (GSA)

When creating of a new multicast group, a new multicast channel has to be distributed to a set of receiver e-NBs. The set of GSAs between MBMS-GW and eNBs could be stable for fixed subscription services, while could change frequently in pay per view services (ex.TV channels) or in the distribution of user generated content (peer to peer).

In the e-MBMS and during the set up of a multicast group, all the eNBs involved in the group set-up have to obtain the GSA key materials almost in the same time. This can be done by establishing a point to point security association (SA) with the Group Controller and Key Server (GCKS) and using this SA to exchange the key material of one specific multicast group [7-9].
The Group Controller and Key Server (GCKS) manage the cryptographic keys used by a multicast group. It also conducts user-authentication and authorization checks on the candidate members of the multicast group [10]. The traffic Model for GSA solution is shown in Figure 2.

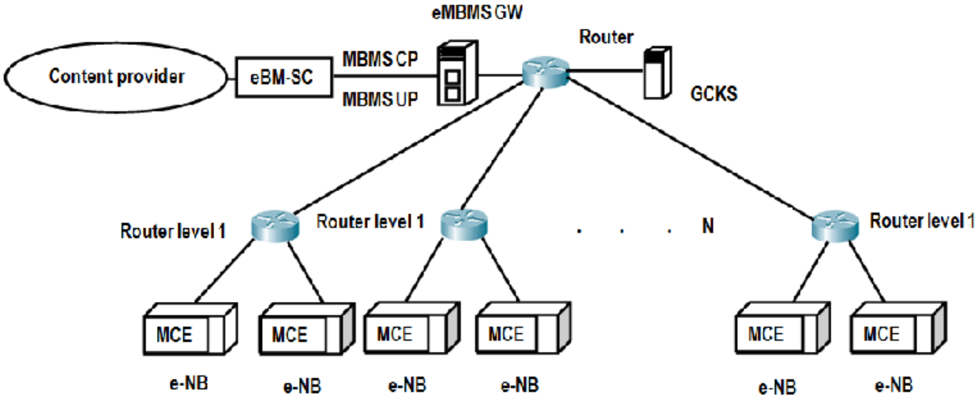

Figure 2.e-MBMS architecture for the GSA solution

2.1. Secure Multicast Overlay (SMO)

In the Secure Multicast Overlay solution, the security associations that compose the overlay is assumed to be static or changing very slowly with time. Figure 3 shows a hierarchical overlay topology with one level of hierarchy, called Level one hierarchical overlay topology (L1HO). The e-NBs are organized in cluster of size C_R, which is the number of e-NBs belonging to the cluster. One e-NB in the cluster is chosen to be the master and the others are the slaves. Both master and slaves eNBs receive packets from the router. However master e-NBs establish SAs with the e-MBMS GW and the slaves establish SAs with the master.

In this topology the eMBMS GW manages only the cryptographic procedures relative to the master eNBs. The cryptographic procedures relative to the slave eNBs are managed by the master eNBs [11]. The traffic Model for SMO solution is shown in Figure 4.

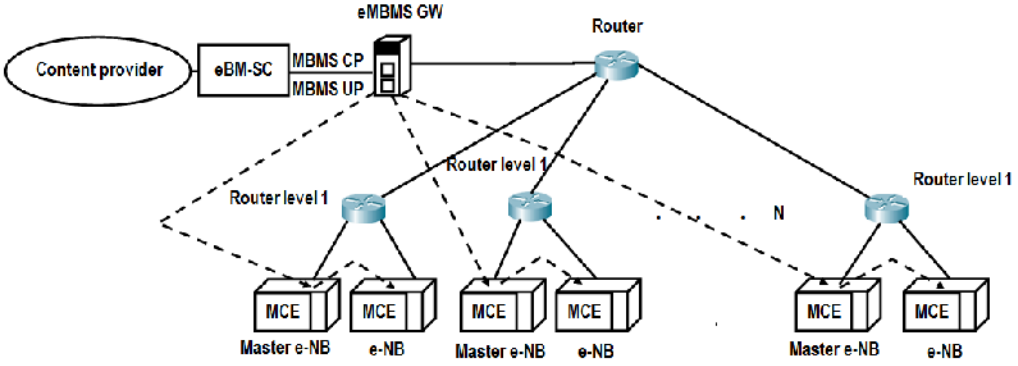

Figure 3. Traffic Model for SMO solution

3. Traffic model Parameters

In order to simplify the analysis, it is convenient to group the flows into sets of flows with similar parameters. The idea is to partition the set of flows into a limited number of groups with homogeneous characteristics.

In this analysis two types of multicast group services are considered:
(1) *Multicast pay per view service* (e.g. TV channels).
(2*) Multicast peer to peer service* (e.g. Twitter, Facebook).
Let G be the number of multicast service groups, where

$$G = 1, 2, 3, \dots \dots \dots ., m \qquad (1)$$

For one multicast service group, e.g. TV, assume N is the total number of multicasted TV channels, and a certain channel is given by n, where

$$n = 1, 2, 3, \dots \dots \dots, N \qquad (2)$$

For each channel assume that the number of active users that receives a flow (e.g. a channel in TV service) is A_i, so the total number of active users in group service m is

$$G_m = \sum_{i=1}^{N} A_i \qquad (3)$$

For simplicity assuming an equal number of active users in each TV channel

$$\therefore \quad G_m = N \times A_N \qquad (4)$$

Let U is the total number of cellular users in one operator network. Within U some active users are receiving a e-MBMS flow and we define x as the e-MBMS activity factor, therefore the
number of users that are receiving e-MBMS flows $= xU$ (5)

Where, $0 \leq x \leq 1$
For each group we define w as the fraction of active users that are receiving a flow in that group.
The Number of users receiving flows of group i = $w_i \times x \times U$ (6)

So we conclude that for group i:

$$N_i \times A_i = w_i \times x \times U \qquad (7)$$

As

N_i: total number of multicasted TV channels in group i.
A_i: number of active users that receives a certain flow in group i.
w_i: fraction of active user that is receiving a flow in that group.
x: e-MBMS activity factor.
U: number of cellular users in one operator network.

4. REKEYING IN MBMS

Key management for users in the communication networks is dependent upon the security of the keys, it is appropriate to devise a fairly complex mechanism to manage them. In group communication many individual mechanisms are involved, with a requirement for unique keys to be sent to each for encryption/decryption of transmitted data.

The Logical Key Hierarchy (LKH) is widely adopted in key management of IP multicast as stated in [12 –14]. It is a tree with single root and two parameters which are the height (h), the longest path from a leaf to the root, and degree (d), which is the maximum number of outgoing edges of a node in the tree. The tree is called key tree. Each leaf in the key tree represents a unique user. Every user owns three keys: (1) individual key, (2) group key and (3) auxiliary key. Individual key is shared with the Key Server (KS). Group key is shared with the KS and all other users in the multicast group. Auxiliary key is stored in an intermediate node, the user, and the KS [15-16].

There are four keys in MBMS: MBMS Traffic Key (MTK), MBMS User Key (MUK), MBMS Service Key (MSK) and MBMS Request Key (MRK) [17]. MRK is used for authentication. MUK is used to protect the distribution of MSK. MSK is used to protect a certain MBMS session [18-19]. It is also used to protect the distribution of MTK; however it is not used to encrypt/decrypt MBMS traffic. MTK is used for encryption and decryption of the data transmitted. MUK and MSK are delivered by using Multimedia Internet Keying (MIKEY). Both BM- SC and User Equipment (UE) must own the four keys.

Two types of LKH will be addressed in this paper, LKH without dynamic rekeying and LKH with dynamic rekeying which will include two cases, changing the degree of the key tree while keeping the height constant, and changing the height while the degree will remain constant.
A comparison will be done for the three cases in terms of computational cost and storage cost, both for server and users.

Computational cost: It is the number of key encryptions and decryptions required by a join or leave request for the server (C_s) and the user (C_u).

Storage cost: the numbers of keys stored in the key server (K_s) and each user (K_u).

Based on studies in [12] and [15]

Average cost per request of the server (C_s) = $\frac{(d+2)\times(h-1)}{2}$ (8)

Average cost per request of the user (C_u) = $\frac{d}{(d-1)}$ (9)

4.1 Logical Key Hierarchy without Dynamic Rekeying in MBMS

Without dynamic rekeying, the key tree will be like that illustrated in Figure 4. K_n represents the four keys stored in the UE for user n. Because there are no intermediate nodes, the height of the key tree is 2. The degree of the key tree is changing according to users joining or leaving a certain group. Based on equations (8) and (9), we can derive the computational cost.

$$C_s = \frac{(d+2)}{2} \quad (10)$$

For the storage cost, the Key server (BM-SC) and all group members share both MTK and MSK. The Key server also shares the MUK and MRK with each individual user. Therefore,

- Total number of keys in the server (K_s) = $2 \times d + 2$ (11)
- Total number of keys for each user (K_u) = 4 (12)

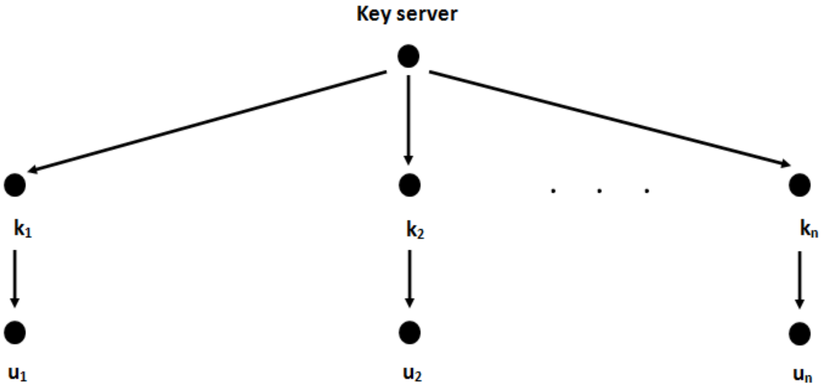

Figure 4. Key tree without dynamic rekeying: LKH with height 2.

4.2 Logical Key Hierarchy with Dynamic Rekeying in MBMS

In the following subsections we are going to address two cases for LKH with dynamic rekeying. The first will be changing degree of the key tree while the height remains constant (h=3). The second will be keeping the degree constant (d=4) and changing the height of the key tree.

4.2.1 Dynamic Rekeying: LKH with Height 3

To support dynamic rekeying in MBMS, construct the key tree as that shown in Figure 5, where MTK, MSK, MUK are the group key, the auxiliary key, and the individual key.

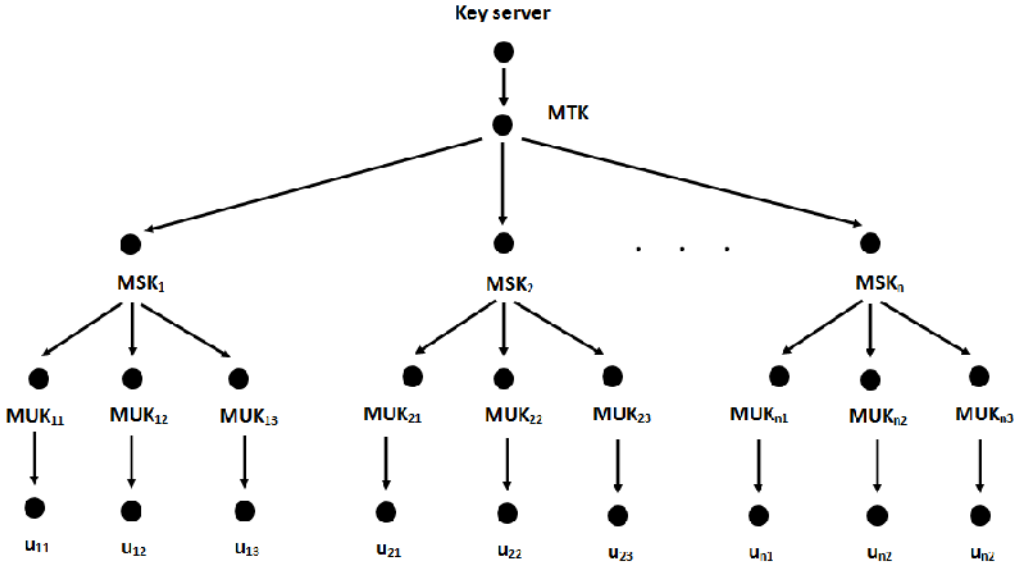

Figure 5. MBMS with dynamic rekeying: LKH with height 3.

MTK is the group key which is used to protect the MBMS traffic. MTK is protected by MSK, which is protected by MUK. The height of the key tree is fixed and equal to 3. When a user joins the multicast group, the degree of a sub-tree is increased. Also based on Equation (8) and (9),

$$C_s = d + 2 \qquad (13)$$

For the storage cost [15]

Total number of keys in the server (K_s) = $\frac{(d^h - 1)}{(d - 1)} + d^{(h-1)}$ (14)

Total number of keys for each user (K_u) = 4 (15)

4.2.2 DYNAMIC REKEYING: LKH WITH DEGREE 4

In [12], the authors prove that when using degree of the key tree equal to 4 this minimizes the rekeying cost. Based on equation (8) and (9), computational cost is reduced significantly when the degree is fixed to 4, but we need increase the height of the key tree when the number of users increases.

$$C_s = 3 \times (h - 1) \quad (16)$$

$$C_u = 1.3333 \quad (17)$$

For the storage cost [15]

Total number of keys in the server (K_s) = $\frac{(4^h - 1)}{(4 - 1)} + 4^{(h-1)}$ (18)

Total number of keys for each user (K_u) = $(h + 1)$ (19)

5. ASSUMPTIONS

There are many multicast services in LTE. This analysis focuses on TV service; Twitter service and Facebook service. Table 1 shows the model assumptions for the model. The values shown in the table are acceptable according to [11] and [20]

Table1.Model assumptions for multicast applications in LTE

Parameter / Service	TV channel service	Twitter	Social network (Facebook)
Population of users (U)	10^4 , 10^7	10^4 , 10^7	10^4 , 10^7
Activity factors (x)	5%	5%	5%
Total number of e-NBs managed by the GW (K)	500 :10^4	500: 10^4	500: 10^4
average rate of service (B)	0.5 : 8 Mbps	50 kbps	1 : 2 Mbps
number of e-NBs served by level one router (C_R)	10 : 100	10 : 100	10 : 100
Refresh frequency of the cryptographic keys (f_{GSA})	1 / hour	1 / hour	1 / hour
Refresh frequency of the cryptographic keys (f_{SMO})	1 / hour	1 / hour	1 / hour
Fraction of active users that are receiving a flow (w)	30%	20%	20%
Span fraction of video traffic flows (s)	1	$1 - \left(\frac{k-1}{k}\right)^{A}$	$1 - \left(\frac{k-1}{k}\right)^{A}$
Number of traffic flows (N)	25, 100	20 , 2000	20 , 2000
Average duration of video flows (T)	1 hour	20 minutes	20 minutes
multicast flow size (A)	1, 6, 1500 , 6000	5 , 50, 5000	5 , 50, 5000

The key tree parameters (h, d) for the three LKH rekeying scenarios are shown in table 2.

Table2. Key tree parameters for different LKH rekeying tree

LKH	Height (h)	Degree (d)
Without dynamic rekeying.	2	Differs according to U
with dynamic rekeying with height 3	3	Differs according to A
with dynamic rekeying with degree 4	Differs according to U	4

6. KEY PERFORMANCE INDECES

The following parameters will be investigated during the analysis:

Gateway Managed SAs (GWMSA), it is the number of SAs connections that a MBMS-GW needs to manage with different eNBs at the same time.

$$\text{GWMSA (GSA)} = \text{N} \quad (20)$$

$$\text{GWMSA (SMO)} = \frac{\text{K}}{\text{C}_\text{R}} \quad (21)$$

Group Setup Rate (GSR), it is the rate of creation of new multicast groups that require a keying procedure.

$$\text{GSR (GSA)} = \frac{\text{N}}{\text{T}} \quad (22)$$

$$\text{GSR (SMO)} = 0 \quad (23)$$

Rekeying Rate (REKR), it is the overall rate of refresh procedures originated by the GCKS for all GSA groups (GSA). Or the overall rate of refresh procedures for each point-to-point SA at the e-MBMS gateway (SMO).

$$\text{REKR (GSA) (TV)} = \text{K} \times \text{N} \times \text{f}_{\text{RK}}^{\text{GSA}} \quad (24)$$

$$\text{REKR (GSA) (Twitter, Facebook)} = \text{s} \times \text{K} \times \text{N} \times \text{f}_{\text{RK}}^{\text{GSA}} \quad (25)$$

$$\text{REKR (SMO)} = \frac{\text{K} \times \text{f}_{\text{RK}}^{\text{SMO}}}{\text{C}_\text{R}} \quad (26)$$

Key Request Rate, For each GSA multicast group, all receivers have to require the key.

$$\text{KRR (GSA) (TV)} = \frac{\text{K} \times \text{N}}{\text{T}} \quad (27)$$

$$\text{KRR (GSA) (Twitter, Facebook)} = \frac{\text{s} \times \text{K} \times \text{N}}{\text{T}} \quad (28)$$

$$\text{KRR (SMO)} = 0 \quad (29)$$

Also we are going to calculate the computational cost and the storage cost for both server and user will be calculated for different number of users (U) and different number of users per traffic flow (A).

7. RESULTS ANALYSIS

Changing number of traffic flows (N):

Figure 6 shows the number of gateway managed security associations (SA's) versus total number of eNBs. The figure shows that for TV, Twitter and Facebook SMO is the best solution for number of eNBs less than 2500. Otherwise the solution will change according to the number of traffic flows.

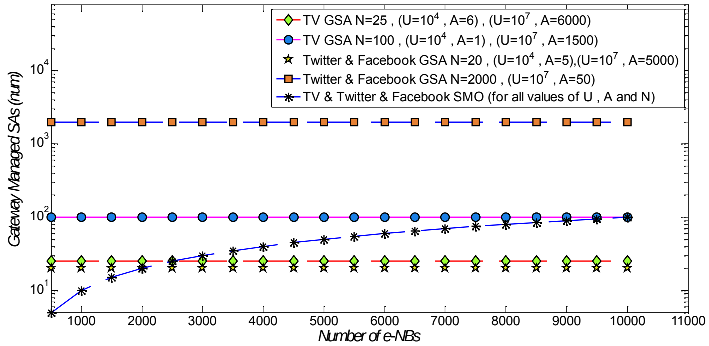

Figure 6. Gateway Managed SAs

Figure 7 shows the group setup rate versus total number of eNBs. The figure shows that for TV, Twitter and Facebook services, SMO solution is the best solution regardless number of traffic flows (N).

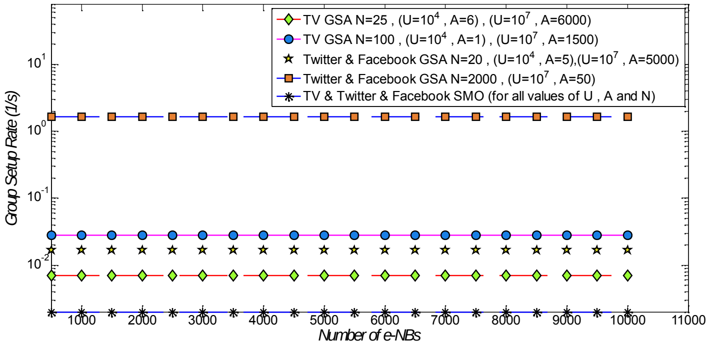

Figure 7. Group Setup Rate

Figure 8,9 shows the rekeying rate and the key request rate versus total number of eNBs. The figures show that for TV, Twitter and Facebook services, SMO solution is the best solution regardless the different number of traffic flows.

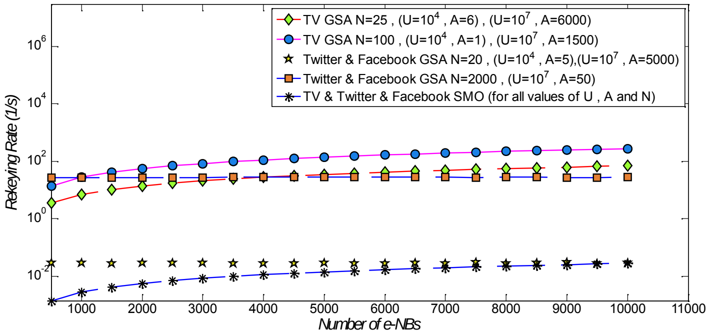

Figure 8. Rekeying Rate

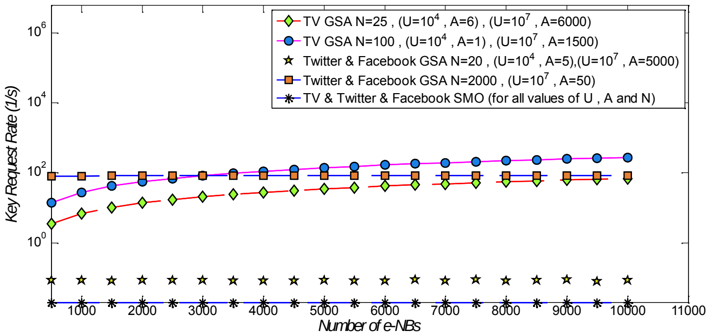

Figure 9. Key Request Rate

__Changing cluster size (C_R):__

Figure 10 shows the number of gateway managed security associations (SA's) versus total number of eNBs. The figure shows that for TV, Twitter and Facebook SMO is the best solution for number of eNBs less than 2500 with cluster size (C_R) equal to 100. Otherwise the solution will change according to C_R.

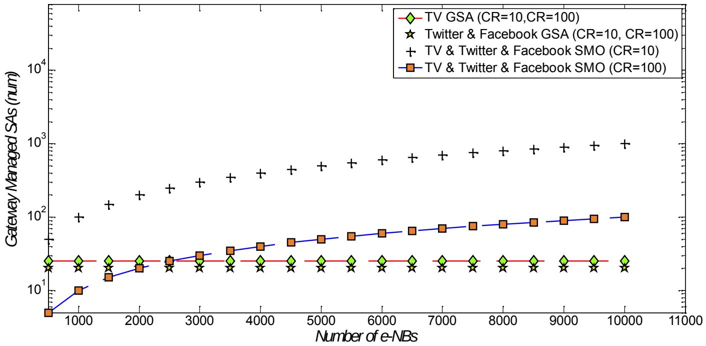

Figure 10. Gateway Managed SAs

Figure 11 shows the group setup rate versus total number of eNBs. The figure shows that for TV, Twitter and Facebook services, SMO solution is the best solution regardless of the cluster size (C_R).

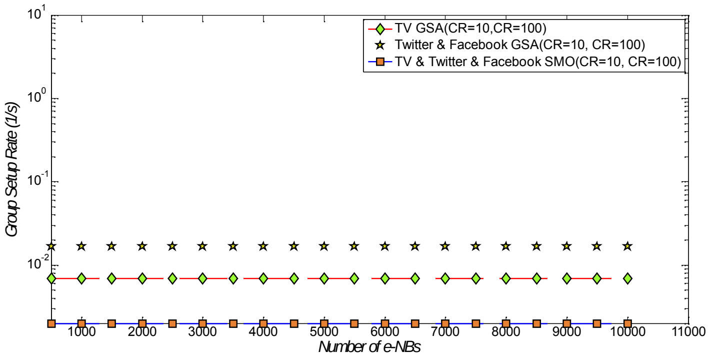

Figure11. Group Setup Rate

Figure 12, 13 shows the rekeying rate and the key request rate versus total number of eNBs. The figures shows that for TV, Twitter and Facebook services, SMO solution is the best solution for both values of the cluster size (C_R).

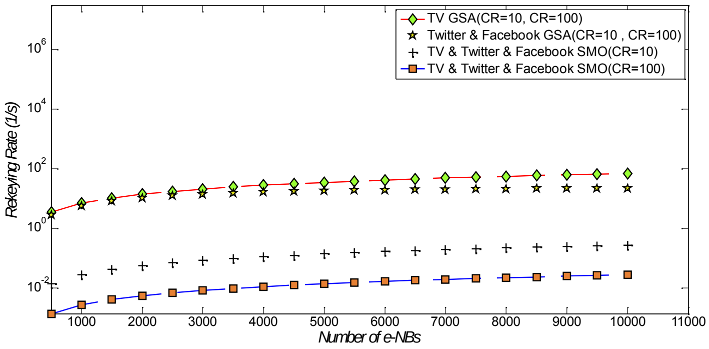

Figure12. Rekeying Rate

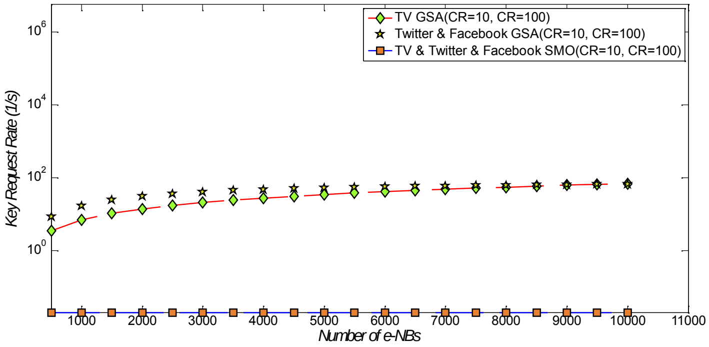

Figure13. Key Request Rate

Table 3 shows the computational cost for the three different approaches of LKH. The results show that the average cost per request of the user (C_u) for LKH without dynamic rekeying is slightly lower than the other two approaches regardless of the number of users. On the other hand the average cost per request of the server (C_s) for LKH without dynamic rekeying is extremely high compared to the other two approaches. When comparing LKH – height 3 with LKH degree 4 in terms of C_s we observe that for small number of users, LKH – height 3 has small values of C_s, but for large number of users, LKH – degree 4 has better results.

Table 3. Computational Cost

Service	Number of users	No Dynamic Rekeying		LKH – Height 3			LKH – degree 4		
		C_u	C_s	d	C_u	C_s	h	C_u	C_s
TV service	150	1.0067	76	6	1.2	8	5	1.333	12
				2	2	4	5	1.333	12
	150000	1.00000667	75001	6000	1.00016669	6002	10	1.3333	27
				1500	1.0006671	1502	10	1.3333	27
Twitter and Facebook	100	1.01	51	5	1.25	7	5	1.333	12
	100000	1.00001	50001	5000	1.00020004	5002	10	1.3333	27
				50	1.0204	52	10	1.3333	27

Table 4 shows that the storage cost is similar in the three different approaches. Although the storage cost in LKH with degree 4 is slightly higher, the difference is minimal. The KS (BM- SC) usually has enough memory to accommodate the increase in memory.

Table 4. Storage Cost

Service	Number of users	No Dynamic Rekeying		LKH – Height 3			LKH – degree 4		
		K_u	K_s	d	K_u	K_s	h	K_u	K_s
TV service	150	4	302	6	4	79	5	6	597
				2	4	11	5	6	597
	150000	4	300002	6000	4	72006001	10	11	61166979
				1500	4	4501501	10	11	61166979
Twitter and Facebook	100	4	202	5	4	56	5	6	597
	100000	4	200002	5000	4	50005001	10	11	61166979
				50	4	5051	10	11	61166979

8. CONCLUSION

The aim of this paper was the performance assessment of the Secure Multicast Overlay (SMO) and the Group Security Association (GSA) in LTE network. From the point of view of the number of Gateway Managed SAs (GWMSAs), and for the three services SMO solution has the best performance for small number of eNBs, otherwise the solution will change according to the number of traffic flows (N) flows and the cluster size (C_R).

In terms of Group Setup Rate (GSR), Key Request Rate (KRR), and Rekeying Rate (REKR) and for the three services, SMO solution is the best solution regardless the different number N and C_R. To increase the performance of SMO solution use large values for C_R.

With quantifying the computational cost and storage cost for Logical Key Hierarchy (LKH) with and without dynamic rekeying, we demonstrate that without dynamic rekeying, the computational cost for server request will increase rapidly when the number of users increases. For storage cost the results show that, the total number of keys stored in the server is huge number of keys when using LKH with dynamic rekeying compared to LKH without dynamic rekeying. the KS (BM-SC) usually has enough memory to accommodate the increase in the number of keys. LKH with dynamic rekeying is the proper approach to be used for rekeying.

Using constant degree or constant height for dynamic rekeying differs according to the number of users.

ACKNOWLEDGEMENTS

I wish to thank everyone who helped me complete this dissertation. Without their continued efforts and support, I would have not been able to bring my work to a successful completion.

REFERENCES

[1] David Lecompte, Frédéric Gabin,, (2012) “Evolved Multimedia Broadcast/Multicast Service (eMBMS) in LTE-Advanced: Overview and Rel-11 Enhancements”, IEEE Communications Magazine, pp 68-74.

[2] Yong Sun , Yu Dong , Zhenmin Zhao, Xiangming Wen & Wei Zheng, (2010) “Enhanced Multimedia Services Based on Integrated IMS-MBMS Architecture in LTE Networks ”,Wireless Communications and Mobile Computing (WiCOM), IEEE 6th International Conference on Networking, , pp 1-5.

[3] Qualcomm, (2012) “LTE eMBMS Technology Overview”, Qualcomm Research San Diego, pp 1-18.

[4] Tara & Ali Yahiya, (2011) *Understanding LTE and its Performance*, Springer Science and Business Media.

[5] Antonios Alexiou, Christos Bouras, Vasileios Kokkinos, Andreas Papazois & Georgia Tseliou, (2011) Forward Error Correction for Reliable e-MBMS Transmissions in LTE Networks, Cellular Networks - Positioning, Performance Analysis, Reliability, Dr.Agassi Melikov (Ed.), InTech.

[6] Antonios Alexiou, Christos Bouras, Vasileios Kokkinos, Andreas Papazois & George Tsichritzis, (2012) *Wireless Multi-Access Environments and Quality of Service Provisioning: Solutions and Application*, IGI Global Disseminator of Knowledge.

[7] T. Hardjono, B. Weis, (2004) “The Multicast Group Security Architecture”, Network Working Group, Request for Comments 3740.

[8] B. Weis, G. Gross & D. Ignjatic, (2008) “Multicast Extensions to the Security Architecture for the Internet Protocol”, Network Working Group, Request for Comments 5374.

[9] M. Baugher, R. Canetti & L. Doneti, F. Lindholm, (2005) “Multicast security (MSEC) group key management architecture”, Network Working Group, Request for Comments 4046.

[10] Petri Jokela, (2009) “Key Management in IP Multicast”, Helsinki University of Technology.

[11] Cristina Basile, Stefano Salsano, Simone Teofili, Michele Di Mascolo & Giuseppe Bianchi, (2008) “Performance analysis of security solutions for e- MBMS”, University of Rome (Tor Vergata), Department of Electronic Engineering, Networking Group, Technical report.

[12] C. K. Wong, M. Gouda, & S. S. Lam, (2000) “Secure group communications using key graphs”, IEEE/ACM Trans. Networking, vol. 8, pp. 16–31

[13] D. M. Wallner, E. J. Harder, & R. C. Agee, (1999) “Key management for multicast: issues and architectures”, Network Working Group, Request for Comments 2627.

[14] B. Briscoe, (1999) “MARKS: zero side effect multicast key management using arbitrarily revealed key sequences” , in Proc. International Workshop on Networked Group Communication (NGC), Pisa, Italy, pp. 17– 20.

[15] Jeng-Feng Weng & Jyh-Cheng Chen, (2010) “Dynamic Rekeying in 3GPP Multimedia broadcast/ Multicast Service (MBMS) ”, IEEE communications letters, vol. 14, no. 4, pp 288-290.

[16] Elina Eidkhani, Melisa Hajyvahabzadeh, S. Anahita Mortazav & Alireza Nemaney Pour, (2012) “CRAW: Combination of Re-Keying and Authentication in Wireless Networks for Secure Multicast Increasing Efficiency of Member Join/Leave and Movement”, International Journal of Computer Networks & Communications (IJCNC), Vol.4, No.4, pp. 107-128.

[17] George Xylomenos, Vasilis Vogkas & George Thanos, (2008) “The multimedia broadcast/multicast service”, wireless communications and mobile computing, volume 8, number 2, pp. 255-265.

[18] Hsia-Hung Ou, Min-Shiang Hwang & Jinn-Ke Jan, (2009) “The UMTS-AKA Protocols for Intelligent Transportation Systems”, EURASIP Journal on Wireless Communications and Networking, vol.2009.

[19] Nick Bone, Herve Ganem, Bojana Jakovljevic, Gorica Nikolic, Aleksandar Obradovic, Shahab Mirzadeh , Oualha Nouha & James Raeburn, (2013) “Solutions for Broadcast / Multicast and Device Management”,European Commission ,Information Society and Media, Exalted, FP7 Contract Number: 258512.

[20] Motorola, (2010) “TD-LTE: Enabling New Possibilities and Revenues for Operators Maximizing adaptable DL: UL ratio and lower spectrum costs”, Motorola solution center.

Authors

Mohsen M. Tantawy received the M.Sc. degree from Cairo University, Egypt in 1998 and the Ph.D. from Ain Shams University, Egypt in 2003. He is currently an associate professor in network planning department in National Telecom. Institute (NTI), affiliate of the Ministry of Communication and Information Technology.

Adly S. Tag Eldien received the B.S. degree in Electronics and communication, Benha University in 1984 and the M.Sc. in computer based speed control of single phase induction motor using three level PWM with harmonic elimination, Benha University, in 1989. The Ph.D. in optimal robot path control, Benha University, in 1993. He is currently an Association prof. in shoubra faculty of engineering and Manager of Benha university network and
information center. and his research interests include, Robotics, Networks, Communication.

Esraa M. Eid received the B.S. degree in Electrical Engineering, Communication from Benha University, in 2008. Now she is a Student of M.Sc.degree in Communication engineering in Benha University, Her research interests include, Mobile communication