ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Group Key Management Based On Chinese Remainder Theorem for Secure Wireless Mobile Multicast

Kiruthika B[1], Sayeekumar M[2]

M.E Student, Dept. of CSE, Muthayammal Engineering College, Rasipuram, India[1]

Associate Professor, Dept. of CSE, Muthayammal Engineering College, Rasipuram, India[2]

ABSTRACT: Addressing key management in mobile multicast communication is currently a booming topic due to the convergence of wireless and mobile technologies. With the proliferation of multiple group based services that are possible to co-exist within a single network, mobile subscribers could subscribe to these services concurrently while ubiquitous. However, the existing group key management (GKM) protocols intend to secure group communication for just a single group service. The GKM approaches involve inefficient use of keys and huge rekeying overheads, hence unsuitable for multiple multicast group environments. In this paper, we propose a novel GKM protocol for multiple multicast groups, called slot based multiple group key management (SMGKM) scheme. SMGKM supports the movement of single and multiple members across a homogeneous or heterogeneous wireless network while participating in multiple group services with minimized rekeying transmission overheads. Unlike conventional GKM protocols, SMGKM protocol can mitigate one-affect-n phenomenon, single point of failure and investment pressure of signalling load caused by rekeying at the core network. Numerical analysis and simulation results of the proposed protocol show significant resource economy in terms of communication bandwidth overhead, storage overheads at the Domain Key Distributor (DKD), mobile receiver and Area Key Distributors while providing intense security.

KEYWORDS: Group key management, mobile multicast, security, wireless networks

I. INTRODUCTION

MULTICAST is a bandwidth efficient technique for delivering group-oriented applications over the internet. These include applications such as video conferencing, interactive group games, video on demand (VoD), and mobile TV services. Multicast content distribution utilizes one-to-many and many-to-many transport communication mechanism. However the development of wireless networks and emergence of portable devices like smartphones, tablets has also increased to meet the demand for these multicast applications. The evolving wireless networks such as WiMAX [1] and 3GPP [2] have standardized the multimedia broadcast/ multicast service (MBMS). MBMS provide efficient delivery of broadcast and multicast services, both within a cell and within the core network. The evolved MBMS in Long Term Evolution (LTE) [3] is a handy example.

However due to open access in wireless networks, the broadcasted multicast services over the air become vulnerable to various security attacks such as eavesdropping opportunities, Denial of service (DoS), physical node capture attacks, impersonation attacks and others [4]. To deliver the multicast content securely only to the group members in wireless networks, an access control mechanism which ensures confidentiality, safeguards digital contents, and simplifies accounting for the broadcasted services is obligatory. This becomes a vital requirement

Consequently, it is predictable that in the future, multiple multicast groups will co-exist within the same network due to the emergence of various group-based applications and computationally fast mobile devices along with increased data rates for next generation wireless networks. Such a situation is probable to cause substantial key management overhead at the service provider (SP) for supporting multi-group services. Thus, the existing GKM schemes for secure wired [6] and wireless mobile [7] multicast networks will suffer from rekeying performance for cumulative multicast services because there are only targeted for a single multicast service. Fig. 1 illustrates an example of a multi-service environment whereby members under different service groups (SG) subscribe to various set of multicast services

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

offered by the service provider in an LTE network for example; Voice service and charged TV streaming with stringent and low delay

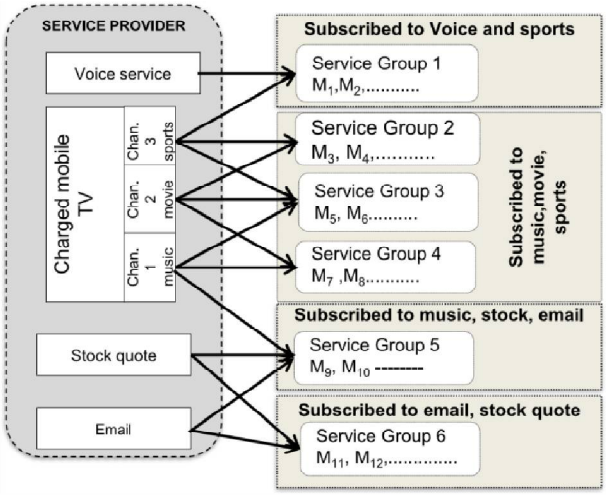


Fig. 1. Multiple multicast service groups' illustration.

sensitive to packet delivery, web browsing and delay tolerant telemetry services like emails based on best effort delivery. Suppose each multicast service is independently controlled by a single GKM protocol according to the existing GKM schemes. If a member participating in multi-services dynamically leaves or joins all the subscribed services, all the affected services would require independent rekeying procedure hence triggering significant rekeying overhead. In addition to host mobility in mobile environments, rekeying overhead is induced twofold since a handover member is considered leaving the currently serving subnet followed by join at the target subnet while maintaining similar services subscribed. Therefore some lightweight access control mechanism need to be addressed to prevent service latency while reducing rekeying latency concurrently.

To solve the rekeying complexity as multicast services cumulate in a single network, we propose a novel slot based multiple group key management (SMGKM) protocol for managing both single-move and multi-moves across a wireless network while seamlessly participating in multi-services with minimized rekeying transmission overheads, reduced communication and storage overheads, no single point of failures, no one-affect-n phenomenon and optimized signalling load at the core network. In SMGKM the key management tasks is offloaded to the intermediate cluster managers called Area Key Distributors (AKD) which establish the necessary key management keys. SMGKM integrate our concept of session key distribution list (SKDL) introduced in [8] for fast and secure authenticated handover along with initial key establishment. SMGKM employ a lighter symmetric encryption suitable for resource constraint mobile devices than heavier asymmetric effort. Compared to the existing schemes, SMKGM save enormous communication bandwidth utilization in the presence of multi-handoffs in multi-services.

In what follows is related work and reference framework which is discussed in Sections 2 and 3 respectively. Section 4 describes the SMGKM novel rekeying strategy in detail on member handoff with its analytical model in Section 5. The performance analysis of the SMGKM in terms of rekeying transmission, communication and storage overheads is described in Section 6. Finally Section 7 concludes the paper.

II. RELATED WORK

Traditional GKM protocols addressing rekeying over wired networks are divided in to centralized, decentralized and contributory schemes [6]. Centralized schemes rely on the centralized server known as the Domain Key Distributor (DKD) for generation and distribution of encryption keys. Contributory scheme has no explicit DKD, thus group members collaborate for group key establishment. Decentralized schemes partition the group in to subgroups each managed by subgroup managers in order to equally distribute the key management tasks hence scalability. Work in [9] further categorizes the GKM as common TEK and Independent TEK per subgroup approaches depending on how the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

TEK is distributed in the framework. Common TEK approaches such as in [5], [10], [11] utilize one TEK for all group members and commonly suffer from one-affect-n phenomenon; thus rekeying of the new TEK affect all the members subscribed to the same group in the entire network whenever a membership change occurs. Independent TEK per subgroup approaches try to alleviate the one-affect-n phenomenon caused by common TEK approaches such as in [12], by enabling each subgroup to independently manage its own TEK, thus rekeying of the new TEK is localized within the affected subgroup during membership change. However the GKM protocols did not consider host mobility during their implementation though they cannot be extended to wireless mobile environment directly.

In order to address rekeying in wireless mobile environment, few GKM protocols [13], [14], [15], [16] have been proposed recently. In addition to dynamic membership change considered for GKM protocols in wired networks, these protocols consider dynamic location change of members over a widely distributed wireless network while seamlessly receiving subscribed multicast services securely. The protocols adopt a decentralized framework for scalability. Work in [7] also categorized them according to common TEK [13], [14], [15], [17] and Independent TEK per subgroup [16] approaches as described in [9] to address similar rekeying issues. However, none of the GKM schemes previously proposed address rekeying for multiple group services. In [18] various rekeying strategies proposed only considers a single multicast service. If for instance M_1 in Fig. 1 perform handoff between clusters i and v while maintaining active subscribed services, voice and sports, the rekeying process is triggered independently for the affected three service groups 1, 2 and 3 in both the old and the target cluster when Baseline rekeying strategy (BR) is used. Though forward and backward secrecy is guaranteed in BR, it leads to extensive rekeying overhead with long service disruptions. Immediate rekeying (IR) strategy solves this problem by rekeying only the local area keys, however it gives huge rekeying overhead whenever members repeatedly handover. A type of Delayed rekeying strategy named (First Entry Delayed Rekeying þ Periodic (FEDRP)) alleviate IR rekeying problem by introducing mobility lists to track and manage host mobility. Henceforth, rekeying is only performed at the target cluster for backward secrecy since a handover member is recorded in the previous cluster list as still valid to the session. When a member finally leaves, all the clusters previously visited by the leaving member

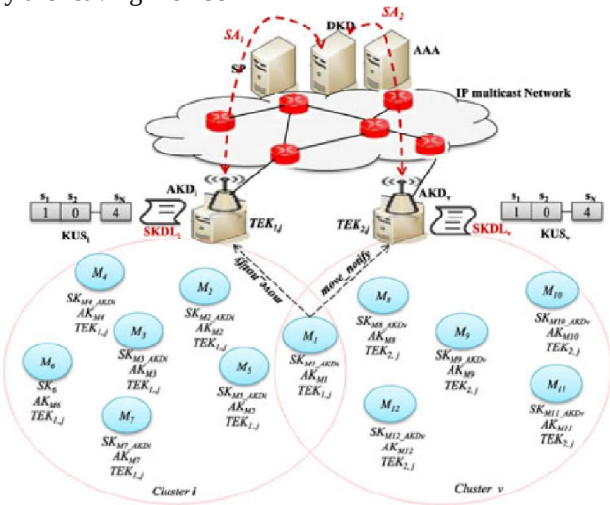


Fig. 2. Reference framework.

undergo rekeying hence causing considerable rekeying overhead for multiple services case. Most GKM schemes such as Decleene et al. [13], GKMF [14], [17], Kellil et al. [15] adopt DR strategy for efficient rekeying though inefficient for multi-services co-existing in a single network. The schemes also suffer from one-affect-n phenomenon which requires all clusters commit to the updated TEK during rekeying. For this reason, we propose a novel key management rekeying strategy, not realized in the design of conventional approaches to address security for multi-service groups subscribed by multi-users as illustrated in Fig. 1. However, this paper only considers dynamic member location change of mobile hosts subscribed to multiple subscriptions without considering dynamic membership change which is also applicable.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

III. REFERENCE FRAMEWORK

Our framework adopts a two tier decentralized framework similar to [13], [14], [15] as shown in Fig. 2.
The first level is the domain level which is the core wired part consisting of Domain Key Distributor for initial key management and authentication procedures. The second level is the area level which is the wireless part consisting of multiple clusters each of which are managed by the Area key Distributor independently. Each cluster contains a set of members subscribed to diverse multicast services who dynamically perform handoff across widely distributed clusters under homogeneous or heterogeneous vendors. However, the framework adopts independent TEK per cluster to alleviate one-affect-n phenomenon and to localize rekeying process. If rekeying process of the TEK is triggered due to joins or leaves emanating from mobility, this is handled locally without disturbing the entire system. In order to unburden the key management and authentication phases of the SMGKM from centralized DKD, we allow the AKDs to verify moving subscribers, generate, update and distribute the service encryption keys. We also introduce AKD to AKD link in the framework similar to X2 interface in LTE [3] to improve the handoff rekeying performance by reducing the investment pressure at the core of the network while giving DKD scalability. Similar to DR, each AKD maintains secure mobility list called Session Key Distribution list to track mobility and reduce the need for rekeying when members handoff while maintaining the subscribed services.
This generic framework can be mapped in to all IP next generation network architectures like LTE and WiMAX. In LTE, the Mobility Management Entity (MME) can perform the role of the DKD and in WiMAX the Connectivity Service Network (CSN) AAA server can perform the DKD duties while the Access Service Network (ASN) gateway can act as the SP. The eNodeB (eNB) or BS correspond to the AKD_i. Though the mappings can be unique, key management, mobility management and authentication phases are maintained in SMGKM.

3.1 Initial Key Distribution

SKDL concept introduced in [8], DKD initially derives the necessary cryptographic keys on group setup and the rest is handled at the cluster level. After successfully registration of mobile receivers $M_i$subscribed to diverse multicast services and knowing their mobility pattern, DKD initially derives the $M_i$short term individual AKD_ispecific session keys (SK_{MiAKDi}) depending on the $M_i$mobility pattern. DKD also derives the $M_i$unique long term authentication key (AK_{Mi}) which is embedded on the mobile device smartcard. The DKD then generate secure session key distribution list for the particular $AKD_i$with rows corresponding to the number of registered $M_i$under cluster area i. Table 1 shows an illustrave example of the generated $SKDL_i$where priority numbers determines either a high speed $M_i$subscribed to services with stringent delay and sensitive to packet delivery or low speed $M_i$subscribed to delay tolerant services.
Each $SKDL_i$row is encrypted using pairwise security association key SA_ishared between the $AKD_i$and the DKD for securely pushing the corresponding $SKDL_i$rows to the AKD_iat cluster i where $M_i$currently resides. The row information is also integrity protected using unique MAC to alleviate replay attacks. Thus each AKD_ihas the capability to modify its own rows without affecting the rows for its neighbors. If members newly join the network, the DKD becomes the initial step to derive its SK_{Mi_AKDi}then forward the $M_i$particular row to its current location so that the corresponding AKD_iupdate its $SKDL_i$rows. Each AKD_ion receiving the $SKDL_i$rows, it can securely establish N TEK_ishares ($TEK_{i,j}$) for N services using Key derivation function (KDF) such as SHA1 [20] without involvement of the DKD hence giving DKD scalability.

IV. PERFORMANCE AND SIMULATION ANALYSIS

The performance of SMGKM scheme is analyzed through numerical analysis and simulations in terms of rekeying transmission overhead corresponding to the additional signalling load caused by rekeying, storage overhead corresponding to the storage capacity of the key management keys stored by the entities (M_i, $AKD_i$and DKD). The communication overheads for both rekeying approaches (pairwise and LKH) as a result of unicast or multicast transmissions of rekeying messages at the cluster level are also considered. Finally the security analyses section considers all types impossible attacks in SMGKM.

4.1 Rekeying Transmission Overhead

Let the rekey signaling message delivery between the DKD and the AKDs be v unit and between the MN and the AKDs be a unit respectively. The parameters v and aare the weightings factors of the signal load at the core network and the wireless part of the framework respectively. They are used to determine link stability. Since the DKD locate the currently serving AKD_iwhich could be far away from the DKD then v >> a. Therefore by using the rekeying transmissions obtained in Table 5, the signalling cost induced by rekeying at the wired and wireless parts of the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

SMGKM when n-moves subscribed to s-multi-services occur can be formulated and compared to the convectional schemes as summarized in Table 7.

As shown in Fig. 9, SMGKM outperforms the conventional protocols by giving minimum rekeying transmissions for increasing number of handoffs and services.

By allowing the AKDs to perform rekeying process gives DKD scalability and reduces the signaling investment pressure at the core network. Therefore our system can be considered as signalling optimizer for efficient bandwidth utilization. Surprisingly IR outperforms GKMF because GKMF involve the DKD on every rekeying process which increases signaling at the core network for cumulative services. However, FEDRP, GKMF and Kellil et al give similar rekeying transmisions at the cluster level. Since the cluster level is bandwidth limited and subject to high packet loss, reduction in the rekeying transmissions depends on the rekeying approach used for efficient bandwidth utilization. Usually LKH rekeying approach [5] is favourable to reduce the rekeying transmission overheads at the cluster level as discussed.

The IR reduces the need to rekey the service keys but triggers local area key rekey only at both clusters. To further reduce communication overheads from IR, both the GKMF and KELLIL et al schemes adopt DR strategy by introducing the use of mobility list as to record handover members such that the previous cluster i induces null communication overhead on handover. This actually improves the bandwidth

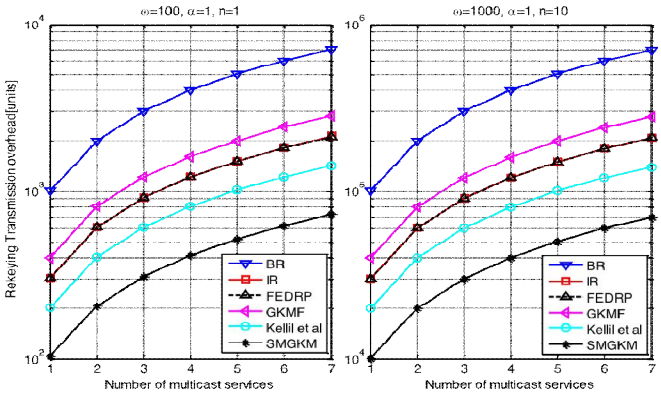
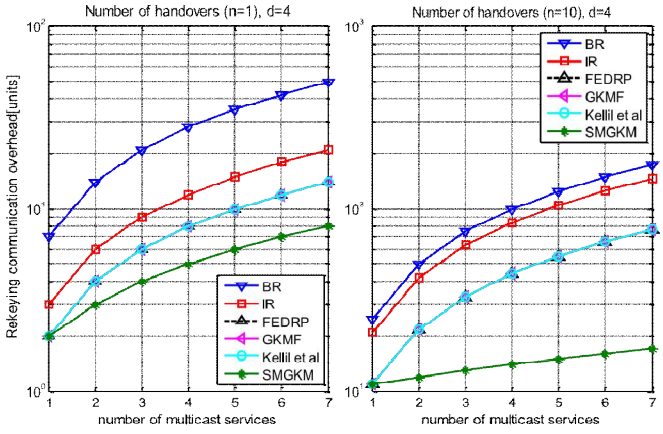


Fig. 9. Rekeying Transmission overhead.

limitations has enforced the introduction of SMGKM scheme which is very adaptive multi-services with multihandoffs. With cryptographically separate keys per cluster in SMGKM, the rekeying of the $TEK_{i;j}$shares get localized hence alleviating one-affect-n phenomenon.SMGKM also minimize the need to introduce easily compromised local area keys like in convectional schemes hence improving security as described in Section 6.5 and storage efficiency at the handover entity



.Fig. 10. Pairwise rekeying communication overheads.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

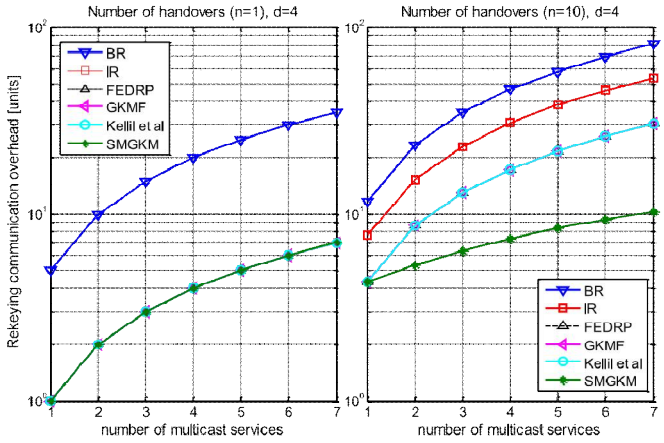


Fig. 11. LKH rekeying communication overheads.

However both GKMF and Kellil et al induce high storage cost at the limited resource member due to introducing more encryption keys which may drain more battery compared to each TEK_ishare which is light to process since $TEK_{i;j}TEK_i$. Thus the sum the $TEK_{i;j}$shares for N services is equivalent to one key in SMGKM.

V. Conclusion and Future Work

In this paper, a new SMGKM scheme has been proposed to improve the key management performance in the presence of multi-moves participating in multi-group services. It considered providing backward confidentiality where mobile receivers dynamically perform handoff while seamlessly maintaining diverse subscriptions. In contrast to convectional schemes targeted for a single service, SMGKM used a new rekeying strategy based on lightweight KUS and SKDL for effectively performing key management and authentication phases respectively during handoff. SMGKM adopted independent TEK per cluster to localize rekeying and mitigate one-affect-n phenomenon. By offloading the key management and authentication phases to the intermediate AKDs massively reduced signalling load at the core network than in convectional schemes hence giving DKD scalability while preventing bottlenecks. The SMGKM analytical model was developed for two rekeying approaches: pairwise and LKH. Numerical analysis and simulation results of the SMGKM performed much better using both rekeying approaches in comparison to previous work. Thus SMGKM have shown significant resource economy in terms of communication bandwidth overhead, storage overheads at the DKD, AKD, and the mobile receiver while providing intense security. Finally, the analytical study was explored by simulation for solving the bandwidth optimization problem in SMGKM which showed efficiency in bandwidth consumption in the presence of multi-services. However, SMGKM is expected to become a practical dynamic solution for securely and efficiently managing multi-services which can be received concurently by huge mobile subscribers in the future wireless networks such as emerging SoftwareDefined Networks.

References

[1] G. S. V. R. K. Rao and G. Radhamani, WiMax: A Wireless Technology Revolution. Boca Raton, FL, USA: Auerbach Publishers, 2008.
[2] 3GPP, “Multimedia Broadcast/Multicast Service; Stage 1 (Release 8),” Technical Specification 3GPP TS 22.146, vol. 8.3.0, (2007-06) , Jun. 2007.
[3] 3GPP, “Digital cellular telecommunications system (Phase 2þ) ; Universal Mobile Telecommunications System (UMTS);LTE; Multimedia Broadcast/Multicast Service (MBMS); Stage 1 (Release 9),” Technical Specification 3GPP TS 22.146, vol. 9.0.0, (2010-01) , 2010.
[4] P. Judge and M. Ammar, “Security issues and solutions in multicast content distribution: A survey,” IEEE Netw., vol. 17, no. 1 , pp. 30–36, Jan./Feb. 2003.
[5] W. Chung Kei, M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” IEEE/ACM Trans. Netw., vol. 8, no. 1 , pp. 16–30, Feb. 2000.
[6] S. Rafaeli and D. Hutchison, “ A survey of key management for secure group communication,” ACM Comput. Surveys, vol. 35 , pp. 309–329, Sept. 2003.
[7] T. T. Mapoka, “Group key management protocols for secure mobile multicast communication: A comprehensive survey,” Int. J. Comput. Appl., vol. 84, pp. 28–38, Dec. 2013.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

[8] T. T. Mapoka, S. Shepherd, R. Abd-Alhameed, and K. Anoh, "Efficient authenticated multi-service group key management for secure wireless mobile multicast, " in Proc. 3rd Int. Conf. Future Generation Commun. Technol., 2014, pp. 66–71.
[9] Y. Challal and H. Seba, "Group key management protocols: A novel taxonomy," Int. J. Inf. Technol., vol. 2, pp. 105–119, 2005.
[10] H. Harney and C. Muckenhirn, "Group key management protocol (GKMP) Specification," RFC 2094, Jul. 1997.
[11] T. Hardjono, B. Cain, and I. Monga, "Intra-domain group key management for multicast security," IETF Internet draft, Sept. 2000.
[12] S. Mittra, "Iolus: A framework for scalable secure multicasting," SIGCOMM Comput. Commun. Rev., vol. 27, pp. 277–288, 1997.
[13] B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, D. Towsley, S. Vasudevan, and C. Zhang, "Secure group communications for wireless networks," in Proc. Commun. Netw.CentricOper.: Creating Inf. Force. IEEE Military Commun. Conf., 2001, vol. 1, pp. 113–117.
[14] L. M. Kiah and K. M. Martin, "Host mobility protocol for secure group communication in wireless mobile environments," Future Generation Commun. Netw., vol. 1, pp. 100–107, 2007.
[15] M. Kellil, J. C. A. Olivereau, and P. Janneteau, "Rekeying in secure mobile multicast communications," United States Patent Application Publications, US 2007/ 0143600 A1, 2007.
[16] S. Gharout, A. Bouabdallah, M. Kellil, and Y. Challal, "Key management with host mobility in dynamic groups," in Proc. 3rd Int. Conf. Security Inf. Netw., 2010, pp. 186–194.
[17] M. L. M. Kiah and K. M. Martin, "Host mobility protocol for secure group communication in wireless mobile environments," Int. J. Security Appl., vol. 2, pp. 39–52, Jan. 2008.
[18] C. Zhang, B. DeCleene, J. Kurose, and D. Towsley, "Comparison of inter-area rekeying algorithms for secure wireless group communications," Perform. Eval., vol. 49, pp. 1–20, Nov. 2002.
[19] J. Loughney, M. Nakhjiri, C. Perkin, and R. Koodli, "Context transfer protocol (CXTP)," IETF RFC 4067, 2005.
[20] S. Kelly and S. Frankel, "RFC4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec," IETF RFC 4868, May 2007.
[21] K. C. Almeroth and M. H. Ammar, "Collecting and modeling the join/leave behavior of multicast group members in the MBone," in Proc. 5th IEEE Int. Symp. High Perform. Distrib. Comput., 1996 , pp. 209–216.
[22] K. C. Almeroth and M. H. Ammar, "Multicast group behavior in the Internet's multicast backbone (MBone)," IEEE Commun. Mag., vol. 35, no. 6, pp. 124–129, Jun. 1997.
[23] C. Kin-Ching and S. H. G. Chan, "Distributed servers approach for large-scale secure multicast," IEEE J. Sel. Areas Commun., vol. 20, no. 8, pp. 1500–1510, Oct. 2002.
[24] L. Kleinrock, Queueing Systems. New York, NY, USA: Wiley, 1975.
[25] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast : Issues and Architecture," National Security Agency, RFC 2627, Jun. 1999.