A Novel Key Management Scheme for Multicast in MANET

S. Silviya¹, N. Subbulakshmi², J. Lavanya³
¹ PG Student (M.Tech), Department of Information Technology, Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, Anna University, Chennai.
² Assistant Professor, Department of Information Technology, Sivanthi Aditanar College of Engineering, Tiruchendur, Anna University, Chennai.
³ silviyait51@gmail.com, lavsjk@gmail.com

Abstract: Mobile multicast communication is currently a strong topic due to the quality of wireless and mobile technologies for key management. The existing group key management protocols intend to secure group communication for just a single group service. In this paper, we propose a novel GKM protocol for multiple multicast groups, called slot based multiple group key management scheme. SMGKM supports the movement of single and multiple members across a homogeneous or heterogeneous for minimized rekeying transmission overheads.

Keywords: Group key management, mobile multicast, security, wireless networks.

I. INTRODUCTION

The standard way to provide access control mechanism for secure multicast communication is by using a symmetric group key, known as Traffic Encryption Key (TEK), shared only by authorized group members. Group messages encrypted with TEK can be decrypted by legitimate group members holding similar TEK therefore assuring secure group communication. Maintaining an efficient key management system is challenging due group membership dynamics caused by member joins or leaves. This triggers update of the TEK through rekeying process. During rekeying process, the key server delivers the new TEK to the existing group members to invalidate the old TEK. This restricts access to the future (prior) messages after member (join) leaves, to satisfy forward (backward) secrecy [1].

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 and wireless mobile multicast networks will suffer from rekeying performance for cumulative multicast services because there are only targeted for a single multicast service.

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.

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.

In SMGKM the key management task 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 for fast and secure authenticated handover along with initial key establishment shown in Fig 1. SMGKM employ a lighter symmetric encryption suitable for resource constraint mobile devices than heavier asymmetric effort.

Fig1: Signal flow for our SMGKM protocol.
II. REFERENCE FRAMEWORK
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.

2.1 Initial Key Distribution
After successfully registration of mobile receivers Mi subscribed to diverse multicast services and knowing their mobility pattern, DKD initially derives the Mi short term individual AKDi specific session keys (SKMi AKDi) depending on the Mi mobility pattern. DKD also derives the Mi unique long term authentication key (AKMi) which is embedded on the mobile device smartcard. The DKD then generate secure session key distribution list for the particular AKDi with rows corresponding to the number of registered Mi under cluster area i.

Each SKDLi row is encrypted using pairwise security association key SAl shared between the AKDi and the DKD for securely pushing the corresponding SKDLi rows to the AKDi at cluster i where Mi currently resides. The row information is also integrity protected using unique MAC to alleviate replay attacks. Thus each AKDi has 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 SKMi AKDi then forward theMi particular row to its current location so that the corresponding AKDi update its SKDLi rows. Each AKDi on receiving the SKDLi rows, it can securely establish N TEKi shares (TEKi;j) for N services using Key derivation function (KDF) such as SHA1 [2] without involvement of the DKD hence giving DKD scalability.

III. NOVAL REKEYING STRATEGY
Each slot l determines the total number of members from a combination of MGk participating in service N where Ai, sn=1. Moreover, each slot can dynamically increment or decrement by 1 whenever a join or leave occur respectively or reset to zero if no member is subscribed to service N. For example, with 12 members, fM1;M2g 2 G1 access fs1g, fM1;M2;M3;M4;M5;M6g 2 G1;G2;G3 access fs2g, fM3; M4; M5; M6; M7; M8g 2 G2; G3; G4 access fs3g,FM5; M6; M7; M8; M9; M10g 2 G3;G4;G5 access fs4g, fM9; M10; M11; M12g 2 G5;G6 access fs5g and fM9;M10;M11;M12g 2 G5;G6 access fs6g.

Therefore the initial KUS generated acquiescent to for the corresponding n(sN) is shown in Fig. 2 with [2, 6, 6, 4, 4] members in the service slots fs1; s2; s3; s4; s5; s6g respectively.

Fig 2: Reference Frameworks

A. Key generation and data confidentiality
Data confidentiality for multiple data streams in the same network can be applied to the generated KUS. Thus in SMGKM, the AKDi initially derive service specific group key (TEKi) which is split in to multiple TEK shares {TEK1;1,TEK1;2 . . . TEKi;j} corresponding to N services such that TEKi;j _ TEKi, where i denotes the cluster and j denotes a particular service[3].

B. Secure Data Transmission
Assuming the SP hold valid TEK shares, it securely transmits the services subscribed to the corresponding Mi under each cluster using a specific bandwidth for that service. Let BW(Sn) denote the bandwidth used to transmit service sN,let C(n(GK)) be the cost of transmitting a unit data to n members Mi for i = 1; . . . n in GK via multicast.

C. Member Handoff with backward secrecy
To address the rekeying problem, only member handoff with backward secrecy is considered in our system since members maintain session continuity while changing point of attachment to the network [5] in Fig 2.

Step 1: M1 simultaneously send a move _notify message to both AKDi and the target AKDi encrypted under its derived SKM1 AKDi to AKDi, i.e.

M1 → AKDi : {move _notify}SKM1_AKDi

Step 2: AKDi on receiving the move _notify message it verifies SKM1 AKDi against the already derived SKM1 AKDi by the DKD stored in the SKDL1 row. If M1 derived SKM1 AKDi matches, then the AKDi can decrypt the move _notify message.However AKDi wait
for a period Tup to accommodate more incoming notification requests.

**Step 3:** AKDi verify the number and IDGj of services subscribed to M1 along with the target AKDv from the notification message. Note that AKDi cannot modify the SKDLv rows of the target AKDv since the assumption is that each row is integrity protected using AKDi specific MAC, i.e. each AKD can access and modify its rows.

**Step 4:** AKDi notices that M1 is subscribed to s1 and s2 from Fig. 1 and start generating the new KUS from the initially generated KUS after Tupelapse. The affected services s1 and s2 require backward secrecy rekeying of TEKi;jVN : Ai:N = 1 to all Mi 2 G1, G2, G3 at the target cluster after the KUS update process by the target AKDv.

**Step 5:** AKDi securely transmit the new KUS to the target AKDv along with the M1 row in the SKDLv via the fast AKDi-AKDv link using context transfer protocol (CXTTP) [6] without involving the DKD. This provides better support for accelearting handoff.

**Step 6:** AKDi finally wait until M1 completely handoff then revokes the M1 row from its SKDLi for security purposes. Note that each AKDi only stores information of the existing members Mi they are currently serving to enhance storage complexity.

**Step 7:** The target AKDv on receiving the new KUS along with its rows, it also performs integrity checks of its rows received before obtaining the already M1 derived SKM1AKDv specific to the target cluster v. From the received new KUS, the AKDv also determines the services subscribed by M1 then undergo KUS update process For the affected services requiring TEKi;j shares update, AKDv update the key shares and wait until M1 signal its interest to move in to cluster v.

**Step 8:** On arrival at the crossover region towards the target cluster v where (Pi <<Pv), M1 knowing the AKMi and detecting the IDAKDi, it derives the SKM1 AKDv using one of prominent KDFs such as SHA.

**Step 9:** The AKDv undergo SKM1_AKDv verification process described in step 2. After verifying the M1 request as well as the services subscribed to M1, it securely transmit the new TEKi:v shares for the affected services (s1; s2) according to the received KUS from AKDi via unicast response message to M1 encrypted under SKM1 AKDv and via multicast response message to the existing members Mv subscribed to the same set of affected services (s1; s2) encrypted with the old TEKi:v shares. i.e:

1)AKDv→M1:{move response(new_TEKi:v)|SKM1_AKDv}
2)AKDv→Mv:{move response(new_TEKi:v)|old_TEKi:v}

**V. REKEYING APPROACH**

**5.1 Pairwise Rekeying Approach**

In pairwise rekeying approach, all the members subscribed to similar group services share common TEKi:v shares. Whenever a member re-joins at the target cluster v, the AKDv multicast the new TEKi:v shares for the affected services (encrypted with the old TEKi:v) to the existing members Mv under cluster v and unicast the new TEKi:v shares to the new joining member M1 from cluster i encrypted by M1 derived secret key (SKM1 AKDv)[7].

**5.2 Logical Key Hierarchy Approach**

In LKH rekeying approach, a full balanced key graph tree of degree d is used to approximate the rekeying overhead at any time. For join operation at the target cluster v, the AKDv where the join occurs should renew each key that is on the path from the leaf that represents the secret key/individual key associated to the new joining member to the root of the tree which denotes the TEK. Consequently, each key from the leaf of the new member to the root is transmitted twice, i.e. transmitted to the new joining member through unicast encrypted under the child key known to the new member, and via multicast to the members that share the node encrypted under its old version.

**VI. CONCLUSION**

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. The SMGKM analytical model was developed for two rekeying approaches: pairwise and LKH. SMGKM is expected to become a dynamic solution for securely and efficiently managing multi-services which can be received concurrently by huge mobile subscriber’s in the future wireless networks.

**REFERENCES**


