



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Security Based Service Key Management for Multiple Group

Jancy Rani.D, Sabarinathan.P

PG Scholar, Dept. of CSE, Pavendar Bharathidasan College of Engineering and Technology, Trichy, Tamilnadu, India

Assistant Professor, Dept. of CSE, Pavendar Bharathidasan College of Engineering and Technology, Trichy,
Tamilnadu, India

ABSTRACT: In wireless and Mobile technologies key Management in mobile multicast is grown rapidly. The convergence of wireless and mobile technologies is one of the reason or cause for the issue. The multiple group based services are possible to exist with a single network; also the subscriber can use these services ubiquitously. The existing system, Group Key Management protocol to provide a secure group communication in single group service. Inefficient use of keys and rekeying overheads are occurs in Group Key Management approaches. The Group Key Management protocol is not suitable for multiple multicast group service. In Proposed system, Slot Based Multiple Group Key Management protocol supports the multiple group services, it can also reduced rekeying transmission overheads. The Domain Key Distributor and Area Key Distributor to providing intense security in terms of communication bandwidth, storage overhead.

KEYWORDS: Group key management, security, multicast service, wireless network

I. INTRODUCTION

Group oriented applications are delivered the internet by using multicast. Multicast is bandwidth efficient techniques for this application. The applications such as mobile TV services, video on Demand, Interactive group games. One-to-many and many-to-many transport communication mechanism was used by multicast content distribution. The multicast application demand to increase the development of wireless network and emergence of portable devices. The multimedia broadcast multicast service (MBMS) was standardized to evolve wireless networks such as WiMax and 3GPP. MBMS is used to distribute the delivering of broadcast and also multicast services, interconnect with cell and core network.

In open wireless network facing many problems due to the security attacks like eavesdropping opportunities, Denial of service, physical node capture attacks, Impersonation attack, and others. In wireless networks, multicast content was securely delivered to the specific group members. The access control mechanism to provide secure multicast communication, it can be used to symmetric group members. Group of messages are encrypted using the TEK and the TEK should decrypted using legitimate group of members, it should to holding the TEK secure group communication. Multi group service was supporting for service providers to overhead the substantial key management. The rekeying complexity was solved by multicast services in a single network. The single and multi move across a wireless network was managing for an SMGKM protocol. It also multi services and minimized rekeying transmission overheads.

II. RELATED WORK

Rekeying over wired networks is divided into centralized, decentralized and contributory schemes in traditional GKM protocols to be addressed. The domain key distributor is also known as the centralized server, it rely to the centralized schemes. The DKD wok is the encryption key will be generating and distributing. The DKD cannot be explicit for the



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

contributory scheme; group key establishment was collaborated to the group members. Subgroup Managers are equally distributed the key management task, and it partitioning the group into subgroup by using Decentralized schemes.

The GKM categorized by common TEK (Traffic Encryption Key) and Independent TEK using subgroup approaches. The common TEK was used to one TEK for all the group members, it commonly affected from one-affect-n phenomenon; thus the all subscribed members are affected to the rekeying of new TEK. Subgroup approaches are tried to alleviate the one-affect-n phenomenon in the Independent TEK, it caused by the common TEK approaches. To addressing the similar rekeying issues are described from the approaches such as common TEK and Independent TEK.

A single multicast service are considered to propose various rekeying strategies the Handoff can be performed between cluster i and v , it also maintain the voice and sports, active subscribed services. The process of rekeying is independently triggered the three service groups 1, 2, and 3 are affected. Baseline rekeying (BR) strategy was used to both the old and the target cluster. Immediate rekeying (IR) strategy can be solved the problem of rekeying only the local area keys. The Mobility lists of track and manage host mobility is to introducing by IR rekeying problem can be alleviate from type of Delayed rekeying strategy. Rekeying is performed at the target cluster only.

Finally the members leaves, clusters are previously meet by the leaving member, in rekeying process. Dynamic memory location is used for changing the sub scriber of mobile host to multiple subscribers without using the dynamic membership

III. PROPOSED ALGORITHM

A. Design Considerations:

- The files are selected and are uploaded into the server.
- Generate the cluster formation of subscribers are developed and for each subscriber within the cluster a separate IP address is generated.
- For each cluster a domain key is automatically generated in a random manner.
- Area keys are randomly generated for each cluster.
- The received file will be in encrypted format.
- To decrypt the file corresponding area key and domain key must be given.

B. Description of the Proposed Algorithm:

The main goal of the proposed algorithm fir symmetric key algorithm is used to the group members are securely retrieve the files. The keys are formed to the encryption and decryption pattern. The algorithms for cryptographic key for both encryption and decryption of the cipher text.

Step 1: Symmetric Key

The keys may be identified or there may be a simple transformation to go between the two keys. The key, in practice, represent shared secret keys between two or more parties that can be used to private information link. This requirement that both users have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public key encryption.

Step 2: Symmetric Encryption

A secret key, which can be a number, a work, or just a string of random letters, is used to the text of a message to change the content in a particular way. This might be as simple as shifting by each letter by a number of places in the alphabet order. As long as both sender and recipient know the secret key, that can be encrypted and decrypt all the messages that used this key.

Step 3: Selection criteria

The DKD has to provide the randomized key to the each group members. The AKD also distribute the key using key update slot to the group member. It performs traffic Encryption key to securely sending the file or anything else. Symmetric key algorithm to provide a security, and also minimized rekeying strategy.

Secure Data Transmission eqn. (1)

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

$$n(S_N) = \sum_{j=0}^k n(G_j) \times A_i N, \quad \text{eqn. (1)}$$

Where $n(S_N)$ denote the total number of members subscribed to service N and $n(G_j)$ the number of members under a specific SG.

Step 4: Actual Rekeying approaches

The rekeying approaches are categorized by pair wise rekeying and logical key hierarchy rekeying. The pair wise rekeying approach is common TEK shares the all subscribed members to similar group services shared. LKH rekeying approaches is full balanced key graph 'd' degree of tree is particularly the rekeying at anytime.

IV. PSEUDO CODE

Step 1: The M_1 groups are simultaneously sent move_notify message to the both AKD_i and target AKD_v was encrypted and it's derived $SK_{M_1-AKD_i}$ to AKD_i .

$$M_1 \rightarrow AKD_i ; \{ \text{Move_notify} \} SK_{M_1-AKD_i} \quad \text{eqn. (2)}$$

Step 2: The Move_notify messages are received from AKD_i , and it verifies SKM, AKD; AKD_i verify and also verify the number and ID_{G_j} of subscribed services to M_1 along with target AKD from the message Notification.

Step 3: The AKD_i was securely sending the new KUS into target AKD_v along with M_1 , AKD finally wait M_1 has been completely handoff, revokes the M_1 from security purpose for SKDL (session key distribution list); the new KUS with rows are receiving from target AKD_v .

Step 4: the affected service was required TEK can share and update, it also update the key share of AKD and also waiting for M_1 signal interested to move to the cluster v.

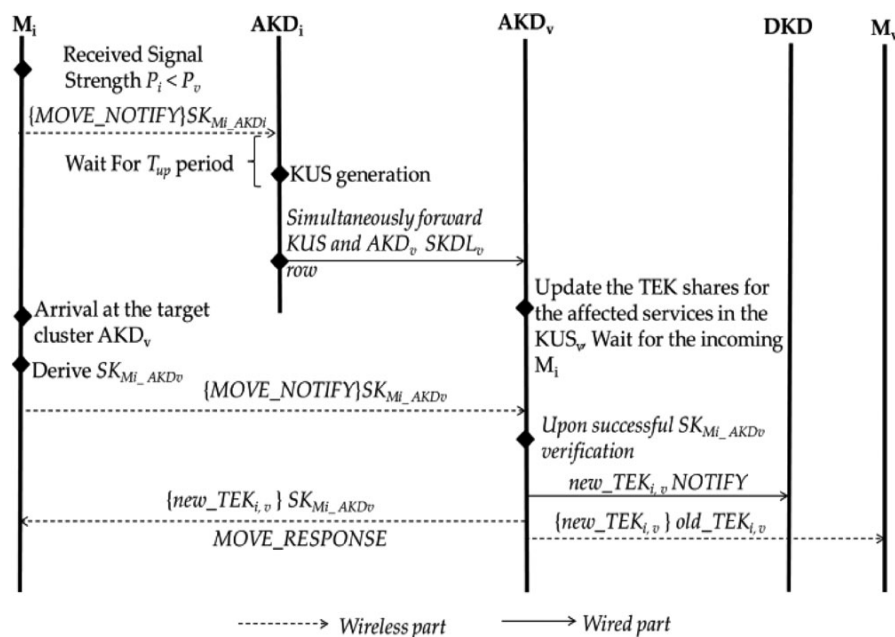


Fig.1. Signal flow for our SMGKM protocol

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

The SMGKM protocol was guaranteed backward secrecy requirement. The updated TEK shares the data transmission was secured using SP (Service Provider).

V. EXPERIMENTAL RESULTS

SMGKM scheme are analyzed the numerical analysis and simulation in terms of rekeying transmission overhead, rekeying communication overhead, storage overhead, bandwidth consumption in SMGKM, security analysis. The Rekey signal messages are delivered into the DKD and AKD in 'w' unit, and also delivered to the MN and the AKD, be α unit respectively. SMGKM using pair wise and LKH rekeying approaches for induced the communication overhead; it also compared the cluster level into conventional approaches.

The service provider is to all the files are selected and are uploaded into the server. Maintaining an efficient key management system is challenging due to group membership. In multicast services, members not only dynamically join or leave the services as addressed in single service scenario.

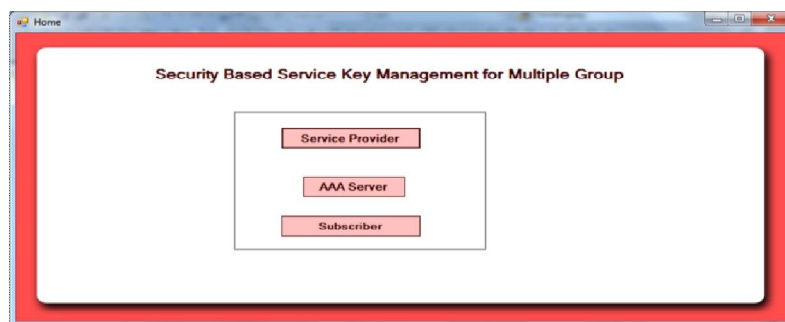
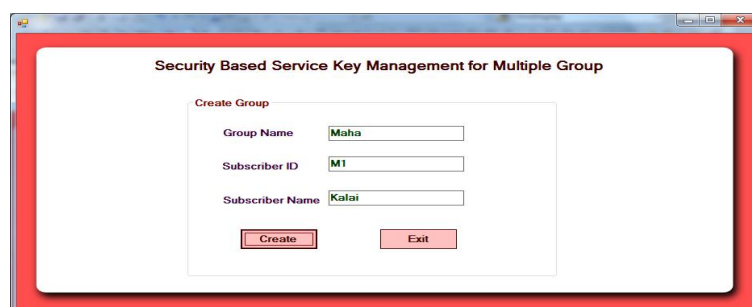


Fig.2.Service provider

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.

During group generation cluster formation of subscribers are developed and for each subscriber within the cluster a separate IP address is generated. The received file will be in encrypted format. To decrypt the file corresponding area key and domain key must be given.



The screenshot shows a window titled "Security Based Service Key Management for Multiple Group" with a "Create Group" form. The form contains three input fields: "Group Name" with the value "Maha", "Subscriber ID" with the value "M1", and "Subscriber Name" with the value "Kalai". Below the fields are two buttons: "Create" and "Exit".

Fig. 3.Group Generation



International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

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 initially generate a group. The existing GKM schemes for secure wired and wireless mobile multicast networks will suffer from rekeying performance for cumulative multicast services.

VI. CONCLUSION AND FUTURE WORK

The presence of multi moves participating multi group services improved the key management performance using new SMGKM scheme. The SMGKM scheme is used to new rekeying strategy for lightweight KUS and SKDL in performance key management and authentication until effectively during handoff. To localize rekeying and mitigate for one-affect-n phenomenon is Independent TEK per cluster can adopt the SMGKM. In terms of communication bandwidth overhead, storage overhead of significant resource economy at the DKD and AKD and mobile receiver is providing the intense security. Finally the SMGKM key management is showed the result is to improve the key management in multiple multicast group services. SMGKM is expected to become a practical dynamic solution for securely and efficiently managing multi-services which can be received concurrently by huge mobile subscriber's in the future wireless networks such as emerging Software Defined 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 2p); 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.