ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

SLOT BASED GROUP COMMUNICATION WITH SINGLE KEY MANAGEMENT IN MANET

Ms. T.Ranjeetha,[#1]M.E.,(CSE),
Bharathiyar Institute of Engineering for Women,
Deviyakurichi
Email id: ranjitharaj92@gmail.com

Ms. M.R. Nithya,[#2],M.E.,
Assistant Professor(CSE),
Bharathiyar Institute of Engineering for Women,
Deviyakurichi,
Email id: nithyarathinam@gmail.com

Abstract -High demand from the Internet Service Providers to carry multimedia services over high speed wireless networks. These networks are describing by high mobility receivers which perform frequent handoffs across homogenous and heterogeneous access networks while maintaining logical connectivity to the multimedia services. In order to ensure secure delivery of multimedia services to certain group members, the conventional cluster based group key management schemes for securing group transmission over wireless mobile multicast networks have been proposed. They lack efficiency in rekeying the group key in the existence of high mobility users which concurrently subscribe to multiple multicast services that co-exist in the same network. The users are expected to drop subscriptions after multiple cluster visits hence promote huge key management upward due to rekeying the previously frequent cluster keys. The multi-serviceto system with completely decentralized authentication and key management functions is adopted to meet the demands for high mobility setting with the same level of security.It shows resource economy in terms of reduced communication and less storage overheads in a high speed status with various vacation.

Key word-Mobile multicast, decentralized authentication, cluster keys.

1. INTRODUCTION

The network is characterized by the absence of central administration devices such as base stations or access points. Multicast is a bandwidth capable technique for delivering group-oriented applications over the internet.These include utilization such as video conferencing, interactive groupgames and mobile TV services. Multicast satisfied distribution utilizes one-to-many and many-to-many to transport communication mechanism.Although adopting centralized approach easy management because the plan of trust is focused on one entity and some transportation overheads are decreased as member of group need to authenticate the main individual only one time, they suffer from some weaknesses as dependencies on a key server leave a single point of failure also, it must be constantly available during group operations and for larger group size, the amount of message communication between the key manager and group members can be badly increased at a same time, which could create bottleneck.To deliver the multicast satisfied securely only

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

to the group members in wireless networks, an access control mechanism which ensures confidentiality, security digitalcontents, and simplifies computing for the broadcasted services is obligatory encrypted using pairwise security association key shared between the key distributor and it is securely pushing the corresponding SKDL rows to the AKD at cluster where M currently resides.

2.EXISTING SYSTEM

Group messages encrypted with TEK can be decrypted by appropriate group members holding similar TEK therefore encourage secure group communication. Maintaining adynamic key management system is challenging due group membership gesture induce by member joins or leaves. This produce update of the TEK through rekeying process. During rekeying system, the key server delivers the new TEK to the existing group members to revoke the old TEK. This can be restrict access to the future (prior) messages after member (join) leaves, to delight forward (backward) secrecy. To simply reduce the key management rekeying overheads, tree GKM protocols have been extensively studied in the literature.

Managing multiple groups with overlapped membership is one of the important issue in group communication scheme. It possible for the members at higher levels to count the keys for its own level along with all its descendant levels just by storing extra pre-positioned information.

3. PROPOSED SYSTEM

In distributed or contributory approach, there is no explicit key entity or center, and all members contribute to managing the keys. Christo Ananth et al. [7] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

Typical GKM schemes for secure wired and wireless multicast networks only target a single multicast service sign up by low mobility users. In inclusion to our multi-service group key management scheme known as SMGKM, devoted to providing secure multi-group align services to mobile users dynamically perform handoff while seamlessly perform in multiple multicast services, now regard rekeying during dynamic movement of high mobility users in multiservice contribution then leave subscriptions after multiple cluster visits.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Decentralized group key management scheme are group manager which is important to govern all group processes, and group members and traffic key is sharedbetween members of a group which is frequently used for encryptingthe data traffic.

4. MODULE DESCRIPTION

4.1 Initial Key Distribution

Key Distributor initially derives the necessary cryptographic keys on group setup and the rest is organized at the cluster matched. After successfully registration of mobile receivers subscribed to diverse multicast services and knowing their mobility patterns. Each SKDL row is encrypted using pair wise security association key shared between the AKD and the DKD for securely pushing the corresponding SKDL rows to the AKD at cluster. Thus each AKD has the capability to modify its own rows without stirring the rows for its neighbors.

In the Initial key distribution user A can send the request to connect with user B, key distributor can forward request to the user. After user confirmation received to distributor then sends the key of area key distributor to user.

4.2Novel Rekeying Strategy

Dynamic membership change measured for GKM protocols in wired networks, these protocols consider dynamic location change of members over a widely appropriated wireless network while seamlessly receiving subscribed multicast services securely. The protocols adopt a decentralized framework for scalability. In the Group Key Management schemes is propose address rekeying for multiple group services.

The novel key management rekeying strategy, not recognized in the design of conventional approaches to address security for multi-service group's signup by multi-users as illustrated. Dynamic member location changes of mobile host's signup to multiple subscriptions without considering active membership change which is also applicable.

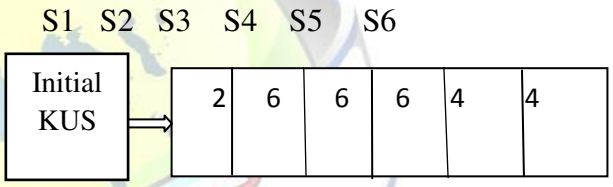

Figure 4.2: Initial generated Key Update Slot

To the access privilege for each service, Key Update slot for N multicast services is initially generated by the trusted DKD on group setup depending on the number of members under GK. The KUS format is divided in to slots of length l bits equivalent to N various services.

Each slot l determines the total number of members from a combination of the participating in service N where N= 1. Each slot can dynamically increment or decrement by 1 whenever a join or leave arise respectively or reset to zero if no member is subscribed to service.

4.3 Key- Request Schemes

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

The two-tier cluster-based decentralized multi-service GKM scheme. It consists of the DKD for initial registration of sign up, initial generation of cryptographic keyparameters for authentication and key management. It also subsists of cluster controllers called AKDs which operate under the jurisdiction of the DKD for securely establishing and assign the group key management keys to valid mobile sign up over a bandwidth limited wireless domain. The mobile users use portable devices like smartphonesto wirelessly to be access their sign up multimedia services over the internet. Each AKD manages the TEK individually per cluster in order to localize group key management. Both the authentication and group key management phases are authorizesecurely from the trusted DKD to the intermediate AKD using a Session Key Distribution List (SKDL) to offer DKD scalability, to prevent bottlenecks and unnecessary delays during the system lifetime. The SMGKM utilizes the multi-service rekeying strategy for dynamic delivery of the TEK group-key-shares destined for mobile users belonging to the same service group.

- Present in the cluster (PIC) users presently being served by the AKD. These are considered as low mobility users assuming they stay long in the utility.
- Absent in the cluster (AIC) users who have frequented numerous clusters served by the target AKD after frequent handoffs. These users are considered to have high mobility.

Clearly it can be realized from the AIC mobile buyer in SMGKM that M1 and M2 in GK have previously visited AKD0, AKD1, AKD2 and AKD3 by performing regular handoffs then finally stay at the target AKD5 before drain contributions. M9 has previously frequent AKD5 and AKD0 before leaving at AKD2.

4.4 Multi-Leaves with Forward Secrecy

Key-request schemes are used, not seeing multi-services and multi-leaves in a wireless mobile network. The key-request schemes attain more productivity by limiting rekeying only to the clusters which have been frequent by a retire user. Thus the rekeying communication overhead it is mainly dependent on the number of clusters that a retire user has frequent. Since the leaving user conserve the local cluster keys for each of the frequent clusters, each previously frequent AKD should unicast rekeying messages counting the updated local cluster keys to PIC users of the frequent clusters.After revise the local cluster keys, each AKD distributes the new TEK from the DKD. This induces rekeying intelligence overhead in the entire wireless network. Though the notifications may be slight in size, they cannot be overlooked in the presence of high mobility users and multi-services demanding TEK update in the network

Thus SMGKM provides access control mechanism which uses the SKDL concept for authentication of highly mobile users before gather the new service group keys used for service access control at the target cluster. The assumption is that a handoff that occurs between two non-adjacent clusters can be possible, which is tolerable enough to make the achievement comparison. Consider a certain cluster v whose AKD initially consists of N mobile users.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

4.5 Communication Overheads

Dynamic multi-service group key management overhead outperforms that of the key-request pattern because high mobility users in key-request schemes maintain the key management keys for the local clusters. This requires rekeying that incurs generous rekeying communication overhead. In contrast, SMGKM only rekeys the distressed clusters where user departure occurs hence reducing communication overheads significantly. If we employ the LKH tree rekeying approach with a equitable tree of degree at the affected clusters, the communication overheads it curtail logarithmically with the number of leaving users for both the schemes.

5. CONCLUSION AND FUTURE WORK

Addressed the inability of existing key-request GKM schemes for secure multicast in high mobility wireless networks by proposing adynamic and feasible solution. The core of the proposed scheme is to decentralize the DKD key management and verification functions. While the DKD only does the initial structure phase of the entire group membership, each AKD keeps path of users during handoff and manages the group TEK division for multiple services independently per cluster to assurance both backward and forward secrecywhen periodic handoffs and multi-leaves participating in multi-services occur respectively. The scheme also achieves high efficiency with compelling reduction in the system conversation overheads as well as reduced storage complication in the communicating agents while preserving secrecy of services. It also reduce the overburdenof the DKD by distributing it to the intermediate AKDs in high mobility.

REFERENCES

[1] Mapoka.T and Shepherd.J,"A New multiple service key management scheme for secure wireless mobile multicast,"IEEE VOL.14,NO.8,AUGUST 2015.

[2] T. T. Mapoka, S. Shepherd, R. Abd-Alhameed, and K. Anoh, "Dynamic authenticated multi-service group key management forsecure wireless mobile multicast, " in Proc. 3rd Int. Conf. Future Generation Commun. Technol., 2014, pp. 66–71.

[3] 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.

[4] 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.

[5] Y. Challal and H. Seba, "Group key management protocols: A novel taxonomy," Int. J. Inf. Technol., vol. 2, pp. 105–119, 2005.

[6] 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.

[7]Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

[8] 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.

[9] 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.

[10] S. Mittra, "Iolus: A framework for scalable secure multicasting," SIGCOMM Comput. Commun. Rev., vol. 27, pp. 277–288, 1997.