ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
August 2014,
Vol. 7, No. (2):
Pgs. 285-291

Key Management Using Dynamic Multicast Functionality of OMCT

VIKRAM M. AGRAWAL

IT Department, BVM Engineering College, India.

(Received: June 20, 2014; Accepted: August 20, 2014)

ABSTRACT

There are many applications like military or public emergency have main concern with secure communication. All this applications use ad hoc environments, so secure key management and message distribution is necessary. The best solution to provide the reliable security to these services is the stipulation of a key management protocol. This paper shows the specific challenges towards key management protocols and different approaches for key management. It also shows the multicast communication with OMCT and its limitations. A new approach, called combination of OMCT with DSDV, can be good. It is not required geographical location information for true connection. It provide high packet ratio with less energy consumption and delay.

Key words: Ad hoc network, Key management, Multicast security, TEK (Traffic Encryption Key), OMCT.

INTRODUCTION

A MANET (Mobile Ad Hoc Network) is a characterized by the deficiency of any fixed infrastructure, so there is no fixed topology in communication networks. The multicast services are developed constantly from last decade. Multicast transmission is an efficient communication method for group oriented applications, such as video conference, interactive multiparty games, software distribution and secures group key distribution. There are no requirements of many resources in multicast transmission so we can consider it as best option. We need to provide authentication, data integrity and data confidentiality need to be provided to stop attacks and eavesdropping. The most suitable solution to provide these services is the establishment of an efficient key management protocol. This protocol is responsible for the generation and the distribution of the traffic encryption key (TEK) to all group members. This key is used for further process for group key management.

There is main challenge of “1 affect n” in multicast key distribution because if any single node join or leave then the TEK is renewed and redistributed every time otherwise face the attack of forward and backward secrecies. To reduce its impact on the protocol performance, several approaches propose a multicast group clustering with removing the limitation of OMCT. Clustering

means to divide the group into several sub-groups (cluster). Each sub-group is managed by a local controller (LC) which is responsible for local key management within its cluster. Thus, when any node Join or Leave procedures, it affects only nodes within the concerned cluster by the rekeying process. Moreover, few solutions for multicast group clustering required the energy issue to achieve an efficient key distribution process, whereas energy constitutes a main issue in ad hoc environments[1, 2].

DSDV with the features of OMCT maintain the table with less energy consumption and delay in packet transmission because it is not required geographical location for true connection.

Requirements for key mangement

In a secure multicast communication, each member holds a key to encrypt and decrypt the multicast data. When a member joins and leaves a group, the key has to be updated and distributed to all group members in order to meet the multicast key management requirements. Efficient key management protocols should be taken into consideration for miscellaneous requirements. Figure 1 summarizes these requirements[14].

Security requirements

Forward secrecy

In this case, users who have left the group should not have authority to access any future key for this particular group. This ensures that a member cannot decrypt data after they leave the group. If node wants to join again then new session will generate for key distribution and older key is discarded forever.

Backward secrecy

A new user who joins the session should not have authority to access old key. This ensures that a member cannot decrypt data which are sent before they join the group. Because some time it may be possible that in intruder enter the group to collect the older messages if he is allowed to see past key then he is able to access the authorised messages which are shared in past session.

Non-group confidentiality

Non group confidentiality means only authorized group member can use the key, so data can be received by only authorized receivers. Users that are never part of the group should not have access to any key that can decrypt any multicast data sent to the group.

Complicity freedom

Any set of fraudulent users or attacker should not be able to deduce the currently used key. It means it is necessary to send key secure manner.

The process of updating the keys and distributing them to the group members is called rekeying operation. A serious problem with any rekey technique is scalability. Because MANET is self organized network so there is frequent possibility of changing the topology of group member. Suppose if any member leaves the group at that time in rekeying system, we need to update the keys of all the users, so key management require large number of keys to exchange in per unit time. So later on we can satisfy the forward and backward secrecies. The number of TEK (Traffic Encryption Key) update messages in the case of frequent join and leave operations affects several QoS characteristics.

Reliability

Packet Drop Ratio

The number of TEK updates messages in the case of frequent join and leave operations, due to this most of the time TEK is used to make updating which induces high packet drop ratio and reduces key delivery ratio which makes it unreliable.

Quality of service requirements

“1 affects n”

If a single membership changes in the group, it affects all the other group members. This happens typically when a single membership change occur all group members commit to a new TEK because if they use the same TEK, just because of feature of MANETs any node (Unauthorized) can join group any time and fail to secure messages.

Energy consumption:

This induces improvement of energy level because in the number of transmissions to all the group members.

End to end delay

Many applications that are built over the multicast services are sensitive to average delay in key delivery. Therefore, any key distribution scheme should take this into consideration and hence minimize the impact of key distribution in the delay of key delivery.

Key Delivery Ratio

This brings number of successful key transmission to all group members without any loss of packet during multicast key distribution.

Man in Middle Attack

it will stop the man in middle attack. Man in middle attack means suppose there is communication between two parties. At time intruder attack in middle during transmission it means any unauthorized node pretend to be actual sender or receive.

To overcome these problems of intruder to pretend authorized sender or receiver, several approaches propose a multicast group clustering [6, 7, 8 and 11]. Clustering is dividing the multicast group into several sub-groups. Local Controller (LC) manages each subgroup, which is responsible for local key management within the cluster or that group.

Thus, after Join or Leave procedures, only members within the concerned cluster are affected by rekeying process, and the local dynamics of a cluster does not affect the other clusters of the group and hence it overcomes "1 affects n" phenomenon. Moreover, few solutions for multicast clustering such as dynamic clustering consider the QoS requirements to achieve an efficient key distribution process in Ad hoc environments.

Existing key management approaches

Key management approaches can be classified into three categories: Centralized, distributed or decentralized. Figure 2 illustrates this classification.

In centralized approach, a designated entity (e.g. the group leader or a key server) is responsible for calculation and distribution of the group key to all the participants. GKMP (Group Key Management Protocol) [12] achieves an excellent result for storage at the members. However, this result is achieved by providing no method for rekeying the group after a member has left, except re-creating the entire group which causes 'n' rekey message

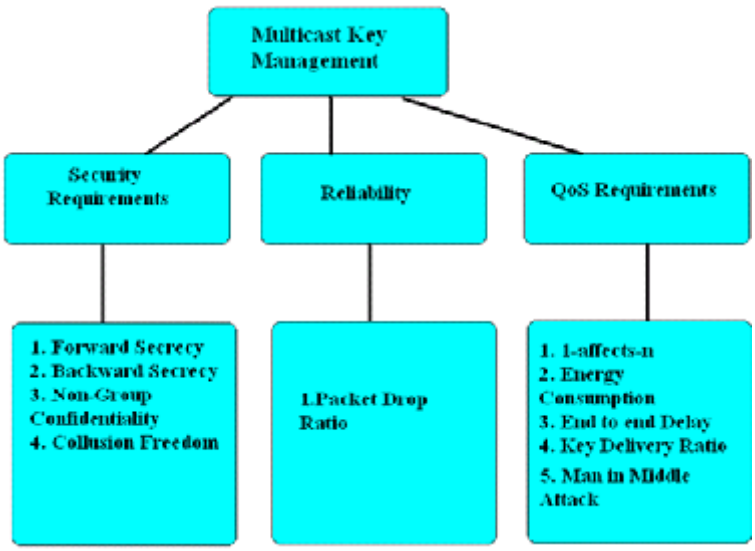

Fig.1: Multicast Key Management Requirements

overhead where 'n' is the number of the remaining group members. Secure Lock [15] also achieves excellent results for storage and communication overheads on both, members and the key server. However, these results are achieved by increasing the computation overhead at the key server due to the Chinese Remainder calculations. But this approach have problem of "1 affects n". The ad hoc network is created for the purpose of where wired network is not reached or communication is established only for particular reason so the movement of node is more in such network and so need to face many problems

Distributed key concurrence protocols do not rely on a group leader or key server which has an advantage over those with a group leader because, without a leader, all members are worked equally and if one or more members fail to complete the protocol, it will not affect the whole group. In the protocols with a group leader, a leader failure is fatal for creating the group key and the operation has to be restarted from scratch. The "1 affects n" phenomenon is not considered, because in distributed protocols all the members are contributors in the creation of the group key and hence all of them should commit to the new key whenever a membership change occurs in the group. In this approaches require algorithm which can generate infinite number of key and just because of number of transmission from every node in group need more energy is consumed.

The decentralized approach divides the multicast group into subgroups; each sub-group is directed by an LC (Local Controller work as server) responsible for security management of nodes in its subgroup. Two kinds of decentralized protocols are distinguished as static clustering and dynamic clustering. Two types of protocols create this approach. The first type uses a local traffic encryption key (TEK) within each cluster, distributed to its local members. When receiving a multicast flow, local controllers must decrypt it with the appropriate key, re-encrypt it with the local TEK of their cluster. The second type uses only one traffic encryption key (TEK) for all group members. The source of the group uses the TEK to encrypt multicast data, and the group members to decrypt it. The challenge of such protocols is to send the traffic encryption key to all members of each cluster, securely and in time [6, 7, 8 and 4]. If uses second set of decentralized approach then ultimate it will work as distributed approach.

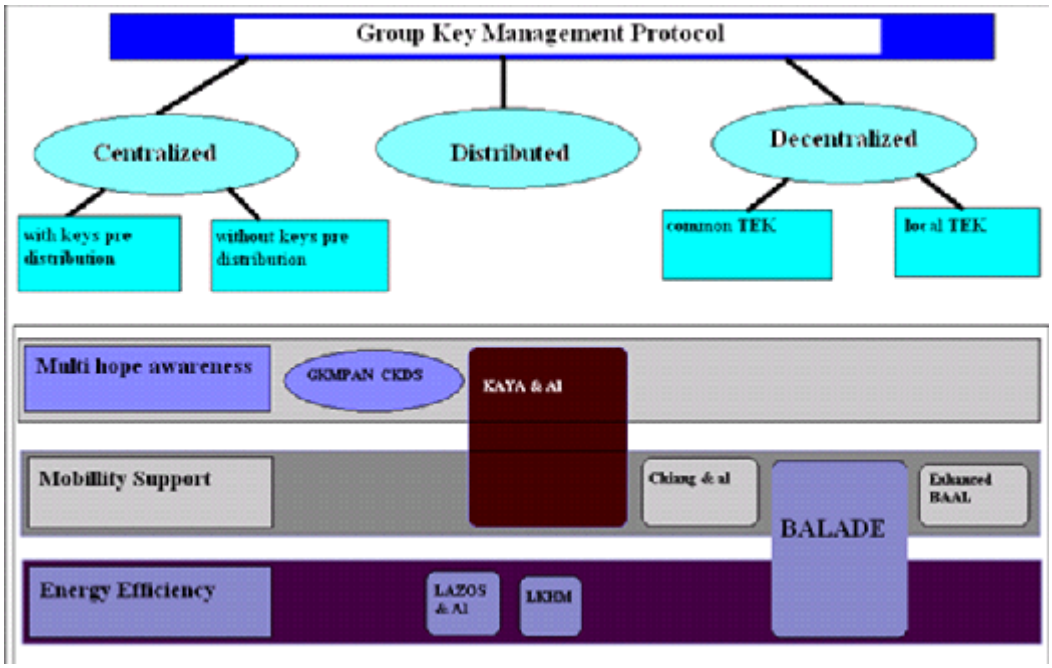

Fig. 2: Existing key management Approaches

In static clustering approach, the multicast group is initially divided into several subgroups. Each group managed by Local Controller (LC). Example: IOLUS [19] belongs to the categories, which are more scalable than centralized protocol. Here Local Controller is responsible of security of all members in group. Dynamic clustering approach aims to solve the "1 affect n" phenomenon. This approach starts a multicast session with centralized key management and divides the group dynamically. Example: AKMP (Adaptive Key Management Protocol) [6], SAKM [13] belong to this approach and are dedicated to wired networks. Enhanced BAAL [8] and OMCT [3, 4, 9, and 10] propose dynamic clustering scheme for multicast key distribution in Ad hoc networks.

OMCT (Optimized Multicast Cluster Tree) is a dynamic clustering algorithm for multicast key distribution dedicated to operate in Mobile Ad hoc networks. This scheme optimizes energy consumption and latency for key delivery. First it elects the local controllers (LC) of the created clusters. OMCT needs the geographical location information of all group members from GPS in the construction of the key distribution tree.

Based on the literature reviewed, Optimized Multicast Cluster Tree (OMCT) is the efficient dynamic clustering approach for secure multicast distribution in Mobile Ad hoc Networks. To enhance its efficiency, it is necessary to overcome the above criteria, as OMCT needs geographical location information in the construction of key distribution tree by reflecting true connectivity between nodes.

To overcome the above limitations another method called Optimized Multicast Cluster Tree with Multipoint Relays (OMCT with MPR)[4] is introduced which uses the information of Optimized Link State Routing Protocol (OLSR) to elect the LCs of the created clusters. OMCT with MPRs assumes that routing control messages have been exchanged before the key distribution. It does not acknowledge the transmission and results in retransmission which consumes more energy and unreliable key distribution due to high packet drop ratio for Mobile Ad hoc Networks.

Limitation of omptimised multicast tree (OMCT)

The major limitations of existing OMCT multicast key distribution approach is as follows.

- Needs geographical location information
- Election of local controllers is based on GPS
- Does not reflect true connectivity between nodes, because each node has ability to move freely and organize by themselves.
- It does not acknowledge the transmission
- Results in retransmission Consumes more energy and delay
- Results in unreliable key distribution
  High packet drop ratio

Moreover, few solutions for multicast clustering such as dynamic clustering provide the QoS requirements to gain an efficient key distribution process in Ad hoc environments.

Future work to overcome limitation of OMCT

As the nodes are dynamic in nature, ensuring effective routing is one of the major challenges for MANET. Destination Sequenced Distance Vector (DSDV) [21] is a table driven proactive routing protocol designed for Mobile Ad hoc Networks. This protocol maintains routing table as a permanent storage. Routes are maintained through periodical and event trigger exchanges the routing table as the nodes join and leave. Route selection is based on optimization of distance vector. It avoids routing loops and each node has a unique sequence number which updates periodically. It is mainly used for intra cluster routing. It allows fast reaction to topology changes. Improvement of DSDV (IDSDV) [16], improves the delivery ratio of Destination-Sequenced Distance Vector (DSDV) routing protocol in Mobile Ad hoc Networks with high mobility

In Ad hoc networks, the nodes move to different location with different topology. Almost all well-known routing protocols are shown to perform poorly for a network where the topology is changing at random. This mobility characterization research is attempting to quantify the randomness in the mobility of the nodes [17, 18]. Most of the research in this area of mobility characterization has however been towards mobility characterization of individual nodes [23].

The IMPORTANT framework [5] characterizes movement based on spatial dependence, relative speed, and other factors and illustrates how these metrics impact unicast routing performance. In [22], the authors have shown that the mobility model used can significantly impact the performance of Ad hoc routing protocols, including the packet delivery ratio, the control overhead and the data packet delay. In many multicast interactions, due to its frequent membership dynamism, it causes node failure, link failure, and power failure. Node failure may cause faults in communication and delay in multicast transmission.

CONCLUSION

The limitations of OMCT point to find out the other approach which can over the problems. The DSDV with some extra functionality definitely give good result than the result given by only OMCT for key management. The DSDV is table driven protocol in which all the detail is maintained about the distribution process like who leave or join the group, which route is used, etc. It uses message exchange scheme for its invalid route reconstruction and has multicast connectivity between nodes. So we can say that if we combine the features of OMCT with DSDV then the secure key management in MANETs network is achieved easily.

REFERENCES

1. L. Lazos and R. Poovendram, "Energy-aware secure multicast communication in Ad Hoc networks using geographical location information," in IEEE Inter-national Conference on Acoustics Speech and Signal Processing, pp. 201-204, 2003.
2. J. E. Wieselthier, G. D. Nguyen, and A. Ephremides, "On the construction of energy-efficient broadcast and multicast trees in wireless.
3. D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," Proc. ACM Mobicom *'94, Dec*. 1994.
4. L. Buttyan, J.P. Hubaux, Report on a working session on security in wireless ad hoc networks, *Mobile Computing and Communications Review* **6** (4) (2002).
5. M. Weiser, the Computer for the Twenty-First Century, Scientiûc American, 1991.
6. Wireless World Research Forum (WWRF): http:// www.ist-wsi.org.
7. James A. Freebersyser, Barry Leiner, A DoD perspective on mobile ad hoc networks, in: Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.
8. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," Proc*. ACM SIGCOMM '***94***,* (1994).
9. S. Giordano, A. Urpi, Self-organized and cooperative ad hoc networking, in: S. Basagni, M.Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.
10. P. Michiardi, R. Molva, Simulation-based analysis of security exposures in mobile ad hoc networks, in: Proceedings of European Wireless Conference, 2002.
11. Elizabeth Belding-Royer, Routing approaches in mobile ad hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York, 2003.
12. Yih-Chun Hu, David B. Johnson, Adrian Perrig, SEAD: secure eûcient distance vector routing for mobile wireless ad hoc networks, in: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCS A 02), New York, June 2002.
13. J.Lundberg, Routing Security in Ad Hoc Networks, 2000. Available from http:// citeseer.nj.nec.com/ 400961.html.
14. A. Perrig, Y. C. Hu, and D. B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks," *Technical Report TR01-384, Department of Computer Science, Rice University*, December 2001.
15. S. Jiang, N. Vaidya, and Wei Zhao, "Prevent Traffic Analysis in Packet Radio Networks,"

in *Proceedings of DISCEX II,* June 2001.

16. M. Bouassida, I. Chrisment, and O. Festor "Efficient group key management protocol in MANETs using multipoint relaying technique", *Proc.IEEE International Conference on Networking*, pp 64, Apr. 2006.
17. A.Boukerche, "Performance Evaluation of Routing Protocols for Ad hoc wireless Networks". *Mobile Networks and Applications* 9, Netherlands, pp. 333-342, 2004
18. Brian P. Crow, Indra Widjaja, Jeon Geun Kim and Prescott T. Sakai, " IEEE 802.11 Wireless Local Area Network," *IEEE Communication Magazine*, **35**(9), 116-126, September 1997.
19. Y. Challal, H. Bettahar, and A. Bouabdallah, "SAKM: A Scalable and Adaptive Key Management Approach for Multicast Communications", *ACM SIGCOMM Computer Communication* Review, pp 55-70, April 2004.
20. G.H. Chiou and W. T. Chen. "Secure Broadcast using Secure Lock", *IEEE Transactions on Software Engineering*, vol 15, Issue 8 , pp 929 - 934 ISSN: 0098-5589 August 1989.
21. Y. Lu, W. Wang, Y. Zhong, and B. Bhargava, "Study of distance vector routing protocols for mobile ad hoc networks", in *PERCOM '03: Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*. IEEE Computer Society, 2003, pp. 187-194.
22. Arun Kumar B. R., Lokanatha C. Reddy, Prakash.S.Hiremath, " A Survey of Mobile Ad Hoc Network Routing Protocols" *Journal of Intelligent System Research*, 1(1) pp. 49-64, *Serials Publications*, New Delhi, 2008.
23. M. Bouassida, I. Chrisment, and O. Festor, "Efficient Clustering for Multicast Key Distribution in MANETs", *LCNS* 3462, pp 138-153, May 2005.