International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:3, No:8, 2009

A Reliable Secure Multicast Key Distribution Scheme for Mobile Adhoc Networks

D. SuganyaDevi, and G. Padmavathi

***Abstract*—**Reliable secure multicast communication in mobile adhoc networks is challenging due to its inherent characteristics of infrastructure-less architecture with lack of central authority, high packet loss rates and limited resources such as bandwidth, time and power. Many emerging commercial and military applications require secure multicast communication in adhoc environments. Hence key management is the fundamental challenge in achieving reliable secure communication using multicast key distribution for mobile adhoc networks. Thus in designing a reliable multicast key distribution scheme, reliability and congestion control over throughput are essential components. This paper proposes and evaluates the performance of an enhanced optimized multicast cluster tree algorithm with destination sequenced distance vector routing protocol to provide reliable multicast key distribution. Simulation results in NS2 accurately predict the performance of proposed scheme in terms of key delivery ratio and packet loss rate under varying network conditions. This proposed scheme achieves reliability, while exhibiting low packet loss rate with high key delivery ratio compared with the existing scheme.

***Keywords*—**Key Distribution, Mobile Adhoc Network, Multicast and Reliability.

I. Introduction

A MANET (Mobile Adhoc Network) is a collection of autonomous mobile nodes that offers infrastructure-free communication over a shared wireless medium. It is formed spontaneously without any preplanning. Multicasting is a fundamental communication paradigm for group-oriented applications such as secure conferencing, visual broadcasts, military command and control, discussion forums, frequent stock updates, pay per view programs, and advertising.

The combination of an adhoc environment with multicast services introduces new challenges towards the security infrastructure to enable acceptance and wide deployment of multicast communication in mobile adhoc environment. [1, 2, 3].

In order to secure multicast communication, security services such as authentication, data integrity, access control and group confidentiality are required [4]. Among which group confidentiality is the most important service for several applications like military and fire brigades. These security services can be facilitated if group members share a common secret, which in turn makes key management a fundamental challenge in designing secure multicast and reliable group communication systems. The Key management includes creating, distributing and updating the keys then it constitutes a basic block for secure group communication applications [5, 6]. One of the primary objectives of any key management scheme is the secure distribution of keying material.

Most of the security services rely generally on encryption using Traffic Encryption Keys (TEKs) and re-encryption is using Key Encryption Keys (KEKs) [7]. 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 above requirements. The process of updating the keys and distributing them to the group members is called rekeying operation [8]. Rekeying is required in secure multicast communication to ensure that a new member cannot decrypt the stored multicast data (before its joining) and prevents a leaving member from eavesdropping future multicast data.

A critical problem with any rekey technique in multicast key distribution is unreliability with high packet loss rates due to frequent node mobility. The rekey process should be done after each membership change, and if the membership changes are frequent, key distribution will require a large number of key exchanges per unit time in order to maintain both forward and backward secrecies. The number of TEK update messages in the case of frequent join and leave operations induces high packet loss rates and reduces key delivery ratio which makes unreliable.

To overcome this problem, several key distribution approaches propose a multicast clustering. [9, 10, 11] Clustering is dividing the group into several sub-groups. An entity called Local controller (LC) manages each subgroup, which is responsible for local key management within the cluster. Thus, after Join or Leave procedures, only members within the concerned cluster are affected by rekeying process, and the local membership dynamism of a cluster does not affect the other clusters of the group.

This paper proposes an enhanced algorithm which combines OMCT (Optimized Multicast Cluster Tree) with DSDV (Destination Sequenced Distance Vector) routing protocol for efficient multicast key distribution in mobile adhoc networks.

Several methods applied in this paper are as follows:

1) DSDV (Destination Sequenced Distance Vector) [12] routing protocol to maintain routing table periodically and event-triggered exchanges the routing table for electing the cluster head and distributing the keys when a node

D. SuganyaDevi is with SNR SONS College (Autonomous), Coimbatore – 641006, Tamil Nadu, India (phone: 098948 95359; e-mail: sugan.devi1@gmail.com).

G. Padmavathi is with Avinashilingam University for Women, Coimbatore-641043, Tamil Nadu, India (e-mail: mail_padma@gmail.com).

joins and leaves. It sends acknowledgement for each transmission in order to reduce the retransmission.
2) MAC 802.11 for providing communication between nodes.
3) Channel bandwidth for minimization of congestion that occurs during transmission.
4) Congestion control mechanism to control flooding message.

The main objective of the paper is design a reliable secure multicast key distribution with proposed enhanced OMCT clustering algorithm with DSDV for mobile adhoc network.

The simulation results in NS2 show that this proposed scheme achieves reliability, while exhibiting low packet loss rate with high key delivery ratio compared with the existing scheme under varying network conditions.

The remainder of this paper is structured as follows. Section II presents the related works about multicast key distribution. Section III describes the proposed enhanced algorithm of OMCT with DSDV for efficient multicast key distribution. Section IV presents the analysis of numerical and simulation results for the proposed scheme. Section V concludes the paper.

II. Related Work

Several Clustering approaches [9, 10 and 11] for securing multicast key distribution in ad hoc networks have been proposed. They are basically classified into two main approaches. They are static clustering and dynamic clustering as shown in Fig. 1.

In Static clustering approach, the multicast group is initially divided into several subgroups. Each subgroup shares a local session key managed by Local Controller (LC). Example: IOLUS [13] and DEP [9] belong to the category.

Dynamic clustering approach aims to solve the “1 affect n” phenomenon. AKMP [10] and SAKM [14] belong to this approach and they are dedicated to wired networks. Enhanced BAAL [10] proposes dynamic clustering scheme for multicast key distribution in adhoc networks.

One approach to distribute group key on multicast environments based on clusters is the Optimized Multicast Cluster Tree (OMCT) [15, 16]. It is a dynamic clustering scheme for multicast key distribution dedicated to operate in ad hoc networks. Its main idea is to elect the LCs of the created clusters.

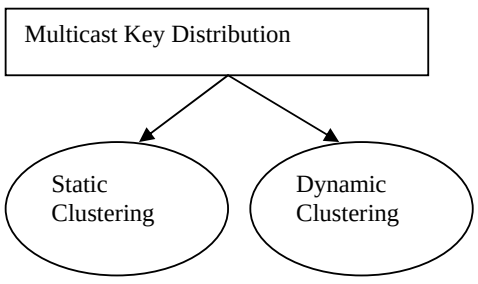

Fig. 1 Classification of multicast key distribution Approaches

OMCT needs the geographical location information of all group members in the construction of the key distribution tree, which does not reflect the true connectivity between nodes. Based on the literature reviewed, OMCT is the efficient dynamic clustering approach for secure multicast distribution in mobile adhoc networks. However knowing the true connectivity between the nodes in mobile adhoc networks simplifies the key distribution phenomenon due to the node mobility. Hence the true node connectivity is taken into consideration for the cluster formation.

To overcome the above limitations another method called Optimized Multicast Cluster Tree with Multipoint Relays (OMCT with MPR) [17] 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 hence results in unreliable key distribution due to high packet loss rate in mobile adhoc networks.

Destination Sequenced Distance Vector (DSDV) [12] 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 periodically and event triggered exchanges the routing table as the node 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. It sends acknowledgement for each transmission in order to reduce the retransmission. Hence it reduces packet loss rate and increases high key delivery ratio in multicast key distribution which is the main issue of mobile adhoc networks. Therefore the existing OMCT algorithm is enhanced by integrating OMCT with DSDV routing protocol. The LCs are elected easily using periodic updates of node join and leave information. The Enhanced OMCT algorithm simulated with network simulator NS-allinone-2.33 and the performance is studied using the metrics namely packet loss rate and key delivery ratio in multicast key distribution.

III. Enhanced OMCT with DSDV

The main idea of Enhanced OMCT is to use DSDV routing protocol to elect the local controllers of the created clusters. The principle of this clustering scheme is to start with the group source Group Controller (GC), to collect its 1-hop neighbors by DSDV, and to elect LCs which are group members have child nodes at the next level. The LC belongs to the unicast path between the source and the child group members.

At this step, the elected LCs covers the group members having 2-hops neighbors of the group source. This scheme iterates until LCs cover all the group members.

The multicast tree is thus constructed using enhanced OMCT with DSDV is shown in Fig. 2.

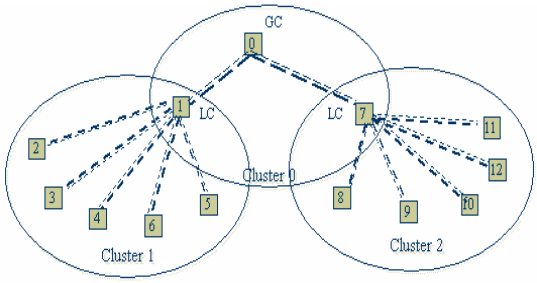

Fig. 2 Enhanced OMCT with DSDV

A. Enhanced OMCT with DSDV Algorithm

The Enhanced OMCT clustering approach is described as follows:

Algorithm 1 Enhanced OMCT_with_DSDV (Cluster head)
//STEP 1
ListLCs = Cluster Head
Listnodes = {1, 2, 3... c} //c is the number of cluster members
//STEP 2
for (i = 1 to List nodes) **do**
if (Listnodes ≠ ϕ) **then**
if (i multicast group) && (i has group members Childs) **then**
ListLCs = ListLCs ∪ {i};
// Add i to the local controllers list
Listnodes = Listnodes / {group members covered by i};
// Remove members covered by i of the members list
OMCT_with_DSDV (i);
// Execute recursively the algorithm applied to i
end if
end if
end for
//STEP 3
if (Listnodes ≠ ϕ) then
for (j = 1 to Listnodesnumber) do
Compute the reachability factor of j: number of members in List nodes, in 1-hop from the node
end for
while (List nodes = i) **do**
// Group of child nodes provide reachability factor
ListLCs = Listnodes {i}; // LC joins the new member lists
ListLCs ≠ Listnodes {i};
// Remove from the members list
end while
end if

B. Key Distribution Scheme

The proposed scheme is to achieve reliable multicast key distribution for mobile adhoc networks. In this proposed scheme, the source encrypts multicast data with the TEK, and then sends it to all the members of the group following the multicast tree. The TEK distribution is achieved in parallel, according to the following steps.

Initially, the entire group members receive from the source by unicast the session key KEK_{csg-0} (key encryption key of the sub-group 0), encrypted with their respective public keys. New clusters will then be created dynamically.

The local controllers form a multicast group GLC (Group of Local Controllers), and share a key called KEK_{ccl}. Each local controller should join this group. The local controllers decrypt this message, extract the TEK, re encrypt it with their respective clusters keys and send it to all their local members. To send the TEK to all the group members, the source encrypts it with KEK_{csg-0} and sends it to all the members of its sub-group as shown in Fig. 3.

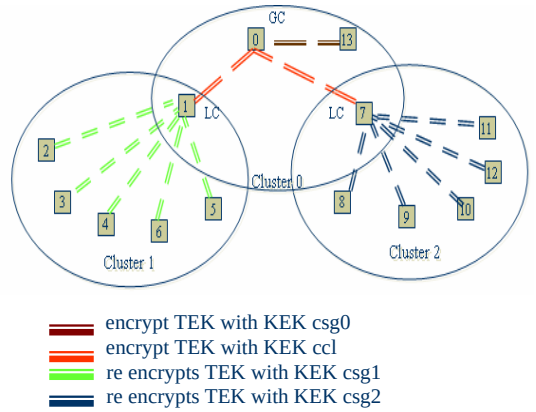

Fig. 3 Multicast key distributions

In the example shown in Fig. 3, the group source GC 0 collects its 1-hop neighbors by DSDV, and elects node 1 and 7 as LCs, which are group members and which have child group members as 2, 3,4,5,6 and 8, 9,10,11,12 respectively. According to the step 3 in the algorithm, if a new member 13 joins the group, based on the connectivity information using DSDV, this node is attached to a particular cluster 0. If the created clusters do not cover group members then the node is selected as local controller for the remaining group members. The major advantage of this solution is to minimize the overhead of decryption and re-encryption process for the local controllers. Hence local controller should only to decrypt and re-encrypt the TEK and not all the multicast flow which in turn makes the multicast key distribution as reliable one.

IV. Analysis of Results

This proposed scheme focuses on the analysis of key distribution scheme. It also evaluates its performance in terms of key delivery ratio and packet loss rate under varying network conditions.

The numeric evaluation of the metrics is as follows.

1) Key Delivery Ratio (KDR): is defined as the number of received keys divided by number of sent keys. This

metrics allows evaluating the reliability of the protocol in term of key transmission from the source to the group members.

$$KDR = \frac{\text{Number of received keys}}{\text{Number of sent keys}}$$

.

2) Packet Loss Rate (PDR): is obtained as subtracting number of packets received at the destination from number of packets send to destination. This metrics allows in evaluating the reliability of the protocol in term of packet loss rate in key transmission from the source to the group members.

PDR = No. of packets sent to destination - No. of packets received at the destination

This section presents analysis of numerical results which are used to compare the performance of Enhanced OMCT with DSDV and OMCT with MPR in varying density of cluster and network surface. The results are obtained in three different network surfaces as 1000*1000, 1500*1500 and 2000*2000 and also with different density of group members as 7, 13 and 28.

The numeric results of both the parameters are given in Table I.

The proposed Enhanced OMCT is approach is also simulated under Linux Fedora, using the network simulator NS2 version ns-allinone-2.33.

The following are the parameters considered.

- The density of group members within the ad hoc network: group members number (7 - 13 - 28)
- Network surface (1000m*1000m, 1500m*1500m, 2000m *2000m).
- The mobility scenarios are generated by the automatic generator *setdest* provided by NS2
- The maximal speed of members is defined at 10km/h (2.77m/sec),
- The pause time is 20 seconds
- The simulation duration is 200 seconds.
- Physical/Mac layer: IEEE 802.11.
- Mobility model: random waypoint model [20] with pause time equal to 20 sec and with maximum nodes movement speed equal to 3 m/s.
- Routing protocol: DSDV

Traffic: only unicast distribution keys traffic exists in the simulation. The source of the group sends the TEK to the LCs, which is forwarded to the local members.

The simulation results are tabulated and shown in Table II.

TABLE I
NUMERICAL RESULTS

Surface	No. of Nodes	Enhanced OMCT with DSDV					OMCT with MPR				
		No. of Packets received	No. of Packets sent	No. of Packet loss	KDR (%)	PDR (%)	No. of Packets received	No. of Packets sent	No. of Packet loss	KDR (%)	PDR (%)
1000*1000	7	5109	6091	982	90	7	3200	5700	2500	60	40
	13	5464	5976	564	96	4	3221	5741	2520	60	40
	28	5464	6028	564	96	4	3801	5602	1801	72	28
1500*1500	7	5305	5787	482	95	5	3245	5805	2560	63	37
	13	5389	5951	562	96	4	3751	8002	4251	69	31
	28	5650	6055	405	97	3	3915	5731	1816	72	28
2000*2000	7	5464	6026	562	96	4	3245	5746	2501	63	37
	13	5452	6016	561	96	4	3954	4977	1023	70	30
	28	5461	6023	562	96	4	3961	5187	1126	72	28

TABLE II
SIMULATION RESULTS

Surface	Nodes	Key Delivery Ratio (%)		Packet Loss Rate (%)	
		OMCT with DSDV	OMCT with MPR	OMCT with DSDV	OMCT with MPR
1000 * 1000	7	93	60	7	40
	13	96	60	4	40
	28	96	72	4	28
1500 * 1500	7	95	63	5	37
	13	96	69	4	31
	28	97	72	3	28
2000 * 2000	7	96	63	4	37
	13	96	70	4	30
	28	96	72	4	28

From the above two comparison tables, it can be observed that Enhanced OMCT gives better performance and achieves reliability in terms of key delivery ratio and packet loss rate compared to the OMCT with MPR algorithm under varying network conditions.

The simulation results are also shown in Fig. 4a and Fig. 4b.

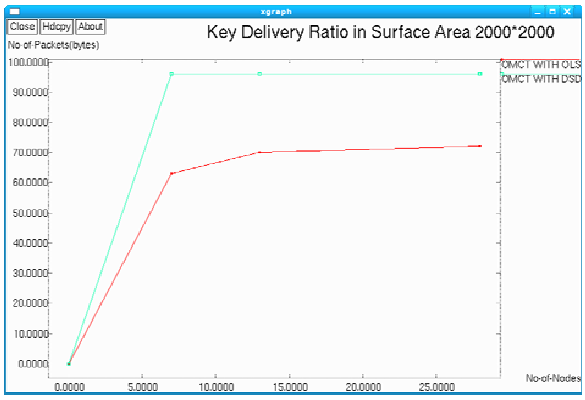

Fig. 4a Key delivery ratio in multicast key distributions

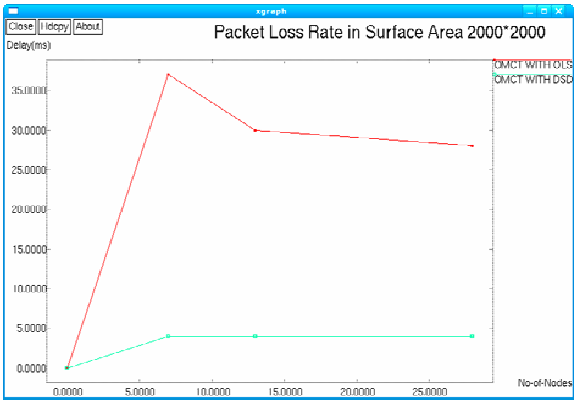

Fig. 4b Packet loss rate in multicast key distributions

V. CONCLUSION

Reliable Secure multicast communication is a significant requirement in emerging applications in adhoc environments like military or public emergency network applications. Membership dynamism is a major challenge in providing complete security in such networks. Some of the existing algorithms like OMCT address the critical problems using clustering approach. However the major challenges in mobile adhoc networks include high packet loss rate which is not attempted in OMCT with MPR and hence results in unreliable key distribution. Therefore an attempt is made to improve the reliability by reducing packet loss rate and increasing key delivery ratio using an algorithm called Enhanced OMCT with DSDV. This algorithm uses DSDV routing protocol for electing LCs. The proposed Enhanced OMCT is tested and the entire experiments are conducted in a simulation environment using network simulator NS2. The results are formed to be desirable and the proposed method is reliable and more suitable for secure multicast key distribution dedicated to operate in MANETs.

REFERENCES

[1] T. Chiang and Y. Huang, "Group keys and the multicast security in ad hoc networks", Proc. IEEE International Conference on Parallel Processing, IEEE press, pp 385-390, Oct 2003.
[2] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks". Proc. 1st ACM workshop on security of ad hoc and sensor networks, ACM Press, pp 94-102.2003.
[3] L. Lazos and R. Poovendram, "Energy-Aware Secure Multicast Communication in Ad Hoc Networks Using Geographical Location Information". Proc.IEEE International Conference on Acoustics Speech and Signal Processing, pp 201-204, Apr 2003.
[4] H. Bettahar, A. Bouabdallah, and M. Alkubeily, "Efficient Key Management Scheme for Secure Application level", IEEE sym. On Computers and Communications, pp 489-497, July 2007.
[5] G.Valle, R.Cardenas, "Overview the Key Management in Adhoc Networks", LCNS 3563, pp 397-406, Aug 2005.
[6] D.Huang, D.Medhi, "A Secure Group Key Management scheme for Hierarchical Mobile Adhoc Networks", Adhoc Networks, pp 560-577, June 2008.
[7] B.Kim, H.Cho, J. Lee, "Efficient Key Distribution Protocol for secure Multicast Communication", LCNS 3043, pp 1007-1016, Apr 2004.
[8] Y. Challal, H. Seba, "Group Key Management Protocols: A novel Taxonomy", International Journal of Information Technology pp 105-118, 2005.
[9] L. Dondeti, S. Mukherjee, and A. Samal, "Secure one-to many group communication sing dual encryption", IEEE sym. On Computers and Communications, pp 1-25, Jul 1999.
[10] H. Bettahar, A. Bouabdallah, and Y. Challal, "An adaptive key management protocol for secure multicast", Proc.IEEE International Conference on Computer Communications and Networks, pp 190-195, Oct 2002.
[11] M. Bouassida, I. Chrisment, and O. Festor, "An Enhanced Hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks". LCNS 3042, pp 725-742, Apr 2004.
[12] K.Rahman, R.Zaman, A.Reddy, " An Efficient DSDV routing Protocol for Wireless Mobile Adhoc Networks and its Performance Comparison", Proc. European Sym. On Computer Modeling and Simulation, pp 508-511, Nov 2008.
[13] S. Mittra, "Iolus: A framework for scalable secure multicasting", SIGCOMM, pages 277–288, 1997.
[14] 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.

[15] M. Bouassida, I. Chrisment, and O. Festor, "Efficient Clustering for Multicast Key Distribution in MANETs", LCNS 3462, pp 138-153, May 2005.
[16] M. Bouassida, I. Chrisment, and O. Festor, "Group Key Management in Manets", International Journal of Network Security, pp 67-79, Jan 2008.
[17] 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.

D. Suganya Devi received her B.Sc (Chemistry) and MCA from PSGR Krishnammal College for Women, Coimbatore in 1996 and 1999 respectively. And, she received her M.Phil degree in Computer Science in the year of 2003 from Manonmaniam Sundaranar University, Thirunelveli. She is pursuing her PhD at Avinashilingam University for Women. She is currently working as a Senior Lecturer in the Department of computer Applications, SNR Sons College, Coimbatore. She has 10 years of teaching experience. She has presented 10 papers in various national and international conferences. Her research interests Multicast Communication, MANET and Network Security.

Padmavathi Ganapathi is the professor and head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 21 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 60 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.