

Dynamic Clustering for QoS based Secure Multicast Key Distribution in Mobile Ad Hoc Networks

Suganyadevi Devaraju[1], Padmavathi Ganapathi[2]

**[1] Department of Computer Applications,
SNR SONS College (Autonomous)
Coimbatore, Tamil Nadu , India**

**[2] Department of Computer Science,
Avinashilingam Deemed University ,
Coimbatore, Tamil Nadu , India**

Abstract

Many emerging applications in mobile ad hoc networks involve group-oriented communication. Multicast is an efficient way of supporting group oriented applications, mainly in mobile environment with limited bandwidth and limited power. For using such applications in an adversarial environment as military, it is necessary to provide secure multicast communication. Key management is the fundamental challenge in designing secure multicast communications. Multicast key distribution has to overcome the challenging element of "1 affects n" phenomenon. To overcome this problem, multicast group clustering is the best solution. This paper proposes an efficient dynamic clustering approach for QoS based secure multicast key distribution in mobile ad hoc networks. Simulation results shows the demonstration of Dynamic clustering approach have better system performance in terms of QoS performance metrics such as end to end delay, energy consumption, key delivery ratio and packet loss rate under varying network conditions.

Keywords: *Mobile Ad hoc Networks, Multicast, Secure Multicast Communication, QOS Metrics.*

1. Introduction

A MANET (Mobile Ad Hoc Network) is an autonomous collection of mobile users that offers infrastructure-free architecture for communication over a shared wireless medium. It is formed spontaneously without any preplanning. Multicasting is a fundamental communication paradigm for group-oriented communications such as video conferencing, discussion forums, frequent stock updates, video on demand (VoD), pay per view programs, and advertising. The combination of an ad hoc environment with multicast services [1, 2, 3] induces new challenges towards the security infrastructure. In order to secure multicast communication, security services such as authentication, data integrity, access control and group confidentiality are required. Among which group confidentiality is the most important service for several applications [4]. These security services can be facilitated if group members share a common secret, which in turn makes key management [5, 6] a fundamental challenge in designing secure multicast and reliable group communication systems. Group confidentiality requires that only valid users could decrypt the multicast data.

Most of these security services rely generally on encryption using Traffic Encryption Keys (TEKs) and re-encryption uses Key Encryption Keys (KEKs) [7]. The Key management includes creating, distributing and updating the keys then it constitutes a basic block for secure multicast communication applications. 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 [8]. Figure 1 summarizes these requirements.

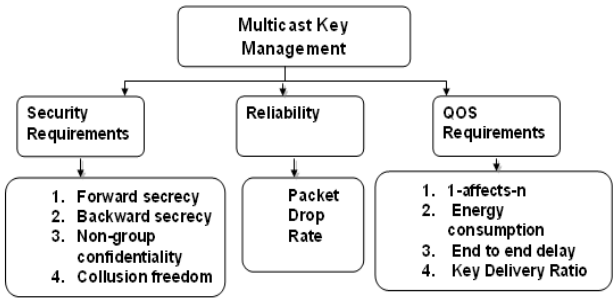

Figure 1. Multicast Key Management Requirements

Security requirements:
Forward secrecy: In this case, users left the group should not have access to any future key. This ensures that a member cannot decrypt data after it leaves the group.
Backward secrecy: A new user who joins the session should not have access to any old key. This ensures that a member cannot decrypt data sent before it joins the group.
Non-group confidentiality: 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.
Collusion freedom: Any set of fraudulent users should not be able to deduce the currently used key.

The process of updating the keys and distributing them to the group members is called rekeying operation. A critical problem with any rekey technique is scalability. The rekey process should be done after each membership change, and if the membership changes are frequent, key management 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 several QOS characteristics as follows:

Reliability:
Packet Drop Rate: 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.

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 requires that all group members commit to a new TEK.
Energy consumption: This induces minimization of number of transmissions for forwarding messages 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 minimizes the impact of key distribution on the delay of key delivery.
Key Delivery Ratio: This induces number of successful key transmission to all group members without any loss of packet during multicast key distribution.

Thus a QOS based secure multicast key distribution in mobile ad hoc environment should focus on security, reliability and QOS characteristics.

To overcome these problems, several approaches propose a multicast group clustering [9, 10, 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. 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 did consider the QOS requirements to achieve an efficient key distribution process in ad hoc environments.

This Paper proposes an efficient cluster-based multicast tree (CBMT) algorithm for secure multicast key distribution in mobile ad hoc networks. Thus this new efficient CBMT approach is a dynamic clustering scheme with Mobility Aware Multicast version of Destination Sequenced Distance Vector (Mobility Aware MDSDV) routing protocol, which becomes easy to elect the local controllers of the clusters and updates periodically as the node joins and leaves the cluster.

The main objective of the thesis is to present a new approach of clustering algorithm for efficient multicast key distribution in mobile ad hoc network by overcoming issues of multicast key management requirements. Extensive simulation results in NS2 show the analysis of the CBMT algorithm for multicast key distribution based on the performance of QOS characteristics.

Hence, this proposed scheme overcomes 1-affects-n phenomenon, reduces average latency and energy consumption and achieves reliability, while exhibiting low packet drop 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 2 presents the related works about Key management and multicast clustering approaches. Section 3 describes the proposed the four phases for efficient CBMT for secure multicast key distribution. Section 4 evaluates the performance characteristics of efficient CBMT with simulation environment for the proposed algorithm and discusses the analysis of the simulation results and Finally, Section 5 concludes the paper.

2. Related Work

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

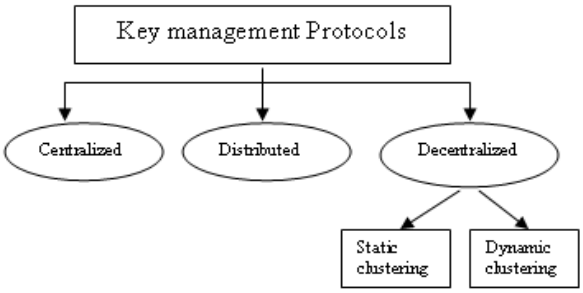

Figure 2: Classification of key management Approaches

2.1 Centralized Approaches

In centralized approaches, 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. Centralized protocols are further classified into three sub-categories namely Pairwise key approach; Secure locks and Hierarchy of keys approach.

Pairwise key approach: In this approach, the key server shared pairwise keys with each participant. For example, in GKMP [12], apart from pairwise keys and the group key, all current group participants know a group key encryption key (gKEK). If a new participant joins the group, the server generates a new group key and a new gKEK. These keys are sent to the new member using the key it shares with key server, and to the old group member using the old gKEK.

Secure Locks: Chiou and Chen [13] proposed Secure Lock; a key management protocol where the key server requires only a single broadcast to establish the group key or to re-key the entire group in case of a leave. This protocol minimizes the number of re-key messages. However, it increases the computation at the server due to the Chinese Remainder calculations before sending each message to the group.

Hierarchy of Keys Approach: Most efficient approach to rekeying in the centralized case is the hierarchy of keys approach. Here, the key server shares keys with subgroups of the participants, in addition to the pair wise keys. Thus, the hierarchical approach trades off storage for number of transmitted messages. The simulations are conducted and the performance is compared for CBMT and OMCT with varying density of cluster and network surface. This comparison is done in terms of end to end delay, energy consumption, key delivery ratio and packet drop ratio.

Logical key hierarchy was proposed independently in [14]. The key server maintains a tree with subgroup keys in the intermediate nodes and the individual keys in the leaves. Apart from the individual keys shared with the key server, each node knows all keys on the path to the root. In root, the group key is stored. As the depth of the balanced binary tree is logarithmical in the number of the leaves, each member stores a logarithmical number of keys, and the number of rekey messages is also logarithmic in the number of group members instead of linear, as in previously described approaches.

One-way function trees (OFT) [15] enables the group members to calculate the new keys based on the previous keys using a one-way function, which further reduces the number of rekey messages. Thus the pair wise key approach exhibits linear complexity. Secure lock, although most efficient in number of messages, poses serious load on the server and can be used only for small groups. All tree-based protocols have logarithmic communication and storage complexity at the members, and linear storage complexity at the key server.

2.2 Distributed Key-Agreement Approaches

With distributed or contributory key-agreement protocols, the group members cooperate to establish a group key. This improves the reliability of the overall system and reduces the bottlenecks in the network in comparison to the centralized approach. The protocols of this category are classified into three sub-categories namely Ring based cooperation, Hierarchical based cooperation and Broadcast based cooperation depending on the virtual topology created by the members for cooperation.

Ring-Based Cooperation: In some protocols, members are organized in a ring. The CLIQUES protocol suite [9] is an example of ring-based cooperation. This protocol arranges group members as (M_1, M_n) and M_n as controller. It specifies a role of the controller that collects contributions of other group members, adds own contribution, and broadcasts information that allows all members to compute the group key.

The choice of the controller depends on the dynamic event and the current structure. In additive events new members are appended to the end of the list CLIQUES do not provide verifiable trust relationship, because no other member can check whether values forwarded by M_i, or the set broadcasted by the controller are correctly built.

Hierarchical Based Cooperation: In the hierarchical GKA protocols, the members are organized according to

some structure. STR protocol [16] uses the linear binary tree for cooperation and provides communication efficient protocols with especially efficient join and merges operations. STR defines the role of the sponsor temporarily and it can be assigned to different members on dynamic events depending on the current tree structure. The sponsor reduces the communication overhead as it performed some operations on behalf of the group. The sponsor is not a central authority. STR provides verifiable trust relationship because every broadcasted public key can be verified by at least one other participant.

Broadcast based Cooperation: Broadcast based protocols have constant number of rounds. For example, in three-round Burmester-Desmedt (BD) protocol [17] each participant broadcasts intermediate values to all other participants in each round. The communication and computational load is shared equally between all parties. This protocol does not provide verifiable trust relationship, since no other group member can verify the correctness of the broadcasted values.

2.3 Decentralized Approaches

The decentralized approach divides the multicast group into subgroups or clusters, each sub-group is managed by a LC (Local Controller) responsible for security management of members and its subgroup. Two kinds of decentralized protocols are distinguished as static clustering and dynamic clustering. In Static clustering approach, the multicast group is initially divided into several subgroups. Each subgroup shares a local session key managed by LC.

Example: IOLUS [18] and DEP [11] belong to the categories, which are more scalable than centralized protocol. 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 [10], SAKM [19] belong to this approach and are dedicated to wired networks. Enhanced BAAL [20] and OMCT [21,22] proposes dynamic clustering scheme for multicast key distribution in ad hoc networks.

OMCT [21,22] (*Optimized Multicast Cluster Tree*) is a dynamic clustering scheme for multicast key distribution dedicated to operate in ad hoc networks. This scheme optimizes energy consumption and latency for key delivery. Its main idea is to elect the local controllers of the created clusters [21,22]. OMCT needs the geographical location information of all group members in the construction of the key distribution tree. Once the clusters are created within the multicast group, the new LC becomes responsible for the local key management and distribution to their local members, and also for the maintenance of the strongly correlated cluster property. The election of local controllers is done according to the localization and GPS (Global Positioning System) information of the group members, 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 ad hoc networks. To enhance its efficiency, it is necessary to overcome the 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) [23] 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 rate for mobile ad hoc networks.

Destination Sequenced Distance Vector (DSDV) [24] 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. Improvement of DSDV (IDSDV) [25, 26], improves the delivery ratio of Destination-Sequenced Distance Vector (DSDV) routing protocol in mobile ad hoc networks with high mobility. It uses message exchange scheme for its invalid route reconstruction but does have multicast connectivity between nodes.

The proposal of this paper is to present a new efficient Cluster Based Multicast Tree (CBMT) using Mobility Aware Multicast version of DSDV for secure multicast key distribution. Mobility aware MDSDV have multicast connectivity between nodes. It sends acknowledgement for each transmission in order to reduce the retransmission. The LCs are elected easily with periodic updates of node join and leave information using multicast

tree. This overcomes the issues of end to end delay, unreliability with high packet drop rate and low key delivery ratio. The efficient CBMT algorithm is simulated with network simulator NS-allinone-2.33 and the performance is studied based on the QOS characteristics in multicast key distribution.

3. Proposed Methodology

The methodology of efficient CBMT is proposed in order to assure reliable QOS based secure multicast key distribution for mobile ad hoc networks. The specific contributions are structured in four Phases.

Phase I : Integration of OMCT with DSDV [27]
- Makes easy election of LC
- Improves key delivery ratio

Phase II : Enhancement of OMCT with DSDV[28]
- Reduces end to end delay
- Consumes less energy

Phase III : CBMT with MDSDV[29]
- Improves reliability
- Reduces packet drop rate

Phase IV: Efficient CBMT
- Improves Key Delivery Ratio
- Consumes Less Energy
- Reduces end to end delay
- Reduces Packet Drop Rate

3.1 Integration of OMCT with DSDV [27]

The main idea of this phase is to integrate OMCT clustering algorithm with 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 GC, to collect its 1-hop neighbors by DSDV, and to elect LCs which are group members and which have child group members (the LC belongs to the unicast path between the source and the child group members).

The selected nodes will be elected as local controllers as shown in figure 3. In the example shown in figure 3, the group source GC 0 collects its 1-hop neighbors by DSDV, and elects LCs node 1 and 7, which are group members and which have child group members as 2, 3,4,5,6 and 8, 9,10,11,12 respectively. The selected nodes will be elected as local controllers.

According to the step 3 in the algorithm, if a new member 13 joins the group then the member do not belong to formed clusters. This approach chooses from these remaining group members the nodes that have the maximum reachability to the others nodes in one hop.

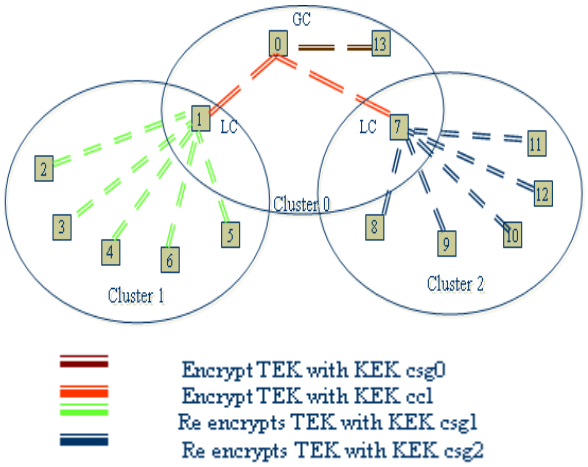

Figure 3. OMCT with DSDV

This reachability information is collected through the DSDV routing protocol, consolidated through OMCT signaling and attached the created cluster. If the created clusters do not cover group members then the node is selected as local controller for the remaining group members. Thus this phase makes easy to elect the local controllers and also increases the key delivery ratio in multicast transmission.

3.2 Enhancement of OMCT with DSDV [28]

The Integration of OMCT with DSDV approach is further enhanced by sending acknowledgement for each transmission using the DSDV routing protocol in order to reduce retransmission. Thus in this phase, it reduces the end to end delay and consumes less energy which makes this approach as an energy efficient.

3.3 Cluster based Multicast Tree with MDSDV [29]

Cluster based multicast tree (CBMT) with MDSDV algorithm is a new reliable version of OMCT with DSDV for secure multicast key distribution in mobile ad hoc networks. It includes key tree engine and forms tree structure based on authentication.

Multicast version of DSDV routing protocol is used to form multicast tree among the group members. Thus this phase proposes a reliable dynamic clustering approach by reducing the packet drop rate and increasing the key delivery ratio.

3.4 Efficient CBMT with Mobility Aware MDSDV

More frequent membership dynamism causes node failure, link failure, power failure which leads to time delay in multicast transmission. Node fails due to movement of

node out of coverage area. Failure of node is easily identified by reachability information of Mobility Aware MDSDV. When a LC fails, it leads to clusterization. Thus this phase proposes an efficient CBMT with Mobility aware MDSDV which improves the performance of QoS metrics.

4. Performance Evaluation and Analysis of Results

The performance of CBMT for multicast key distribution is evaluated in terms of QoS characteristics as metrics and simulated using NS2 version ns-allinone-2.33 [30].

4.1 Performance Metrics

The QOS metrics are namely end to end delay in key distribution, energy consumption, Key delivery ratio and packet drop rate of multicast key distribution.

- **Key Delivery Ratio** is defined as the number of received keys divided by number of sent keys. This metrics allows evaluating the reliability of the protocol in terms of key delivery ratio in key transmission from the source to the group members.
- **Energy Consumption** is defined as the sum of units required to the keys transmission throughout the duration of simulation.
- **End to end Delay:** The average latency or end to end delay of keys transmission from the source to the receivers. This metrics allows evaluating the average delay to forward a key from a LC to its cluster members.
- **Packet Loss Rate:** 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 terms of packet loss rate in key transmission from the source to the group members.

4.2 Simulation Environment

The proposed CBMT using MDSDV is simulated under Linux Fedora, using the network simulator NS2 version ns-allinone-2.33. This simulation environment is defined by the following parameters as shown in table I.

The simulations are conducted and the performance is compared for CBMT and OMCT with varying density of cluster and network surface. This comparison is done in terms of end to end delay, energy consumption, key delivery ratio and packet drop ratio.

Table 1: Simulation Metrics

The density of group members	7, 13, 28 and 50 nodes
Network surface	(1000m*1000m, 1500m*1500m, 2000m *2000m).
The maximal speed	10km/h (2.77m/sec)
The pause time	20 seconds
The simulation duration	200 seconds
Physical/Mac layer	IEEE 802.11
Mobility model	Random waypoint model
Routing protocol	Mobility Aware MDSDV

4.3 Analysis of Simulation Results

This section presents analysis of simulation results to compare the performance of efficient CBMT with Mobility aware MDSDV and CBMT in varying density of nodes and network surface. This simulation results shows that the efficiency is improved by efficient CBMT approach of multicast key distribution in terms of end to end delay of key distribution, energy consumption, key delivery ratio and packet loss rate compared to the OMCT. The simulation results illustrate the comparison of efficient CBMT with Mobility aware MDSDV and OMCT as shown in fig.4a – 4d. Indeed, this approach of CBMT divides the multicast group with the effective connectivity between nodes. It allows fast reaction to topology changes.

Figure 4 a Average End to end Delay

Figure 4a and 4b illustrates that the average delay of key distribution and the energy consumption are better with this approach of efficient CBMT with mobility aware MDSDV than OMCT. This is due to the fact that it sends acknowledgement for each transmission in order to reduce the retransmission. Hence it reduces average end to end

delay and energy consumption of multicast key distribution in efficient CBMT compared to OMCT.

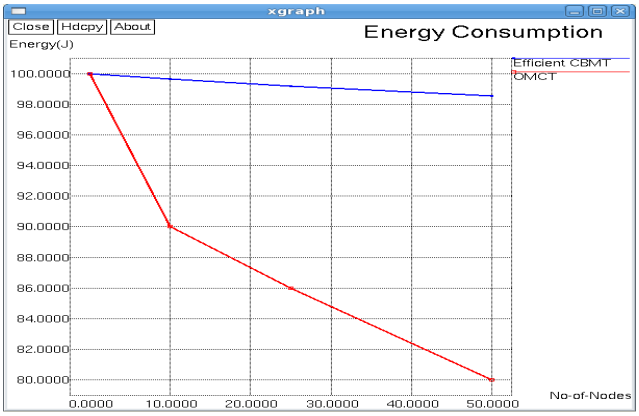

Figure 4 b Energy Consumption

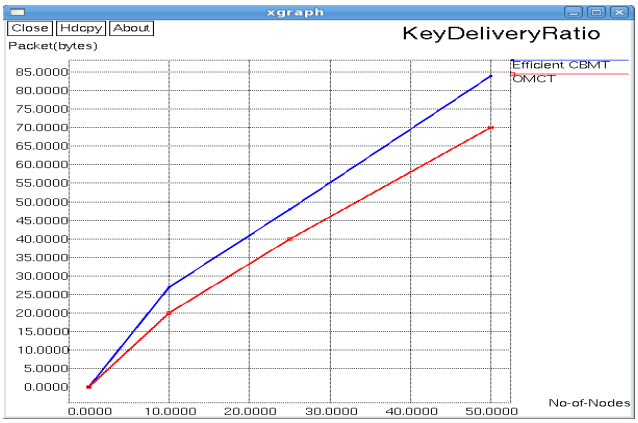

Figure 4 c Key Delivery Ratio

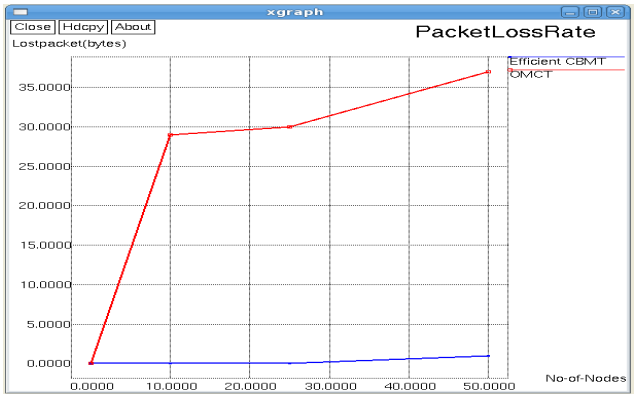

Figure 4 d Packet Loss Rate

From the figure 4c and 4d, it can be observed that Efficient CBMT gives better performance and achieves reliability in terms of key delivery ratio and reduces packet loss rate compared to the OMCT algorithm under varying network conditions.

5. Conclusion

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 like 1-affects-n phenomenon and delay issues. Therefore an attempt is made to improve the performance in terms of QoS metrics as node increases by using an approach of efficient Cluster Based Multicast Tree algorithm for secure multicast communication. This algorithm uses Mobility aware Multicast version of DSDV routing protocol for electing LCs. The proposed efficient CBMT 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 efficient and more suitable for secure multicast communication 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] H. Harney and C. Muckenhirn. Group key management protocol (gkmp) specification. RFC2093, 1997.
[13] G. H. Chiou and W. T. Chen. Secure Broadcast using Secure Lock. IEEE Transactions on Software Engineering, August 1989.
[14] Chung KeiWong, Mohamed Gouda, and Simon S. Lam. Secure group communications using key graphs. IEEE/ACM Trans.2000.
[15] Alan T. Sherman and David A. McGrew. Key establishment in large dynamic groups using one-way function trees. 2003.
[16] Yongdae Kim, Adrian Perrig, and Gene Tsudik. Tree-based group key agreement. ACM Trans. Inf. Syst. Secur., 2004.
[17] Mike Burmester and Yvo Desmedt. A secure and scalable group key exchange system. Information Processing Letters, May 2005.
[18] S. Mittra. Iolus: A framework for scalable secure multicasting. In SIGCOMM, pages 277–288, 1997.
[19] Y. Challal, H. Bettahar, and A. Bouabdallah. SAKM: A Scalable and Adaptive Key Management Approach for Multicast Communications. ACM SIGCOMM, April 2004.
[20] M. Bouassida, I. Chrisment, and O. Festor. An Enhanced Hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks. In Networking 2004, Greece, May 2004.
[21] M. Bouassida, I. Chrisment, and O. Festor. Efficient Clustering for Multicast Key Distribution in MANETs. In Networking 2005, Waterloo, CANADA, May 2005.
[22] M.S. Bouassida, I. Chrisment and O.Feastor. Group Key Management in MANETs, May 2006.
[23] M. Bouassida, I. Chrisment, and O. Festor: Efficient Group Key Management Protocol in MANETs using the Multipoint Relaying Technique. International Conference on Mobile Communications 2006.
[24] http://en.wikipedia.org/wiki/ DestinationSequenced_ Distance_Vector_routing.
[25] T. Liu & K. Liu, Improvement on DSDV in Mobile Ad Hoc Networks, IEEE, China, 2007, pp.1637-1640
[26] A H A Rahman, Z A Zukarnain, “ Performance Comparison of AODV, DSDV and I-DSDV routing protocols in Mobile Adhoc Networks”, European Journal of scientific Research, pp 566-576, 2009.
[27] D.Suganyadevi, G.Padmavathi, “A Reliable Secure Multicast Key Distribution Scheme for Mobile Adhoc Networks”, World Academy of Science, Engineering and Technology, Vol. 56, 2009, pp 321-326.
[28] D.SuganyaDevi., G. Padmavathi, "Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for Mobile Adhoc Networks," in International Conference on Advances in Recent Technologies in Communication and Computing, 2009, pp.934-938.
[29] D.SuganyaDevi., G. Padmavathi, "Cluster Based Multicast Tree for Secure Multicast Key Distribution in Mobile Adhoc Networks," International Journal of Computer Science and Network Security, Vol. 9, No. 9, 2009, pp. 64-69.
[30] The Network Simulator NS-2 tutorial homepage, http://www.isi.edu/nsnam/ns/tutorial/index.html

SuganyaDevi Devaraju 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 an Assistant Professor in the Department of computer Applications, SNR Sons College, Coimbatore. She has 11 years of teaching experience. She has presented 15 papers in various national and international conferences. She has 6 publications in various international journals. Her research interests Multicast Communication, MANET and Network Security.

Dr. Padmavathi Ganapathi is the professor and head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 22 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 120 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.