Energy Efficient CBMT for Secure Multicast Key Distribution in Mobile Ad Hoc Networks

D.Suganyadevi*a, Dr. G.Padmavathi
b

aDepartment of Computer Applications, SNR SONS College, Coimbatore-641006, India
bDepartment of Computer Science, Avinashilingam Deemed University for Women, Coimbatore-641043, India

Abstract

Multicast key distribution in mobile adhoc networks is challenging due to its inherent characteristics of infrastructure-less architecture with lack of central authority and limited resources such as bandwidth, time and power. In many multicast interactions, a new member can join, a current member can leave at any time and existing members must communicate securely using multicast key distribution within constrained energy for mobile adhoc networks. This paper proposes a new efficient cluster based multicast tree (CBMT) algorithm for secure multicast key distribution, in which the source node uses a Multicast version of the Destination Sequenced Distance Vector (MDSDV) routing protocol to consume less energy. It also reduces end to end delay in multicast transmission. Simulation results show the efficient CBMT using MDSDV have better system performance in terms of QOS metrics such as energy, latency, key delivery ratio and packet drop rate under varying network conditions. This proposed scheme achieves reliability, while exhibiting low packet loss rate with high key delivery ratio.

Key words: CBMT, MDSDV, Mobile Adhoc Networks, Secure Multicast Communication.

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 using 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 [8]. Efficient key management protocols should be taken into consideration for miscellaneous requirements.

* Corresponing Author. Tel.: +91-9894895359.
E-mail address: sugan.devi1@gmail.com.
1.1. 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 secrecy. The number of TEK update messages in the case of frequent join and leave operations induces several QOS characteristics as follows:

1.2. 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.

1.3. 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]. 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.

The main objective of the paper is to present a new approach of clustering algorithm for efficient multicast key distribution in mobile adhoc network by overcoming issues of energy and latency and unreliability with high packet drop rate. Extensive simulation results in NS2 show the analysis of the efficient CBMT for secure 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 efficient CBMT for secure multicast communications. Section 4 evaluates the performance and discusses 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 1 illustrates this classification.
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. GKMP [10] 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 induces O(n) rekey message overhead where ‘n’ is the number of the remaining group members. Secure Lock [11] achieves also 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.

Distributed key agreement protocols do not rely on a group leader which has an advantage over those with a group leader because, without a leader, all members are treated 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.

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 [12] belongs to the categories, which are more scalable than centralized protocol. Dynamic clustering approach aims to solve the “1 affects n” phenomenon. This approach starts a multicast session with centralized key management and divides the group dynamically. Example: AKMP [13], SAKM [14] belong to this approach and are dedicated to wired networks. Enhanced BAAL [15] and OMCT [16, 17, 18] propose dynamic clustering scheme for multicast key distribution in adhoc networks.

OMCT (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. 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 adhoc 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. 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 adhoc networks.

Destination Sequenced Distance Vector (DSDV) 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 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) [19, 20], 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 an efficient Cluster Based Multicast Tree (CBMT) using Multicast version of DSDV routing protocol for secure multicast key distribution. 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 energy consumption, end to end delay, unreliability with high packet drop rate and low key delivery ratio.

This is the enhanced version of CBMT algorithm with DSDV which is simulated with network simulator NS-allinone-2.33[21]. Its performance is compared with CBMT based on the QOS characteristics for multicast key distribution.
3. Efficient CBMT With Mobility Aware MDSDV

The proposed approach is to achieve secure multicast communication for mobile adhoc networks. This approach uses Multicast version of DSDV routing protocol to maintain routing table periodically. It forms multicast tree among the group members. Each node can determine their present physical location. It quickly adapts to the topology changes. It is used to discover alternate route for failure of existing route. It also sends acknowledgement for each transmission in order to reduce the retransmission. Thus the approach of CBMT using MDSDV tends to have multicast connectivity between the nodes.

The approach of Efficient CBMT with mobility aware MDSDV is described in five phases as shown in figure 2, with specific notations.

- **Phase 1: Authentication**: For each node, assign certificate key to verify its node identity. Each node has IP address, node address and certificate key. Certificate key and its IP address encrypt to form a public key. Thus, each node is authenticated based on broadcast request and reply.

```
mgk→LCik: Join_Request, Pub_mgk
LCik→mgk: Join_Request
mgk→LCik: Join_Reply, Pub_mgk, {CBID_mgk} Pri_mgk
```

![Figure 2 Flowchart of Efficient CBMT](image-url)
• **Phase 2: Cluster Head Election:** Initially the list of Local Controllers (LCs) contains only the source Group Controller GC. Then, GC collects all its 1 hop neighbors by MDSDV routing protocol. 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). Verify for each one if it is a group member and if it has child group members then add the LC to the list of LCs. Thus, LCs are selected as cluster heads for its corresponding group members.

• **Phase 3: Cluster Formation:** All the members reachable by this new LC will form a new cluster. If group members that exist and do not belong to the formed clusters then choose the nodes that have the maximum reachability to the others nodes in one hop from the remaining members. This reachability information is collected through the MDSDV routing protocol. Thus, nodes are selected as local controllers for the remaining group members and forms new cluster.

• **Phase 4: Secure Multicast Communication:** 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 cluster sub-group 0), encrypted with their respective public keys. 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.

   \[
   \forall mg_k, CGk \rightarrow mg_k : \{\text{TEK}, \text{Num}_\text{Seq}, KEK_{\text{CSG}ik}, \text{IDG}, \text{IDCG}, \text{Pub}_{CG}, \{\text{CBID}_{CG}\} \text{ Pri}_{CG}\} \text{ Pub}_{mg_k}
   \]

• **Phase 5: Node mobility:** For frequent node mobility, a new member may join a group or an existing member may leave a group. To ensure secure multicast communication, both forward and backward secrecy has to be maintained.
  - **Forward Secrecy:** When a node leaves the multicast group, it cannot decrypt the future data. It is known as leave operation. The leave operation is in two cases:
    - When an ordinary node leaves, it gives less effect in multicast transmission. The leave operation of an ordinary node is specified as follows:
      \[
      \text{Leave Procedure} \\
      \text{mg}_{ik}: \text{outgoing member leaving a group} \\
      \text{for } mg_{ik}: \text{Local member,} \\
      \text{mg}_{ik} \neq \text{mg}_{ik\_outgoing} \\
      \text{LC}_{ik} \rightarrow mg_{ik}: \{\text{ID}_{LC}, \text{KEK}_{\text{CSG}ik}\} \text{ Pub}_{mg_{ik}}
      \]
    - When a local controller leaves, it leads to clusterization. It first sends the leave notification to the group controller and then all the members of the current LCs are merged with the other cluster based on the reachability information obtained by the MDSDV routing protocol.
      \[
      \text{Leave Notification} \\
      \text{LC}_{ik} \rightarrow \text{GLC}: \{\text{ID}_{LC_{ik}}\} \text{ KEK}_{\text{CCL}} \\
      \forall j \neq i, \text{ GC}_{k} \rightarrow \text{LC}_{ik}: \{\text{ID}_{GC}, \text{new}_\text{KEK}_{\text{CCL}}\} \text{ Pub}_{CL_{jk}}
      \]
      \[
      \text{Merge} \\
      \forall mg_{ik}, \text{ LC}_{ik}: \{\text{ID}_\text{cluster}, LL_{LC_{ik}}\} \text{ KEK}_{\text{CGG}ik}
      \]
  - **Backward Secrecy:** When a new node joins the multicast group, it cannot decrypt past encrypted data. It is known as Join operation. Each new node joins is authenticated based on broadcast request and reply.
    \[
    \text{Join Procedure} \\
    \text{for old-mg}_{ik}: \text{old member of cluster} \\
    \text{LC}_{ik} \rightarrow \text{old-mg}_{ik}: \{\text{ID}_{LC}, \text{KEK}_{\text{CSG}ik}\} \text{ old}_\text{KEK}_{\text{CSG}ik} \\
    \text{LC}_{ik} \rightarrow mg_{ik}: \{\text{ID}_{LC}, \text{TEK}, \text{KEK}_{\text{CSG}ik}\} \text{ Pub}_{mg_{ik}}
    \]
Thus the approach of an efficient Cluster Based Multicast Tree (CBMT) using mobility aware Multicast version DSDV is described in five phases in order to have secure multicast communication in MANET. This approach overcomes the issues that occur due to node mobility.

4. Performance Evaluation and Analysis of Results

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

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.

- **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.
- **Energy Consumption** is defined as the sum of units required to the keys transmission throughout the duration of simulation.
- **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.
- **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 efficient 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 1.

The simulations are conducted and the performance is compared for efficient CBMT with MDSDV and CBMT with DSDV under 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>
<thead>
<tr>
<th>Table 1 Simulation Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>The density of group members</td>
</tr>
<tr>
<td>Network surface</td>
</tr>
<tr>
<td>The maximal speed</td>
</tr>
<tr>
<td>The pause time</td>
</tr>
<tr>
<td>The simulation duration</td>
</tr>
<tr>
<td>Physical/Mac layer</td>
</tr>
<tr>
<td>Mobility model</td>
</tr>
<tr>
<td>Routing protocol</td>
</tr>
</tbody>
</table>
4.3. Analysis of Simulation Results

This section presents analysis of simulation results to compare the performance of efficient CBMT and CBMT in varying density of nodes and network surface.

This comparison results shows that the efficiency is improved by 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 CBMT. The simulation results illustrate the comparison of efficient CBMT with CBMT as shown in fig.3a – 3d. Indeed, this approach of efficient CBMT with MDSDV divides the multicast group with the effective connectivity between nodes. It allows fast reaction to topology changes.

The average delay of key delivery and the energy consumption are better with this approach of efficient CBMT. 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 CBMT. It can be observed that efficient CBMT gives better performance and achieves reliability in terms of key delivery ratio and packet loss rate compared to the CBMT 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 energy issues. Therefore an attempt is made to reduce the energy consumption and end to end delay and improve the key delivery ratio 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


