CHAPTER VIII

EFFICIENT CBMT

8.1 Efficient CBMT with Mobility Aware MDSDV
8.2 Phases of Efficient CBMT
8.3 Performance evaluation
8.4 Simulation Results
8.5 Analysis of Efficient CBMT
8.6 Chapter Summary
In many multicast interactions, due to its frequent membership dynamism, which causes node failure, link failure, power failure that leads to time delay in multicast transmission. In a cluster, due to the mobile characteristics of MANET, each member can move within the network. The movement in the cluster is in such a way that a member can join a cluster or an existing member can leave from the cluster. Member node may fail due to movement of node out of coverage area.

In a clustering approach, all LCs send periodical Hello messages containing their identities and coordinates. Thus the member moving in the network receives the hello messages from LCs and chooses the nearest LC to join according to its reachability information. Due to frequent mobility, a member may leave the cluster or disappear because of any resource problem. This failure of an ordinary member creates less effect in rekeying.

When an LC moves in the network, it must have previously sent a notification message to all its cluster members to move to the nearest LCs. Then these LCs may decide for reclustering. When an LC disappears due to node failure, it may cause problem in communication and delay in multicast transmission. Thus the frequent topology changes may break existing routing paths. So a routing protocol should quickly adapt to the topology changes and efficiently search for new paths. Failure of node should be identified by reachability information of neighbouring nodes. This can be done with the aid of suitable mobility aware routing protocol that reacts efficiently to the topology changes.

**Specific Problems**

Frequent membership dynamism of mobile nodes in Mobile ad hoc network causes specific problems which are as follows,
Efficient CBMT

- Node failure,
- Link failure,
- Power failure
- Delay in multicast transmission.

These problems of the membership dynamism can be overcome by using mobility aware MDSDV routing protocol. It allows fast reaction to topology changes and is specially designed for MANET. Hence, this phase proposes an Efficient CBMT with mobility aware MDSDV for secure multicast communication. It tolerates the faults that occurs due to node failure.

8.1 Efficient CBMT with Mobility Aware MDSDV

The main objective of the proposed approach is to achieve efficient secure multicast communication for mobile ad hoc networks. This approach uses Mobility Aware 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 able 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 efficient CBMT using Mobility Aware MDSDV tends to have multicast connectivity between the nodes.

8.1.1 Efficient CBMT Algorithm

The main idea of Efficient CBMT is to use Mobility aware Multicast DSDV routing protocol to elect the local controllers of the created clusters by considering the node failure. The CBMT algorithm generates a cluster based multicast tree for secure communication. However topology changes due to node failure, may vary with the number of members in a cluster. This may cause faults.
in multicast communication. Hence an improvement of the CBMT algorithm is then essential in tolerating the faults that is caused due to node failure, considering the number of members of each new cluster. The principle of the proposed clustering approach is described in steps as follows.

**Step 1:**

Initialization of the list of LCs(ListLCs) with GC, the source node and listing all the nodes.

**Step 2:**

Sort the node list (Listnodes) in the ascending order to their 1-hop distance compared to the current LC.

**Step 3:**

Traverse all the Listnodes, if the visited node is a member of the multicast group and at the same time it has a child node then add the node to the list of LC(ListLCs). Remove the members covered by this LC from the list of group members (Listnodes).

**Step 4:**

If there exists any group members which do not belong to the formed clusters. This step chooses the nodes from the remaining group members that have the maximum reachability to the other nodes in one hop. This reachability information is collected through the Multicast version of DSDV routing protocol.

**Step 5:**

Repeat step 2 to step 4 until all the group members covered by its clusters. When the created clusters are not yet cover the group members and hence the nodes are selected as local controllers for the remaining group members.
Step 6:

Traverse the formed cluster, due to membership dynamism, if a cluster has group members more than the maximum threshold, then split the cluster and elect the new LC based on the one hop distance reachability information.

Step 7:

Traverse the formed cluster, If the cluster has group members lower than the minimum threshold, then traverse the group members of this cluster and try to move them to the nearest cluster.

Thus the efficiency of CBMT approach is improved, while forming highly correlated clusters based on the two thresholds. Thus this approach is considered as an Efficient CBMT. The improvements in the efficient CBMT with mobility aware MDSDV approach for multicast key distribution are described in Algorithm 8.1 as follows:

Algorithm 8.1 Efficient CBMT (Cluster Head)

//STEP 1
ListLCs = Cluster Head
Listnodes = {1, 2, 3... c} //c is the number of cluster members

//STEP 2
While (Listnodes ≠ φ) do
  Sort_Listnodes( ); // sort the list of members

//STEP 3
for (i = 1 to c) do
  if (Listnodes ≠ φ) then
    if (i ∈ multicast group) && (i has child group members) then
      ListLCs = ListLCs ∪ {i};
      // Add i to the local controllers list
      Listnodes = Listnodes - {group members covered by i};
// Remove members covered by i from the members list
    CBMT (i);
    // Execute recursively the algorithm applied to i

end if
end if
end for

// STEP 4
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 = ListLCs ∪ {i};
    // LC joins the new member lists
    Listnodes ≠ Listnodes - {i};
    // Remove from the members list
end while
end if

// STEP 5
LC = i;
ListLCs = ListLCs ∪ {LC};
    // Add LC to the local controller list
end while

// Step 6
for ( n = 1 to ListLcs ) do
    for ( m = 1 to Listnodesnumber) do
        for ( z = n to ListLCs) do
if \((d(z),m) \leq \text{max\_distance}\) & \(\text{Listnodesnumber}\{z\} < \text{Max\_Threshold}\) then
\[\text{Listnodes}\{n\} = \text{Listnodes}\{n\} - \{m\};\]
// Remove m of the local members from n
end if
end for
end for
end for
end for

// Step 7
for (n = 1 to ListLcs) do
  for (m = 1 to Listnodesnumber) do
    for (z = n to ListLCs) do
      if (Listnodesnumber\{n\} < Min\_Threshold) then
        Listnodes\{z\} = Listnodes\{z\} \cup \{m\};
        // Add m of the local members to list of z
      end if
    end for
  end for
end for
end for

8.2 Phases of CBMT

The approach of Efficient CBMT with mobility aware MDSDV is described in five phases in Figure 8.1 with specific notations as follows

i) Authentication

ii) Cluster head Election using CBMT

iii) Cluster Formation

iv) Multicast Key Distribution
v) Node Mobility

- **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.

**Node Authentication and Access Control**

\[
\text{mg}_k \rightarrow \text{LC}_{ik}: \text{Join}\_\text{Request}, \text{Pub}_{mg_k}
\]

\[
\text{LC}_{ik} \rightarrow \text{mg}_k: \text{Join}\_\text{Request}
\]

\[
\text{mg}_k \rightarrow \text{LC}_{ik}: \text{Join}\_\text{Reply}, \text{Pub}_{mg_k}, \{\text{CBID}_{mg_k}\} \text{ Pri}_{mg_k}
\]

- **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.

- **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.
Efficient CBMT

Chapter 8

Figure 8.1 Flowchart of Efficient CBMT

For each node u

Initialize source as GC

Authentication

Phase: 1

Cluster Head (LC) Election

Cluster formation

Phase: 2

Phase: 3

Multicast Key Distribution

Phase: 4

Is there Node Mobility?

Yes

Is Join/Leave?

Yes

Is Node Failure?

Yes

No

Is LC?

Yes

No

Is GC?

No

Yes

Secure Multicast Communication

Is LC?

Yes

No

Is GC?

Yes

No

Leave

New Node Join

No

No

No
• Multicast Key Distribution: 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 the session key from the source by unicast KEKcsg-0 (key encryption key of the cluster sub-group 0), encrypted with their respective public keys. 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.

\[
\forall mg_k, CG_k \rightarrow mg_k : \{\text{TEK, Num\_Seq, KEK\_CSG}_{OK}, \text{IDG, IDCG, Pub\_CG, \{CBID\_CG\} Pri\_CG} \text{ Pub}_mg_k
\]

• Node mobility: For frequent node mobility, a new node may join a group or an existing node may leave a group or fails due to any resource problem. To ensure secure multicast communication, both backward and forward secrecy has to be maintained.

  o Join Operation: When a new node joins the multicast group, it cannot decrypt past encrypted data. It is known as Backward Secrecy. Each new node is authenticated based on broadcast request and reply.

  \[\text{Join Procedure}\]

  for old-mg_k: old member of cluster

  \[LC_{ik} \Rightarrow old_{mg_{ik}} : \{ID_{LC}, KEK\_CSG_{ik}\} old_{KEK\_CSG_{ik}}\]

  \[LC_{ik} \rightarrow mg_{ik} : \{ID_{LC}, TEK, KEK\_CSG_{ik}\} \text{Pub}_mg_{ik}\]
o **Leave Operation**: When a node leaves the multicast group, it cannot decrypt the future data. It is known as forward secrecy. Frequent node mobility may cause node failure due to any resource problem. The leave operations are in three cases.

- **When a group controller fails**, it stops the multicast communication and resumes with another source.

- **When a local controller leaves the group or fails**, the members of the group are merged with the nearby groups by executing the MDSDV algorithm.

**Leave Notification**

$$LC_{ik} \rightarrow GLC: \{ID_{LC_{ik}}\}KEK_{CCL}$$

$$\forall j \neq i, GC_k \rightarrow LC_{ik}: \{ID_{GC}, new\_KEK_{CCL}\}Pub_{CL_{jk}}$$

**Merge**

$$\forall mg_{ik}, LC_{ik}: \{ID_{cluster}, LL_{LC_{ik}}\} KEK_{CGG_{ik}}$$

- **When an ordinary node leaves or fails**, it gives less effect in multicast transmission. The leave operation of an ordinary node is specified as follows:

**Leave Procedure**

$$mg_{ik}: \text{outgoing member leaving a group}$$

for $$mg_{ik}: \text{Local member},$$

$$mg_{ik} \neq mg_{ik\_outgoing}$$

$$LC_{ik} \rightarrow mg_{ik}: \{ID_{LC}, KEK_{CSG_{ik}}\}Pub_{mg_{ik}}$$
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 of end to end delay in multicast transmission and also tolerates the fault that occurs due to node failure.

8.3 Performance Evaluation

The performance of efficient CBMT for multicast key distribution is evaluated in terms of QoS characteristics as metrics. The QoS metrics considered are end to end delay in key distribution, energy consumption, Key delivery ratio and packet drop ratio of multicast key distribution. The performance is evaluated and compared for efficient CBMT with MDSDV and existing OMCT clustering approach 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.

8.4 Simulation Results

This section presents analysis of simulation results to compare the performance of efficient CBMT and OMCT in varying density of nodes and network surface. This comparison result 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 drop ratio compared to the existing OMCT clustering approach.

The simulation results illustrate the comparison of efficient CBMT with OMCT as shown in Figures. 8.2a – 8.2d. 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 while forming highly correlated clusters, the LC consumes less energy to communicate with its members. Each cluster managed by an LC close to its group produce less delay in multicast key distribution. Hence it reduces average end to end delay and energy consumption of multicast key distribution in efficient CBMT compared to OMCT. It can be observed that efficient CBMT gives better performance and achieves
reliability in terms of key delivery ratio and packet drop ratio compared to the OMCT algorithm under varying network conditions.

This simulation results show that the efficiency is improved by CBMT approach for secure multicast communication in terms of fault tolerance compared to existing OMCT as shown in Figure 8.3.

![Figure 8.3 Fault tolerant in multicast transmission](image)

As number of nodes increases, it increases the fault-tolerance in key distribution.

### 8.5 Analysis of Efficient CBMT

A Performance model is developed to evaluate the performance of secure multicast communication of the efficient CBMT for mobile ad hoc networks in terms of QoS metrics and fault tolerance due to node failure. This section presents analysis of simulation results to compare the performance of proposed efficient CBMT with Mobility aware MDSDV, proposed CBMT and existing OMCT in increasing number of nodes. 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 drop ratio compared to proposed CBMT and the existing OMCT.

The analysis of simulation results illustrate the comparison of efficient CBMT, CBMT and OMCT as shown in Figures 8.4a. – 8.4d.

**Figure 8.4a. End to end Delay**

**Figure 8.4b. Energy Consumption**

Figures 8.4a. and 8.4b. illustrates that the average delay of key distribution and the energy consumption are better with this approach of efficient CBMT than CBMT and existing 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.

From the Figures 8.4c. and 8.4d., it can be observed that Efficient CBMT gives better performance and achieves reliability in terms of key delivery ratio and reduces packet drop ratio compared to the CBMT and the existing OMCT algorithm under varying network conditions.
This simulation results show that the efficiency is improved by CBMT approach for secure multicast communication in terms of fault tolerance compared to the CBMT and OMCT as shown in Figure 8.5.

As number of nodes increases, it increases the fault-tolerance in key distribution. Indeed, this approach divides the multicast group with the effective connectivity between nodes.
It allows fast reaction to topology changes. This is due to the fact that it sends acknowledgement for each transmission in order to reduce the retransmission. Hence it tolerates the fault that occurs due to node failure of multicast transmission in efficient CBMT compared to OMCT.

**Specific Advantages**

Some of the Specific advantages of Efficient CBMT with Mobility aware MDSDV routing protocol over the existing OMCT approach are as follows.

- Failure of node is easily identified by reachability information of MDSDV.
- Tolerates the Fault.
- Reduced end to end delay.
- Less energy consumption.
- Increased key delivery ratio.
- Reduced Packet Drop ratio.

**8.6. Chapter Summary**

Frequent Membership dynamism is a major challenge in providing complete security in Mobile Ad hoc networks. Existing algorithm like OMCT address the critical problems using clustering approach like “1 affects n” phenomenon, energy and end to end delay issues of multicast key distribution. Therefore an attempt is made to further reduce the energy and end to end delay and improve the reliability by reducing packet drop ratio and increasing key delivery ratio using an algorithm called Cluster Based Multicast Tree algorithm multicast key distribution.
This approach is further improved in efficiency as number of nodes increases by using an approach of efficient Cluster Based Multicast Tree algorithm for secure multicast communication. This approach further reduces the end to end delay and improves the fault tolerance as the number of node increases for fault tolerant 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 MANET.

Publications of Phase V :

- **International Journals**


International Conference