Analysing the Effect of Cluster Strategies in Multicast Traffic using TAM Protocol for Ad-hoc Networks

S Deepakraj\textsuperscript{1}, Dr. R. Thamilselvan\textsuperscript{2}

\textsuperscript{1,2}Department Of Information Technology, Kongu Engineering College, Erode, Tamilnadu, India

sdpeakit@gmail.com\textsuperscript{1}, r_thamilselvan@kongu.ac.in\textsuperscript{2}

\textbf{Abstract}— Ad-hoc networks generally play a vital role in emerging technologies. The limited communication and computation resources, the unguaranteed connectivity to trusted authorities make known security solutions for wired networks. A novel Tiered Authentication scheme for Multicast traffic (TAM) has large scale of ad-hoc networks. Nodes are grouped into the cluster. Cross-cluster multicast traffic includes a Message Authentication Code (MAC) that is based on set of keys. Each cluster uses unique subset of keys. TAM is combination of secret information asymmetry and the time information asymmetry for inter cluster and intra cluster networks. The topologies used are flat, spanning tree, balanced tree to reduce bandwidth overhead and delivery delay. These topologies are compared for numerical and analytical results that demonstrate the advantage of TAM.

\textbf{Keywords}— Multicast Communication; Message Authentication; Ad-Hoc Networks; Network Topologies

\section{I. INTRODUCTION}

The Ad-hoc networks have been challenging for the engineering community and research. Digital battlefield, air born safety and border protection are example of wireless ad-hoc networks applications. The ad-hoc networks are based on node energy and proper communication capabilities. More ad-hoc networks are very large set of nodes with dynamically changing network topology. The solutions must be scalable to support networks covering vast areas with a large set of nodes that communicate over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks. Group communication is considered as a critical service in Ad-hoc networks due to their inherently collaborative operations, whereas the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. Mobile Ad hoc Networks is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration.

Mobile Ad hoc Networks are self-organizing and self-configuring multi hop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner engaging them in multi-hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network.

All nodes are capable of movement and can be connected dynamically in an arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move. In this type of network, some pairs of terminals may not be able to communicate directly with each other and relaying of some messages is required so that they are delivered to their destinations. Such networks are often referred to as multi-hop networks. The nodes of these networks function as routers which discover and maintain routes.

The network services need to achieve the following security goals: (1) Confidentiality: The Confidentiality is achieved by encrypting the transmitted data. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network. (2) Source Authentication: In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key. (3) Message Integrity: In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as in the classic ACID model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

II. PROBLEM DEFINITION

Clustering has Inter cluster authentication and Intra cluster authentication. Mainly the inter cluster authentication and the intra cluster authentication is the same authentication process. Sometimes use of secret asymmetry for both clustering results in the problem of time delay and also the time asymmetry for both clustering results in the problem of security. Also both the cluster authentication is performed using public key. TAM traffic is designed by private key in inter cluster and intra cluster authentication. The multicast communication is performed by Inter cluster and Intra cluster.

The intra cluster is performed by time asymmetry and the inter cluster is performed by secret asymmetry in the various cluster networks. The TAM [3] traffic is mainly used for different types of tree creation and also with authentication purpose using Message Authentication Code (MAC). So, the performance of TAM is a comparison of bandwidth overhead and delivery delay in different cluster size. The maximum degree of node is based on the balanced tree. And also the balanced tree is having many child nodes from root node. A linear spanning tree in the degree of the individual node is ≤ 2. The flat approach is worst in the case of bandwidth overhead and delivery delay in various cluster size. So, that the same cluster size comparison of spanning tree and also d-balanced tree comparison of bandwidth overhead and delivery delay.

III. PROPOSED WORK

A. Intra-cluster authentication

The Grouping nodes in the clusters enables having a reasonably tight bound on the end-to-end delay of packet delivery and will enable the use of a time asymmetry based authentication scheme. The intra cluster authentication is within the cluster transmission so it does not provide any security. Because the MAC will be attached to the packet so the overhead will occur in the network. The Intra cluster is only based on the time asymmetry and clock synchronization using the clock jitter. Intra-cluster authentication is used for TAM.

The TAM traffic is based on TESLA [1] protocol for time asymmetry using clock jitter. The TAM traffic is supported to a small amount of diameter in cluster. A source node generates a chain of one time use keys using hash function and shares only that last generated key with the receiver. A message can be authenticated only when the key used in the chain is revealed. A key cannot be used outside its designated time interval and the message will be ignored if the MAC is based on an expired key [5]. Continuously clock synchronization is required to make sure that source and destination have the same time reference for key expiration. The advantages are:

1) The MAC overhead is small
2) A single MAC is used per every multicast packet for all receivers.

The maximum end to end delay experienced by an intra-cluster multicast will be mostly dependent on the cluster size.

B. Inter-cluster authentication

The Inter Cluster Authentication is based on time asymmetry [3] and it requires clock synchronization and it does not support for large networks. Fig.3.1 inter-cluster multicast traffic, TAM applies a strategy based on secret information asymmetry and engages the cluster heads in the authentication process. Basically, the source “s” that belongs to Cluster will send the multicast packets to the other heads of all clusters that have designated receivers.

The inter-cluster authentication is used for Message Authentication Code (MAC). The source will generate a pool of M keys. Each of the cluster head (N_{CL}) in the network will be assigned a share L of keys, with M < L < \text{N}_{CL}. So the cluster networks also having different type of topology is based on location will form of cluster and one node act as a cluster head in that topology and others node act like as gateway and the message will be transferred to the gateway in the cluster networks. The cluster head knows about others nodes information and location of particular node in network of different topology.

---

**Fig.3.1. Message Flow**

The inter-cluster authentication is used for Message Authentication Code (MAC). The source will generate a pool of M keys. Each of the cluster head (N_{CL}) in the network will be assigned a share L of keys, with M < L < N_{CL}. So the cluster networks also having different type of topology is based on location will form of cluster and one node act as a cluster head in that topology and others node act like as gateway and the message will be transferred to the gateway in the cluster networks. The cluster head knows about others nodes information and location of particular node in network of different topology.
C. Cluster formation

An ad-hoc network is a collection of autonomous nodes that together set up a topology without the support of a physical networking infrastructure. The communications among the nodes are via multi-hop routes using Omni-direction wireless broadcasts \(^4\) with limited transmission range. In the system model the nodes are grouped into the cluster. The cluster formation can be based on location and radio connectivity. The node which is first in the network is selected as cluster head. The clusters are established securely by using pre-distributed public key, employing a robust trust model. The cluster network is better supported for routing of multicast traffic and the performance gain dominates the overhead of creating and maintaining the cluster.

Environment setup:

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Cluster</td>
<td>5 (Each cluster have 10 nodes)</td>
</tr>
<tr>
<td>Channel</td>
<td>Wireless channel</td>
</tr>
<tr>
<td>MAC type</td>
<td>802.11</td>
</tr>
<tr>
<td>Antenna</td>
<td>Omni Antenna</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Cluster radius</td>
<td>2 and 4</td>
</tr>
</tbody>
</table>

D. Effect of the node degree

The average bandwidth overhead in the simulation experiments in the network connectivity is varied. The results for both TAM traffic and the flat approach are plotted. The performance drop is attributed to the fact that more clusters are formed in the simulation and MAODV \(^6\) is not formed by the balanced tree so TAM still sustains its performance edge over the flat approach. It is worth noting that a significant boost in the connectivity of the network makes a major positive impact on TAM performance, while the flat approach does not benefit as the reason is a fixed cluster radius, increasing the node degree grows the cluster size and decreasing the number of clusters. The node degree has a positive impact on the delivery delay.

E. Effect of cluster radius

The cluster radius is result of bandwidth overhead as a function of the cluster radius. The number of nodes is fixed at 50 and the results for d=2 and d=4, where the increase in the cluster radius lower the overhead, because of the decrease in the cluster count.

F. Configuring TAM protocol

Both security and performance factors have to be considered when employing TAM. With respect to resilience of impersonation and replay attacks, TAM limits the effect of a node compromise within a cluster. If a cluster member is captured, the TESLA-based intra-cluster authentication will deem any attempt by an adversary to launch these attacks ineffective. Meanwhile, the vulnerability to these attacks due to the capture of a CH node is still limited within the cluster since only the key share of the compromised CH node will be uncovered and the adversary will not be able to fool other cluster-heads. However, a compromised CH cannot be prevented from launching impersonation and replay attacks against the members of its own cluster. Although the probability of capturing a CH is significantly low given the low CH count within the node population, it is advisable to have small clusters in order to mitigate the effect when it happens. While a large value of \(k\) seems to be advantageous for TAM’s bandwidth overhead and would not cause a concern about the delivery delay, the management complexity of a cluster usually grows significantly with the increase in the cluster radius. The larger cluster radius will result in an increased intra-cluster delay variability which is not suitable for one way hash chain multicast authentication methods. A TAM system with a cluster radius of 2 or 3 would yield a major performance gain over current multicast schemes and strike a balance between the objectives of achieving high network performance and increasing resilience to impersonation and replay attacks.

G. Analyzing for TAM protocol

Flat topology: A flat topology has a worst performance in terms of the number of transmissions corresponds to having a linear spanning tree of all N nodes. The flat topology is form of looping format in network so the message will pass through to the all nodes and reach destination so every node have take time for transmission and number of nodes will be added in flat topology so the bandwidth overhead also increase at the time of transmission. To calculate the bandwidth overhead formula is using Equation (3.1) and delay formula using Equation (3.2).

To find the bandwidth overhead and delay of Flat Topology:

\[
\text{BW overhead}_{\text{flat}} = \text{packet rate} \times \frac{\text{overhead/packet}}{\text{transmit}} \quad (3.1)
\]

\[
\text{Overall delay}_{\text{flat}} = \text{levels in tree} \times \frac{\text{packet size}}{\text{time to transmit a bit}} \quad (3.2)
\]

Spanning tree topology: A linear spanning tree in this context refers to the case in which the node degree of the individual nodes is \(\leq 2\) and a path from a source to a receiver may have to include the other entire \(N-2\) nodes, i.e., requiring \(N-1\) transmissions.
The spanning tree doesn’t form looping in network so the path is very large to message will be reach to destination in the network. These transmissions are also sequential with an additive delay and also many numbers of nodes will be act as intermediate node so bandwidth also more overhead compare to flat topology so the spanning tree is worst case of bandwidth over head and delivery delay. To calculate of bandwidth overhead formula is using Equation (3.3) and delay formula using Equation (3.4).

To find the bandwidth overhead and delay of linear spanning tree:

\[
\text{Worst BW overhead} = R \times (N-1) \times B \times \left\lfloor \log_2 N \right\rfloor \quad \text{(3.3)}
\]

\[
\text{Worst overall delay} = (N-1) \times (\text{Data} + (B \times \lfloor \log_2 N \rfloor)) \times \lambda \quad \text{(3.4)}
\]

Where, 
- \( R \) – Packet rate, \( N \)- Number of nodes
- \( B \) – Mac size of B Bits, \( \lambda \) - Time to transmit a bit

Balanced tree topology: The balanced tree results in best performance to achieve over a balanced tree. Degree (\( d \)) is calculated by Equation (3.5) the maximum degree a node in the network. The balanced multicast tree is a construct of the number of transmissions will depend on the Height (\( h \)) and is calculated by Equation (3.6) of the tree. The balanced tree have root node and that root node have child nodes so these way of topology is created by balanced tree. Here the child node is perfect match and is not a perfect match compared to the tree of child node. So the source and destination path is based on shortest path and also selected if path is based on child node in the cluster network. Calculate the bandwidth overhead using Equation (3.7) and delay using Equation (3.8).

\[
\text{Degree} (d) = 1 + d + d^2 + \ldots + d^d = (d^{d+1} - 1) / (d - 1) \quad \text{(3.5)}
\]

\[
\text{Height} (h) = \log_2 \left( \left( d - 1 \right) N + 1 \right) - 1 \quad \text{(3.6)}
\]

To find the bandwidth overhead and delay of balanced tree:

\[
\text{BW overhead} = \frac{\text{packet rate}}{\text{packet (MAC size) times transmit}} \times \text{overhead}
\]

\[
\text{Overall delay} = \text{levels in cluster tree} \times \text{packet size} \times \text{time to transmit a bit} \quad \text{(3.7)}
\]

In Fig. 4.1 the flat topology has a problem of loop formation so that more number of nodes will be added to the network and the bandwidth overhead will be more. In spanning tree, there will be no loop but incurs a problem of linear transmission. The transmission of data is based on N-1(neighbor node) from the source node so the bandwidth over head will be highly increased. But in the case of balanced tree there will not be any loop formation since it is based on cluster radius height and also the transmission will be based on root node and leaves node in the tree. Therefore the delay will be very less in balanced tree.

In Fig. 4.2 the flat topology has a problem of loop formation. Hence the delay will be more. In spanning tree, there will be no loop but incurs a problem of linear transmission. Hence there will be considerable delay.
But in these cases of balanced tree there will not loop formation since it is based on cluster radius height. Therefore the delay will be very less in balanced tree. Thus the balanced tree is the best case for delivery delay in the cluster radius of d=2. So the number of radius size is varying, that performance also is different in the network.

V. CONCLUSION AND FUTURE WORK

The hybrid approach method is mainly used to combine the existing approaches such as time and secret-asymmetry. In the existing system these methods are used separately. The inter-cluster uses the concept of time asymmetry which results in lack of security and intra-cluster uses the concept of secret asymmetry which results in more delay. The proposed system mainly provides accurate time and secret asymmetry. Mainly the intra-cluster is used for time-asymmetry and the intra-cluster is used for secret asymmetry. Here comparisons are made between flat topology, spanning tree, balanced tree in various networks. Hence the performance of these networks is worst case in flat and spanning tree and the best case in balanced tree of bandwidth overhead and delivery delay. The future work can be extended to improve the cluster strategy and routing schemes.

REFERENCES


