Implementation of Secure Clustering in Manet Using Mobile Agent

Rajesh Kumar¹, Prof. S Niranjan²
¹Research Scholar, Mewar University, Gangrar, Chittorgarh, Rajasthan-312 901, India
²Professor, Mewar University, Gangrar, Chittorgarh, Rajasthan-312 901, India
¹rkvashisth83@gmail.com, ²niranjan.hig41@gmail.com

Abstract- This paper deals with secure clustering in MANETs having main emphasis on security by utilizing mobile agent with clustering algorithms. MANET is composed of peer nodes with equal networking capabilities which are able to function as mobile routers i.e. to forward packets and maintain routes. Packets forwarded in multi-hops from the source nodes to the destination nodes can go without the need for underlying fixed network infrastructure (e.g. routers and base stations). MANET uses the network topology that is autonomously formed and continuously changes according to the mobility of the nodes and as per the nature of the problem. One of the main challenges in an ad hoc network is the design of robust as well as secure routing algorithms that will adapt to the frequent and randomly changing network topology. All nodes use two mobile agents in coordination with security manager to perform routing and clustering operations. We will identify various parameters for improving network performance in the proposed secure clustering operation. The proposed work concerns with improvement for the existing clustering algorithm under the energy parameter specification. The effective route here is defined for clustered communication. An inter cluster and intra cluster communication is here performed under mobility vector. The proposed work will also emphasize on distance, security and energy adaptive algorithms that is suggested to generate effective as well as secured communication route and analyze the work under different parameters which enhances the security, authentication and stability of the network in a more efficient way.

Keywords- Mobile ad hoc network (MANET), Mobile agent (MA), Ad hoc on demand distance vector (AODV), Route Request (RREQ), Route Reply (RREP), Security Interfacing (SI), and Network Simulator 2 (NS2).

1. INTRODUCTION

The distance and energy adaptive algorithms are important parameters for effective and secure communication. We presented the distinguishing features those make subtle difference between the existing and the proposed work are as follows:

1. All the above algorithms have overhead involved as they have to transfer their routing tables to other nodes over the network. They either transfer them on time-based approach or event based approach. This problem does not exist with an algorithm as there is no need for the transfer of the routing tables.

2. Some of the algorithms do not support multiple paths and hence there is no possibility of load balancing, in case the optimal path is heavily congested and algorithm supports generation of multiple paths and hence favours load balancing [1].

© 2015, IJCSMC All Rights Reserved
➢ **Security:**

In a mobile ad hoc network, the nodes are shared and the information travels among multiple nodes before the final delivery. In such case, it is required for communication channel to maintain security so that no intermediate node or any external node captures the communication information. Such kind of network also suffers from different kind of security threats such as DOS attack. As of the public network, mobile network also suffers from high security risks and having the problem of stolen information and heavy traffic that gives the insecure wireless link over the network [9].

➢ **Routing in Manet**

Routing protocols are mainly used for determining optimal packet routes for sending data between source and destination. Exchanging route information, gathering information about route breaks, repairing broken routes, load balancing are also some of the useful features of routing protocols.

- **Unipath Routing Protocols** are designed to provide the unipath between source and the destination by establishing the multihop wireless link between nodes those are in communication range of node. Here each node behaves like router for finding routes and maintaining them.

![Classification of Routing Protocols in MANET](image)

The two components of unipath routing protocols are i) Route Discovery: finding a route between a source and destination. ii) Route Maintenance: repairing a broken route or finding a new route in the presence of a route failure. There are two types of unipath routing protocol table driven and reactive routing protocol [7].

- **Table Driven Protocols** are also known as proactive protocol that evaluates the routes periodically and maintains routes for each node in the network i.e. each node has full topological view and when the packet is need to be transferred route is already known. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network.

- **Multipath Routing Protocols** consist of finding multiple routes between a source and destination node. These multiple paths between source and destination node pairs can be used to compensate for the dynamic and unpredictable nature of ad hoc networks. The multi-path routing could offer several benefits: load balancing, fault-tolerance, higher aggregate bandwidth, lower end-to-end delay, etc. [8]
II. RELATED WORK

The work done by earlier researchers under different parameters are discussed below:

<table>
<thead>
<tr>
<th>Year</th>
<th>Research Development</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>The author presented secure network architecture with problem identification and solution identification and analytical work to handle the security challenges and to summarize the key issues related to the work. Further outline of the work was presented as to how to attain the ad hoc security and the current state of routing, DOS prevention and key management schemes. The author also defined the security analysis under different network environments [6].</td>
<td>Fei Hu</td>
</tr>
<tr>
<td>2012</td>
<td>The author has performed a work on the performance of mobile network in realistic environment and analyzed the work under different real time situations and defined work on different simulators. The work is here been checked on different scenario, shapes to attain the effective output from the system. The node analysis over the system is performed under blocked condition [11].</td>
<td>Chirag Kumar</td>
</tr>
<tr>
<td>2011</td>
<td>The author defined a distributed and dynamic topology control mechanism in sensor network to attain the critical performance. The Topology control algorithm is defined with the sensor nodes connected to the single link network and with TDMA based protocol specification and design in the requirement phase. The results so obtained from the system shown that the higher data reliability and the control system would achieve an effective network environment [9].</td>
<td>Zinon</td>
</tr>
</tbody>
</table>

Table 1: Work Done By Different Authors

- **AODV PROCESSING**: When a node originates some data and wants to send it to another node. It will take the following actions as same as what AODV defines. As route discovery operates entirely on demand, if no route is available the node will initiate the route discovery protocol to dynamically discover a new route to that destination node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello interval</td>
<td>1.5 s</td>
</tr>
<tr>
<td>Maximum rate for sending replies for a route</td>
<td>1/s</td>
</tr>
<tr>
<td>Active Route timeout</td>
<td>300 s</td>
</tr>
<tr>
<td>Route reply lifetime</td>
<td>300 s</td>
</tr>
<tr>
<td>Allowed hello loss</td>
<td>2</td>
</tr>
<tr>
<td>Request retries</td>
<td>3</td>
</tr>
<tr>
<td>Time between retransmitted requests</td>
<td>3 s</td>
</tr>
<tr>
<td>Time to hold packets awaiting routes</td>
<td>8 s</td>
</tr>
</tbody>
</table>

Table 2: Constants Used in the AODV implementation

According to the formal description of AODV, this RREQ, AODV needs to keep track the following information for each route:

- Destination IP Address: IP Address for the destination node.
- Destination Sequence Number: Sequence number for this destination.
- Hope count: Number of hops to the destination.
- Next Hop: The neighbour which has been designated to forward packets to destination for this route entry.

Life Time: The tie for which the route is considered valid [8]. Packet could be a separate IP packet, used only to carry this route request option, or the sender can include the route request option in an existing packet that needs to send to the destination. Figure 2 shows the propagation of RREQ packet. In this example, the route discovery initiator S creates a route request packet. When a node receives the route request packet, it first should check whether it is the target of the route discovery [10].
III. PROPOSED WORK

The proposed work concerns with the effective distance and energy consumption for creating an efficient mobile network communication link that specially concerns with strong security architecture [13]. The performance parameters we take for communication over the network resulting in a substantial loss of energy. This work also emphasizes to generate an energy adaptive communication path so that the reliable communication path will be generated i.e. an important aspect in the security architecture.

![Fig.2 Propagation of RREQ](image1)

![Fig. 3 Propagation of RREP](image2)

The improvement in the existing clustering algorithm is done under the energy parameter specification. The effective route is defined for clustered communication. An inter cluster and intra cluster communication is performed under secure mobility vector. The parameters which we have already taken are shown in the Simulation environment for showing the results. We are using the NS2 simulator for the purpose.

a) Problem Statement

The Proposed work is concerned with the security of the mobile network that emphasizes the clustering and the specification of inter cluster along with intra cluster communication over the network. Based on the clustering architecture, the communication is done using mobility prediction model that is more secure as compared to the existing one. The cluster selection is performed under throughput, effective rate and idle rate analysis. The most complex as well as secured architecture for mobile network is our proposed cluster architecture that mainly focuses on the security as well as other aspects that is essential for a secured architecture. When complexity of the network increases as the mobility over the clustered nodes is changing, the proposed work suits best. It is highly desired that we have to create an efficient MANET by using mobile agent with more distance and less energy consumption with improved security [1].

b) Objectives

The proposed work is aimed to achieve the QOS in mobile clustered network for efficient security mechanisms. The objective of the work is to define an improved clustered communication under defined analysis parameter.

The work is divided in terms of smaller research objectives given as under:

1. Study of different parameters that will affect the network QOS as well for secure routing algorithm.
2. Implementation of MANET in scenario under NS2 in respect of architectural specifications using mobility model in clustered network.
3. Conclude the results from the different aspects like security, throughput, energy consumption and analysis that work in the simulated environment for comparing the results with previous ones.

c) Security Interfacing For Proposed Work

Security interfacing for clustering in MANETs includes interfaces that define services for the following well-known areas of computer security: Authentication, Message Protection (including encryption for guaranteeing confidentiality as well as integrity), Access Control, Auditing, and Non-repudiation [12]. The latter two provide means to achieve some degree of accountability. In addition, Cluster Security describes interfaces that can be used for coping with the tedious, but very crucial task of security management/ administration (e.g. assigning policies to domains). Furthermore they take care of specific problems with object-oriented (security) systems, such as the delegation of rights. In order to meet its objectives, Clusters Security interfacing design is based on some general principles. The most important ones are transparency, scalability, flexibility, and inter
operability, presented in the following. The functionality of Security interfacing is provided in three distinct levels of increasing functionality. For these security aware applications non-repudiation is also relevant.

- **Security Interfacing Does The Following Function[14]:**
  - Transparency: application-level objects should be unaware of security services which are used.
  - Control: client/object should be able to specify security requirements
  - Security policies: specified by policy objects
  - Administrative domain where client/server is executed determines set of security services.

![Security Interfacing of Clusters with Mobile Agent](image)

Fig. 4 Securities Interfacing of Clusters with Mobile Agent

**d) Network Model**

In this analysis model, the system will consist of a different kind of network with the following assumptions, in which:

- The clustered network is defined where each cluster is controlled by the cluster head called controller node.
- The network includes the inter cluster and intra cluster communication.
- The communication is performed via cluster head.
- Location of all nodes and coordinators is dynamic.
- If the coordinator nodes is present, it will control a set of nodes
- A network can have one or more coordinator depending on the network size and density.

**e) Assumptions**

The assumptions associated with this presented work are given here under

- The nodes are defined in fixed geographical area.
- Nodes are defined with energy specification.
- Nodes are not fully secured from attacks.

The energy dispersion with each communication activity is constant [3]

**f) Flow Chart**

The proposed work flow is implementation of the network algorithm with those scene and scenario specification so that effective network construction has been defined. The algorithm is here been defined in the form of network construction and communication steps. The algorithmic representation of proposed work is shown in figure 5.
Initialize Network Area with \( N \) nodes

Define the coordinator nodes over the network to control the secured network communication

Setup the source and destination node

Setup the communication and traffic parameters to perform the secured network communication

Simulate the network under defined parameters

Perform the analysis under different vectors

STOP

Fig. 5 Flow Chart of Proposed Work

g) Cost Model

In order to compare the various network topologies and the scenarios some parameters are required. This helps us in estimating the network cost. The ad hoc network cost is basically in terms of communication over the network. Here the communication estimation is further divided in few parameters: [3]

1. Number of Packets Transferred: It is basically the throughput that represents the number of packets successfully received by the sink node. The receiving packets are compared with sending packets and the ration represents the throughput.

   The throughput is given by

   \[
   \text{Throughput} = \frac{\text{Number of Packet Received}}{\text{Number of Packets Sent}} \times 100
   \]

2. Number of Packets Lost: It is the parameter according to which the cost of network will be estimated. It is just opposite to the previous cost estimator. It defines the number of packets lost over the network. The reason of lost can be some attack, delay or the transmission ratio. Here we are comparing the packet loss ratio respective to the communication over the network on different topology, scalability and clustering parameters.

   1. Data Rate:

      It defines the data rate on which the communication is performed. The data rate is defined in terms of bit rate and byte rate. This rate is also defined with delay parameters also. Here the delay is because of setup phase. For the actual topological comparison we keep the data rate constant. The data rate can vary over the communication over the network.

   2. Delay Rate:

      It is basically the delay in setup phase. For different topologies the delay rate can be different. If the delay rate is high it can slow down the communication and can result in terms of packet loss over the network. Here the work is presented in form of delay analysis over the network [3].
h) Proposed Algorithm [5]
Algorithm
{
1. Define a Clustered Network with N Nodes and M Clusters.
2. For K=1 to L
   [Process all clusters]
   {
3. For I=1 to M
               [Process all nodes]
               {
4. Dist=CalcDistance(Node(I),Cluster(K))
5. If (Dist<SensingRange)
               {
6. Cluster(K).Add(Node(I))
   }
   }
7. Setup Random Directional Mobility Model for Each Node over the network
8. Send the Randomized Communicating Nodes called Src and Dst
9. If (Src.Cluster=Dst.Cluster)
       [Perform Communication within Cluster]
       {
10. Set CommunicationType="Intra-Cluster"
11. Set Communication(Src, Src.Cluster)
       }
13. Else
       [Perform Inter Cluster Communication]
       {
14. Set CommunicationType="Inter-Cluster"
15. Set Communication(Src,Src.Cluster)
17. Set Communication(Dst.Cluster,Dst)
       }
18. For X=1 to Y
    {
19. If (Dist(Node(X),Node(X).Cluster)>SensingRange)
        {
20. For P=1 to M
21. [Identify the Effective Cluster in range)
        {
22. If (Dist(Node(X),Cluster(P))<SensingRange)
        {
23. Perform Throughput, IdleRate and Effective Rate Analysis called Performance Vector
24. If(PerformanceVector>MaxPerformanceVector)
25. {
26. MaxPerformanceVector=PerformanceVector
27. Index=P
        }
        }
28. Set Node(X).Cluster=Index
    }
29. Perform the Communication with new cluster head
30. Analyze the network under different communication vectors
}
IV. SIMULATION MODEL & TOOLS

We use NS2.35 to simulate our proposed protocol. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. It is most popular simulator in scientific environment. It has the functionality to notify the network layer about link breakage. One of the popular network simulators is QualNet: based on GloMoSim. It is used as tool for simulation and supports the following Protocols/Models: [15]

a. Wired Networking
b. Routing: Multicast, Unicast and Hierarchical Routing, etc.
c. Traffic Sources: WEB, FTP, TELNET, CBR etc
d. Transportation Sources : TCP, UDP etc
e. QoS: IntServ and DiffServ Wireless Networking

Ad hoc routing and mobile IP

a. MAC layer Protocol: TDMA, CDMA, IEEE Mac 802.x, etc.
b. Physical layers: different channels, directional antenna.
c. Routing Protocol: AODV, DSDV, DSR, etc.

![Fig. 6 Overview of Simulation Model](image)

- **NS2 Research Actions**
  1. NAM: Network animator. Visualized trace tool (not really).
     Pre-processing:
     Traffic and topology generators
  2. Post-processing:
     Simple trace analysis, often in Awk, Perl (mostly), or tcl.
  3. NS2: the simulator itself, now version: ns-2.35
     We will work with the part mostly.

![Fig. 7 NS2 Directory Structure](image)

A) Parameters & Results under Simulation Environment

The results are simulated by using NS 2.35 simulator for different parameters and their corresponding values are given in the table:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS 2.35</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>50</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>100 Sec</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512</td>
</tr>
<tr>
<td>MAC Type</td>
<td>802.11</td>
</tr>
</tbody>
</table>
Table 2. Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coverage Range</td>
<td>990x990</td>
</tr>
<tr>
<td>Network Type</td>
<td>Clustered</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Way Point</td>
</tr>
<tr>
<td>Number of Clusters</td>
<td>5</td>
</tr>
</tbody>
</table>

B) For Implementation of Inter and Intera Clusters Communication We Follow the Steps Given Below

Step 1: Clustering Architecture

The figure 8 shows the clustered architecture of network node Model. Network is divided into 5 clusters at the initial phase. The selection of cluster is here defined under the distance parameter. [2]

Step 2: Coverage Range

The figure 9 shows the clustered architecture of node placement in network. The network is divided in 5 clusters at the initial phase. The cluster member selection is here defined under the distance parameter. In above figure the green nodes represent the represents the energy effective mobile nodes and blue nodes represent the cluster of node. The circles are defined to represent the mobility of nodes.

Step 3: Identification of Routes

The figure 10 shown below is for the clustered architecture of network node placement. The network is divided in 5 clusters at the initial phase. The cluster member selection is here defined under the distance parameter. The blue nodes represent the cluster nodes and the green nodes represent the energy effective mobile nodes. The network nodes represent the route identification phase.
Step 4: Route Generation

Figure 11 is showing the clustered architecture of network node placement. The network is divided in 5 clusters at the initial phase. The cluster member selection is here defined under the distance parameter. Here the blue nodes represent the cluster nodes and the green nodes represent the energy effective mobile nodes. The network nodes represent the route Generation phase.

Step 5: Intera Clusters Communication

The figure 12 shown below is for the clustered architecture of network node placement. Here the blue nodes represent the cluster nodes and the green nodes represent the energy effective mobile nodes. The network nodes represent the route based communication over the network. The figure is also showing the data drop over the communication [2].
Fig. 12 Clustered Architecture (Communication)

**Step 6: Inter Cluster Communication**

Here figure 13 is showing the clustered architecture of network node placement. Here the blue nodes represent the cluster nodes and the green nodes represent the energy effective mobile nodes. The network nodes represent the inter cluster communication over the network. The figure is also showing the data drop over the communication.

Fig. 13 Clustered Architecture (Inter Cluster communication)

C) **Plotting of Result in Xgraph:**

The Xgraph program draws a graph on an X display given data read from either data files or from standard input if no files are specified. It can display up to 64 independent data sets using different colours and/or line styles for each set. It annotates the graph with a title, axis labels, grid lines or tick marks, grid labels, and a legend.

Fig. 14 Packet Transmission Analysis

Above figure 14 shows the node packet communication analysis over the network. Here X axis represents the simulation time and y axis represents the packet loss over the network. Figure shows that the communication is being increased over the networks [15]
Fig. 15 Packet Loss Analysis

Figure 15 is showing the Packet Loss Analysis over the network. Here X axis represents the simulation time and y axis represents the packet loss over the network. Figure shows, as the cluster formation is done, the packet loss is increased initially after that as the route established no more packet loss occurs. As the route reconfiguration over the network is performed, the packet loss occurs.

Fig. 16 Expected Communication Analysis

Here figure 16 is showing the expected communication analysis over the network. Here X axis represents the simulation time and y axis represents the expected communication over the network. Figure shows, the expected communication increase continuously over the network.

Fig. 17 Last Packet Time Analysis

Here figure 17 is showing the last packet time analysis over the network. Here X axis represents the simulation time and y axis last packet time analysis over the network. Figure shows, the packets are continuously transmitted over the network.
Fig. 18 Bytes Transmission Analysis

The figure 18 shows bytes communication analysis over the network. Here X axis represents the simulation time and y axis represents the byte communicated over the network. Figure shows that the communication is being increased over the networks without any interruption.

Fig. 19 Bit Rate Analysis

Above figure 19 is showing the bit rate analysis over the network. Here X axis represents the simulation time and y axis represents the bit rate analysis over the network. Figure shows that the communication is being increased over the networks without any interruption.

Fig. 20 Bit Rate with Delay Analysis

Here figure 20 is showing the bit rate with delay analysis over the network. Here X axis represents the simulation time and y axis represents the bit rate analysis communicated over the network. Figure shows that the communication is being increased over the networks without any interruption [15].
Fig. 21 Packet Loss Rate Analyses

Here figure 21 is showing the Packet Loss Rate Analysis over the network. Here X axis represents the simulation time and y axis represents the packet loss rate over the network. Figure shows, the as the cluster formation is done, the packet loss is increased initially after that as the route established no more packet loss occur. As the route reconfiguration over the network is performed, the packet loss occurs.

Fig. 22 Packet Delay Analysis

Here figure 22 is showing the Packet Delay Analysis over the network. Here X axis represents the simulation time and y axis represents the packet delay over the network. Figure shows, the as the cluster formation is done, the packet delay is increased initially after that as the route established no more communication delay.

V. CONCLUSION & FUTURE SCOPE

A MANET is the most busy and required public area network. The most challenging and important thing in mobile network is Mobility Vector, and Security. The function of the node is defined in the form of clustered mobile communication in real scenario. We use directional mobility model for communication over the mobile network. This is one of the effective ways for inter cluster and intra cluster communication over the network. It increases the performance and security of the network and at the same time reduces the packet loss rate. The proposed work includes the cluster based communication within the network for both inter and intra cluster communication. The intelligent cluster selection technique is defined based on throughput, capacity and idle rate based evolution and the work is done in NS2 environment. The analysis of work is done under different parameters such as packet transmission, loss rate, communication rate and communication delay. The protocol is used here is AODV.
Here we find the limitation of protocol in respective of the environment. In future, enhancements can be done in following ways:

- The work is here tested for directional mobility model; in future some other mobility models can also be implemented.
- In this work, the mobile network is considered. In future, PAN or the sensor area network can be considered.

References

[1]. www.google.co.in/cluster of mobile.


[15]. www.isi.edu/nsnam/ns/ the network simulator NS2.