Trust Worthy Architecture Implementation for Mobile Ad hoc Networks

D.Saravanan¹, R.M.Chandrasekaran², B.Vishnu Prabha³ and V.R.Sarma Dhulipala⁴

¹Assistant professor, Department of Computer Science & Engineering, Pavendar Bharathidasan College of Engineering & Technology, Tiruchirappalli, Tamil Nadu, India
²Email: dsarav23@gmail.com
²professor, Dept of CSE, Annamalai University, Chidambaram, Tamil Nadu, India
²Email: aurmc@sify.com
³Lecturer, Department of Computer Science & Engineering, JJ College of Engineering & Technology, Tiruchirappalli, Tamil Nadu, India
³Email: vishnuprabha@gmail.com
⁴Assistant professor (Physics), Center for Convergence of Technologies, Anna University of Technology, Tiruchirappalli, Tamil Nadu, India
⁴Email: dvrsarma@gmail.com

Abstract— A mobile ad hoc network is a wireless communication network that does not rely on a fixed infrastructure and is lack of any centralized control. The wireless and distributed nature of mobile ad hoc networks poses greater challenges like security, mobility, scalability, reliability and other attributes of trust worthy communication. In this paper we implemented a framework for mobile ad hoc networks by checking the simulation for various service metrics of mobile ad hoc networks. This framework implementation also provides optimum quality of service metrics, while being readily adaptable to widely differing applications, different hardware and software providers and changing technologies.

Keywords— MANET, Security, Mobility, Scalability, Reliability and Quality of Service.

I. Introduction

Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes spread over in the mobile ad-hoc environment that communicate with each other without any centralized access points, infrastructure, or centralized administration. Providing trust worthiness for a MANET is a major issue because of the dynamically changing network topology [1]. In this paper we provide an implementation of trust worthy architecture. Implementation provides trusted services, as well as protection of confidential information, secure communication, secure routing protocol usage, secured mobility model, reliable communication and provide optimum quality of service metrics for the mobile ad hoc networks. Mobile Ad-hoc Networks are more prone to physical threats because of the dynamically changing network topology [1]. The secure routing and key management mechanism are used to discover secure paths and subsequent communications [2]. Mobility is the major challenge in the mobile ad hoc environment because the mobile ad hoc node movements are varied time to time. We are not able to predict the movement pattern of the mobile node. For this above stated reason security in mobility is major challenge. In this paper we provide a complete security in mobility model selection by referring various developed ad hoc networks.
Fig. 1 Mobile Ad hoc Network Scenario

Fig. 1 shows the mobile nodes are spread over the mobile ad hoc environment. The node having higher network resources selected as a Trusted Authority. All mobile nodes in a mobile ad hoc network are registered with the trusted authority for node authentication.

II. Framework:

Trust worthy architecture consists of three modules and the architecture provides optimum quality of service metrics for the mobile ad hoc environment [14]. Trust evaluations are based on the direct and recommended trust held for one or more nodes involved in the context. We characterize open distributed-system network-oriented architectures capable of fulfilling critical security, mobility, reliability, scalability, and performance requirements, while being readily adaptable to widely differing applications, different hardware and software providers. A node's direct trust is based on the evidence captured by its security models during the one-to-one experiences with the other node.

Trust worthy architecture

Fig. 2 Trust Worthy Architecture
Trustworthy architecture consists of SMR model (security, mobility, reliability model for trust) and it provides trustworthy services, secure communication, secured mobility model, reliable communication and optimum quality of service metrics for mobile ad hoc networks.

III. Design of experiment

For the analysis, network simulator ns2 is used. Ns2 supports emulation with very less effort as it provides graphical analysis. Also execution time for the scenarios is less comparatively. For these reasons, network simulator ns2 was chosen for the experiments [2]. The mobile nodes were randomly distributed and follow random waypoint mobility model for routing packets from the source to the destination node. The below table simulation parameters define the parameters that are used in our simulation.

<table>
<thead>
<tr>
<th>Simulation Tool</th>
<th>Network Simulator 2 – ns2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrain Dimension</td>
<td>1500x1500</td>
</tr>
<tr>
<td>Mobile Nodes</td>
<td>5</td>
</tr>
<tr>
<td>Simulation time</td>
<td>200ms</td>
</tr>
<tr>
<td>Node level security</td>
<td>Authentication &amp; information encryption</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>Ad hoc On demand Distance Vector - AODV</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Waypoint</td>
</tr>
<tr>
<td>QOS Metrics</td>
<td>Good put, Delay, Hop count, Packet Delivery Ratio and Control Overhead</td>
</tr>
</tbody>
</table>

INPUT: \((n_1 \ldots n_i)\) - mobile nodes, N-Number of mobile nodes.
OUTPUT: G, D, HC, PDR and CO - good put, delay, hop count, packet delivery ratio control overhead respectively.

Fig.3 Steps involved in the implementation of TWA

IV. Models, Results and Discussion:

A. Security Model

Security is difficult to achieve in such networks as the networks are not conducive to centralized trusted authorities [3]. The security solutions that have been deployed for wired networks are not directly portable to ad hoc networks. The difficulty arises as a result of sporadic wireless medium, dynamic network topology and constraint battery resources. The security of the Trust Worthy architecture is achieved using key management mechanism between the sender and receiver [4]. Key exchange (symmetric and asymmetric) occurred only between the trusted parties. The framework only allows authenticated node to the further processing.
B. Node Authentication

Node authentication is performed using trusted authority registry. Trusted Authority (TA) authenticate the mobile node for communication. Functionalities of the TA for reliable communication are mobile node registration, certifying the mobile node for communication for saving network resources else the node has to check for authentication whenever the node starts communication. The trusted authority also monitors each and every mobile node in the trusted network.

Node Authentication:
1. Mobile node enter the mobile ad hoc network for communication.
2. Set T be the trusted authority (mobile node having higher resource)
3. Trusted authority (T):
   a. Mobile node registration.
   b. Certifying the mobile node for communication.
   c. Tracing the node behavior.

Fig. 4 Pseudo code - Node Authentication

The above pseudo code implementation provides five main security services for MANETs are Authentication, Confidentiality, Integrity, non-repudiation and availability.

Data Encryption E(n):

1. \( n=xy \& f(n) \) where \( p=x-1 \), \( q=y-1 \); \( x \) and \( y \) of bit length, e.g. 1024 bits
2. \( n=xy \& f(n)=pq \) where \( p=x-1 \), \( q=y-1 \) \( n \) is known as the modulus
3. Choose an integer \( e \), \( 1<e<0 \) (%(n)) such that \( \text{gcd}(e,f(n))=1 \)
4. Asymmetric key->(n,e) Symmetric key->(n,d)
5. Original information->m
6. Computes the encrypted information \( c=m^e \mod n \).
7. Send encrypted information to the receiver.
8. Use Symmetric key(n,d) to decrypt information by the receiver \( m=c^d \mod n \).

Fig. 5 Pseudo code - Data Encryption

C. Routing protocol

Secure ad hoc routing protocols (SAR) are used for routing packets. The position of the nodes cannot be determined. During data transmission, it is possible that the destination node may be several hops away from the source. So, the routing protocol to be used is selected dynamically. This selection depends upon the location of source and destination nodes. In this paper we are using AODV routing protocol for routing packets from source to the destination. In mobile ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks [3]. The attacks may include injecting erroneous routing information, replaying old routing information, and distorting routing information [5].

Selection of Secure Routing protocol (RP):

1. $r_1, r_2, \ldots, r_m$ Mobile ad hoc routing protocols like AODV, DSR, DYMO, ZRP
2. $\text{RP} \rightarrow \gamma_p \{r_1, r_2, \ldots, r_i\}$
   a. $\gamma_p(\cdot) \rightarrow \text{performance comparison of routing protocol}$
   b. Apply the routing protocol $\{r_1, r_2, \ldots, r_i\}$ to mobile nodes $(n_1, n_2, \ldots, n_i)$
   c. $\gamma_p \{r_1, r_2, \ldots, r_i\} = \text{routing protocol which provides optimum QOS metrics.}$
3. $\text{RP} = \text{AODV}_{\text{rp}}$

Fig. 6 pseudo code – selection of secure routing protocol

D. Mobility Model

The mobility model is designed to describe the movement pattern of mobile users, and how their location, velocity and acceleration change over time. The security in mobility model is urging because intrusion and malicious attacks are easily happened during the node movement in this paper we are using random way point mobility model [7] in which nodes move independently to a randomly chosen destination with a randomly selected velocity [7]. Prevention of intrusion, malicious attacks and flooding attacks are possible because the movement pattern is randomly selected from time to time [11].

Mobility Model (Mm) Selection:

1. $\text{Mm} = \eta_\{m_1, m_2, m_3, \ldots, m_i\}$
   a. $\eta(\cdot) \rightarrow \text{performance comparison of mobility model}$
   b. Apply the mobility model $(m_1, m_2, m_3, \ldots, m_i)$ to mobile nodes $(n_1, n_2, \ldots, n_i)$
2. $\text{Mm} = \text{Random waypoint Mm}$

Fig. 7 pseudo code – mobility model selection

Table II- Mobility

<table>
<thead>
<tr>
<th>Time in ms</th>
<th>Node position</th>
<th>Node position + Mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.6</td>
<td>(60,30)</td>
<td>(330,30)</td>
</tr>
<tr>
<td>1.1</td>
<td>(330,30)</td>
<td>(500,30)</td>
</tr>
</tbody>
</table>

Fig.8 Node Mobility (Random Waypoint)

Figure 8 represents the random waypoint movement pattern of the mobile node. Position of the node in the
network changes randomly in accordance with time.

E. Reliability Model

The number of packets received by different members of a group is highly variable [8]. Reliability model provides Reliable delivery of messages and Error free delivery of messages [4][9]. The trust worthiness of the MANET is achieved only through the reliable communication between the nodes in a mobile ad-hoc environment. The characteristic of Trust worthy Architecture such as security, mobility and scalability is validated only through the reliable communication [13].

<table>
<thead>
<tr>
<th>Time in ms</th>
<th>No of packets sent</th>
<th>No of ACK packets received</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.2</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>0.8</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>1.3</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

TABLE III- RELIABILITY

Reliable Communication Validation:
1. Reliable Communication under process
   a. Optimum QOS metrics \{G,D,HC,PDR &CO\} is obtained.
2. Else node id enter into the geographic hash table.

F. QoS Metrics for MANET

The optimum quality of service of the MANET is achieved only when the node and the ad hoc environment is trust worthy. Various QoS metrics [10] considered for the analyses are Good put, delay, PDR, control overhead, jitter and hop count [10]. The optimum quality of service of the MANET is achieved only when the node and the ad hoc environment is trust worthy. Various QoS metrics [10] considered for the analyses are Good put, delay, PDR, control overhead, jitter and hop count [10].
TABLE IV - QOS METRICS

<table>
<thead>
<tr>
<th>Node Id</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good Put</td>
<td>980</td>
<td>670</td>
<td>800</td>
<td>500</td>
<td>400</td>
</tr>
<tr>
<td>Average End-End Delay</td>
<td>250</td>
<td>200</td>
<td>76</td>
<td>45</td>
<td>30</td>
</tr>
<tr>
<td>Packet Delivery Ratio</td>
<td>750</td>
<td>512</td>
<td>478</td>
<td>289</td>
<td>180</td>
</tr>
<tr>
<td>Control Overhead</td>
<td>80</td>
<td>34</td>
<td>62</td>
<td>20</td>
<td>16</td>
</tr>
</tbody>
</table>

QOS METRICS

![QOS Metrics Graph]

Fig.11 QOS Metrics Analysis

G. Hop Count

Figure 12 shows HC, the number of jumps packets take to reach the desired destination from source.

TABLE V- Hop Count

<table>
<thead>
<tr>
<th>Node Id</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hops</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
V. Conclusion and Future work

In this paper we have proposed the trust worthy architecture for manet, then we showed the security, mobility, reliability (SMR) model and other metrics of trust are involved in the architecture to achieve the trust worthiness of the network. The goal of the our work is to provide the network designer to follow the architecture model with multiple views on concept of trust, realizing the parameters and metrics we introduced here, must be considered for the developing the trust worthy system for manet. By introducing the SMR model in the architecture, we hint the other researches to focus on developing the trust worthy architecture with some more suitable attributes like scalability, self-configurability and availability.

44References

