Trust Worthy Architecture Implementation for Mobile Ad hoc Networks

D.Saravanan[1], R.M.Chandrasekaran[2], B.Vishnu Prabha[3]and V.R.Sarma Dhulipala[4]

1Assistant professor, Department of Computer Science & Engineering, Pavendar Bharathidasan College of Engineering & Technology, Tiruchirappalli, Tamil Nadu, India
1Email: dsarav23@gmail.com
2professor, Dept of CSE, Annamalai Univeristy, 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.

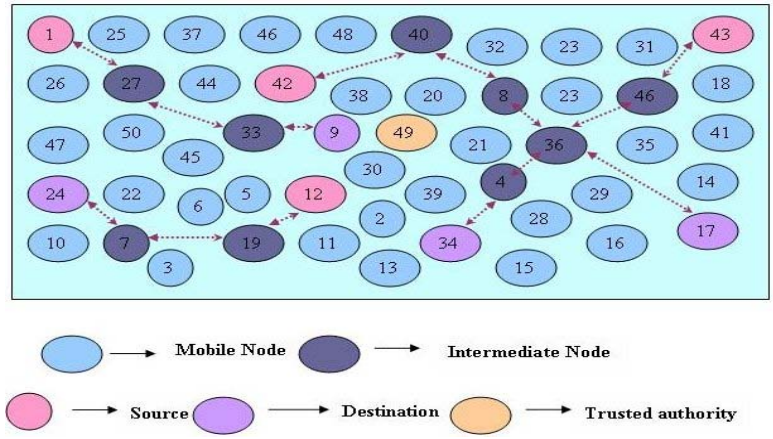

Fig.1 Mobile Ad hoc Network Scenario

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

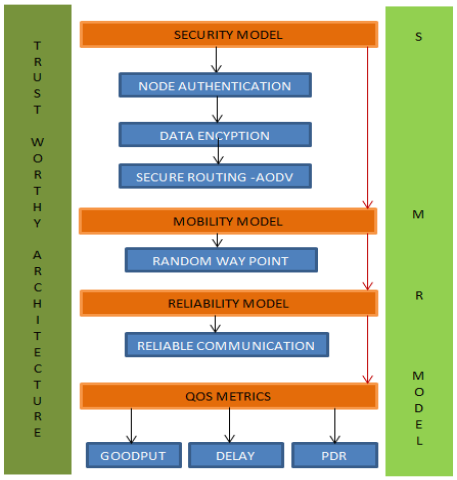

Fig .2 Trust Worthy Architecture

Trust worthy 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 I simulation parameters

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

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.

1. Node Authentication
2. Data Encryption E(n)
3. Selection of secure routing protocol (RP)
4. Mobility Model (Mm) Selection
5. Reliable Communication Validation
6. Go to the STEP 2 until network finishes the communication
7. Communication under process

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 start communication, The trusted authority also monitor the 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 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. RP-> γp { $r_1, r_2 \ldots r_i$}
   a. γp( )-> 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. γp { $r_1, r_2 \ldots r_i$}= routing protocol which provides optimum QOS metrics.
3. RP= AODV $_{rp}$;

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 of 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. Mm=$\eta\{m_1, m_2, m_3 \ldots m_i\}$
   a. η ( )-> 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. Mm= Random waypoint Mm

Fig.7 pseudo code – mobility model selection

Table II- Mobility

Time in ms	Node position	Node position + Mobility
0.6	(60,30)	(330,30)
1.1	(330,30)	(500,30)

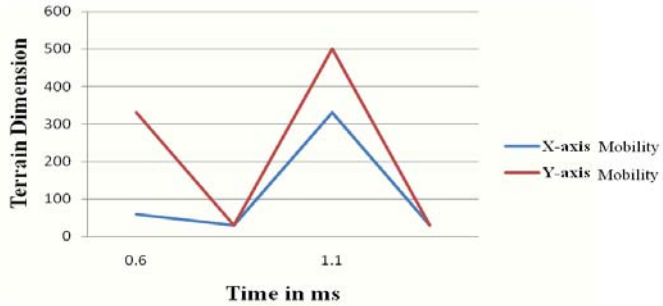

Fig.8 Node Mobility (Random Waypoint)

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].

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.

Fig.9 pseudo code Reliable Communication validation

TABLE III- RELIABILITY

Time in ms	No of packets sent	No of ACK packets received
0.2	13	13
0.8	16	16
1.3	12	12

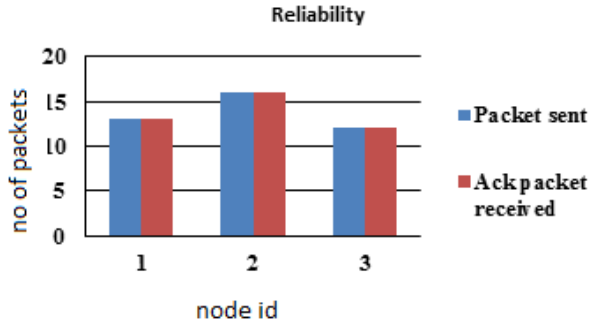

Fig.10 Reliability

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

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

QOS METRICS

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

Node Id	0	1	2	3	4
Hops	1	1	1	1	1

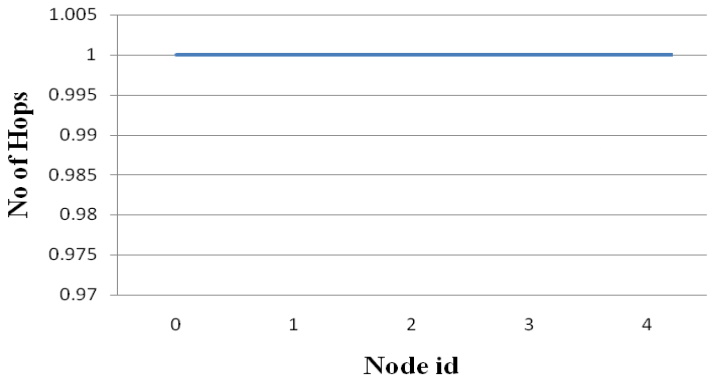

Fig.12 Hop Count

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

[1] Balakrishnan, V. Varadharajan, V. Tupakula, U. Lucs, P. Macquarie Univ., Sydney.: Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks. In IEEE Wireless Communication Systems ISWCS 2007. 4th International Symposium on Publication Date: 17-19 Oct. 2007 pp 592--596 (2007).

[2] In-Sung Han Jin-Mook Kim Hwang-Bin.: Service Discovery and Delivery System Based on Trust in Mobile Ad-Hoc Network. In Information Science and Security, 2008. ICISS. International Conference on Publication Date: 10-12 Jan.2008 pp 171--176 (2008).

[3] Balakrishnan, V. Varadharajan, V. Tupakula, U. Lucs, P. Macquarie Univ., Sydney.: TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks" In 15th IEEE International Conference on Networks, 2007. ICON

[4] 2007. pp 182--187 (2007).

[5] Celeste Campo, Florina Almenarez, Daniel Dıaz, Carlos Garcıa-Rubio, Andres Marın Lopez.: Secure Service Discovery based on Trust Management for ad- hoc Networks. In Journal of Universal Computer Science, vol. 12, publication date : 28 mar 2006 © J.UCS pp 340--356 (2006).

[6] Ngai, E.C.H. Lyu, M.R.: Trust- and clustering-based authentication services in mobile ad hoc networks. In IEEE 24th International Conference on Distributed Computing Systems Workshops, 2004. Publication Date: 23-24 March 2004 pp 582--587 (2004).

[7] Animesh Kr Trivedi1, Rajan Arora1, Rishi Kapoor, Sudip Sanyal1 and Sugata Sanyal : A Semi-distributed Reputation-based Intrusion Detection System for Mobile Adhoc Networks. In India Journal of Information Assurance and Security pp 265--274 (2006).

[8] Tracy Camp, Jeff Boleng, Vanessa Davies.: A survey of mobility models for ad hoc network research. In interscience conference on Wireless Communications and Mobile Computing Volume 2 Issue 5, Published Online: 11 Sep 2002

[9] Pages 483--502 (2002).

[10] Harbin, China, ISBN: 0-7695-3072-9.Alexandre Viejo, Francesc Seb´e and Josep Domingo-Ferrer.: Aggregation of Trustworthy Announcement Messages in Vehicular Ad Hoc Networks. In IEEE Vehicular Technology Conference, 2009. VTC Spring 2009.Publication Date: 26-29 April 2009 pp 1--5 (2009).

[11] Ranveer Chandra, Venugopalan Ramasubramanian, Kenneth P. Birman.: Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks. In 21st IEEE International Conference on Distributed Computing Systems , 2001 pp 275.(2001).

[12] R.Sivaraman, V.R.Sarma Dhulipala, L.Sowbhagya, B.Vishnu Prabha.: Comparative Analysis of QoS Metrics in Mobile Ad Hoc Network Environment. Accepted on Academy publishers IJRTE 2009 pp. 69--71(2009).

[13] V.R. Sarma Dhulipala, RM.Chandrasekaran, and R.Prabakaran, "Timing Analysis and Repeatability Issues of Mobile Ad-Hoc Networking Application traffics in Large Scale Scenarios", Anna University Tiruchirapalli / Center for Convergence of Technologies,

Tiruchirapalli, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, pages 463-467, Academy Publishers, May 2009.

[14] Khalaf. R, Rubin. I, "Throughput and Delay Analysis in Single Hop and Multihop IEEE 802.11 Networks Broadband Communications", 3rd International Conference on Broadband Communications, Networks and Systems, BROADNETS 2006, pages 1-9, Oct 2006.

[15] Ranveer Chandra Venugopalan Ramasubramanian Kenneth P. Birman "Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks "Department of Computer Science Cornell University, Ithaca, NY 14853, USA (2000).

[16] V.R. Sarma Dhulipala, B. Vishnu Prabha, and RM. Chandrasekaran "Trust Worthy Architecture for Mobile Adhoc Networks", CCIS 70, pp. 557–560, 2010, Springer-Verlag Berlin Heidelberg 2010