International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2015 Volume 2, Issue-3
Email: editor@ijermt.org www.ijermt.org

SECURING COMMUNICATION IN MANETS THROUGH TRUSTWORTHINESS USING NS2

Priyanka Garg
M.Tech Scholar, CSE Dept,
HEC, Kurukshetra University
Haryana, India

Ms. Pooja Narula
Assistant Professor CSE Dept
HEC, Kurukshetra University
Haryana, India

ABSTRACT:
The mobile ad hoc network is the fastest growing area of research in which the performance evaluation has its own place. The current and future applications forced the research community to look at the dependability and the security aspects as eavesdropping and jamming. MANET assumes that all nodes in the network are secure and they can communicate with each other securely. But actually the nodes are not secure. Therefore, the security in MANET is a main issue. In this paper, Trustworthiness and Intrusion Detection System are applied on the Ad-hoc on demand distance vector routing protocol (AODV). This scheme increases the Packet Delivery Ratio (PDR) and decreases delay. The work is implemented and simulated on NS2.

KEYWORDS: MANET, AODV, IDS, PDR.

INTRODUCTION:

A mobile ad hoc network (MANET) is a collection of mobile computers or devices that cooperatively communicate with each other without any pre-established infrastructures such as a centralized access point [1]. Existing routing protocols use the shortest path to select the route for the communication. AODV is one of the routing protocols which use the shortest path as their route selection criterion. Sometimes the shortest path selected for communication is not secure. There may be malicious nodes exist in the path. The path may not be best due to congestion in the network. The source does not have any information about the secure but the route reply contains information about number of hops, route freshness, sequence numbers, id of source and destination. Therefore, the security is a main concern in AODV routing protocol. [2]

In our work to be described in the thesis, we focused on designing a secure routing mechanism for MANET. Our solution is introducing the trustworthiness and IDS on the routing protocol. When the combination of both is applied on the routing protocol then the communication may be a secure communication.

Trustworthiness is a scheme in which the communication is based on the trust value. The trust value is calculated on the basis of how many times the route is used for communication. If the route is used for more number of times then the trust value is high and that path is used for the communication i.e. Nodes are allowed to participate in routing based on their trust values.

Intrusion Detection System is a system which is used to detect the intrusion in the system. Intrusion Prevention is almost impossible to achieve all the times. Hence, more focus is on Intrusion Detection. Therefore, the only functionality of IDS is to detect the intrusion not prevention. Intrusion Detection gathers the data from system operation at run time. IDS can be classified into three broad categories: anomaly-based detection, signature-based detection, specification-based detection.

VULNERABILTIES IN MANET

Vulnerability means weakness in the security system. The mobile ad-hoc network is more vulnerable than the traditional wired networks. Therefore, the security is more difficult to achieve in the wireless networks.

Various vulnerabilities in mobile ad-hoc networks are as follows:

- **LACK OF CENTRALIZED MANAGEMENT:**
  Due to the lack of centralized management facility, the attacks are difficult to detect because in highly dynamic and large scale networks, the traffic is very difficult to monitor. Therefore, the malicious activities are difficult to detect. Lack of centralized management facility will impede the trust management for the nodes in the ad hoc network [5].

- **NO PREDEFINED BOUNDARY:**
  In mobile ad-hoc network, the physical boundary inside the network cannot be defined. Due to the absence of boundary, the nodes have freedom to join, leave and move inside the network.
  Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks [5]. There are various attacks which include tempering, replay and Denial of Service (DoS) attack [6].

- **RESOURCE AVAILABILITY:**
  Resource availability is a major issue in MANET. In such challenging environment, it is difficult to provide secure communication and protection against threats and attacks. However, this lead to security techniques and architectures which can protect against threats.

- **LIMITED POWER SUPPLY:**
  Due to the mobility of nodes in the network, the nodes consider that there is restricted power supply in the network. However, the wired networks have infinite power supply because they can get electric power supply from the outlet.
  The limited power supply causes the problem of denial of service (DOS) attack. Since the attacker knows that the target is battery restricted, it can send the large number of packets by which the target will trap in time consuming tasks and it will go out of service because it has out of power.
  When the node finds that there is a limited power supply, it may behave in a selfish manner.

- **SCALABILITY:**
  Since in MANET, the nodes are mobile. Due to the mobility of nodes, the scale of nodes keeps changing all the time i.e. it is difficult to predict how many nodes are there in the network. However in the traditional wired networks, the nodes in network are predefined. Therefore, scalability is a major issue. Hence concerning security, it is difficult to handle large networks as compared to small ones.

PROPOSED WORK:

1. **MOTIVATION**:
   The Mobile Ad hoc Network performs differently according to situations and environment. The nature of self-organization and the limitation of individual resources, MANET always confront security and selfishness issues. Studying these issue possess by trustworthiness of MANETs provides a great knowledge and motivation to do the research work in this field.

2. **FORMULATION OF PROBLEM:**
   MANET is a collection of wireless mobile nodes that communicate with each other using multi-hop wireless links without any existing network infrastructure or centralized administration .Each node in the network behaves as a router and forwards packets for other nodes. MANET assumes that each node in the network is trustworthy. Due to this reason it is vulnerable to various attacks. So in order to study the effect of different attacks on this network formulation would be executed with the OTCL language and data will be analyzed by NS2

3. **SECURITY GOALS:**
   Security services include the functionality required to provide a secure networking environment. The main security service can be summarized as follows:

- **AUTHENTICATION:**
  This service verifies user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each entity is what it tells. And next, it must assure that the third party doesn't interfere by impersonating one of the two authentic parties for the purpose of authorized transmission and reception.

- **CONFIDENTIALITY:**

This service ensures that the data transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques.

- **ACCESS CONTROL:**
  This limits and controls the access of such a resource which can be an application or a host system.
- **INTEGRITY:**
  The function of integrity control is to assure that the data is received in verbatim as sent by authorized user. The data received contains no modification, deletion or insertion.

4. PROBLEM DEFINITION:

A Mobile Ad hoc Networks (MANET) is an autonomous collection of mobile nodes and there is no fixed infrastructure, so it is more vulnerable to attack and the problems related to the routing and security. Security is a primary concern in almost all the application scenarios and in order to provide the secure communication between the mobile nodes. The open and dynamic nature of MANET makes it more vulnerable to attacks and cripples many MANET operations. Security plays an important role in mobile Ad hoc networks because of its inherent vulnerabilities.

The research problem is how to provide security protection to the network. The major challenges include dynamic topology, decentralized control, limited resources, and the lack of information dissemination control.

So to overcome these problems every node must have some capability to trust another node in order to save its time, battery, bandwidth and other non-renewable resources. In this dissertation we tried to develop such a trust value in each node of the network node, so that every node can confidently forward its data packet to the next node in the network. For this we use intrusion detection system to find a threshold value a node has to have trust.

5. PROTOCOL USED IN SIMULATION:

AODV: AODV is basically an improved DSDV. AODV is a reactive self- starting and large scale routing protocol [7]. It basically works on two terms i.e. Route Request (RREQ) and Route Reply (RREP). In AODV, mobile nodes quickly obtain the routes for new destination. AODV avoids the Bellman-Ford "counting to infinity" problem and the operation of AODV is loop-free.

AODV maintains the routing table which carries six terms:

- Destination IP address
- Source IP address
- Broadcast-ID
- Source Sequence Number
- Destination Sequence Number

The process of communication in AODV is that when the source node wants to send the data to the destination node, the RREQ message is broadcasted. The neighbouring nodes broadcast its message to their neighbours and the process continues until the message is received by the destination. Each neighbour sends the route reply message (RREP) to the source. The reply is sent using the reverse path [1, 8, 9].

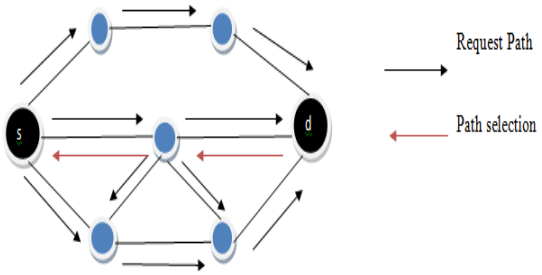


Fig. 1 AODV Communication Process

6. METHODOLOGY:

The proposed scheme consists of three modules. Firstly, we assume the existence of centralized intrusion detection system, which is responsible for calculating the trusted threshold value and broadcast it to each node in the network. Now every node must know its neighbour's average packet received (trust value (TV)). Now the when a node wants to communicate with other node it broadcast route request procedure according to following algorithm. Then in return the reply is send according to the route reply algorithm by checking its threshold value.

6.1 FLOWCHART DESCRIPTION:

We assume that:

a. Each node in the network has the ability to recover all of its neighbors;

b. Each node in the network can broadcast some essential messages to its neighbors with high reliability;

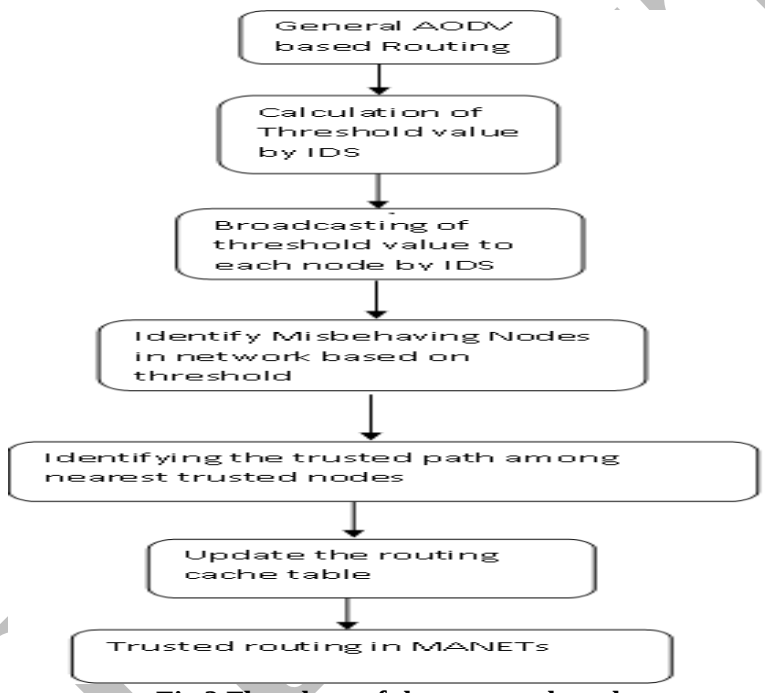


Fig.2 Flowchart of the proposed work

6.2 ALGORITHMIC DESCRIPTION:

ASSUMPTIONS:

1.Presence of centrally controlled intrusion detection system.

a. Ability to sense the presence of each node.

b. Avg_packet_reeived% is calculated by IDS.

c. Trusted Threshold Value (TTV) = Avg_packet_reeived%.

2. Now route from source to destination is not selected on shortest path bases but on best possible path bases.

3. Threshold value is broadcasted to every node in the network.

I) DIFFERENT APPROACHES FOR RESULT ANALYSIS

PARAMETER	VALUE
Traffic Type	TCP
Number of Nodes	25, 50, 75, 100
Area Covered	1000 X 1000
Speed of the Node's	1,2 m/s
Routing Approaches	AODV, TAODV
Mobility Type	Critical Mobility

Result analysis is a critical component of systems researches that allows evaluation of new ideas and methodologies, identification of problems and bottlenecks and optimization of existing system. There are three approaches to result analysis:

- **PROTOTYPING**

In prototyping we need to build a system and see how it works. Prototyping is not feasible and is time consuming especially for large scale systems. It also provides controllability and observability.

- **ANALYTICAL**

In analytical approach we build a software model of the system. It has emerged as an attractive alternative that is heavily used in result analysis of computer systems.

- **NETWORK SIMULATOR**

Trace support NS is a discrete event driven and object oriented network simulator developed at UC Berkely written in OTCL and C++. It implements the networking protocols such as UDP and TCP, traffic source behavior such as FTP, Web, Telnet, VBR, and CBR, queue management mechanism such as RED, Droptail and CBQ. It also supports for simulation of multicast protocols over wired and wireless (local and satellite) networks.

NS-2 is a discrete event network simulator in which physical activities are translated to events; events are processed in the order of their occurrences. The simulation time is progressed with the events getting processed. Typically, it can configure transport layer protocols, interface queues, routing protocols and also link layer mechanisms. We can easily see that NS2 provide us a whole view of the network construction and also maintains the flexibility for the user to decide or check. Thus, just this one software can help us simulate nearly all parts of the network. This definitely will save us great amount of cost invested on net work constructing.

1. SIMULATION ENVIRONMENT

Table1: Parameters for Simulation Environment

Here the basic parameters of the proposed approach are presented respective to the simulation environment. The approach is implemented with NS2 simulator and the graph is used as the tool for the analysis.

The mobile Adhoc network of 25, 50, 75, 100 nodes is constructed in the NS2 with the boundary area of 1000m X 1000m with the use of TCl script. The nodes are mobile with the initial energy, speed and threshold energy as shown in the table. AODV and TAODV routing protocol is used here as the protocol for the analysis.

2. SIMULATION ANALYSIS

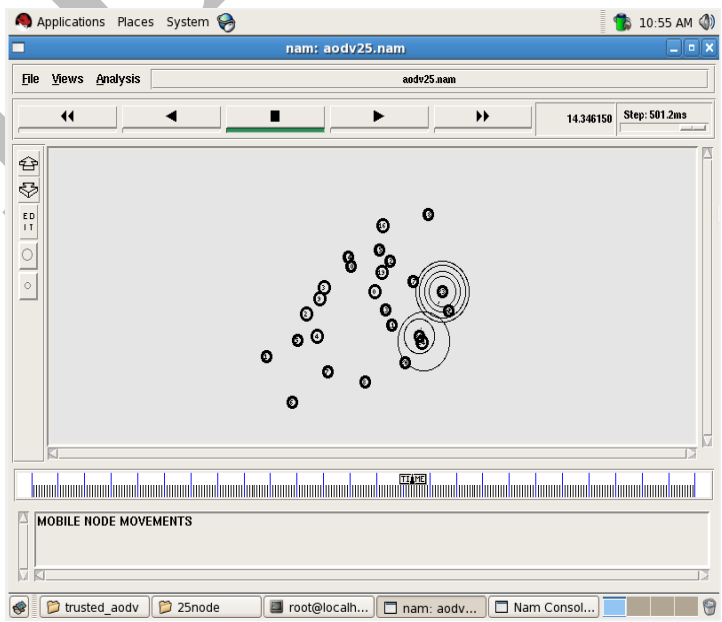
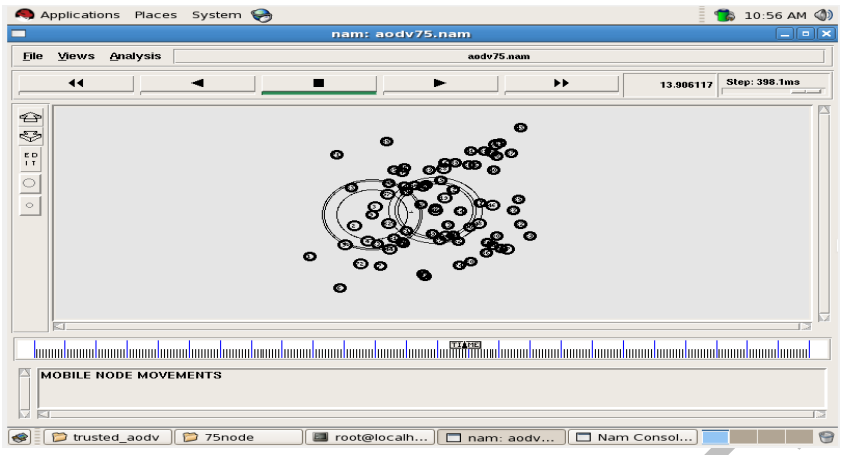


Fig.3: Animation of simulation for 25 node s

Fig.5: Animation of simulation for 75 nodes



II) RESULTS

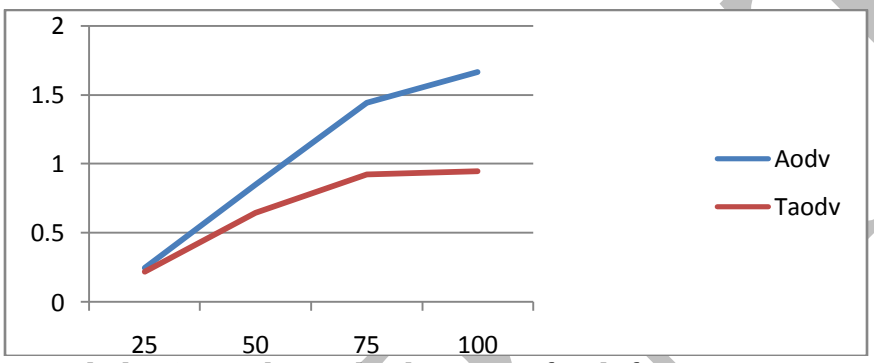


Fig.7: Graph showing End to End Delay vs no. of node for 25, 50, 75, 100 nodes

The above compared end to end delay is of the scenario's when of AODV and TAODV protocols. Here we can clearly see the performance of TAODV is better as compared to AODV protocol.

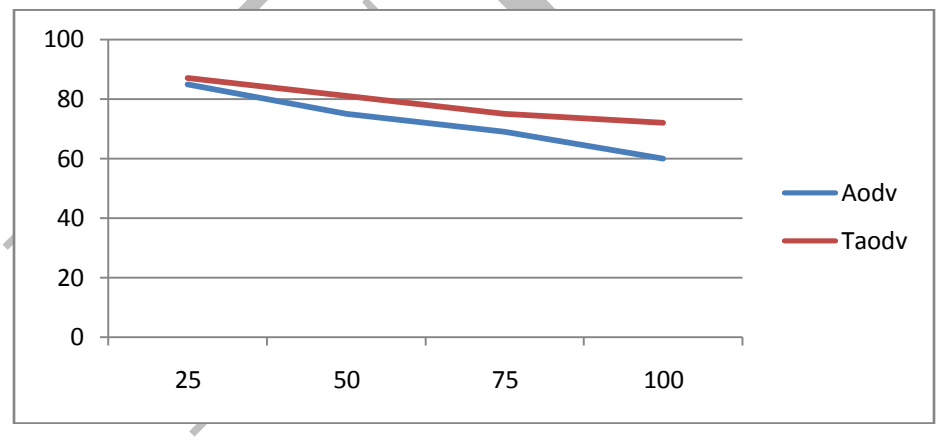


Fig.8: Graph showing comparison packet delivery ratio percentage vs no. of node for 25, 50, 75, 100 nodes.

The above graph shows the packet delivery ratio percentage vs no. of nodes for 25, 50, 75, 100 nodes with AODV and TAODV protocols. Here, we can clearly see that performance of TAODV is better than simple AODV protocol.

CONCLUSION:

In this paper, we propose a trustworthy approach to provide efficient communication in the network. The effectiveness of the proposed technique depends on the assumption that initially, IDS work efficiently and calculate a trusted threshold value. We assume the presence of a centralized intrusion detection system, which is responsible for distributing the calculated trusted threshold value in the network. This research addresses related works on security issues and trust establishment schemes. A proposal to effectively proving trust factor for efficient communication in the network using AODV Protocol is discussed. A better understanding and modeling of the security attacks is needed in MANETs if efficient secure routing algorithms are to be built in the network.

REFERENCES:

1. Chin-Yang Tseng, Poornima Balasubramanyam, Calvin Ko, Rattapon Limprasittiporn, "A Specification-based Intrusion Detection System for AODV", University of California.
2. Kamal Deep Meka, Mohit Virendra, Shambhu Upadhyaya, " Trust Based Routing Decisions in Mobile Ad hoc Networks", State University of New York at Buffalo, New York.
3. ankaj Sharma , Yogendra Kumar Jain, "Trust based secure AODV in MANET", JGRCS, Volume 3, No. 6, June 2012.
4. Jimmi Gronkvist, Anders Hansson, and Mattias Skold, "Evaluation of a Specification-Based Intrusion Detection System for AODV", The Sixth Annual Mediterranean Ad Hoc Networking WorkShop, Corfu, Greece, June 12-15, 2007.
5. Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks", University of Maryland.
6. Priyanka Goyal, Vinti Parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM, Vol.11, January 2011.
7. Taneja, S., and Kush, "A Survey of routing protocols in mobile ad hoc networks", International journal of innovation management and technology.
8. Amit Shrivastava, Aravinth Raj Shanmogavel ,Avinash Mistry, Nitin Chander , Prashanth Patlolla, Vivek Yadlapalli, "Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols ",Department of Computer Science, Lamar University.
9. Charles E_ Perkins and Elizabeth M. Royer," Ad_hoc On Demand Distance Vector Routing" ,University of California.
10. Adnan Nadeem, Michael Howarth, " A Generalized Intrusion Detection & Prevention Mechanism for Securing MANETs".
11. Yinghua Guo, Steven Gordon, "Ranger, a Novel Intrusion Detection System Architecture for Mobile Ad Hoc Networks".
12. Ajay Jangra, Nitin Goel, Priyanka & Komal Bhatia: "Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture".
13. C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols", Pearson Education, New Delhi, 2004
14. Kamal Kant & Lalit K. Awasthi "Unicast and Multicast Routing Protocols for MANETs: A Comparative Survey".
15. Dalip Kamboj and Pankaj Kumar Sehgal, "A Comparative Study of various Secure Routing Protocols based on AODV", International Journal of Advanced Computer Science and Applications,Vol. 2, No. 7, 2011, pp 80-85.
16. G.S. Mamatha and Dr. S. C. Sharma, "A Highly Secured Approach against Attacks in", International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010, pp 815-819.
17. Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443.