ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Detection of Routing Misbehaviour in MANET using the Trusted AODV Protocol

Poorva P.Joshi[1], AjitKumar R.Khachane[2]

PG Student, Information Technology, Vidyalankar Institute of Technology, Wadala, India [1]

Professor, Information Technology, Vidyalankar Institute of Technology, Wadala, India [2]

Abstract: A Mobile Ad-hoc Network is a Decentralised Network and is a group of mobile nodes that are dynamically and arbitrarily located in such a way that the interconnections between the nodes keep on changing continuously such a decentralised network is not secure and can face many security issues one of them is attack by malicious nodes in the network, Such an attack is serious threat in MANET. The performance of AODV and Trusted AODV without any malicious nodes in the network was analysed earlier. The malicious nodes can attack can attack the control packet and misbehave in the Network. This paper introduces a trusted path irrespective of the longest or the shortest path which is capable of detecting the malicious nodes in the Network. Further the performance of Trusted AODV and General AODV with malicious activities is analysed which results that the Trusted AODV detects the malicious nodes in the Network and its performance is better as compared to AODV giving satisfactory Results.

Keywords: Trust, TAODV, malicious-nodes, MANET

I. INTRODUCTION

An ad-hoc network comprises of mobile nodes that cooperate with each other using wireless connections to route both data and control packets within the network. They are characterized by the use of wireless links, dynamically changing topology, multi-hop connectivity and decentralized routing mechanism and decision making.[1] Mobile ad hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology. [2] The primary goal of MANET is to find an end to end path or route, minimizing overhead, loop free and route maintenance.[11]The nodes in the network act as a host as well as a router but the network topology is dynamic because the nodes keep on changing their positions in the network. The ad-hoc networks are more vulnerable to threats as compared to traditional networks due to lack of infrastructure. A malicious node can be threat to route discovery process and the data forwarding phase of the routing protocol if it is not secured.[3] We design our secure routing protocol based on Ad hoc On-demand Distance Vector (AODV) routing protocol The new protocol, called TAODV (Trusted AODV), has several salient features: Nodes perform trusted routing behaviour mainly according to the trust relationships among them; A node who performs malicious behaviour will eventually be detected and denied to the whole network[4] This protocol TAODV (TrustedAODV) extends the widely used AODV (Ad hoc On demand Distance Vector) routing protocol and employs the idea of a trust model to protect routing behaviour in the network layer of MANETs[8]

II. LITERATURE SURVEY

Mobile ad-hoc Network is capable of Independent operations which operates without base station infrastructure nodes cooperate with one another to provide connectivity in the network and operates without Centralized administration. The ad-hoc networks do not have any fixed infrastructure here the nodes depend on each other to keep the network connected. Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel. We do not concern the security problem introduced by the instability of physical layer or link layer [8] Here are some assumptions for the Network 1.Each node in the network has the ability to recover all of its neighbours; 2.Each node in the network can broadcast some messages to its neighbours with high reliability; 3.Each node in the network has a unique ID, the physical network interface address that can be distinguished from others. In MANETs, an untrustworthy node can wreak considerable damage and adversely affect the quality and reliability of data. [10].The proposed scheme Trusted AODV assures that the data packets are not handled over to the malicious nodes. Based on the trust value a node is selected to perform packet transfer. This Proposed protocol results in higher percentage of successful data delivery compared to AODV.[3] Two new control packets are added to AODV protocol i.e. trust request packet(TREQ) and trust reply Packet (TREP) and routing table is modified by adding one new field: route trust. The RREP packet of AODV is also modified by extending two new fields: neighbour list and route trust.[9] By Implementing the Proposed Trusted AODV routing Protocol the following changes to the earlier implemented results can be obtained. The Normal AODV is largely affected by the malicious activities in the Network but The Trusted AODV is just affected partially as by time the selfish node will be identified and weeded out of the network.[3]

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

III. TRUSTED AODV

Ad-hoc network consists of mobile nodes which are randomly scattered within the network. The main aim is to mask the route path between the source and destination from all the other nodes, so as to avoid any kind of directed attacks[12]. In this work the AODV routing protocol is embedded along with the trust function. The communication between the nodes in the mobile Ad-hoc network depends on the cooperation and the trust level with its neighbours.[6].They are characterized by the use of wireless links, dynamically changing topology, multi-hop connectivity and decentralized routing mechanism and decision making.[1].Each node in the Network is assigned with a trust value which is used further in the entire communication process in the network. The following are the steps in the algorithm which are used to detect the malicious nodes in the Network making it more secure.

Step 1:-
Initially trust value is assigned to all nodes in the network Using trust value ( ).

Step 2:-
Source node broadcast request to all its neighbouring node using SRREQ().In this function hop count is initialized. Scheduler class is invoked to run the simulation.

Step 3:-
Neighbouring node receives the request then it will check whether if it is destination node or not. If it is Destination node then it will check for the trust value specified by the source node in the packet's information and will communicate with a SREP( ) otherwise forward request to its neighbouring node. This will check in RREQ( ) function.

Step 4:-
After confirming that it is not destination, it will further forward request to all its neighbouring node using FREQ( ) . Hop count is increased at each node.

Step 5:-
If there is any malicious node in the network the intermediate node will check with its trust value. If the trust value of the malignant node is below the specified threshold trust value that the network assigned to all the nodes .There is no packet loss but the malicious nodes is weeded out of the Network and the communication continues.

Step6:-
The Intermediate node will continue to FREQ() to all the Neighbouring node

Step 7:-
If it is destination and the trust value is matched then its sends reply using SREP() Trust value is updated for all nodes in the path from destination to source node. Here the Source node becomes destination for the current node.

Step 8:-

8.1 After receiving the reply then the decision will be taken whether the index node is destination or not using RREP( ).

8.2 If it is not destination then it will forward reply till if find its destination.

IV. SIMULATION RESULTS

4.1 Simulation Environment:

The evaluation of performance of MANETs routing Protocols TAODV and AODV are based on following metrics.

Simulation environment is as follows:

Parameter	Value
Network Area	800m*800m
No of Nodes	30,50,75,80,90,120
Routing Protocol	TAODV,AODV
Traffic type	CBR
Simulation time	50sec
NS2 Version	2.34
Transmission range	100meters

4.2 Analysis and Results Comparison:

In this section we evaluate the performance of TAODV and AODV protocols on the following parameters:

4.2.1 **Packet Delivery Ratio /Packet Delivery Fraction (PDR/PDF):**

The ratio between the number of packets that are received and the number of packets sent. The Greater the value of PDR means Better performance of the protocol

No of Nodes	PDR for TAODV	PDR for Normal AODV
30	85.7865	99.4975
50	81.1881	61.809
75	85.57	60.8247
80	73.399	61.3065
90	72.7723	60.9137
120	43.4783	4.92611

TABLE 1: PDR for Manet's routing Protocols

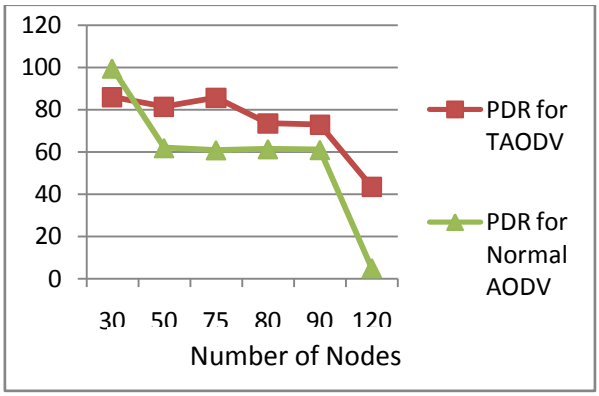

Figure 1: Comparison of the protocols of MANETs with respect to PDR.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

4.2.2 **Routing Overhead (ROH):**

The routing overhead measures by the total number of control packets sent divided by the number of data packets delivered successfully.

No of Nodes	Normalised Routing Overhead TAODV	Normalised Routing Overhead Normal AODV
30	10.0296	0.30303
50	16.5732	1.11382
75	23.6628	1.52542
80	30.5638	1.80328
90	33.3265	2.00833
120	71.8889	17.9

TABLE 2: Routing Overhead for Manet's routing Protocols

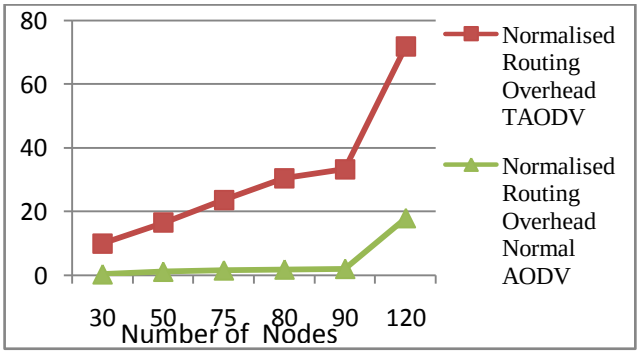

Figure 2: Comparison of the protocols of MANETs with respect to ROH.

4.2.3 **Throughput:**

Throughput is the total of all bits (or packets) successfully delivered to individual destinations over total-time / total time (or over bits-total / total time) and result is found as per KB/Sec.

No of Nodes	Throughput TAODV	Throughput AODV
30	17998.3	21135
50	17511.9	13135.1
75	18330.1	12575.9
80	15858.2	13024.1
90	15649	12796.2
120	9592.67	1065.44

TABLE 3: Throughput for Manet's routing Protocols

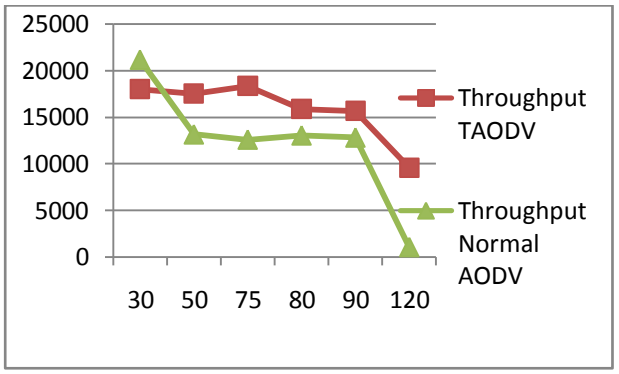

Figure 3: Comparison of the protocols of MANETs with respect to Throughput

4.2.4 **Packet Dropping ratio:**

Packet loss occurs when one or more packets of data travelling across a network fail to reach their destination.

No of Nodes	Packet Drop TAODV	Packet Drop AODV
30	14.2132	0.502513
50	18.8119	38.191
75	14.4279	39.1753
80	26.601	38.6935
90	27.2277	39.0863
120	56.5217	95.0739

TABLE 4: Packet Drop for Manet's routing Protocols

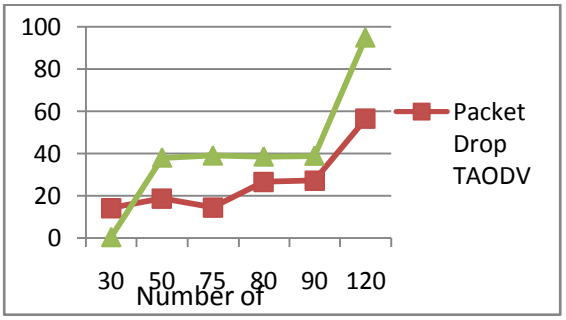

Figure 4: Comparison of the protocols of MANETs with respect to Packet Drop.

V. CONCLUSION

The Simulations Results shows that the Performance of Trusted AODV Routing protocol for MANET gives satisfactory Results than the Normal AODV protocol. Trusted AODV also detects the malicious nodes in the Network and weeds them out of the Network without affecting the whole network. The future Enhancement for the work would be to compare the other protocols using the Concept of Trust

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

ACKNOWLEDGMENT

I would like to sincerely thank to Prof AjitKumar R.Khachane for his expert guidance and timely inputs..

REFERENCES

[1] Improving Route Selection Mechanism using Trust Factor in AODV Routing Protocol for Manet by R. S. Mangrulkar Assistant Professor. B.D.College of Engineering, Sevagram, Wardha, Maharashtra, India Pallavi V Chavan Assistant Professor. B.D.College of Engineering, Sevagram, Wardha, Maharashtra, India.

[2] A Survey and Comparative Study Of Ad-hoc Routing Protocols in Mobile Ad-hoc Network Prof. AjitKumar R.Khachane1, Poorva P. Joshi2 1Associate Professor, 2Student, Information Technology Dept., Vidyalankar Institute of Technology, University of Mumbai, (India).

[3] Effect of Malicious Nodes for MANET Protocols Poorva P.Joshi1, AjitKumar R.Khachane2 *1*PG Student, Information Technology, Vidyalankar Institute of Technology, Wadala, India1 .*2*Professor, Information Technology, Vidyalankar Institute of Technology, Wadala, India2.

[4] TAODV: A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks

[5] Trust Based Adaptive on Demand Ad Hoc Routing Protocol Rajiv K. Nekkanti Computer Science Dept, Auburn University, Auburn, Alabama Chung-wei Lee Computer Science Dept, Auburn University, Auburn, Alabama – 36830

[6] Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing Ashish Sharma 1, Dinesh Bhuriya 2 , Upendra Singh 3 , Sushma Singh 4 1 HOD Govt. Women's Polytechnic, Indore 2 Lecturer Govt. Women's Polytechnic, Indore 3,4 SGSITS-INDORE.

[7] COMPARATIVE analysis of trust based and intrusion based black hole prevention in aodv in manet rajshekhar tiwari & manish sharma Department of Electronics & Communication Engineering, Sanghvi Institute of Management & Science, Indore, Madhya Pradesh, India

[8] A Trust Model Based Routing Protocol for Secure Ad Hoc Networks Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu Department of Computer Science and Engineering The Chinese University of Hong Kong Shatin, N.T., Hong Kong

[9] A SURVEY ON TRUST BASED SECURE ROUTING IN MANET Mousumi Sardar1 and Koushik Majumder2 Department of Computer Science & Engineering, West Bengal University of Technology, Kolkata, India

[10] Trust based Ad hoc On-demand Distance Vector for MANET Yogendra Kumar Jain Pankaj Sharma Head of Department Department of Computer Science & Engineering Department of Computer Science & Engineering Samrat Ashok Technological Institute Samrat Ashok Technological Institute Vidisha, M.P., India Vidisha, M.P. ykjain_p@yahoo.co.in

[11] QOS Assertion in manet routing based on trusted aodv (st-aodv) Sridhar Subramanian1 and Baskaran Ramachandran2 1Department of Computer Applications, S.A.Engineering College, Chennai, India. 2Department of Computer Science & Engineering, CEG, Guindy, Anna University,Chennai India.