Detection and Prevention for Jamming Attack in MANET using TAODV Protocol

Soneram verma[1], Prof. Maya Yadav
Pursuing M.Tech[1], Asst. Professor[2]
Sanghavi Institute of Management and Science,Indore (M.P), India
sims0837@gmail.com

---***---

Abstract -*MANET (Mobile Ad Hoc Network) could be a collection of self configurable mobile nodes wherever every node acts as a router for different nodes, which permits knowledge to travel, utilizing multi-hop network paths. MANETs are vulnerable to various attacks in the least layers, because the design of most MANET routing protocols assumes as if there is no malicious intruder node within the network. The main aim of this work is to develop trust based on-demand routing protocols for knowledge transmission below jamming attack in MANET. The proposed protocols should be efficient in terms of Packet Delivery ratio, End-to-End Delay, normalized routing load (NRL), Residual Energy and Throughput. Based on the motivations to produce new security measures to be incorporated in popular routing protocols AODV, the aim of this work has been implement secure on-demand routing (TAODV) protocols for data transmission in MANET and detect jamming node in MANET scenario using TAODV protocol. Also Prevent the network from jamming attack and improve the packet delivery fraction, throughput and end-to-end delay, normalized routing load, Residual Energy even with the presence of jamming attacks. The results of both AODV and TAODV compare to analyze that of those 2 types of protocols provides higher performance.*

***Key Words*:*Keywords*:- Mobile Ad-hoc Network (MANET), NS-2.35, jamming attack, AODV and TAODV routing protocol.**

1.INTRODUCTION

Emergence of moveable wireless communication devices and ascension in cellular technology have created mobile ad hoc networks (MANET) widespread in civil and military applications. The interest in ad hoc networks stem from its ability to produce instant networking resolution in an area wherever the cellular infrastructure is either very costly or impossible to deploy. MANETs will be deployed while not the necessity for any mounted infrastructure like base stations. Nodes in MANET assemble among themselves to determine the network dynamically. They act as a source similarly as router. As a resource they generate the packet and as a router they forward the packet. Packets are transmitted from source to destination in multihops. MANETs has tremendous applications each in military and civil (medical, mobile computing, disaster recovery) [7]. Applications of MANET depend on the effectiveness of routing protocol. Nodes in MANET are high-powered by electro-chemical batteries whose capability is restricted. Service and/or replacement these batteries might not be possible.

1.1 Related work

A malicious or venomous node can continuously transmit a radio signal with the purpose to block any type of legitimate access to the medium or infer with the reception. This phenomenon is termed as jamming and the existing malicious node are termed as jammers. The messages can easily be corrupted by jamming or interfering with the Radio signals. A powerful transmitter is a vital tool that is required by the attacker to generate strong signal that has the potential to thrash the targeted signals and obstruct communications. Jamming attacks can be mounted from a remote location to the target networks. Signal jamming could be in the form of random noise and pulse.

Jamming is actually a type of DOS attack where malicious node aims at determining frequency of communication so as to launch this attack. Jammer along with the security threats transmits signals and thereby leads to prevention of legitimate packets [11]. There aredifferent types of jamming attacks such as trivial jamming attacks, periodic jamming attacks and reactive jamming attacks.

Jamming is a serious hazard, in this attack a jamming node falsely advertise shortest path to destination node and drop all data packet in it. In this work, we have surveyed and find out the malicious nodesrelated problem in MANET in terms of increasing end to end delay. Also, we have surveyed and compare the existing solution to jamming attack on AODV protocol and their demerit.

2. Proposed methodology

The following flow of steps is the detailed description of the TAODV algorithm.

Step 1: Nodes are connected with each other for relaying messages in mobile ad-hoc network. Every node is initialized with Trust index=0.5.

Step 2: Source node transmits the route request packet to its neighbor nodes for relaying messages to the destination.

Step 3: Neighbor node first checks the route in its cache memory, if it exists, then it sends a route reply to the source node.

Otherwise, intermediate nodes send same route request to its neighbors and further to other intermediate nodes until the destination is found.

Step 4: When a route reply message is received from the neighbor nodes. Source node first checks sequence number and trust index of replying nodes, and select the highest reputed node for relaying messages.

Step 5: Source node transfers the message through the selected neighbor nodes.

Step 6: If a message is delivered correctly then the trust value of the neighbor is increased If not delivered then the trust value isdecreased.

Step 7: All the nodes having trust index less than 0.5 are termed as jamming nodes and these nodes are black listed.

Most Reliable	Unrealiable	Reliable	Action		Action
		≥0.5	Request and check again		
	<0.5		Disbelief the node		
>0.5			Trusted node		

3.Simulation andResults

3.1. Simulation results for packet delivery ratio

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Packet delivery ratio under Jamming attack detection and its prevention through Trust based mechanism i.e. Attack, pre (prevent) and without attack for the various node density

$$\text{Packet Delivery Fraction} = \frac{\text{Total No. of Packet Receiv}}{\text{Total No.Packet Send}}$$

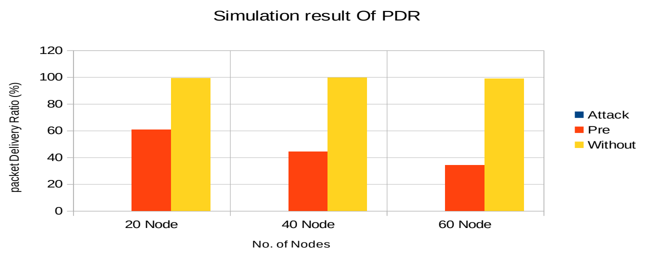

Figure:3.1 Packet Delivery Ratios comparisons

3.2 Simulation results for throughput

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Throughput under jamming attack detection and its prevention through Trust based mechanism i.e. Attack, pre and without attack for the various node density.

$$\text{Throughput} = \frac{\text{Total No. of Successfully Received Packet}}{\text{Total Simulation Time}}$$

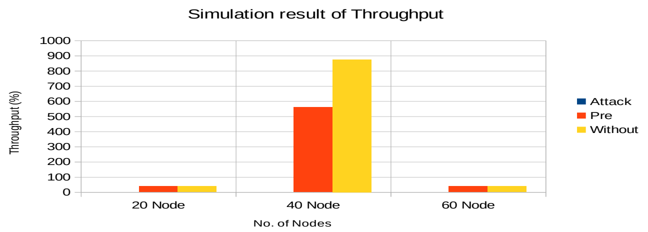

Figure:3.2 Throughputs comparisons

3.3Simulation results for end to end delay

This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes. Figure and table shows the End to End Delay under Jamming attack detection and its prevention through Trust based mechanism i.e. Attack, pre and Without attack for the various node density.

$$\text{E2E Delay} = \text{Receiving Time} - \text{Sending Time}$$

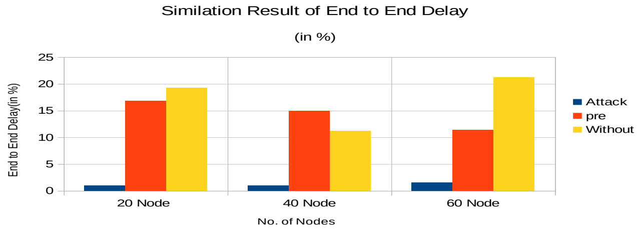

Figure:3.3 End to End Delays comparisons

3.4 Simulation results for residual energy

It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%.The unit of it will be in Joules. Figure and table shows the density.Residual Energy under Jamming attack detection and its prevention through Trust based mechanism i.e. Attack, pre and without attack for the various node

Residual Energy = Total Energy - Consume Energy

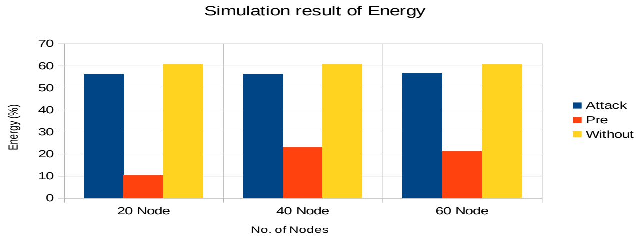

Figure:3.4 Residual Energy comparisons

3.5Simulation results for routing overhead or normalized routing load

This is the ratio of overhead bytes to the delivered data bytes. The transmission at each hop along the route is counted as one transmission in the calculation of this metric. The routing overhead of a simulation run is calculated as the number of routing bytes generated by the routing agent of all the nodes in the simulation run. This metric has a high value in secure protocols due to the hash value or signature stored in the packet. Figure and table shows the Routing Overhead under Jamming attack detection and its prevention through Trust based mechanism i.e. Attack, prevent and Without attack for the various node density.

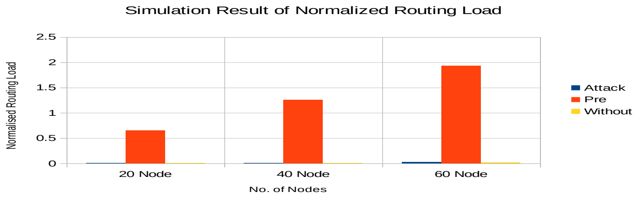

Figure:3.5 NormalizedRouting load comparisons

4.CONCLUSION

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment. , the detection and prevention of jamming attack in the network exists as a challenging task. In this work analyzed the effect of jamming attack in the performance of AODV protocol and prevent the network from jamming attack using TAODV protocol. The simulation has been done using the network simulator (NS-2.35). The performance metrics like packet delivery ratio, NormalizedRouting load (NRL), throughput and average end to end delay has been measured and analyzed with the variable node density. From the simulation results it is clear that when the jammer node exists in the network, it can be affected and decreased the performance of AODV routing protocol.

In this work, we simulated AODV protocol with different density, where each one has 20 nodes, 40 nodes, 60 nodes and also simulated the same scenarios after introducing single jamming Node into the network. Moreover, we simulated Secure AODV as per algorithm for detection of Jamming attack. Finally compare the results of solution with normal AODV under attack by varying different network parameters using same scenarios in NS-2.35. Our simulation results are analyzed above. Analyzing the results of PDR, throughput, End to end delay, NRL and improve result during jamming attack.

References

[1] Dorus.R,Vinoth.P,"MITIGATION OF JAMMING ATTACKS IN WIRELESS NETWORKS", 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013)

[2] Vani. S, Rachelin Sujae. Packet Hiding Methods for Preventing Selective Jamming Attacks, INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY, ISSN: 2277-9655, Vani, 2(4): April, 2013

[3] M.VamsiKrishna, R.Sudhakishore. Network Packet Jamming Detection And Prevention Using Hiding Method International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 2 –Nov 2013

[4] Aashish Mangla , Vandana. Detection of Physical Jamming Attacks in MANETs. International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6, June 2015

[5] Ashwini Magardey, Dr. Tripti Arjariya. Secure Detection and Prevention Scheme for Jamming Attack in MANET. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14

[6] Mourad Elhadef, Azzedine Boukerche, and Hisham Elkadiki. Diagnosing mobile ad-hoc networks: two distributed comparison-based self-diagnosis protocols. In Proceedings of the 4th ACM international workshop on Mobility management and wireless access, pages 18{27. ACM, 2006.

[7] Abderrahmane Baadache and Ali Belmehdi. Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks. Computer Networks, 73:173,184, 2014.

[8] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, and Piet Demeester. An overview of mobile ad hoc networks: Applications and challenges. Journal-Communications Network, 3(3):60,66, 2004.

[9] Humayun Bakht et al. Survey of routing protocols for mobile ad-hoc network. International Journal of Information and Communication Technology Research, 1(6), 2011.

[10] Samba Sesay, Zongkai Yang, and Jianhua He. A survey on mobile ad hoc wireless network. Information Technology Journal, 3(2):168,175, 2004.

[11] Imrich Chlamtac, Marco Conti, and Jennifer J-N Liu. Mobile ad hoc networking: imperatives and challenges. Ad hoc networks, 1(1):13,64, 2003.

[12] Anuj Rai, Rajeev Patel, RK Kapoor, and DS Karaulia. Enhancement in security of aodv protocol against black-hole attack in manet. In Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, page 91. ACM, 2014.

[13] Charles E Perkins and Elizabeth M Royer. Ad-hoc on-demand distance vector routing. In Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on, pages 90,100. IEEE, 1999.