Performance Evaluation of AODV protocol using Mobile adhoc Network under malicious attack

Pritesh Vasava
Department of Electronics and Communication Engineering
Babaria Institute of Technology, Vadodara, Gujarat, India

Urvik Shah
Department of Electronics and Communication Engineering
Babaria Institute of Technology, Vadodara, Gujarat, India

Vinit Parmar
Department of Electronics and Communication Engineering
Babaria Institute of Technology, Vadodara, Gujarat, India

Abstract- Owing to a very hectic life, nowadays, the information needs to be accessible anywhere and anytime. With Technological advancements, Mobile ad-hoc networks have become one of the most important avenues. It is a technology which primarily deals with continuously moving users, consequences of which, are the network problems like Power management, Scalability, efficiency, life time of the node and network and most importantly secured communication. The main objective of the paper is to compare the AODV protocol for MANET without malicious node topology to the MANET with malicious node topology.

Keywords –MANET, Malicious attack, Hacker.

I. INTRODUCTION

A mobile adhoc network is an infrastructure less [3] mode, in which communication between source and destination is possible through multiple hops. Also the location of each and every node including source and destination continuously changes with respect to time. So these types of networks are very important as per today's use.

Figure 1 Mobile Adhoc Network

The above figure shows node to node communication in MANET topology. To establish and maintain such mobile network is a big task .There are number of issues which offer a good challenge to the existence of such networks. Communication should be made reliable and secure.

II. APPLICATION OF MANET

With the increase of portable [2] devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. Ad-hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or

inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy, applications that move from traditional infrastructure environment into the ad-hoc context, a great deal of new services can and will be generated for the new environment.

Military Battlefield: Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

MANET-VoVoN: A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels.

III. PROBLEMS IN MANET

A. Challenges in Manet:–

There are different challenges in Manet like power management [1], scalability, life time of nodes and networks, security etc. This paper focuses on the Security aspect of the Manet which is quite more vital in today's life. If the network is not secure [8] than it is of no use as data can be hacked or manipulated by intruders which not acceptable at all.

B. Malicious Attack:–

Before discussing any attack [9] first it should be understood how exactly communication takes place in a Manet. Suppose there are five nodes in a network. Node 1 is a source and Node five is destination. So, the path available for communication between node N1 and N5 may is from N1-N2-N3-N4-N5. Now what should node N1 will do to send a PREQ to neighbor node, Here, It is N2 which will check whether N2 itself is a destination or not. If the packet is not for N2, it forwards PREQ to neighbour and so on and send acknowledge back to N1.

Now while transforming data from N1 to N5, what this intermediate node tends to do, is saving of the resources like power. So what they do is they see whether the packet is for them or not, if not, they will simply drop the packet or they will go in sleep mode. This is normally defined as a hacker (attacker) [6] in the network. This activity is known as a malicious activity. The act of such a node can vary.

C. Effect of such attack on a Network:–

Usefulness of network depends upon the study [5,8] of various parameters like throughput, energy saved, packet delivery ratio, end to end delivery, etc. A normal topology without any malicious attack will definitely produce results better than the network affected by the malicious attack. In this research paper, the malicious node will simply drop the packets which do not belong to it. In this way it will reduce the throughput of the network which is not acceptable at all.

IV.WORKING OF AODV

In AODV [4], the network is silent until a connection is needed. At that point the network node that needs a connection broadcasts a request for the same. The same message is forwarded to the further nodes by an intermediate node and meanwhile it records the beacon message it heard from the previous node, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.

When a link fails, a routing error is passed back to a transmitting node, and the process repeats. Much of the complexity of the protocol is to lower the number of messages to conserve the capacity of the network. For example, each request for a route has a sequence number. Nodes use this sequence number so that they do not repeat route requests that they have already passed on. Another such feature is that the route requests have a "time to live" (ttl) number that limits the number of times they can be retransmitted. Another such feature is that if a route request fails, another route request may not be sent until twice as much time has passed as the timeout of the previous route request.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

V.IMPLEMENTATION AND RESULTS

A.Implementation of the Simulation Scenario:

Table -1 Simulation Parameters

Dimension	900x900
Protocol	AODV
No. of Nodes	30
Max speed	30
Pause time	5
Initial Energy	100 J
MAC	802_11
Generation	Using Setdest command
Simulation Tool	NS-2.34

B.Simulation Scenario:–

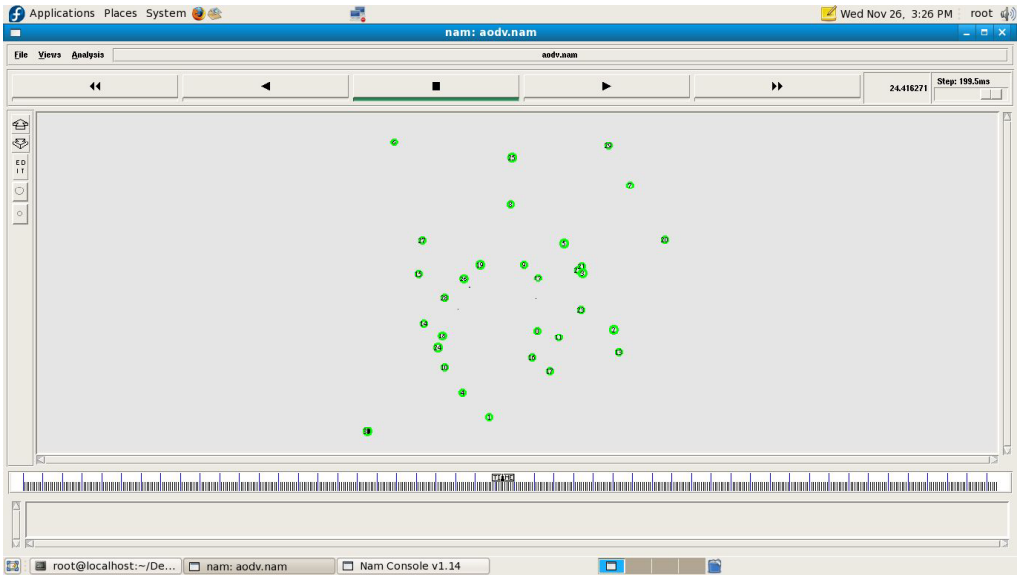

Figure 2 Simulation of AODV without Malicious Attack

Figure 3 Simulation of AODV with Malicious Attack Route Discovery

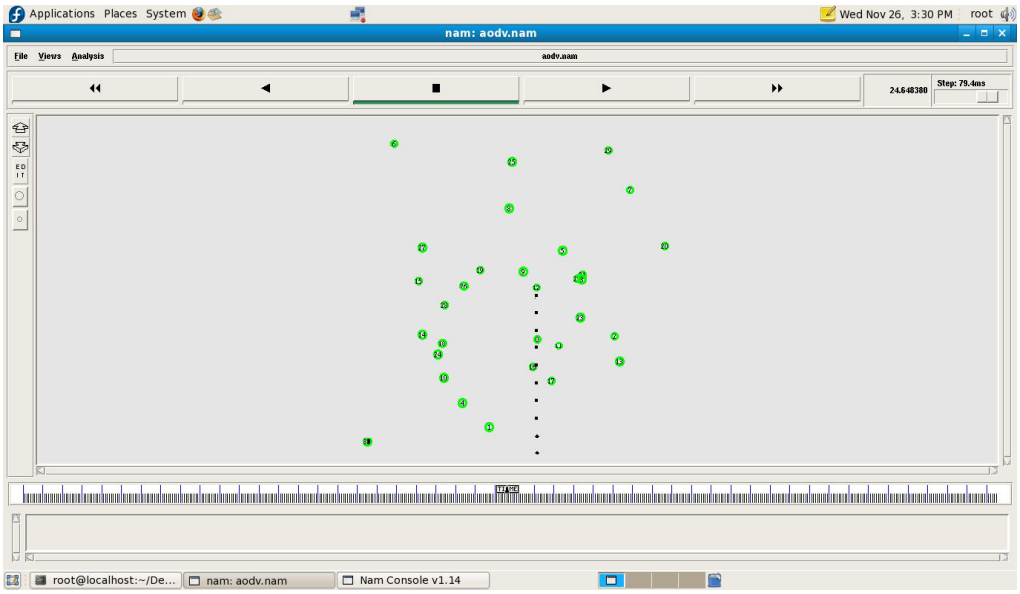

Figure 4 Simulation of AODV with Malicious Attack Packets Dropped

Figure 5 Simulation of AODV with Malicious Attack Packets Dropped

C. Tabular Result–

Sr. No.		No of nodes	Remaining Energy	Packet Sent	Packets received	End to end delay	pdf	throughput	Routing Load	Routing Over head
1	AODV(Without Malicious Attack)	30	3801	3000	2764	0.847	92.11	113kbps	0.117	324 packets
2	AODV(With Malicious Attack)	30	3849.53	3000	1819	0.007	60.63	74kbps	0.054	100 Packets

VI.CONCLUSION

From the above simulation results it is clearly observed that the pdf (packet delivery ratio) of AODV under Malicious attack has decreased which decrease the efficiency of the Network. Also other parameters are adversely affected.

VII.ACKNOWELDGMENT

The authors are thankful to Shri S.K.Patel and Dr. Jaymin Bhalani for their support and encouragement during the research endeavor. We would like to thank Department of Electronics and Communication, BITS Edu Campus, India, for cooperation in the research work.

REFERENCES

[1] Priyanka Goyal, Vinti Parmar, Rahul Rishi, , " MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[2] Himadri Nath Saha and Debika Bhattacharjee, " Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques"

[3] IRSHAD ULLAH, and SHOAIB UR REHMAN," Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols," Master thesisat school of engineering at Blekinge Institute of Technology.

[4] Ranjeet Suryawanshi and Sunil Tamhankar, " Performance Analysis And Minimization Of Black Hole Attack In MANET", Applications (IJERA), Vol. 2, Issue4, July-August 2012, pp.1430-1437.

[5] A.Rajaram and Dr. S. Palaniswami " Malicious Node Detection System for Mobile Ad hoc Networks", (IJCSIT) Vol. 1 (2) , 2010, 77-85.

[6] Abhay Kumar Rai, Rajiv Ranjan Tewari, Saurabh Kant Upadhyay" Different Types of Attacks on Integrated MANET-Internet Communication", (IJCSS) Volume (4): Issue (3).

[7] Priyambada Sahu, Sukant Kishoro Bisoy and Soumya sahoo., Detecting and Isolating Malicious Node in AODV Routing Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 66– No.16, March 2013

[8] Bing Wu, Jianmin Chen, and Jie Wu, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Chapter 12 from °c 2006 Springer

[9] Manjeet Singh, and Gaganpreet Kaur "A Surveys of Attacks in MANET" IJARCSSE Volume 3, Issue 6, June 2013.