International Journal of Advanced Science and Technology
Vol.82 (2015), pp.63-70
http://dx.doi.org/10.14257/ijast.2015.82.06

Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Adhoc Networks

Kulbir Kaur Waraich[1] and Barinderpal Singh[2]

[1]*Research Scholar CSE Department, DAV University Jalandhar Punjab*
[2]*Research Scholar CSE Department, DAV University Jalandhar Punjab*
[1]*sbmk91@gmail.com*, [2]*barinderpal.singh013@gmail.com*

Abstract

A mobile Adhoc Network is a collection of various mobile nodes that can change it and configure itself on the network. In MANET, Ad-hoc On-Demand Distance Vector (AODV) floods the packets to discover route. In Ad hoc On Demand Vector (AODV) routing protocol for MANET (Mobile Ad hoc Networks), malicious nodes can easily disrupt the communication because of inherent limitations. In this paper, performance of AODV Routing Protocol is analyzed with and without malicious attack. A malicious node disrupts the limit and floods the network with false control packets. Malicious node affects the whole network as it consumes more bandwidth and drops packets which in turn degrade the performance of AODV routing protocol. Performance is carried out under various parameters like Throughput, packet delivery ratio, packets dropped and normalized routing load.

Keywords: *MANET, AODV, Throughput, Packet Delivery Ratio, Packets Dropped, Normalized Routing Load, NS2*

1. Introduction

An Adhoc Network forms a network without any centralized control and central administration and consists of various mobile nodes that are interconnected with each other Development of various routing protocols is done in different types of adhoc networks like MANETs, VANETs and FANETs. In recent years interest on Manets are at high level because of reduced infrastructure costs, ease of establishment, fault tolerance etc. Manets are more reliable and provides hop to hop and multihop communicaton. In Manets communication takes place between intermediate nodes dynamically. Security is the main issue in manet because wireless means of communication is more affected for security. Since Manets possesses distributed networks so ensuring security in such networks is a big challenge. Also it affects the performance of routing protocols in manets.

2. AODV Routing Protocol

AODV is Ad hoc On-Demand Distance Vector routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. In AODV the communication among nodes take place only when required. It is a combination of on demand and distance vector. It includes two main functions route discovery and route maintenance. It first discovers the route by sending route requests RREQ to each and every node in the network and then route maintenance takes place. Every RREQ contains source identity, destination identity, source sequence number, destination sequence number, time to live etc. Every time a node increases a sequence number and notices change in the neighborhood topology.

ISSN: 2005-4238 IJAST

AODV defines no special security mechanisms. So an impersonation attack can be easily done. These attacks makes existing nodes malicious which joins the network and start behaving as malicious by dropping packets and advertising wrong routing information. If any node starts acting malicious, route error message will be generated and then malicious node id detected and isolated so that proper communication can be done from source to destination.

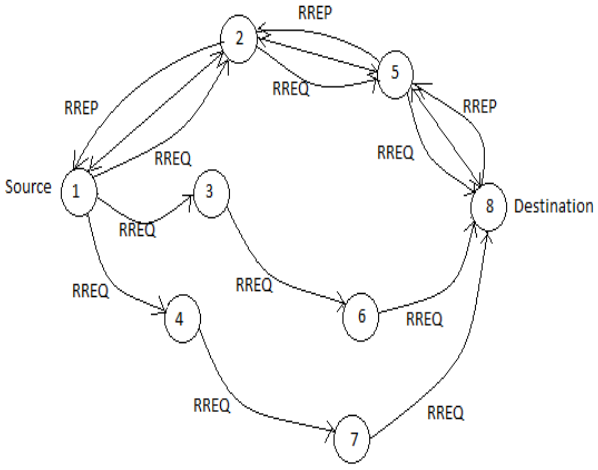

Figure 1. Control Messages in AODV Protocol

3. Role of Malicious Node

In AODV routing protocol malicious nodes can easily disrupt the communication among nodes. The malicious nodes may launch DOS attack that is not part of route. Once a route is established any node that is not part of any route may cease forwarding legitimate packets.

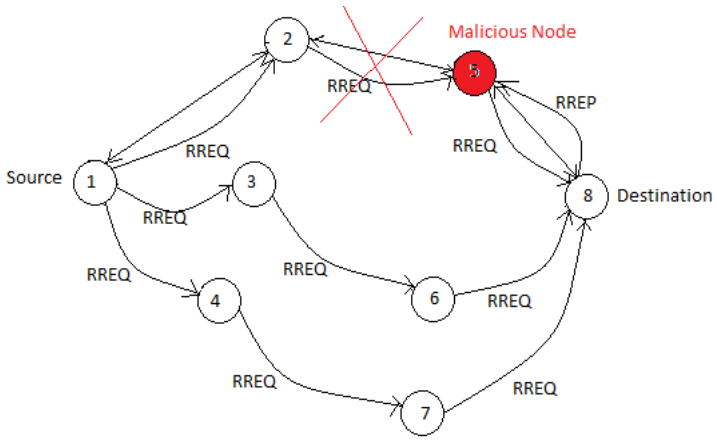

Figure 2. Malicious Node Behaviour

3.1. Problem due to Occurrence of Malicious Node

AODV applies route formation by including various control messages that are route request (RREQ) and route reply (RREP). Each time a data packet is received by a node, it checks whether it has a route to the destination or not. If the node has route to destination

then it generates the RREP and if it does not have route to destination then it rebroadcast it to the neighboring nodes. There is a limit to route requests that a particular node generates. However a malicious node ignores this limit and floods the network with too many fake control packets so that the source node cannot process the genuine packets.

3.2. Effect of Malicious Node

AODV routing protocol is vulnerable to malicious behavior. When a node sends packets to the destination without any failure then it acts as a genuine node. During malicious attack, a node starts behaving as malicious by keeping all packets with itself and not forwarding to the destination node. After receiving all the packets, malicious node starts dropping all these packets which affects whole network by degrading the performance of network.

3.3. Algorithm to Create Malicious Node

To create malicious node, we have to apply changes in two files i.e. aodv.cc and aodv.h

a. Aodv.cc

To make system malicious/hacker, we have to use following algorithm:

```
If(strcmp(argv[1],"hacker")=0)
{
Malicious=true;
Return tcl_ok;
}
If route doenot exists,packets are dropped
If(malicious==true)
{
Drop (p,drop_rtr_no_route);
}
```

b. Aodv.h

```
bool = malicious;
```

After making changes in aodv.cc, then aodv.h is used for calling purpose.

4. Performance Metrics

4.1. Simulation Methodology

Performance of various routing protocols is different based on different working. Simulation is carried out to analyze the performance. Simulation analyzes the performance of routing protocols before applying in real applications. To carry out simulation several simulators are available. In this paper working is done by using event driven NS2 (Network Simulator) and for the analyses AWK script is used.

4.2. Network Simulator

Network Simulator is a tool that is used to carry the performance of routing protocols of wired and wireless networks. In this approach NS2 tool is used to carry out the performance of AODV routing protocol under different parameters. NS2 is very useful tool since it is event driven simulation tool. It has proved useful in studying the nature of communication networks. It includes several components that is used to analyze performance of routing protocols. Some of the main components are: NS, Tcl/Tk, Nam, Zlib, Xgraph, Awk script. Installation of NS2 is done using these components. NS2 suit can be installed in the Unix based machine. Initially NS2 is installed and then it is validated and verified by using various commands.

4.3. AWK Script

Awk script is used for data extraction from trace files of routing protocols. This is used to carry out the performance of routing protocols under various parameters. In this paper AWK script is used to extract the data and analyze the performance under parameters namely throughput, packet delivery ratio, packets dropped and normalized routing load. We have to make AWK program files for these parameters according to which it extracts the data. The AWK script runs by using following command:
Awk –f programfile tracefile

4.4. Simulation Methods and Parameters

In this work the performance of AODV routing protocol is carried using with or without malicious attack. The tcl (tool command language) coding is used to define all parameters used in this performance analysis. Scenario files are created by using network simulator. The random way point mobility model is used for movement of nodes. Wireless channel is used for wireless connection and signals are propagated using omni antenna. Two scenarios are created *i.e.*, with malicious attack and without malicious attack. CBR and UDP traffic is used to carry out performance of both these scenarios. For the simulation different number of nodes (20,40,60,80,100) were initially positioned at random locations over 1000 m x 1000 m area. The simulation time is 120 seconds. The network of 2, 4, 6, 8 numbers of malicious nodes are created. Additionally, every node has a radio range of 250 meters and the IEEE 802.11 WLAN MAC protocol was used.

4.5. Parameters Used

To determine the behaviour and performance of AODV routing protocol with and without malicious attack various performance metrics are to be used.

4.5.1. Throughput

It is referred as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput is expressed as bytes or bits per sec (byte/sec or bit/sec).

*Throughput = (Number of data packets Received * Packet size * 8) /Simulation Time*

4.5.2. Packet Delivery Ratio

It is termed as the ratio of packets that are successfully delivered to destination compared to the number of packets that have been sent out by the source. It can be calculated as:
*Packet Delivery Ratio = received packets/generated packets * 100*

4.5.3. Packets Dropped

It is the difference between number of packets sent and received. It can be calculated as:
Packet loss = Data Packet Sent - Data Packet Receive

4.5.4. Normalized Routing Load

It is calculated by dividing the total number of routing packets sent by the total number of routing packets received.
NRL = routing packets/received packets

5. Result Analysis

In this work the performance analysis is carried out by varying two parameters *i.e.*, Number of nodes and number of malicious nodes. In this AODV routing protocol is used in which performance is carried out with and without malicious attack.

SIMULATION PARAMETERS	VALUES
Channel Type	Wireless
Propagation Model	Two Ray Ground
No. of Nodes	20,40,60,80,100
Traffic type	CBR
Data Payload	512 bytes/packets
Mac Type	802_11
Transmission Range	250
Speed	0-20 m/sec
Area of Simulation	1000 x 1000
Number of malicious attacks	2, 4, 6, 8, 10
Time of Simulation	120 sec

5.1. Graphs

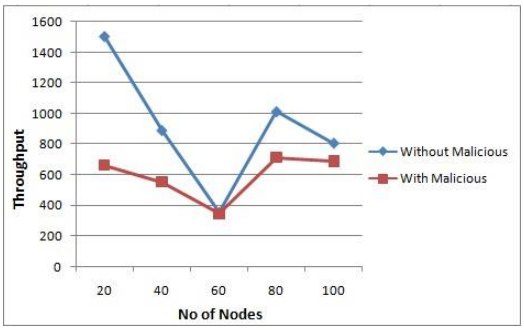

Figure 1. Throughput

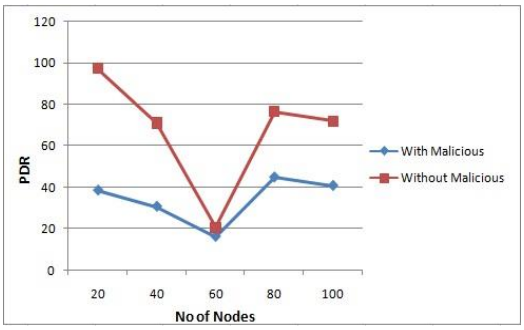

Figure 2. Packet Delivery Ratio

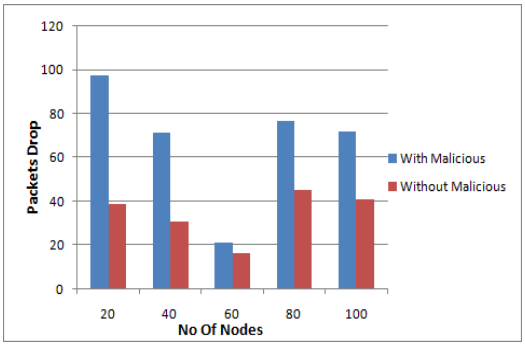

Figure 3. Packets Dropped

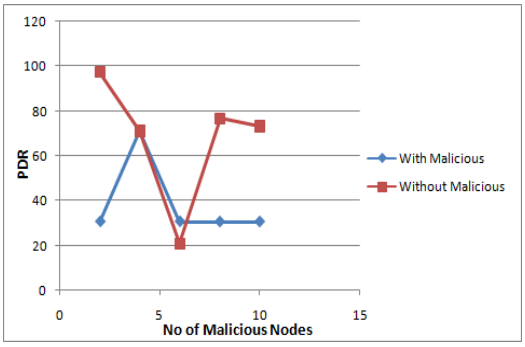

Figure 4. PDR under no. of Malicious Nodes

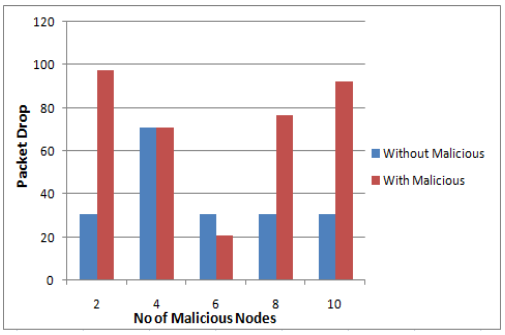

Figure 5. Packets Dropped under no. of malicious nodes

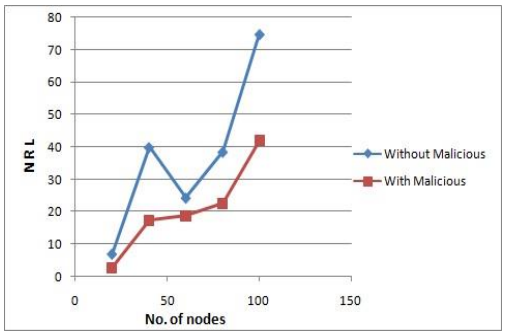

Figure 6. Normalized Routing Load

From above Graphs it is very clear that performance of AODV under malicious nodes is degrading as compared to performance of AODV without Malicious Nodes. In Figure 1, it is clear that throughput under malicious node decreases gradually but under without malicious nodes it increases gradually regarding various numbers of nodes. In Figure 2, The PDR under malicious attack is much less than under without malicious nodes. So number of packets dropped in malicious AODV will be greater as in Figure 3, Then in Figure 4 and Figure 5 comprises of performance of AODV under different number of malicious nodes. In Figure 6, Normalized Routing Load is calculated under malicious and non malicious nodes.

6. Conclusion

In this an attempt has been made to find impact of malicious node in AODV routing protocol and measure the performance with and without the malicious node. Result shows that throughput and packet delivery ratio of normal AODV is much better than AODV with malicious attack. Under malicious attack AODV drops more packets with increase of number of attacks. It is found that performance of routing protocol (AODV) degrades by introducing malicious nodes but have less routing overhead as compared to normal AODV. In future an effort can be made by including any denial of service attacks in the whole network with detection and prevention techniques.

References

[1] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad hoc Routing Protocols", Proceedings of the 2003 Annual IEEE Information Assurance Workshop, **(2003)** June.
[2] Y. Tung, M. Alkhatib and Q. S. Rahman, "Security Issues in Ad-Hoc on Demand Distance Vector Routing (AODV) in Mobile Ad-Hoc Networks", IEEE, **(2005)** April.
[3] P. Ning and K. Sun, "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols", Ad Hoc Networks, Elsevier, vol. 3, no. 6, **(2005)**.
[4] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks", Ad Hoc Networks, Elsevier, vol. 6, no. 4, **(2008)**.
[5] I. Raza and S. A. Hussain, "Identification of malicious nodes in an AODV pure ad hoc network through guard nodes", Computer Communications, Elsevier, vol. 31, no. 9, **(2008)** June.
[6] L. Chunlin and Y. Peyan, "Performance evaluation and simulations of routing protocols in ad hoc networks", Computer communications, Elsevier, vol. 30, no. 8, **(2008)** June.
[7] G. Mishra, Y. K. Jain and S. Aggarwal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)", IEEE International Conference, **(2009)** December.
[8] M. Patel and S. Sharma, "Detection of malicious attack in MANET a behavioral approach", IEEE Advance computing conference, **(2013)** February.
[9] M. Amaresh and G. Usha, "Efficient malicious detection for AODV in mobile ad-hoc network", IEEE Recent Trends in Information technology, international conference, **(2013)** July.
[10] K. Kaur Waraich and R. Kaur, "Security against DDoS Attacks in MANETs", International Journal of Computer Science and Mobile Computing, IJCSMC, vol. 3, no. 3, **(2014)** March.

[11] S. Preet Singh and B. Singh, "Routing Algorithm in MANET", International Journal of Engineering and Innovative Technology (IJEIT), vol. 3, no. 9, **(2014)** March.

Authors

Kulbir Kaur Waraich, research Scholar Computer Science & Engineering Department from DAV University Jalandhar, Punjab (INDIA). B. Tech. Professional with specialization in Information Technology from SBBSIET (PTU) Jalandhar, Punjab (INDIA). Member of Computer Society of India. Participated in Paper Presentation organized during National Conference on impact of Science and tech. Research Publications in various international journals.

Barinderpal Singh, research Scholar Computer Science & Engineering Department from DAV University Jalandhar, Punjab (INDIA). B.Tech. Professional with specialization in Information Technology from SBBSIET (PTU) Jalandhar, Punjab (INDIA). Member of Computer Society of India. Publications in various international journals, international non-paid journals and international conference.