Implementation and Prevention of DOS Attack in Malicious Environment on AODV Routing Protocol

Varsha G. Tank[1] **Dhaval Patel**[2]
[2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Hasmukh Goswami College of Engineering, Vahelal

Abstract— The Mobile Ad-hoc Network (MANET) is a concept base on wireless medium and straightforward to establish and having dynamic topology. The mobile Ad-hoc networks are exposed to various networks attacks because MANET operational environment is open and dynamic or live. MANET uses the Routing protocols for data transfer. Malicious node is the one type of mobile node but its work is completely different compared to normal Mobile nodes. Malicious nodes have capability to change or remove Routing Information. Now a day's attackers are trying to effect servers and networks with DOS (Denial of Service)attack. We have shown a implementation of DOS attack process and it prevention process in AODV routing environment. Malicious or selfish node carries attacks on the networks so it directly effects to the routing Performance. We have measured throughput, end to end delay and packet Delivery ratio.

Keywords: Malicious Node, MANET, Flooding, attack, AODV

I. INTRODUCTION

Wireless networks have become progressively more popular in the past few spans, particularly within the 1990's when they are being amended to enable mobility and wireless devices became popular.Wireless networks provide connection flexibility between users in different dwellings. Moreover, the network can be extended to any place or building. It doesn't require any wired connection.They can be classified in two main categories: Networks with fixed infrastructure and Ad hoc wireless networks (9)(18) as shown in Figure 1.

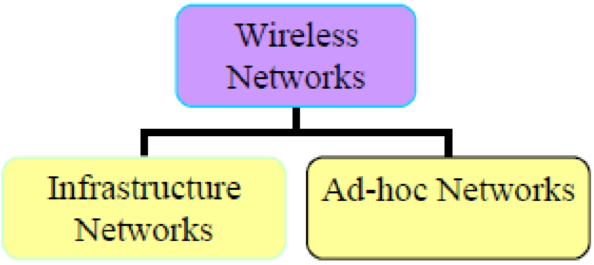


Fig. 1: Wireless Networks Categories

In infrastructure network an Access Point (AP) denotes a central coordinator for all nodes. An access point (AP) can act as a router in the network, or as a bridge. Examples for this type of networks are GSM and UMTS cellular networks (9). Whereas a wireless ad hoc network is a decentralized type of wireless network. It means ad hoc networks have no fixed infrastructure or administrative support, because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks (18). The topology of the network changes dynamically as mobile nodes joins or leaves the network (9).

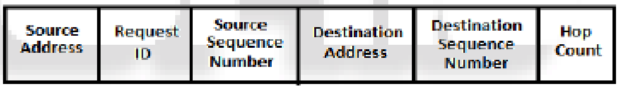
II. AD HOC ON-DEMAND DISTANCE VECTOR (AODV)ROUTING PROTOCOL

The AODV(3), Ad-hoc means node move or connected or disconnected with the networks any time, On Demand means when source wants to send data to the destination, Distance means find the distance between source to destination in terms of number of hopeand Vector means list whatever store the information list.AODV is based on the concept of Bellman-Ford distant vector algorithm.AODVdefines a route to a destination node only when a node wants to send a packet routes arepreserved as long as they are required by the source.Sequence numbers guarantee thefreshness of routes and the loop-free routing.

AODV use following control for path or route establishment (7).

A. *Route Request (RREQ)*

When a route is not available for the destination, source node transmit/ broadcast the route request message. A route request packet (RREQ) is flooded to entire network. The RREQ has the following fields:

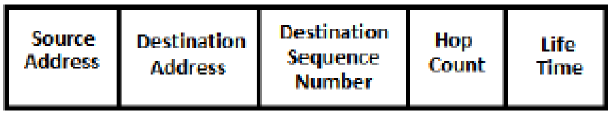


Source Address	Request ID	Source Sequence Number	Destination Address	Destination Sequence Number	Hop Count

Fig. 2: RREQ Format

B. *Route Reply (RREP)*

In Route Reply if a node is the destination, or has a valid route to the destination, it unicasts a route reply message (RREP) back to the source. Destination use the unicast route for reply message to source, neighbour node make next hop entry for destination and forward the reply. If source receives multiple replies that time source node use one with shortest hop count route/path. This packet has the following information.



Source Address	Destination Address	Destination Sequence Number	Hop Count	Life Time

Fig. 3: RREP Format

C. *Route Error (RERR)*

All nodes monitor their own neighbouring nodes. When a node in a living route gets disconnected or lost, a route error message (RERR) is generated to alert the other nodes on both sides of the link of the loss of this particular route. In AODV routing protocols detect the node and if possible do the local repair.

D. SSN (Source Sequence Number)

Sequence number used by AODV to avoid loop free routing and to measure the “freshness” of route details. Proceeding to broadcasting RREQ, RREP,
and RERR message, AODV need to increment its sequence number.

III. SECURITY ATTACKS

The networking environment in wireless systems makes the routing protocols vulnerable to attacks securing wireless ad-hoc networks is a extremely challenging dispute. There is no any central coordination in MANET so it is more vulnerable to cyber-attacks than wired network. There are a number of attacks that affect MANET. These attacks can be classified into two types: (1) Externalattack: External attackers are mainly from outside the networks who want to access the network and when they are able to access the network they start sending false data packets, denial of service attack in order to disrupt the performance of the whole network (2)Internal attack:The attacker has normal access to the network and also participates in the normal activities of the network in internal attack. The attacker gets access to network as new node either by cooperating a current node in the network or by malicious pretence and starts its malicious performance. Internal attack is more complicated attacks then external attacks.

A. Attacks on AODV

Following attacks can be launched against the AODV routing protocol.

1) Denial of Service Attacks

This attack aim to attack the accessibility of a node. If the attack is Successful the services will not be available (2). The attacker generally uses radio signal jamming and the sequence tiredness method. Denial of Service (DOS) is the degradation or avoidance of valid use of network resources (13).

2) Flooding Attack

The flooding Attack is a denial-of-service attacks in which malicious node sends the useless packets to demolish the valuable network resources. Flooding attack is possible in on demand routing protocol (2). Based on the type of packet used to flood in the network, flooding attack can be categorized in two types. (1) RREQ flooding: In the RREQ flooding attack, the attacker sends many RREQ packets atparticular timeinterval to the IP address which does not exist in the network and disable the limited flooding feature. On demand routing protocol usethe route discovery process to obtain the route between the two nodes (2) DATA flooding: In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packet uses the network resources so user in network cannot able to use the resources for valid communication.

3) Impersonation Attack

Impersonation attack is a severe threat to the security of mobile ad hoc network. If there is not a proper authentication mechanism among the nodes, the opponent can capture some nodes in the network and make them look like gentle nodes (2).In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviours such as propagate fake routing information and gain inappropriate priority to access some confidential information.

4) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential facts that should be kept secret in communication. The information could include the location, public key, private key or even passwords.

5) Sinkhole Attack

The attacking node tries to offer a very attractive link. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

6) Sybil attack

The Sybil attack especially aims at distributed system environments. The attacker plays multiple roles. It tries to act as several different identities/nodes rather than one.

7) Traffic Analysis

It is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

8) Black Hole

It is a kind of selfish node that just drops the packets and hence the transmission further (2). A suspicious node diverts the destination by sending incorrect RREP (route reply) message that it has a latest route with minimum hop count to destination and then it drops all the receiving packets.

a) Gray hole attack

Gray hole attack is an extended version of Black hole attack in which a malicious node behaves unpredictably. We can categorize Gray hole attack by its behaviour (9): In first kind of Gray hole attack, the malicious node drops packets for a specific time and behaves normally during the remaining time; in second kind of attack, the malicious node may drop certain kind of packets while forwards all other packets; in third kind of attack, the malicious node may drop certain kind of packets for certain time only and later on it behaves as a normal node. Due to these characteristics, detection of Gray hole attack is not an easy task during data transmission phase (13).

IV. RELATED STUDY

Here we have analysed some related works to avoid Denial of Service attacks:

(1) In (1) The Authors has proposed technique depends on the selection of threshold values. All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighbouring nodes. This research addresses associated works on security issues and trust founding schemes. A proposal to effectively prevent flooding attack using AODV Protocol is discussed in this paper. A better understanding and modelling of the security attacks is needed in MANETs if efficient secure routing algorithms are to be built in the network. They have used parameters like Number of malicious nodes, Number of connections, Node moving speed.

(2) In (17) this approach CORE mechanism that enhances watchdog for monitoring andisolating selfish nodes based on a subjective, indirect and functional reputation ispresented. The reputation is calculated based on various types of information on eachentity's rate of collaboration. Since there is no motivation for a node to maliciouslyspread harmful information or data about further nodes, denial of service attacks usingthe collaboration technique itself are prevented (17)

(3) In (14) define the detection scheme can be described as follow: the node listens periodically to its neighbourhood, and collects information about the forwarded packets for its neighbors. They have proposed an approach which can efficiently detect Gray hole attack in MANETs. The list of detected malicious nodes can be useful to discover secure paths from source to destination by avoiding this type of denial of service.

V. Proposed System

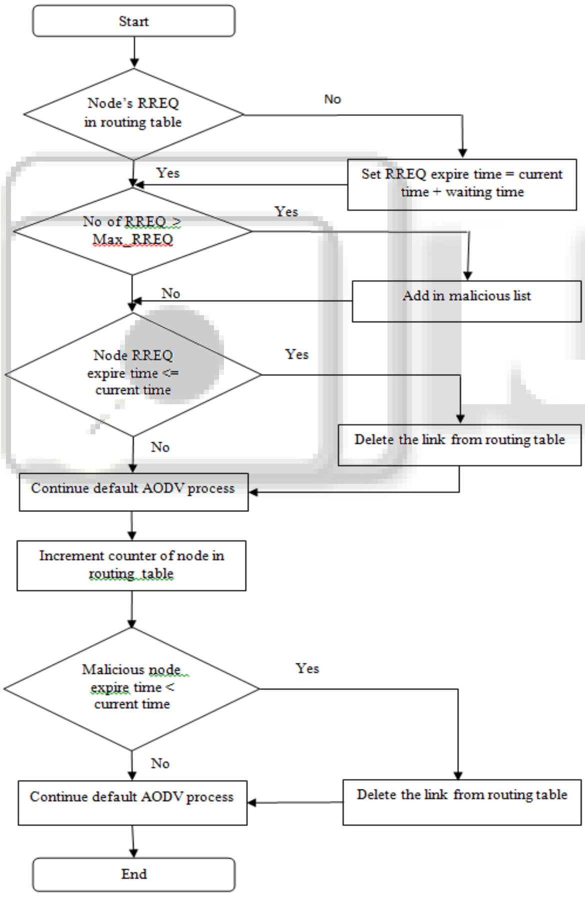

Start
Node's RREQ in routing table
No
Set RREQ expire time = current time + waiting time
Yes
No of RREQ > Max_RREQ
Yes
Add in malicious list
No
Node RREQ expire time <= current time
Yes
Delete the link from routing table
No
Continue default AODV process
Increment counter of node in routing table
Malicious node expire time < current time
Yes
No
Continue default AODV process
Delete the link from routing table
End

Fig. 4: Flowchart of Proposed Scheme

Proposed schema work as follows.

– Whenever the network start for Mobile Adhoc Network, according to this scheme it will check first if the node's route request in routing table or not. If node route request is not in the routing table then itfirst enter the entry of that node in the routing table and set the expire time of node roué request and request =1.

– If entry is already in the routing table then it will check how many route requests come from that node and it will compare it with MAX_RREQ which is 8. If it exceed then we declare as Malicious node add it in Malicious node list, also we set the expire time of malicious node.

– If node request less than max request then there is two choices either its entry expires or not, if entry expires then we remove the entry from routing table. If not then continue default AODV process and increment the request counter of particular node in routing table.

– After removing the link of malicious node from malicious node list after the session expires. May be possible after some time malicious node stop doing malicious thing means stop DOS attack. It may be possible after some time it behave as malicious node, so again it will check for the malicious node expire time.

– We should remove it from malicious node list and forward its route request. After entries of malicious node expire then we remove it from the malicious node list. If node entry is expiring then we can remove it from the malicious list and declare that node is as malicious node. So like this way we can detect the malicious node from network, and we can stop the DOS flooding attack in AODV.

VI. Experimental Results

After the Appling the proposed algorithm in NS2.34 using following parameter we got result which is given below:

Parameters	Values
No. of Nodes	25,50,75,100
Area Size	1000*1000m
MAC	802.11
Simulation Time	100,200,300,400 sec
Traffic Source	CBR
Bandwidth	10mb
Data Rate	10mb
Routing Protocol	AODV
Transmission Protocol	UDP
No. of malicious node	2

Fig. 5: Parameter Used in Implementation

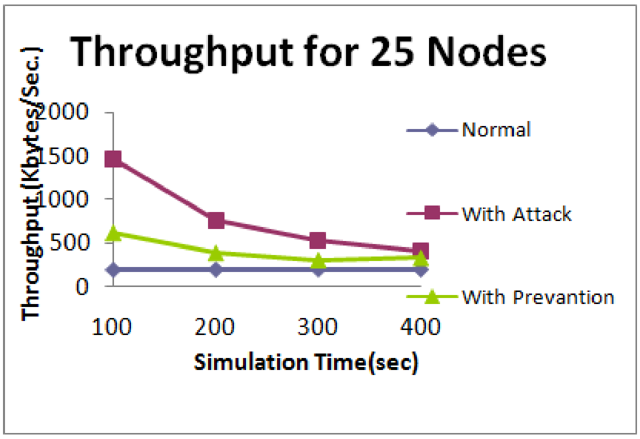


Fig. 6: Throughput Vs. Simulation Time

Figure6 in normal scenario we got high throughput and in attack scenario throughput has decreased than after we have applied our proposed algorithm to prevent the attack and increases the throughput compare to attack scenario.

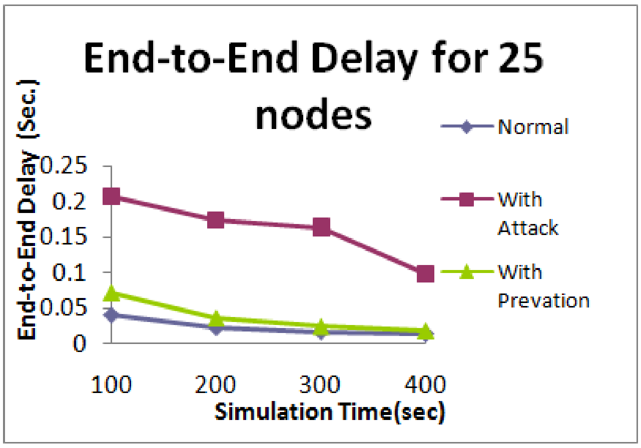


Fig 7: End to End Delay Vs. Simulation Time

Figure 7Simulation result shows variation of the average End-to-End Delay with various simulation time 100 to 400 Seconds. Sometime it has decreased due to some mobile node because they movedin the whole networks so message did not reach on time. Due to flooding attack source node not able to send original message to destination that's why End to End delay decreased in Attack scenario.

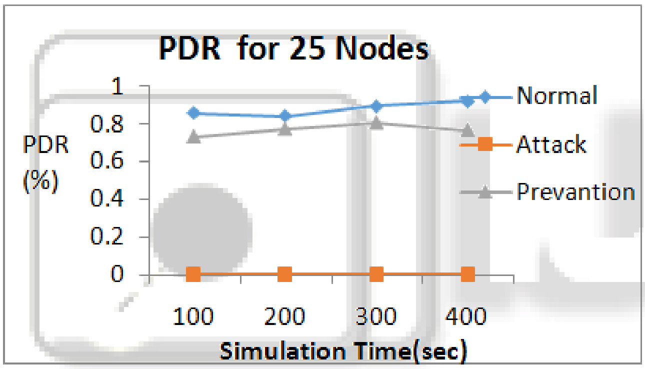


Fig 8: Packet Delivery Ratio Vs. Simulation Time

Figure8shows the simulation time when we simulate normal network scenario at that time we got high packet delivery ratio but opposite in the attack scenario malicious or selfish node continuously send the packet on network so at that time we got 0 PDR and after using the proposed algorithm we got the increases average packet delivery ratio.

VII. Conclusion and Future Works

Now days MANET is became most popular. The AODV routing Protocols also one of the best for the data transfer. Due to open environment the security threat or malicious node directly affect the performance of the AODV routing protocol. As malicious node is the main security threat that effect the performance of the AODV routing protocol. This problem has found because mainly required the routing performance in malicious environments. Its detection and prevention is required because it is the secure data transfer matters. Therefore end of this research work we have detected the malicious node and improve the routing performance in malicious environment for Denial of Service (Flooding attack) attack in terms of throughput, PDR and end to end delay.

In future using this research work we are trying to more secure the AODV routing protocol and by performing some changes in existing proposed scheme to prevent another attack like DDOS for more improvement in the AODV Routing performance.

Reference

[1] Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, “Flooding Attack Prevention in Manet”, International Journal of Computer Technology and Electronics Engineering (IJCTEE)Volume 1, Issue 3 ISSN 2249-6343

[2] Meenakshi Patel And Sanjay Sharma," Detection of Malicious Attack In Manet A Behavioral Approach ", IEEE, 2012 , 978-1-4673-4529-3/12

[3] Namrata Marium Chacko, Shini Sam And P.Getzi jeba leelipushpam “A Survey on Various Privacy And Security Features Adopted In Manets Routing Protocol” , IEEE , 2013, 978-1-4673-5090-7/13

[4] Ashok M. Kanthe, Dina Simunic and Ramjee Prasad “Effects Of Malicious Attacks In Mobile Ad–Hoc Networks”, IEEE, 2012, 978-1-4673-1344-5/12

[5] Saleh Ali K.Al-Omari and Putra Sumari “An Overview of Mobile Ad Hoc Networks For The Existing Protocols And Application”,Journal on Applications of Graph Theory In Wireless Ad-Hoc Networks And Sensor Networks, 2010, Vol.2, No.1

[6] Kavita Taneja and R. B. Patel, “Mobile Ad Hoc Networks: Challenges And Future”, Proceedings of National Conference on Challenges & Opportunities In Information Technology, 2007, Coit

[7] Mr. B. Karthokeyan, Mrs. N.Kanimozhi and Dr.S. Hari Ganesh “Analysis Of Reactive AODV Routing Protocol For MANET” IEEE, 2014, 978-1-4799-2877-4/14

[8] Vijay Kumar, Rakesh sharma, Ashwani Kush, "Effect Of Malicious Nodes On AODV in Mobile Ad Hoc Networks", International Journal of Computer Science And Management Research, 2012, ISSN 2278-733X Vol 1 Issue 3

[9] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts and Mahendra Srivastava, “ An Overview Of AODV Routing Protocol” IJMER, 2012, ISSN: 2249-6645, Vol.2, Issue.3

[10] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, “A Survey Of Routing Attacks In Mobile Ad Hoc Networks” IEEE Wireless Communications, 2007

[11] Teerawat Issariyakul, Ekram Hossain “Introduction To Network Simulator Ns2” , Springer Science+Business Media, 2009

[12] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala “Dos Attacks In Mobile Ad-Hoc Networks: A Survey”, IEEE, 2012, 978-0-7695-4640-7/12

[13] Rutvij H. Jhaveri, Ashish D. Patel And Kruti J. Dangarwala “Comprehensive Study of Various DOS Attacks and Defense Approaches in MANETs”, IEEE 2012, ISBN : 978-1-4673-5144-7/12

[14] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, D. Gaiti, “Denial of Service (DOS) Attacks Detection in

MANETs Through Statistical Models", IEEE, 2014, 978-1-4799-5490-2/14

[15] Leena Sahu, Chaitali Sinha, "A Cooperative Approach For Understanding Behavior of Intrusion Detection System in Mobile Ad Hoc Networks", IJCSMA, 2013, ISSN: 2321-8363, Vol.1 Issue. 1

[16] QuanJia, Kun Sun,AngelosStavrou, "Capman:Capability-Based DefenseAgainst Multi-Path Denial Of Service (DOS) Attacks In MANET " U.S. Government Work

[17] Pietro Michiardi and Refik Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks" Institut Eureco, Sophia Antipolis, France Core Mechanism

[18] Dr.S.S.Dhenakaran,A.Parvathavarthini,"An Overview of Routing Protocols in Mobile Ad-Hoc Network", IJARCSSE, 2013

[19] Savithru Lokanath and Aravind Thayur, "Implementation of AODV Protocol and Detection of Malicious Nodes in MANETs", IJSR, 2013, Volume 2 Issue 11

[20] Bhupendra Patel, Anurag Gupta, Nabila Hyder, and Kamlesh Rana, "AODV Routing Protocol Performance in Malicious Environment", Springer International Publishing Switzerland, 2014, Networking and Informatics - Volume 2, Smart Innovation, Systems And Technologies 28