ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

Sinkhole Attack detection and prevention in MANET & Improving the performance of AODV Protocol

[1]Rajeshwar L. Balla, [2]Venugopal Kotoju

[1]Research Scholar, [2]Asstt. Prof.
Vits, Karimnagar
[1]raju.bl75@gmail.com, [2]kotojuvenu@gmail.com

Abstract: MANET is one of self configuring fastest emerging wireless technology. MANET is multi-hop wireless network of autonomous mobile nodes with no preset infrastructure where each node can move in any direction as well play a role of router. Dynamic nature of this network makes routing protocols to play a prominent role in setting up efficient route among pair of nodes. Therefore many proactive, reactive & hybrid routing protocols have been proposed, among which one of well known is AODV due to its high performance gain. Cooperative nature of nodes exposes MANET to various kinds of passive & active attacks. Sinkhole is one of severe kind of attack which attempts to attract most of network traffic towards it & degrade the performance of network. this paper, shows performance metrics as throughput, PDR, End to end delay & Packet loss. Simulation is carried out using widely used simulator NS2.

Keyword: NS2, MANET, Vulnerability, Active, Passive, Sinkhole.

I. INTRODUCTION

MANET is multi-hop wireless network of autonomous mobile nodes with no preset infrastructure where each node can move in any direction as well play a role of router. To facilitate communication in adhoc network, a routing protocol is vital whose primary goal is to establish accurate & efficient route between pair of nodes, due to this lot of routing protocols have been proposed for MANET & its success depends on people's confidence in its security. It is being used in most of applications, ranging from military to civilian, where each node acts as router. To facilitate communication in adhoc network, a routing protocol is vital whose primary goal is to establish accurate & efficient route between pair of nodes, due to this lot of reactive, proactive & hybrid routing protocols have been proposed for MANET & its success depends on people's confidence in its security.

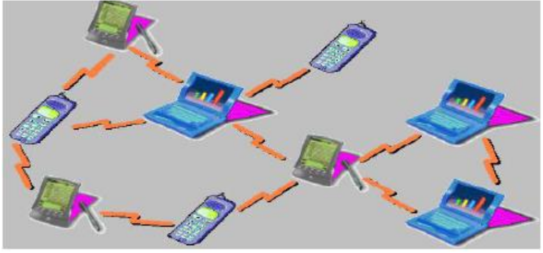

Fig. 1 Structure of MANET

The routing protocols mainly classified into three major categories proactive, reactive & hybrid. Proactive protocols continuously learns topology of the network by exchanging topological information among network nodes, where each node builds its own routing table which it can be use to find path to destination. But a sinkhole is one of severe representative attack in MANET under which AODV needs to be evaluated, where malicious node attempts to draw all network traffic towards it by broadcasting fake routing information & modify or drops packets sent for forwarding which leads to performance degradation of network. The performance of any routing protocol can be realized quantitatively by means of various performance metrics such as PDR packet delivery ratio, end to end delay, and throughput & packet loss [4].

II. ADHOC ON- DEMAND DISTANCE VECTOR(AODV) PROTOCOL

AODV is motivated by limited bandwidth that is available in the media that are used for wireless communications is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of route discovery and route maintenance from DSR, plus the use, sequence numbers, and periodic update packets from DSDV. The main benefit of AODV over DSR is the source route does not need to be included with each packet. This results in a reduction of routing protocol overhead. Unfortunately, AODV requires periodic updates which consume more bandwidth than is saved from not including source route information in the packets. AODV discovers a route through network wide broadcasting. There are four control messages are used by AODV described as below.

1. Routing Request (RREQ):

When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network which contains the following fo rmat [6] .

Source Address	Request ID	Source sequence No	Destination Address	Destination Sequence No	Hop Count

Fig.2 RREQ Format

2. Routing Reply (RREP):

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. This message has the following format [9].

Source Address	Request ID	Source sequence No	Destination Address	Destination Sequence No	H Cc

Fig.3 RREP Format

3. Route Error Message (RERR):

All nodes monitor their own neighborhood and broadcast message when: A node detects that a link with adjacent neighbor is broken.z

Unreachable Dest IP Add	Unreachable Dest Seq No

Fig.4 RREP F ormat

4. HELLO Messages:

Each node can get to know its neighbourhood by using local broadcasts, so called HELLO messages. Nodes neighbors are all the nodes that it can directly communicate with. Although AODV is a reactive protocol it uses these periodic HELLO messages to inform the neighbors' that the link is still alive. The HELLO messages will never be forwarded because they are broadcasted with TTL = 1. When a node receives a HELLO message it refreshes the corresponding lifetime of the neighbor information in the routing table.

III. WORKING OF AODV

When a node wishes to send a packet to some destination. It checks its routing table to determine if it has a current route to the destination. If yes, forwards the packet to next hop node If No, it initiates a route discovery process [8].

a. Route discovery

It begins with broadcasting of RREQ to its neighbors specified for certain destination. Once an intermediate node receives a RREQ, It check its routing table for route to dest If found send RREP to source If not found it rebroadcast RREQ to its neighbor nodes by setting up a reverse route path to source node in its route table. It ignores RREQ if it is processed already [6]. Finally on reaching RREQ to destination node, It uincast RREP to source node by using reverse route to source node. The above procedure can be described visually as follows

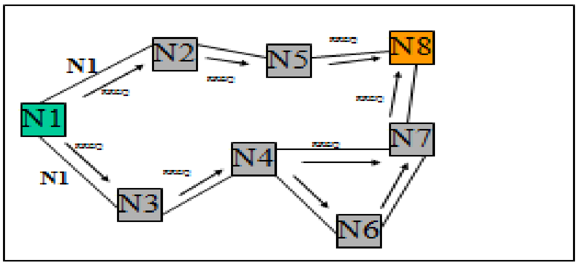

Figure. 5 Route Discovery

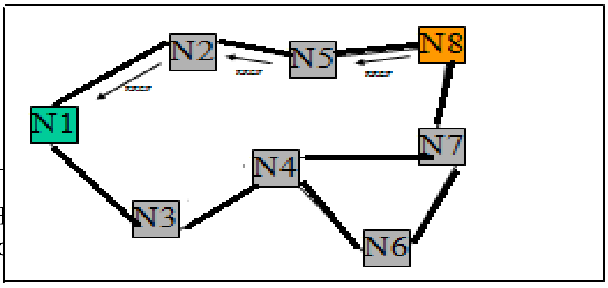

Figure. 6 Route Reply

b. Route Maintenance Stage

A hello message is broadcasted by active nodes periodically. If no hello message from a neighbor. The upstream node will notify the source with an RERR packet & entire routes based on the node is invalidated. Source will initialize a new route discovery stage and flood the RREQ packet [8]. Above procedure can be realized in the following figure

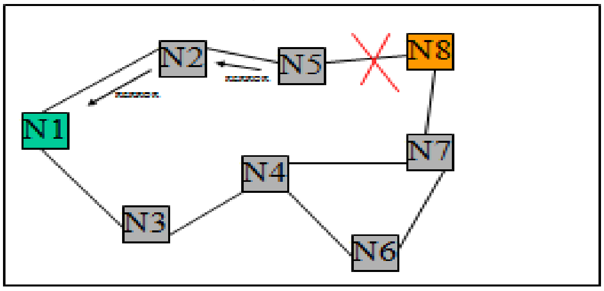

Figure.7 Propagation of RERR

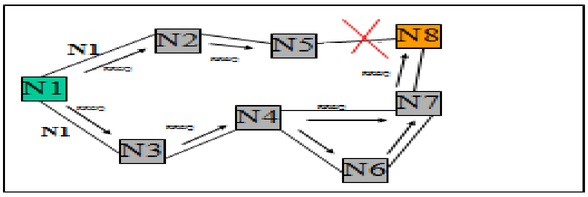

Figure.8 Route Rediscovery

IV. PROBLEMS OF SINKHOLE ATTACK

In this type of attack sinkhole node tries to attract data to itself by convincing neighbors through broadcasting fake routing information & let them know itself on the way to specific nodes. Through this procedure, sinkhole node attempts to draw all network traffic to itself. Thereafter it alters the data packet or drops the packet silently. It increases network overhead, decreases network's life time by boosting energy consumption; finally destroy the network [7].

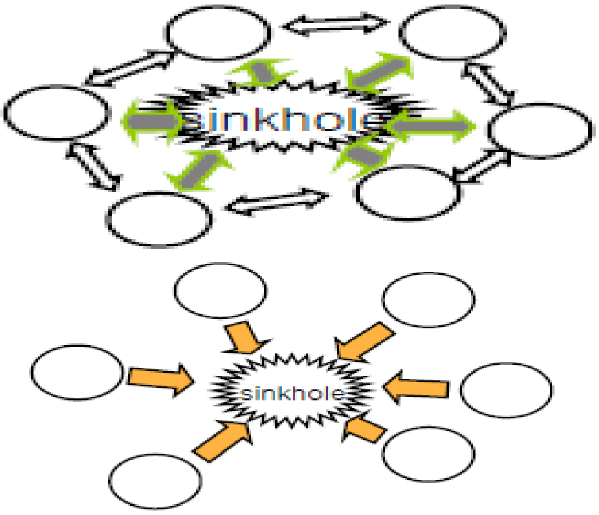

Figure.9 Sinkhole Problem

In AODV protocol, sinkhole attack is set up by modifying sequence number in RREQ, higher the sequence number, then route will be more recent the packet contains. Sinkhole node selects the source, destination node. It observes the source node's sequence number carefully, and generates bogus RREQ with selected source, destination and higher sequence number than observed source sequence number. It then broadcasts the bogus RREQ. Nodes that take this bogus RREQ recognize that this route could be a better route to the source than incumbent route.

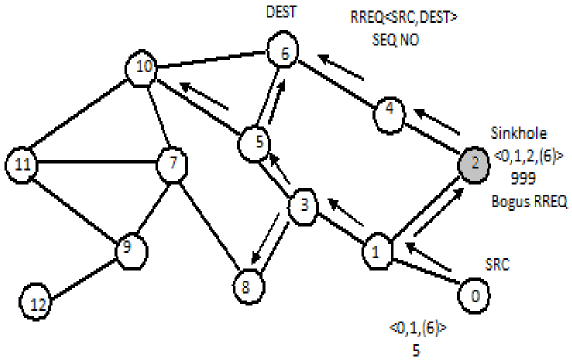

Figure.10 Bogus RREQ Propagation

Fig.10 shows the propagation of the bogus RREQ packet. Sinkhole node 2 makes the bogus RREQ. Sequence number of bogus packet is 999, much higher than original source's, 5.

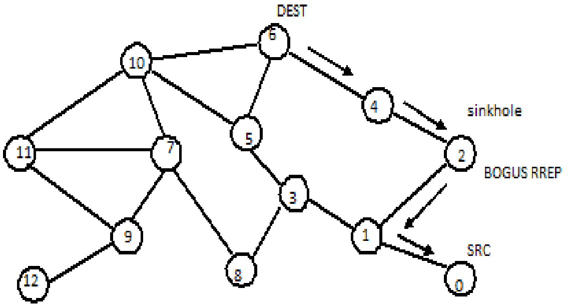

Figure. 11 Bogus RREP Propagation

Bogus RREP is shown in Fig 11 where destination node thinks that route having sinkhole node is shortest, to reach to source node. Sinkhole node 2 can easily repeat this procedure & can draw all local network traffic to itself. Thereafter node 2 can do malicious acts including dropping, or modifying the traffic.

V. Algorithm For Detection & Prevention

```
At Intermediate Node: AODV
Step 1: (Initialization Phase)
Start Route Discovery process from Source Node.
Step 2: (Storage Phase)
Store Route Requests in RR-Table
Step 3: (Investigation Phase)
Select Src_Seq_No of Current RREQ
Check(Src_Seq_No of Previous RREQ from table)
Seq_No_Diff = Src_Seq_No_CurRREQ - Src_Seq_No_PrevRREQ
If (Src_Seq_No_CurRREQ >>> Src_Seq_No_PrevRREQ)
{
Mali_Node = NID
Discard RREQ Entry.
}
Step 4: (Resumption Phase)
 Call SendRequest Method of default AODV Protocol
```

Abbreviations Used In Algorithm

Src_Seq_No - Source Sequence Number
NID- Node ID
RRTable- Route Routing Table
Src_Seq_No_CurRREQ - Source Sequence Number of current Route Request
Src_Seq_No_PrevRREQ- Source Sequence Number of Previous Route Request
Mali_Node- Malicious Node

VI. EVALUATION METRICS

Performance of AODV protocols in MANET can be realized by quantitative study of values of different metrics used to measure performance of routing protocols which are as follows.

- Average end-to-end delay

It is defined as average time taken by data packets to propagate from source to destination across a MANET. This includes all possible delays caused by buffering during routing discovery latency, queuing at the interface queue, and retransmission delays at the MAC, propagation and transfer times the lower value of end to end delay means the better performance of the protocol [4].

End to end delay = Σ (arrive time - send time)

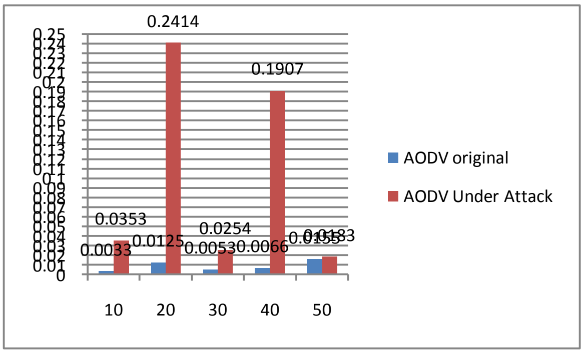

Fig: 12 End to End Delay with & without sinkhole attack

Analysis:

From above table we can say that value of end to end delay is decreasing initially but it slightly increases finally for original AODV where as values for AODV under attack increases suddenly & is highest for 20 nodes but decreases at last for 50 nodes when compare to original AODV.

- Packet Delivery Ratio

It's a ratio of the number of packets received by the destination to the number of packets send by the source This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means better performance of the protocol.

PDR = Σ No of packet receive / Σ No of packet send

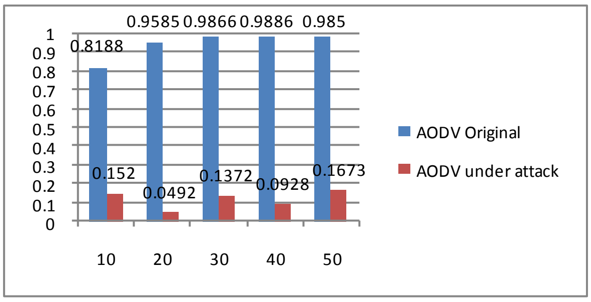

Fig 13 PDR VS No of nodes for AODV with & without sinkhole attack

- Packet Loss

It is the measure of number of packets dropped by nodes due to various reasons. The lower value of the packet lost means the better performance of the protocol [10].

Packet lost = No of packet send – No of packet received.

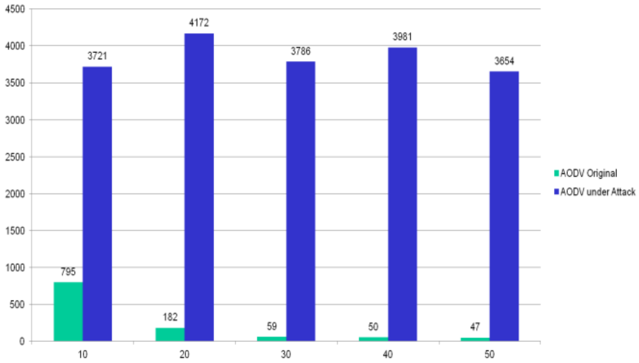

Fig 14 Packet Loss VS No of nodes for AODV with & without sinkhole attack

- Network Throughput

Throughput is the number of data packets delivered from source to destination per unit of time. Throughput is calculated as received throughput in bit per second at the traffic destination.

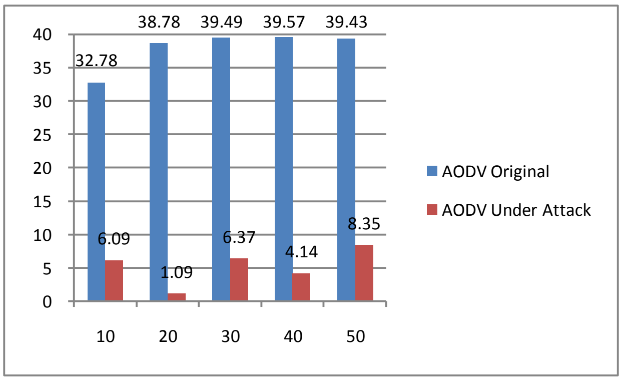

Fig 15 Throughput VS No of nodes for AODV with & without sinkhole attack

VII. CONCLUSION

evaluated the performance of very popular on demand routing protocol AODV comparatively with sinkhole & without sinkhole attack by observing change occurred in the value of various performance metrics such as PDR, end to end delay, throughput & packet loss, as well obtained simulation results by varying number of nodes in the network from 10 to50 & found that the performance of AODV is very severely affected by sinkhole attack specially for 30 nodes. AODVs performance deteriorates for higher number of nodes under attack. At the same time values of PDR for secure AODV is improved compare to sinkhole AODV when we vary nodes from 10 to 50. Thus we can say that PDR of AODV is improved for secure AODV which degraded due to sinkhole attack.

VIII. REFERENCES

[1] Laxmi Shrivastava, Sarita S.Bhadauria, G.S.Tomar," Performance Evaluation of Routing Protocols in MANET with different traffic loads", International Conference on Communication System Network Technologies IEEE 2011.

[2] Asma Tuteja, & Rajneesh Gujral, "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", International Conference on Advances in Computer Engineering IEEE 2010.

[3] Sudhir Agrawal, Sanjeev Jain & Sanjeev Sharma," Mobility based Performance Analysis of AODV and DYMO under Varying Degree of Node Misbehavior", International Journal of Computer Applications (0975 – 8887) Volume 30– No.7, September 2011.

[4] Subramanya Bhat.M & Shwetha.D," A Performance Study of Proactive, Reactive and Hybrid Routing Protocols using Qualnet Simulator" International Journal of Computer Applications (0975 – 8887)Volume 28– No.5, August 2011.

[5] Vijayalakshmi M. & Avinash Patel ," Qos Parameter Analysis On Aodv And Dsdv Protocols In A Wireless Network", Vijayalakshmi M.Indian Journal of Computer Science and Engineering Vol. 1 No. 4 283-294.

[6] Kisung Kim and Sehun Kim," A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks", Korea Advanced Institute of Science & Technology Korea.

[7] Benjamin J. Culpepper, H.Chris Tseng," Sinkhole Intrusion Indicators in DSR MANET", First International Conferenc on broadband networks IEEE 2004.

[8] Thanachai Thumthawatworn†, Tapanan Yeophantong and Punthep Sirikriengkrai," Adaptive Sinkhole Detection on Wireless Ad Hoc Networks", Assumption University, Thailand. IEEE 2006.

[9] Marchang N, Datta R., "Collaborative techniques for intrusion detection in mobile ad-hoc networks", Ad Hoc Networks 2008;6:508–23.

[10] Ian D Chakeres & Elizabeth M Belding Royer," AODV Routing Protocol Implementation Design".

[11] Harris Simaremare & Riri Fitri Sari," Performance Evaluation of AODV variants on DDOS, Blackhole & Malicious Attacks",International Journal of Computer Science & Network Security,Vol 11 No 6,june 2011.

[12] Preeti Bhati, Rinki Chauhan, & R K Rathy,"An efficient Agent based AODV Routing Protocol in MANET", International Journal on Computer Science & Engineering Vol No 7 july 2011.

[13] Rajan Bansal, & Himani Goyal," Analytical Study the performance Evaluation of Mobile Adhoc Network using AODV Protocol", International Journal of Computer Application Jan 2011.

[14] H A Esmailli, M R Khalil Shoja,"Performance Analysis of AODV under BlackHole Attack through use of OPNET Simulator", World of Computer Science & Information Technology journal 2011.

[15] Luke Klein-Berndt ,"A Quick Guide to AODV Routing",Wireless Communication technology group National Institute of standard & Technology.

[16] Mouhamad IBRAHIM and Giovanni NEGLIA," Introduction to Network Simulator".

[17] NS-2, The ns Manual (formally known as NS Documentation) available at http: //www. isi.edu/nsnam/ ns/doc

[18] Analysis of the Effect of Sinkhole Attack on AODV Protocol In Mobile Adhoc Network by Nisarg Gandhewar

[19] Review on Sinkhole Detection Techniques in Mobile Adhoc Network by Nisarg Gandhewar