ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Implementation of Intrusion Detection System against Black hole attack in AODV

S.V.Anusha
M.Tech Student,
Bheema Institute of Technology (BITS),
Adoni, JNTU University, Anantapur.

B.Prabhakara Reddy
Associate Professor,
Bheema Institute of Technology (BITS),
Adoni, JNTU University, Anantapur.

Abstract:

In Mobile Wireless Ad Hoc Networks (MANET) acts as both transmitter and router in a network without any specified infrastructure. It should explore its local neighbors and with them it will communicate with the nodes which are out of transmission range of the source node. Due to the open structural dynamic topology of MANET unguarded to security attacks. Ad hoc On-demand Distance Vector (AODV) is one of the best routing algorithm. AODV is mostly affected by a security problem called Black Hole attack in which a unknown affected node produces a fake route reply message that it has a fresh node to the destination. In this paper Intrusion Detection and Response Protocol for MANETs is examined that performs better than AODV in the presence of Black Hole attack in terms of false responses.

Security in MANETs against Black Hole attack is provided by using IDSAODV routing protocol and the results are demonstrated using an optimized Network Engineering Tool NS-2, through various Quality Of Service parameters such as Packet Delivery Ratio, End to End Delay, Throughput and Overload based on UDP analysis.

1. Introduction:

A mobile Ad Hoc Network is a collection of wireless nodes that are stamina to communicate with each other without any particular infrastructure. It is a dynamic autonomous system of mobile hosts that are connected in wireless manner without central administration. MANETs have its worth on applications such as search and rescue, military fields, disaster recovery, sensor networks etc.

A Mobile Ad Hoc Network is a tremendous system in which the mobile nodes are capable of moving in a random fashion. MANETs have constantly changing topologies, limited bandwidth, battery, lifetime characteristics which are required for its flexible nature which brings specific security problems compared to wired networks.As a result wireless network MANETs are easily effected by different attacks.A MANET is determined with its availability, confidentiality, authentication, integrity and non-repudiation. One of the most likely preferred routing protocols in MANETs is the Ad Hoc On Demand Vector (AODV) routing protocol which is initiated on-demand. AODV is unguarded to famous Black Hole attack which is a denial of the service attack in which the effected node attracts the packets gaining a fresh enough route to the destination by dropping all the packets reaching at the source node. The Black Hole node having a fake route firstly uses the AODV protocol to expose itself as a valid route to the destination, in order to intercept the packetsand then it consumes the interceptedpackets.Intrusionwhich is an attempt to change the integrity, confidentiality is solved by Intrusion Detection Systems (IDS). In this paper we determine the effect of Black Hole node on AODV protocol by considering the results through the Network Simulator NS-2. Then we introduce IDSAODV and re-examine the results and plot the difference in its behavior. This difference is graphically represented by plotting the graphs in NS-2.

2.AODV Protocol in MANETS:

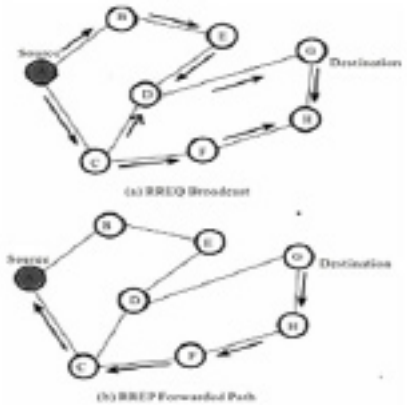
Ad-hoc On-Demand Distance Vector Routing (AODV):

A Reactive Protocol typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

It is a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a Path Discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. AODV utilizes destination sequence numbers to ensure all intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Destination sequence number is greater than or equal to that contained in the routes are loop-free and contain the most recent route information.

Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ,

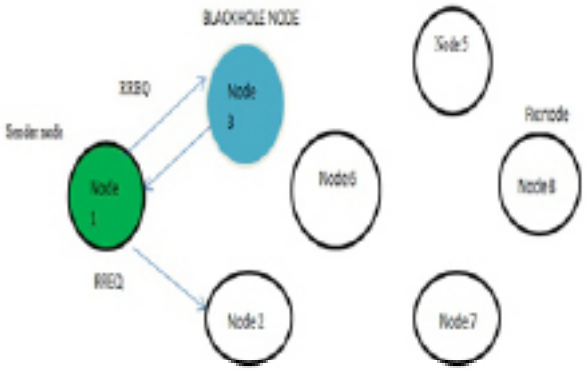


AODV Routing protocol in MANET:

greater than or equal to that contained in the RREQ. During the process of forwarding the RREQ, once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ.

2.Black Hole attack in MANETS:

Black Hole nodes generally never send exact information, in fact it waits for RREQ message from the neighbor nodes and receives RREQ from them and sends fake RREP message which gives false path to the destination without checking in the routing table. The malicious node assigns itself a higher sequence number in the routing table before remaining nodes sends the RREP message, as a result the neighbor think that path is found and simply ignores there RREP message and starts sending the data packets over false path. The effected node attacks all RREQ messages from all over the routes. As a result all the data packets are send to the single point which is called BLACKHOLE conveying swallow of all RREQ messages.



In the figure node 1 is the sender which it wants to send the data packets to node 4 which is the destination node. Node 1 broadcasts the RREQ packets to all nodes in its range, here nodes 3 and 2 are in range of node 1. Assume node 3 a malicious node, whenever node 3 receives the message it instantly responses and send RREP to node 1 with high sequence number node 1 assumes that it received the message from node 4 and sends the data packets to the destination node 4 but in the middle node

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3(black hole node) captures the UDP packets and do not send the TCP acknowledgement as it is blocked by Black Hole node.

3.Proposed work and implementation:

3.1 Proposed mechanism:

In this mechanism we measure the effect of Black Hole attacks in Wireless Adhoc Networks. To achieve this we simulate the Wireless Adhoc Network using NS-2-(network simulator version 2) scenarios which includes the Black Hole Adhoc network node.

To simulate the Black Hole node in a Wireless Adhoc network we implement a new protocol that drops the data packets after attracting themselves. To evaluate the performance black hole attack we implement the Black hole attack in AODV routing protocol and measure the performance metrics with and without black hole attack.

To display the effect of Black Hole attack we create a cache to store the information about the reply from various nodes this cache is executed with new protocol called IDS (Intrusion Detection System) in AODV called IDSAODV which has the entry of each reply from nodes of the network.

Whenever a Black Hole node receives a request it instantly gives a reply without knowing the shortest path. The reply time of Black Hole node is minimum compared to other replies in order to get the secured and shortest path. The sender waits till all the replies are received and then compares the reply time and choose the path with minimum nodes and shortest reply time compared to the first received one.

3.2 Implementation:

The experiments for evaluation of the proposed mechanism are established in Network Simulator NS-2. The performances of the three statistics are examined i.e., AODV protocol, Black Hole attack in AODV protocol and Intrusion Detection in AODV protocol (IDSAODV). The simulation parameters are as below.

Simulation Duration	100 sec
Dimension simulated area	800×800 m
Number of nodes	10-100
Movement model	Random waypoint
Maximum Speed	1-15m/sec
Total number of flows	5
Traffic type	UDP, CBR
Packet rate	0 packets/sec
Data Payload	1024 byte/packet
Host pause time	0.2 sec.
Transmission range	100 m

4.Experiments and Results:

The analysis cross check the experiment results of the simulation. The data is grabbed from the trace file of each program i.e., AODV.tr,BLACKHOLEAODV.tr, IDSAODV.tr .and evaluate the performance metrics such as PDR (Packet Delivery Ratio), End-to-End Delay, Throughput, Normalized routing overhead. These matrices are important because of its performance analysis of network.

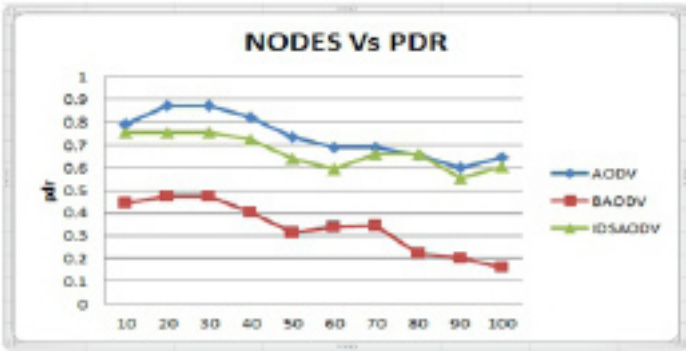


Fig:1 Scenario for Packet Ratio(PDR)

Figure 1 shows the simulation graph for number of nodes and PDR. Here x-axis is number of nodes and y-axis is PDR. In AODV the PDR is high but with the implementation of black hole AODV it decreases enormously. Similarly with the implementation of IDSAODV it increases again. In the same environment it reflects a wide variation with the increase of black holes, respectively.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

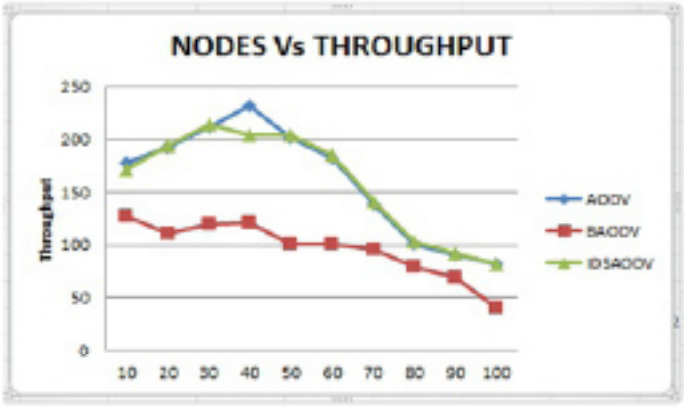


Fig: 2 scenarios for Throughput

Figure 2 shows the simulation graph for no of nodes and throughput. Here x-axis is nodes of nodes and y-axis is throughput. In AODV throughput is high but with the implementation of black hole AODV it decreases. Similarly, with the implementation of IDSAODV it increasesrespectively.

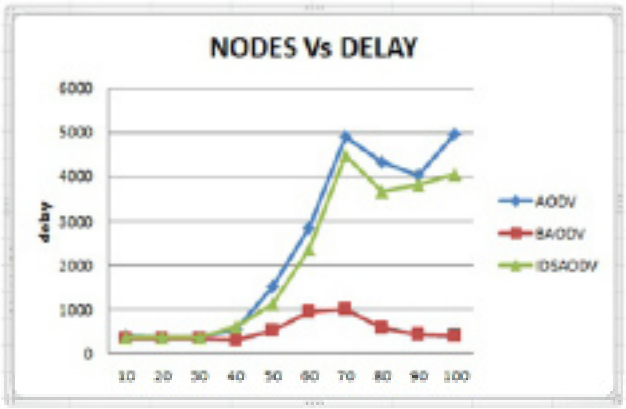


Fig: 3 scenarios for End To End Delay

Figure 3 shows the simulation graph for no of nodes and end-to-end delay. Here x-axis is nodes of nodes and y-axis is end-to-end delay. In AODV the end-to-end delay is high but with the implementation of black hole AODV it decreases enormously.

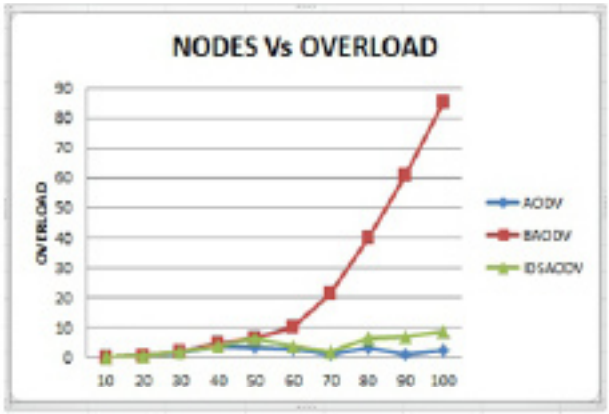


Fig: 4 scenarios for Normalized Overhead.

Figure 4 shows the simulation graph for number of nodes and normalized overhead. Here x-axis is nodes of nodes and y-axis is normalized overhead. In AODV the normalized overhead is very low but with the implementation of black hole AODV it increases to extreme level. Similarly with the implementation of IDSAODV it decreases.

5. Conclusion and Future Work

5.1 Conclusion:

In this paper, the issue of Black Hole attack and its effects on the AODV routing protocol has been discussed. Few methods to overcome this problem has been proposed. The route discovery process in the AODV is susceptible to Black Hole attack, therefore it is vital to have an efficient security method build into the AODV protocol in order to mitigate the effects caused.

Intrusion Detection System (IDS) is designed to prevent the effect of Black Hole attacks in Mobile Ad Hoc Networks. We implemented a solution in simulation with some scenarios which reduces the effect of Black Hole nodes. IDS controls the effect of Black Hole attack on AODV protocol to improve the network performance by maintain the Quality of Services parameters such as Packet Delivery Ratio (PDR), End-to-End Delay, Throughput, Normalized overload shown in the graphs above.

The enhancement only involves a minute modification that does not change the existing AODV protocol scheme. The solution is also light and suitable for most resource constraint devices.In NS-2, the network is constructed using nodes which are connected using links. Events are scheduled to pass between nodes through the links. Nodes and links can have various properties associated with them.

5.2 Future Scope:

We have investigated the effects of Black Hole attack in Adhoc networks. In our survey we have used the AODV protocol but other protocols can also be used to examine the results in the future. Different protocols exhibit different results. Therefore the best routing protocol for minimizing the Black Hole attack could be determined.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

But detection of Black Hole node is another future work. In our work we tried to detect and eliminate the Black Hole effect. There are many IDS systems. These IDS are tested to give the best results. There are also other types for eliminating the Black Hole effect depending on the type of connections either TCP or UDP.

References:

[1] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Second International Conference on Intelligent Systems, Modelling, and Simulation,2011.

[2]Jonsoon, U., Alriksson, F., Larsson, T., Johansson, P., and Maguire, G. Q. MIPMANET: Mobile IP for mobile ad hoc networks. Proceedings of the First Annual Workshop on Mobile Ad Hoc networking and computing (MobiHOC), Aug. 2000.

[3]B. Dahill, B. N. Levine, E. Royer, and C. Sheilds, "A secure routing protocol for Ad Hoc networks" in proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[4]Y. Hu, A. Perrig and D. Johnson, Ariande: "A Secure On-demand Routing Protocol for Ad Hoc Networks, in proceedings of ACM MOBICOM'02, 2010.

[5]Elizabeth Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[8] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, "ENHANCED INTRUSION DETECTION TECHNIQUES FOR MOBILE AD HOC NETWORKS", IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Dec. 20-22, 2007. Pp.1008-101.

[9] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc on-demand distance vector (AODV) routing", Internet Draft, RFC 3561, July 2003.

[10] S. Marti, T. Giuli, K.Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in-Proceedings of MOBICOM 2000, pp. 255-265, 2000.

About Authors:

Regards,
S.V. ANUSHA.

PRABHAKARA REDDY BAGGIDI

gave intense guidance to my paper who is currently working as Professor and HOD, Dept. of ECE, Jawaharlal Nehru Technological University, Anantapur, Andhra Pradesh, India., India. He received B.Tech degree from JNTU College of Engineering, Anantapur, Andhra Pradesh, India in 1982, M.Tech degree from Sri Venkateshwara University, Tirupathi, and Andhra Pradesh, India in 1994 and Ph.D. degree from J.N.T University, Hyderabad, and Andhra Pradesh, India in 2003.

He is having 85 National and 5 International publications to his credit. He is the member of IE (India), Member of ISTE, and NAFEN. He guided many academic projects for the last 16 years of teaching experience. His areas of research are Signal & Image Processing, Microcontroller Applications and Embedded Systems, and areas of interest on Mobile Ad hoc Networks and Optical Networks].