World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:8, 2014

Back Bone Node Based Black Hole Detection Mechanism in Mobile Ad Hoc Networks

Nidhi Gupta, Sanjoy Das, Khushal Singh

***Abstract*—**Mobile Ad hoc Network is a set of self-governing nodes which communicate through wireless links. Dynamic topology MANETs makes routing a challenging task. Various routing protocols are there, but due to various fundamental characteristic open medium, changing topology, distributed collaboration and constrained capability, these protocols are tend to various types of security attacks. Black hole is one among them. In this attack, malicious node represents itself as having the shortest path to the destination but that path not even exists. In this paper, we aim to develop a routing protocol for detection and prevention of black hole attack by modifying AODV routing protocol. This protocol is able to detect and prevent the black hole attack. Simulation is done using NS-2, which shows the improvement in network performance.

***Keywords*—**Ad hoc, AODV, Back Bone, routing, Security.

I. Introduction

A Mobile Ad hoc Network (MANET) is a self-leading network of mobile nodes joined via wireless links. Mobile ad hoc networks (MANET) are dynamic and don't have any infrastructure, formed by a self-ruling system of mobile nodes that are connected with wireless links [1]. Nodes in MANETs communicate with each other through a message transmission, without any centralized administration. Each node in MANET not only acts as a router but also as a host to forward the data packets to intermediate/ destination node. Only those mobile nodes which are within transmission range of each other's, can transmit packets directly using wireless links else, they need to depend on other nodes to forward packets as routers. It means that the performance of the network highly depends upon the support of the other nodes.

AODV is an on-demand source initiated routing protocol. It uses broadcast route discovery mechanism [2]. Every mobile node keeps a routing table that contains up to date neighbor node information for a route to the destination node. AODV has following three primary objectives [3].

1. Route discovery packets are broadcasted only when obligatory.
2. To differentiate between local connectivity management (neighborhood detection) and general topology maintenance.
3. To broadcast information about changes in local network to those adjacent mobile nodes those are concerned in receiving the information.

Whenever a source node is interested in data transmission to a destination node, it checks in its routing table, if it's routing table has a fresh enough route, it uses that route for sending the packets otherwise, and it broadcasts the Route Request (RREQ) message to its neighbors to initiate route discovery procedure. RREQ is further propagated until it reaches to the destination or to the node having fresh enough route to the destination. Each RREQ receiver, intermediate node modifies its routing table for source node and the forwarder of RREQ message.

On having a fresh route to a destination node or intermediate node, a node transmits Route Reply (RREP) packet to the RREQ sender node. RREP is unicast. Node receiving the RREP makes an entry for the node that forwarded the RREP message and forwards the RREP in reverse direction. When source node receives the RREP message, it renews its routing table by updating an entry for the RREP sender node and for the destination node. After completion of route discovery procedure, source node initiates the message dissemination to the destination by forwarding data packets to the neighbor node which has replied first with RREP.

Due to, wireless links mobile ad hoc networks are more vulnerable to attacks. These links provides an easier way to attackers to go inside the network and interrupt the ongoing communication [4], [5]. Malicious nodes cause different kinds of attacks that can impairment a network and make it untrustworthy for message transmission. Black hole attack is one among them. In black hole attack, a malicious node shows itself to have the shortest path to a destination in any network. This can lead to Denial of Service (DOS) [6] by tumbling the already received packets. When these malicious nodes proceed together as a set is called cooperative black hole attack.

In this paper, we proposed a framework which uses following technique to detect and remove the black hole nodes. In this technique [7], at first, a backbone network is developed over the ad hoc network through reliable nodes. When source node wants to initiate message dissemination process, it needs to obtain an IP address by requesting nearest backbone node for an unused IP address. After getting RIP, the source node starts route discovery procedure by sending RREQ not only for fresh route but also for RIP. After receiving the RREQ, black holes forward RREP for route discovery and also for RIP. When source node receives the

Nidhi Gupta is a M.Tech scholar at Computing Science and Engineering Dept., Galgotias University, Greater Noida, India (Phone no.: 07727050711; e-mail: nidhiyashsinghal@gmail.com).

Sanjoy Das and Khushal Singh are Asst. Professors at Computing Science and Engineering Dept., Galgotias University, Greater Noida, India (e-mail: sanjoy.das@galgotiasuniversity.edu.in, khushal.singh@galgotiasuniversity.edu.in).

RREP for the RIP from any of the route then black hole detection procedure is initiated by source node.

In Section II, related work on detection & prevention of black hole attacks is discussed. In Section III, we define the network model and assumptions made for solution. In Section IV, we discuss the methodology and algorithms and simulation and results are shown in Section V. Finally the conclusion & discussion of future work is discussed in Section VI.

II. Related Work

Researchers have proposed various techniques to detect and prevent black hole attacks, review of these techniques have presented below:

Deng et al. [8] have proposed a solution to prevent this black hole attack by making modifications to the AODV protocol. In this algorithm, when a node receives an RREP packet, it verifies the neighbor node on the route to the destination using another path. To confirm the continuation of the next hop node and the routing metric value (i.e. the hop count) with the next hop node, this checking is performed [9]. Further reply packet is sent back to source node from the next hop node of the neighbor node to confirm the route information. In case, when neighbor node neither finds a link to sender of RREP nor a route to the destination node then RREP sender node is considered as suspicious node. This technique does not work with cooperative black hole attack.

A mechanism has been proposed by [10] to reduce the Black hole attack via the judgment process which uses honesty of a node that is determined from the opinions of neighbor nodes of a node in a network. While transferring the data packets, each node must show its honesty. After receiving the first RREP packet, node transmits packet to source node and initiates judgment process for the RREP sender [9]. In judgment process, the neighboring nodes are asked to send their opinions about RREP sender node. Result of judgment process depends on the opinions received from all nodes of network. After receiving all the opinions, based on number rules, it is decided whether the replier is a malicious node or not. The major shortcoming of this solution is that neighbors can also give wrong opinion.

Sun B. et al. [11] proposed a detection mechanism which works on neighborhood-based approach to identify the black hole nodes in a network. In this approach, like AODV, Source node sends RREQ to initiate a routing discovery, to find out the reliable path to the destination. Using the neighbor set information; a solution is derived to manage the black hole attack. Solution consists of two parts: detection and response. In detection procedure, following are the two major steps:

Step 1. To collect neighbor set information.

Step 2. To determine the existence a black hole attack.

In Response procedure, Modify-Route Entry (MRE) control packet is sent by source to destination to create an accurate path from source to destination by modifying the routing entries of the intermediary nodes.

S. Banerjee et al. [12] has also proposed an algorithm for detection & removal of Black/Gray Holes. In this algorithm, data traffic is divided in to small sized blocks, before transmission; to detect and remove the malicious nodes while transmission. The neighbors of each node, monitors the flow of traffic. Acknowledgements are used by source and destination nodes to check the data loss & the possibility of a black hole. But this mechanism fails sometimes by giving wrong output that a node is misbehaving, but really it is not.

Tsou P.-C. et al. [13] designed a novel solution named Bait DSR (BDSR) scheme to prevent the collaborative black hole attacks. In this solution, proactive and reactive both approaches are used to design a hybrid routing protocol in the beginning of routing stage [9]. Before initiating route discovery procedure, source node transmits bait RREQ packet. There is no fixed and existent target address of bait RREQ. This approach uses similar method as used in DSR to avoid the traffic jam problem caused by bait RREQ. This bait RREQ attracts the fake RREP and malicious nodes can be identified to avoid black hole attack. In this mechanism, RREP's additional field records the location of RREP sender. With the help of recordings, source node can identify the location of malicious nodes. All of the responses received from adversaries should be dropped. Once the attackers are discovered, original DSR route discovery procedure is used for communication.

Watchara Saetang and Sakuna Charoenpanyasak [14] proposed credit based mechanism to check the reliability of the next hop. In proposed approach, the credit is initiated, in a route discovery phase. The definition of credit is:

Hop count*3; initial state
Credit = Credit+2; when destination node sends credit acknowledge
Credit-1; send 1 packet

Note: Credit Max = 5*(Hop count+2)

Until the receiving of RREP from an intermediate node/ destination node, source node circulates RREQ to other nodes and starts route discovery procedure. RREP receiver will assign a credit to the RREP sender. When a node in the path sends one packet, one credit is reduced from the next hop node. After receiving a data packet, Credit Acknowledge (CACK) is sent back to a source node [9]. While transmission of CACK back to source node, intermediate node will modify credit of the next hop by adding 2. This increment indicates a higher trust level of the next hop. On the other hand, if CACK is not received, credit will be decreased. A node will be malicious if its credit reaches to zero and marked as a blacklist.

P. Agarwal et al. [15] have proposed a technique for detecting the black hole nodes. In this algorithm, a backbone network of trusted nodes is established over ad hoc network. An end to end checking is performed by source and destination nodes to verify whether all the data packets reached to the destination with the support of the backbone network of strong nodes. If a failure is encountered in cross checking the nodes, then the backbone network starts a procedure for detecting the suspicious nodes.

In this method, state full approach of IP address allocation [16], [17] is used along with this concept of backbone nodes.

III. Network Model & Assumptions

To approach this problem some assumptions are made which are as follows:

1) To select some nodes which are trustworthy and influential in terms of battery power and range? These reliable nodes are called Back Bone Nodes (BBN). BBNs have special function distinct from normal nodes and form a Back Bone Network.
2) Network is divided in to several grids, for the coordination between BBN and normal nodes.
3) Nodes entering in the network capable of finding their respective grid locations.
4) The number of BBNs is less than the number of normal nodes at any point of time.

A. State full Allocation of IP Address

In this method state full approach has been used for IP address configuration. In MANETs, there are two approaches of IP address configuration; one is state full and another is stateless approach.

In the stateless approach [16], an unconfigured host itself acquires its own IP address with random assignment and duplicate address detection mechanism is used to attain address uniqueness. No allocation table is kept in stateless approaches.

In the state full approach unlike state less approach, an unconfigured host requests it's neighboring MANET to work as proxies to acquire an 'IP' address.

B. Core Maintenance of the Allocation Table

In this mechanism, we are using stateless approach thus unconfigured hosts will request back bone network to obtain IP address. Only Backbone network in MANET has authority to allocate the IP addresses for unconfigured hosts. This mechanism works on assigning a conflict free address to all newly entered nodes by using multiple disjoint address spaces [15]. Each BBN generates the unique numbers that are for that host. All the nodes in the MANET must have accessibility to the Backbone Nodes (BBN) all the time.

IV. Methodology & Algorithm

The objective of this mechanism is to discover the set of suspicious nodes locally at each node when they perform as a source node. As discussed in the assumptions, our mechanism utilizes the concept of Core Maintenance of the Allocation Table i.e., whenever a new node enters in to the network, it broadcasts a request message to obtain IP address. On receiving this message, one of the free IP addresses is randomly assigned to new node by the backbone node. After receiving the assigned IP, new node sends back an acknowledgement to the BBN. As only BBN nodes are responsible for the assignment of IP addresses, that's why only BBN is aware of availability of restricted IPs of the network.

A. Back Bone Node Based Black Hole Detection Algorithm (BBNBD)

This algorithm shows the steps to be followed to detect the black hole nodes. Algorithm is divided in to following four phases:

1) Phase-I Backbone Node (BBN) Selection Procedure:

Step 1. Suppose, there are N number of normal nodes in a network and M number of nodes are selected as BBN which are reliable and influential in terms of battery power and range. Only BBNs are responsible for assigning the IP addresses to the newly entered odes in the network.
Step 2. (N-M) nodes will participate in message dissemination.
Step 3. Assign Restricted IP to (N-M) nodes.

2) Phase-II Actions Executed by Source Node (SN)

Step 1. SN will send a Request for RIP to BBN.
Step 2. BBN reply with RIP.
Step 3. SN will initiate Route Discovery procedure by sending RREQ along with RREQ for RIP.

RREQ is sent not only for route discovery but also for RIP again to find out the black hole nodes (as it is clear only BBNs are responsible for assigning RIPs and all the reliable nodes are aware of this).

Step 4. SN waits for Route Reply (RREP).

3) Phase-(III) Actions Executed by Intermediate Node (IN) /Destination Node

Step 1. After receiving RREQ from the SN, it first updates its routing table by making an entry for the RREQ receiver node.
Step 2. If received node is destination node or it has route to destination node, it will send RREP to SN, otherwise; simply forward the packet to its neighbor.
Step 3. After receiving a RREP, Route information is recorded in its routing table & then forwards the RREP in the reverse direction.
Step 4. When it receives a request to enter into the promiscuous mode, a process to listen the network will be initiated for all the packets intended to that particular IP address (which sent RIP again) & monitors its neighbors, for the flow of the dummy data packets. The request of entering into promiscuous mode is received only when the RREP for RIP is also received along with RREP for route discovery as all reliable nodes know the fact that only BBNs are responsible for assigning RIPs.
Step 5. In case, if normal data packet loss is found extremely less than the dummy data packet at any suspected node, it informs back the IP of this IN.

4) Phase-IV Black Holes Detection and Removal Process

5) Actions Executed by Source Node on Receiving the RREP

Step 1. If SN receives RREP only for RREQ of destination not for RIP, it continues the transmission of data through the route normally.

Step 2. If the RREP is received for the RIP, black hole detection procedure is initiated by source node. It sends a request to the neighbors of next hop for RIP, to enter into promiscuous mode. These nodes listen to packet intended to specified destination node along with the packet it intended to them. In promiscuous mode nodes are responsible for the monitoring of packet flow of dummy packets sent by SN and also transmit the monitor message to the next hop of dummy data packets & so on. When these promiscuous nodes find the dummy data packet loss, it informs SN about this IN.

Step 3. To detect the black hole, feedback received from the different paths is verified and the information is broadcasted all over the network to all the nodes, to mitigate the effect of the Black Holes.

V. Simulation & Result

This section elaborates simulation parameters, performance metrics used to evaluate network and simulation results which are as follows:

A. Simulation Parameters

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Simulator	NS-2[ver. 2.35][18]
Simulation Time	15 Sec
Number of Mobile nodes	15
Propagation Model	Two way ground
Mobility Model	Random way point
Pause Time	.05 Sec
Traffic Model	CBR
Terrain Area	800m x800m
Transmission range	250m
Routing Protocol	AODV

B. Performance Metrics

For evaluating the performance of this protocol, three parameters throughput, packet drop rate and delay are considered.

Throughput is the total number of delivered data packets per second.

Packet Drop rate is the ratio of data packet lost to the total number of packets generated by the source.

End to End Delay is defined as the average end to end delay of data packets from senders to receivers.

C. Results

After running the simulation following results are generated:

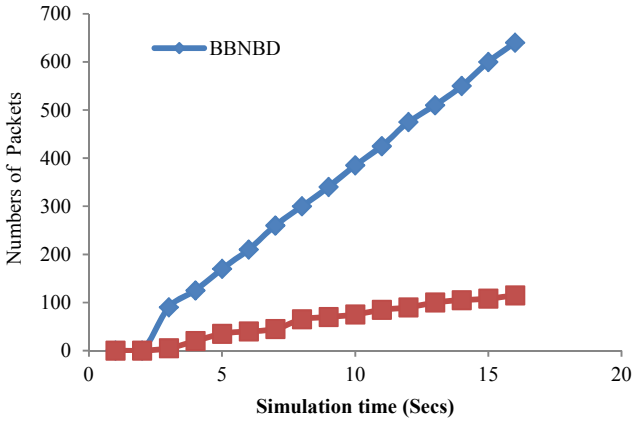

Fig. 1 Throughput

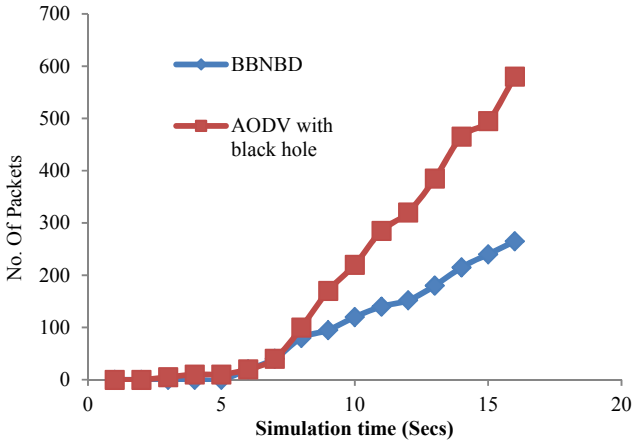

Fig. 2 Packet drop rate

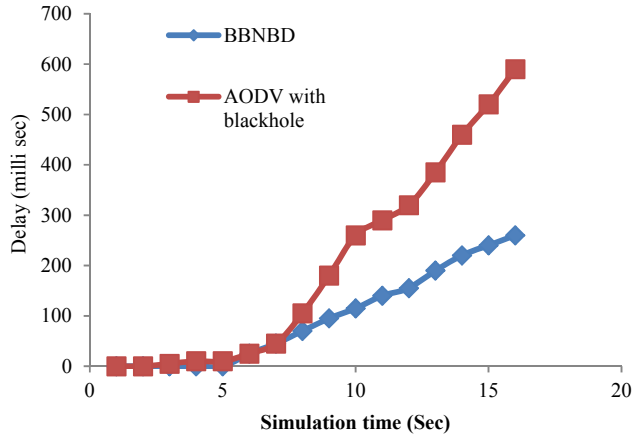

Fig. 3 End to end delay

These graphs are showing that when the above approach is applied in the network, black hole attack is detected and prevented to improve the performance of the network.

VI. Conclusion & Future Scope

Black hole attack is a well-known security threat. In this paper, a mechanism is proposed to prevent black hole attack.

AODV has been enhanced by using the concept of back bone nodes with the restricted IPs. We have simulated the proposed scheme and analyzed its results. Our solution increases throughput and decreases delay and packet drop rate.

As future work, we plan to develop simulations to examine the performance of the this solution on basis of various other security parameters like memory usage, normalized routing overhead, mobility, increasing number of malicious nodes, increasing number of nodes and we also plan to study the effect of GRAY hole nodes (nodes which changes their behavior trusted node to black hole) and techniques for their detection & prevention.

REFERENCES

[1] S. Basagni, M. Conti, S. Giordano, I. Stojmenovi, "Mobile Ad Hoc Networking", IEEE Press and John Wiley & Sons, Inc., 2004.
[2] M.S. Corson and A. Ephremides, "A distributed routing Algorithm for Mobile Wireless Network", ACM J. Wireless Networks, 1(1), Jan. 1995.
[3] C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Mobile Computer Systems and Applications, 1999, pp. 90–100.
[4] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
[5] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesi , Blekinge Institute of Technology Sweden, 22nd March 2007.
[6] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Network Security. On Signals and Communication Technology, Springer, New York, 2009.
[7] Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications (0975 - 8887), 2010, Volume 1, No. 22, pp. 38-42.
[8] H. Deng, W. Li and D.P. Agrawal, "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, October 2002, pp. 70- 75.
[9] Nidhi Gupta, Sanjoy Das, Khushal Singh, "A Comprehensive Survey and Comparative Analysis of Black Hole Attack in Mobile Ad Hoc Network", World Academy of Science Engineering and Technology, International Journal of Computer, Information Science and Engineering, vol. 8, no. 1, 2014.
[10] M. Medadian, A. Mebadi, E. Shahri, "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., Dec.2009, pp.530-535, 15-17.
[11] B. Sun, Y. Guan, J. Chen, U.W. Pooch , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
[12] S. Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.
[13] P.C. Tsou, J. M. Chang, L, H. C. Chao, J. L. Chen , " Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, Feb. 2011, pp. 13-16.
[14] W. Saetang and S. Charoenpanyasak, "CAODV Free Blackhole Attack in Ad Hoc Networks" Conference on Computer Networks and Communication Systems, IPCSIT vol.35, 2012, pp. 63- 68.
[15] P. Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Suwon, Korea, 2008, Pages 310-314.
[16] S. Indrasinghe, R. Pereira, J. Haggerty, "Conflict Free Address Allocation Mechanism International for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07).
[17] M. Mohsin and R. Prakash,"IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016.
[18] The Network Simulator - NS-2 (http://www.isi.edu/nsnam/ns/build.html).