An Enhanced Approach for Detecting Black Hole Attacks in MANET

Pratima Sarkar
Department of Computer
Science and Engineering
Sikkim Manipal Institute of Technology
Sikkim, India

ABSTRACT
The proposed paper is enhanced version of our previous paper" A cryptographic approach towards Black Hole Attack Detection" accepted in CNSA 2012 gives solution for false reply from a node and confirms reply is coming from destination node in Black Hole attack. This paper proposed an algorithm for detecting malicious node that drops packet and the node that gives false reply to the source node. In this work detection of false reply by a malicious node and also detecting a node that drops the packets. Detection in both the cases is performed locally using the previous node of the attacker. This paper uses two acknowledgements for detecting malicious node. By using this algorithm the security mechanism overhead would be decreased, throughput also increased and reduced end-to-end delay. The graphs at the result section shows improvement in network performances in the presence of black hole attacks and it can do so with a negligible level of additional overhead.

Keywords
Mobile Ad hoc Networks Routing, Intruder Detection; DOS; Black Hole Attack

1. INTRODUCTION
A mobile ad hoc network (MANET) [1] is a set of mobile nodes and they communicate with each other via wireless connection. In MANET structure of the networks changes dynamically as each node have some speed. Each node of the network work as a router and has capability to identify path for a given destination node. In MANET due to absence of central control, security is one of the major issues. There no central authority to identify malicious node. However, due to some fundamental characteristics [2], ad hoc network is particularly vulnerable to attackers, and routing plays an important role in the security of entire ad hoc network and is not trivial to solve.

The security threats have been extensively discussed and investigated in the wired and wireless networks [3], the correspondingly perplexing situation has also happened in MANET due to the inherent design defects [4]. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks [5], routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, et cetera [6]. Especially, the misbehavior routing problem [7] is one of the popularized security threats such as black hole attacks.

In MANET, there are many routing technology and routing protocols, like AODV (Ad Hoc On-demand Distance Vector Routing). In AODV routing protocol for transmission of information two phases are required: route discovery phase and properly packet delivery. AODV routing protocol allows mobile nodes to find out routes quickly for a destinations. In case of link breakage and any changes in network topology always updates timely manner. Controlled packed used by AODV protocol is Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) and these message types are received via UDP. In AODV the source node sends a routing request packet RREQ to its neighbor's node. When the destination node received RREQ, it send routing response packet RREP to the source node via same path. On receiving the RREP by the source node it started transmission of data to the destination node along the corresponding opposite direction of the fastest RREP. In Black Hole attack malicious nodes send fastest reply to source node so it can able to attack traffic of the network. After receiving packets from other node it simply drops the packets instead of forwarding it. So performance of the network decreases drastically.

2. PROPOSED SOLUTION
It is observed from the state of the art studies that most of the existing intrusion detection schemes suffer from communication overhead, due to the frequent monitoring involved. This may prove to be dangerous in case of high traffic. In the following section, a novel technique for intrusion detection is proposed to reduce the overhead problem only by using controlled packets of small size and also gives the solution for two problems related with Black Hole Attack these are false reply from malicious node and packet dropping by the selfish node.

2.1. Solution for false reply from malicious node

2.1.1. Logic Description
In this solution two acknowledgements are used to detect false reply from a node. In figure 1 at first node 1 broadcast RREQ to its neighbor nodes and neighbor nodes again propagates RREQ to its neighbor nodes, to find the destination node. So RREQ packet send by node 1 is received by the node 2 and 3 then again node 2, 3 do same to the other neighbor nodes. In this way finds its destination node 7 via node 4 and 5. Now node 3 sends false reply RREP to the source before real destination then source sends packet via this node. In this case node 3 does not send RREQ to other neighbor node and simply drops.

To solve this problem two reply messages are used one is RREP another is ACK. This ACK is send by a node to previous to previous node of that node for example in the figure 1 node 7 to 4, node 5 to 2 and node 4 to 1.That means this ACK conforms that each intermediate node must sends RREQ to its neighbor node until it reaches to destination node. In case of node 3 no such ACK message received by node 1 as node 3 does not sends the RREQ request packet

further. So after time out it intruder is detected by following algorithm.

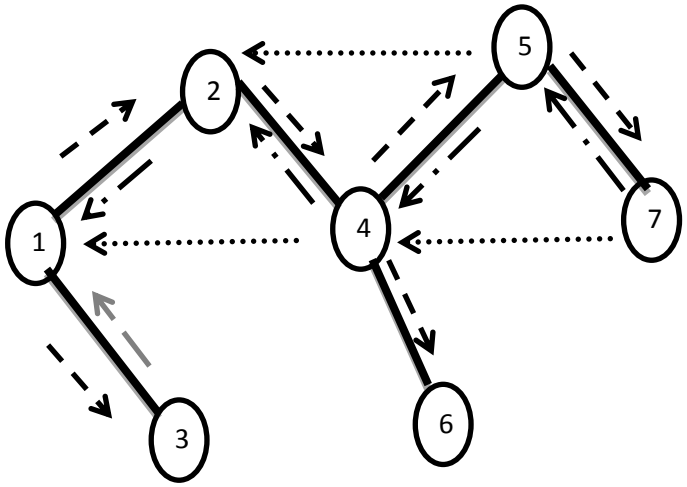

Figure 1

RREQ
RREP
ACK
FALSE RREP

2.1.2. Algorithm

T_{ACK} =>Time between sending RREQ request and received ACK by any node.

T_{THR} =>Maximum time take to reach ACK to the source node.

T_{RREP} =>Time between sending RREQ request and received RREP by starting node.

Algorithm for intermediate node:

Send RREQ request to find the path. RREQ Request must remember the path (identification of previous node and previous to previous node) so it can send ACK message target node.

Do until ACK reaches to the start node
Note time and starts counter by node
DIS: Node waits for RREP and ACK //AFTER DESTINATION DISCOVERED
IF RREP received then
Waits for ACK
IF $T_{ACK} > T_{THR}$ THEN
Stop counter and through an alarm
next node suspected as an
Intruder node.
ELSE
goto DIS for previous
IF source node received ACK on time then route is all right.

Algorithm on Source Node

sends RREQ
Starts timer
Call INTERMEDIATE NODE
waits for ACK and RREP
IF $T_{ACK} > T_{THR}$ AND $T_{RREP} > T_{THR}$ THEN
through an alarm
ELSE
Route is all right.

2.2. Solution for problem packet dropping by selfish node

2.2.1. Logic Description

After path detection from source to destination node data packets are dropped by malicious node. To detect malicious node following algorithm is used. In the fig 2 node 5 does not sends data packet to the node 7 so packets is lost, does not reached to its destination. To detect intruder one reply message ACKR used by the receiver of packet node 5 to node 2 this is pervious to previous node of 5.We assume that each node have one counter and it starts the counter at the time of sending packet and waits for ACKR reply.

Now one threshold value is used i.e T_{ACKR} which gives the maximum time taken to receive the ACKR reply. If counter value exceeds the threshold value then it through an alarm and it shows packet does receive the node. In figure 2 node 4 does not received reply from node 7 in proper time so node 5 suspected as an intruder.

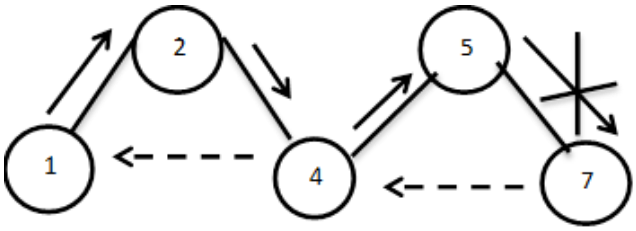

Figure: 2

Data packet Transmission

ACKR

ACKR =>Reply message from packet receiver to previous to previous node.(In fig:2 node 3, 5 to 2, 4 to 1, 7 to 5)

T_{ACKR} =>Maximum time to reach ACKR.

T_{COUNT} =>time between sending data and received ACKR.

2.2.2. Algorithm

For each node exists in the path

Send data packet to the next node and starts the counter

Waits for ACKR

IF $T_{COUNT} > T_{ACKR}$ THEN

Alarm started

Else

No response

3. SIMULATION ENVIRONMENT

For simulation of this work NS2 is used. For making network layout TCL script is used and for changing AODV protocol C++ language is used.

In this work 5 scenarios are created for simulating each of the parameter. Number of nodes varies with each scenario and number of black hole node is fixed. Following table describes rest of the parameters.

Table 1: Simulation Parameters

Parameters	**VALUE**
Simulator	NS-2 Version 2.35
Area	1000m*1000m
Simulation Time	20s
Number of nodes	10 to 50
Traffic model	CBR
Mobility model	Random way point
Routing Protocol	AODV
Channel	Wireless Channel
Link Layer Type	LL
Antenna Type	Omni direction
Number of malicious nodes	5
Mac protocol	802.11
Data rate	10kbps
Data packet	512 bytes/packet
Examined Approaches	Without attack and under attack
Number of connection	10 TO 30

4. RESULT

This study adopted the following main performance metrics to evaluate the performance proposed security algorithm.

Network Throughput

Throughput is the number of data packets are sent from source to destination per unit of time. Throughput is calculated as received throughput in bit per second at the traffic destination. This graph shows throughput variation after applying proposed solution

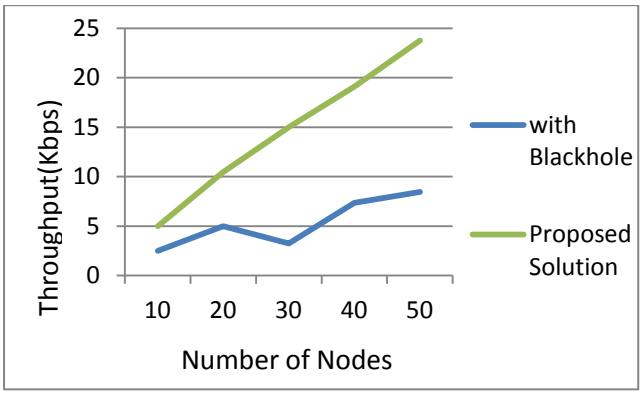

Figure 3: Number of nodes vs Throughput

In the above figure throughput is plotted with respect to increasing number of nodes in presence of black hole attack and with proposed solution. From the figure 3 it possible to conclude that proposed solution gives better throughput. After detection of malicious node and avoiding that node throughput increases. In case of black hole attack it drops packet thus reduces throughput. Here still gradually throughput increases because number of malicious nodes are fixed but number of connection increases.

Average end-to-end Delay

The end-to-end delay is the average time elapsed for all data packets reached successfully from the source node to the destination. Below graph shows effect of end-to-end delay with respect to number of nodes.

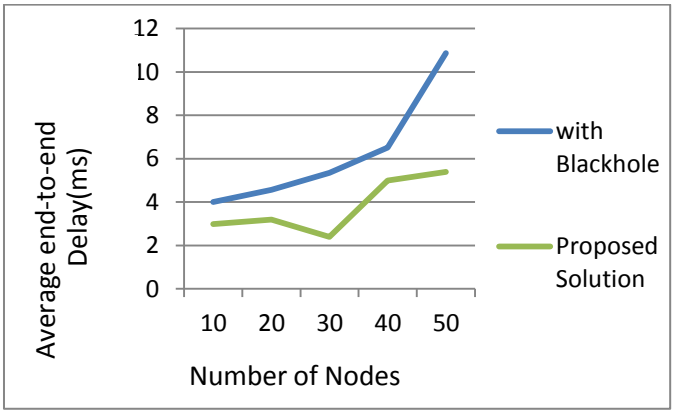

Figure 4: Number of nodes vs Average end-to-end delay

From the above figure it is possible to conclude that average end-to-end delay has decreased after using proposed solution. In black hole attack with increasing number of node average end-to-end increases almost exponentially.

Routing Overhead

The routing overhead is measured as the average number of routing control packets (RREQ, RREP, ACK, ACKR) exchange by all the nodes in the network during the AODV routing process performed. This metric affects battery power consumption, and bandwidth utilization. In the following figure 5 it is shown that number of controlled packet increased than AODV algorithm but does not have huge difference because in case of route discovery it uses one packet extra ACK and for packet received acknowledgement using one packet ACKR. They are of small size and using UDP protocol.

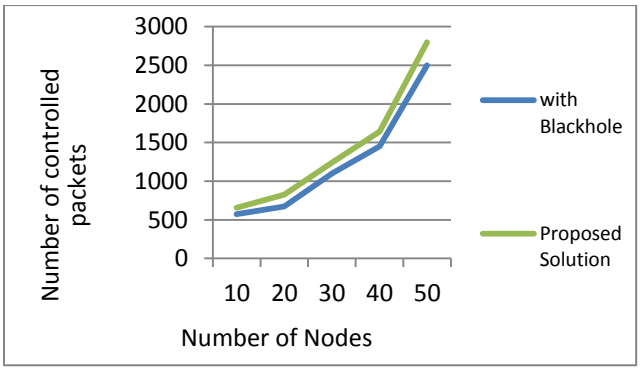

Figure 5: .Number of nodes vs number of control packets

5. CONCLUSION

The art studies that most of the existing intrusion detection schemes suffer from network overhead by increasing number of controlled packets of small size. In MANET, the malicious nodes with some misbehavior are common, one type of such attack is Black Hole Attack in AODV routing protocol. In this attack selfish node gives false reply to source node. If this reply comes before destination node reply then it creates problem. Above proposed solution for Black Hole Attack problem try to optimize end to end delay, throughput and network overhead also tries to detect the nodes which send false reply to source node and selfish node in the network. To optimize delay and network overhead this algorithm limits the number of control packets. Less number of routing information are used in ACK and ACKR packets to reduce the network overhead. This paper uses two acknowledgements to find out selfish node and confirm that reply comes from destination node and packet reached to the destination properly. As a result of simulation, throughput increases with increasing number of nodes. In Fig 4 average end-to-end delay slightly increases with number of nodes because of number of connection increased. But in Fig 5 number of controlled packet almost double of only ADOV algorithm still it would not increase traffic more as size of the packet and distance travelled by the packet is very less.

6. FUTURE SCOPE

This work proposed an algorithm for detection of Black Hole attack but in case of collaborative Black Hole attack unable to determine solution. This work can be extended to find out collaborative Black Hole attack.

6. REFERENCES

[1] Royer E.M.,(1999)"A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks",[J]. IEEE Personal Communication. 4(2) : pp.46-55.

[2] Mishra, A, Nadkarni, K, & Patcha, A,(Feb 2004)"Intrusion Detection in Wireless Ad Hoc Networks",IEEE Wireless Communications", VOL.11pp.48-60

[3] Zhou L & Chao H-C (2011)" Multimedia Traffic Security Architecture for the Internet of Things. IEEE Network "25(3):29–34.doi: 10.1109/MNET.2011.5772059

[4] Yang H, Lou H, Ye F & Lu SZhang L (2004)", Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications "11(1):38–47. doi:10.1109/ MWC.2004.1269716

[5] S, Reddy BVR, & Hoda MN (2010) "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption. IET Communications", 4(17):2084–2094. doi: 10.1049/ietcom.2009.0616

[6] Wu B, Chen J, Wu J & Cardei M (2007) "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks ",In: Xiao Y, Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York

[7] Marti S, Giuli TJ, Lai K & Baker M (2000) "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Paper presented at the 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts,

[8] H.Deng, W. Li & D. Agrawal (2002)" Routing security in ad hoc networks. IEEE Communications Magazine", vol. 40, no. 10, pp. 70-75.

[9] Mehdi Medadian, M.H. Yektaie & A.M Rahmani(2009)" Combat with Black Hole Attack in AODV routing protocol in MANET",IEEE.

[10] Songbai Lu, Longxuan, Li Kwok-Yan Lam & Lingyan Jia (2009)" SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security.

[11] Lien-Wen Wu & Rui-Feng Yu (2010)" A Threshold-Based Method for Selfish Node Detection in MANET", IEEE, pp 875-882.

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

[13] Akanksha Saini & Harish Kumar (December 2010) "Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Issue 2.

[14] Pratima Sarkar & Rituparna Chaki (2012) "A cryptographic approach towards Black Hole Attack Detection" Accepted in CNSA-2012 Chennai.