Prevention of Black hole Attack in AODV protocols for Mobile Ad Hoc Network by Key Authentication.

***Mr. G*olok Panda**[1]
Department of CSE
Sharda University, India

Mr. Gouri Shankar Mishra[2]
Department of CSE
Sharda Univercity, India

Mr. Ashok Kumar Sahoo[3]
Department of CSE
Sharda University, India

ABSTRACT

Ad-hoc network is an autonomous mobile node. It is a set of temporary based networks, which has not fixed infrastructure. The Ad-hoc networks are very much positive towards attack by malicious node due to its vulnerabilities nature of routing protocols. There are large numbers of attacks affect the Ad-hoc networks. In between these attacks one is very much known as Black Hole Attack. The main propose of this paper is to prevent the intruders which carry the black hole node by key authentication manner and prevents it for doing any misbehave in network.

***Keywords*:** *Wireless ad hoc network, black hole, security, Key authentication.*

I. INTRODUCTION

The application of networks ranges from research to battlefield and academics to situations like natural calamities, which can be constructed with or without fixed infrastructure. A network without any fixed infrastructure consisting of a number of nodes which moves arbitrarily and works as a router as well as transceiver is known as Ad hoc Network.

The nodes communicate by sending packets to other nodes in its radio range. The ad hoc network is characterized by a number of attributes like self-organization, self-configuration, dynamic topology, restricted power, temporary network, lack of infrastructure, etc. These attributes make the ad hoc network applied in various areas, such as disaster recovery operations, smart building, military operations etc. Application fields like military operations are sensitive and prone to security attacks.

The security aspects of ad hoc networks is very challenging due to the reasons that the network is having dynamic topology, arbitrary movement of nodes, absence of fixed infrastructure, insecure wireless communication links and resource constraints.

Security attacks

Some mechanisms which help to prevent, detect and respond to security attacks in ad hoc network [9]. The goal of security is to counteract all kinds of attack to provide security services. The security services are as follows:

• **Authentication:** Ensures that the originator of a packet is the node that is claimed.

• **Access control:** Unauthorized access to resources is not allowed.

• **Confidentiality:** The packets should not be protects overall content or a field in a message. Confidentiality can also be required to prevent an adversary from undertaking traffic analysis.

• **Privacy:** Prevents adversaries from obtaining information that may have private content. The private information may be obtained through the

analysis of traffic patterns, i.e. frequency, source node, routes, etc..

• **Integrity:** Ensures that a packet is not modified during transmission.

• **Authorization:** Authorizes another node to update information (import authorization) or to receive information (export authorization). Typically, other services such as authentication and integrity are used for authorization.

• **Nonrepudiation:** Proves the source of a packet. In authentication the source proves its identity. Nonrepudiation prevents the source from denying that it sent a packet.

• **Freshness:** Ensures that a malicious node does not resend previously captured packets.

• **Availability:** Mainly targets Denial of Service (DOS) attacks and is the ability to sustain the networking functionalities without any interruption due to security threats.

• **Resilience to attacks:** Required to sustain the network functionalities when a portion of nodes is compromised or destroyed.

The rest of the paper is structured as follows: In section II, the black hole attack in MANETs is discussed. In section III summarizes related works and detailed description of the proposed algorithm is discussed in section IV. In section V, it represents the simulation results and in section VI, we draw a conclusion and address the future work.

II. BLACKHOLE ATTACK

The major principal of routing protocols of MANET is to establish an proficient, straight and shortest path in between communication nodes or entities. Generally the routing protocol in ad-hoc networks are divided into categories, *proactive* and *reactive* [4]. In proactive routing protocols, the information about route is stored in route table and updates it periodically, such as DSDV [5]. In reactive routing protocols, the information are exchanged in between nodes when they needed such as AODV [6] and DSR [7].

I. AODV

AODV stands for Ad hoc On-Demand Distance Vector. The route discovery will not be started until it is required (on demand). The protocol operates in two processes: Route discovery and Route maintenance. Route discovery mechanism helps when the sender has no option to route its data packet, i.e. no route information avails in Route Table (RT). The sender node relays a *Route Request* (RREQ) packet into the network. A node receives a fresh *Route Request* will check its Route Table for confirmation about the route to destination. If the node is destination then it sends Route Reply (RREP) packet to source. If it is not, then the node is forwarded the RREQ to its neighbor nodes for confirmation. Before forwarding, it keeps reverse path to the source node in its Route Table. Route Table records the route information of the next hope, the distance and the current highest sequence number it has seen. Mainly route maintenance informs to source node about new route discover, the unfortunate comes when changes in the network topology and invalidate the stored route information.
Every point has some pros and cons. Like this the AODV has some limitations, which makes the annoyance in communication. The weakness of AODV as follows [10]:

1. ***Rush attack with RREQ***: This attack means suppress of the valid RREQ sent by a real originator.

2. ***False message propagation with RREQ***: The goal of this attack is reroute the traffic through the malicious node, and then throw it away.

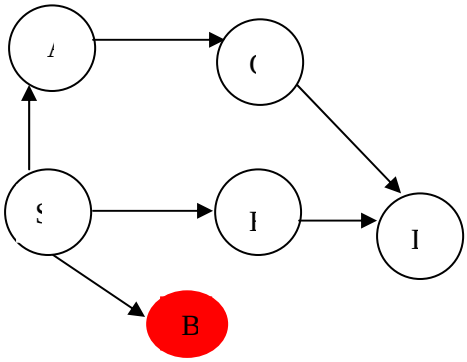
3. ***False reply with RREP***: This attack seizes a request with an answer, before it reaches its destination.

4. ***False message propagation with RREP***: In this attack, the malicious node tries to reroute traffic

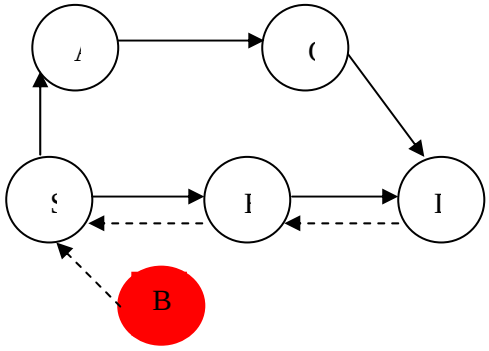
by using false RREP. The purpose is to abandon the traffic.

II. Black hole Attack

The communication in between two nodes take place when both of them are actively participates in data exchange process. The source node wants exchange some information or sends data to the destination node, then it checks its *Route Table* whether the route available or note, if not then it will initiate the route discovery process. We assume node B to be a malicious node (See Fig. 1). Using the routing AODV protocol the source node relay broadcast the RREQ message to its neighbors. Then the malicious node B claims that it has the route to the destination node after receiving a RREQ by RREP message. The destination node also sends the response of RREQ. If the RREP message of destination node has been reached before the message of malicious node then it works well. If not then the malicious node misbehave as it wish. Suppose the malicious node's response message has reached at source node first, the source node feels that the route discovery process has been completed. Then it ignores all the response messages and ready to send the data packets. The data packets are transmitted through forged routing. It implies that the malicious node success in its dirty work and consume the route and dropped all packets. Node B could be referenced as black hole in network, we called as black hole attack [11].



(a) Propagation of RREQ



(b) Propagation of RREP message

Fig. 1: Black hole attack

III. RELATED WORK

There are a large number of methods or proposes have been authored to detect the black hole attack.

In [8] *Hongmei Deng et al*. has been proposed a solution for single black hole node detection. In this method, each intermediate node send backs next hop information and RREP message. When the source node receives the reply message, it does not send the data packets immediately. The node takes out the next hop information from the reply packet and then sends a *Further-Request* to next hop for verification of route existence in between intermediate node who node who sends back the Further Reply (FRP) message, and that it has a route the destination node.

In [9]*Luo Junhai et al*. proposed a method to prevents the black hole attack by authentication mechanism. The authentication mechanism, based on the hash function, the Message Authentication Code (MAC), and Pseudo Random Function (PRF), is proposed for black hole prevention on top of Ad-hoc On-demand Distance Vector (AODV).

In [12] *M. Khalili shoja et al*. proposed a hash chain mechanism to prevent the black hole attack. Black hole attack is based on alteration of sequence number and hope count. In this mechanism, when an intermediate node receives RREQ or RREP, check an extra field to verify sequence number and hop count. The hash_RREQ and hash_RREP fields are add with RREQ and RREP field respectively. A seed value should be choose randomly for calculating hash function.

IV. PROPOSED ALGORITHM

In this paper, we propose a new algorithm based on AODV routing protocol. In AODV, there is a HELLO message is broadcasted to its neighbor for showing the presence in network. There is also a routing table maintain by all nodes for temporary basis those who are in active state.

The total bits consume by these routes discovery and route maintenance is 32 bit each. In both RREQ and RREP packets the 9 bits *Reserved Sector* will be there.

	0	1	2	3	4	5	6	7	8		
	Reserved										

Fig. 2: Reserved bits in RREQ & RREP

Our main aim is not to increase the size of packet and also not the support the overhead of network.

The proposed algorithm is based on the Key Mechanism process. In this algorithm we have to go through some phases like pseucode for key generation and key comparison.

Pseudocode for Key Generation:

1. Consider the IP address of node
2. Conversion process of IP address into binary form (X).
3. X << 12
4. Z = X AND Y (Y bit stream)
5. Key (K) = 9 bits of Z

The spoofer always tries to trace the subnet of IP address. Due avoid this attack we take 12 digit left shift of the binary numbers. Then we take an AND operator for reshuffling or making the number to very complex. After key generation completed, the key will be fitted in the 9 bits reserved sector in packets.

The packet has information about originator IP address, Destination IP address, Destination Sequence no., Hope count and Life time.

The HELLO message has been broadcasted to its neighbor nodes. When the node got HELLO message then next pseudocode will be applied for confirmation about the node's status.

Pseudocode for Key authenticating:

1. IP address of originator that broadcast the HELLO message
2. Repeat the step of pseudocode for Key Generation 2 to 5.
3. K2 fetched from the reserved bits.

```
4.  {
            If K1 = = K2
            trust[i]=1
            else
            trust[i]=0
    }
```

Where [i] = node id of sender.

After comparing the both key, the trust value will be decided. The result shows that 1 then the node will be normal or trusty node. If the result shows that 0 then the node will be malicious. The key comparison value will be updated in routing table time to time. From the zero trust value messages will not accept at any cost.

V. SIMULATION

In this section we discussed about our simulation environment and its results. The simulation process has been carried out in QualNet 5.2. The well furnished methods and an improved version of random waypoint model is used as the model of node mobility. Performance has been taken in different scenarios and different parameter in between AODV and Secured AODV protocols. The Secured AODV (AODVs) protocol is based on our algorithm. The different parameters are:

First packet received: This parameter indicates that how much time will be required for route establishment process.

Total packets received: This parameter shows that total no. of packets received after completion of simulation.

Throughput: The total number of packet received per unit time. In another term, throughput is the packet size (in term of bits) that is going to be transmitted divided by the time that is used to transmit these bits.

Average End-to-End Delay of Data Packets: The average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. The end-to-end delay includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays at MAC layer, etc.

Average Jitter: It is the variation of time of the packet latency across the network. The packet jitter is an average of the deviation from the network mean latency.

There are some metrics that taken for simulation. These metrics has been helped to fetch the better performance in our simulation.

Table 1: Simulation Parameters

Parameters	Values
Traffic type	CBR
Simulation duration	100 sec
Simulation area	1000 * 1000 m
Number of mobile nodes	100
Transmission range	200 m
Movement model	Random waypoint
Maximum speed	5 m/sec
Packet rate	4 packets / sec
Packet size	512 bytes
Number of malicious nodes	4,8,12,16,20
Host pause time	30 sec
Transmission speed	10 Mbps

In Fig. 2 the first packet received timing has been drawn in a line chart.

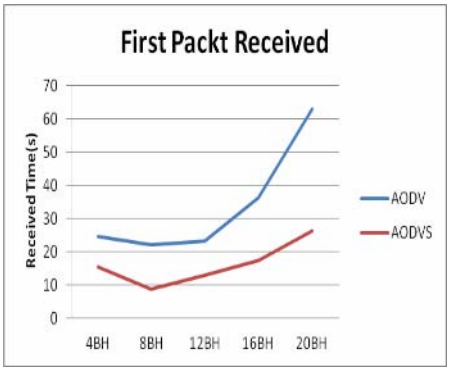


Fig. 2: First Packet Received

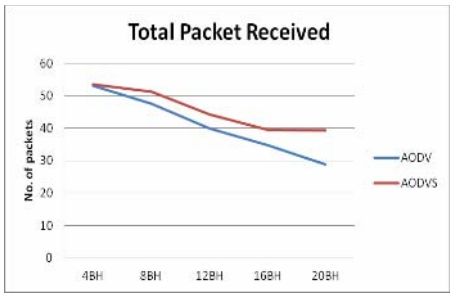


Fig. 3: Total Packet Received

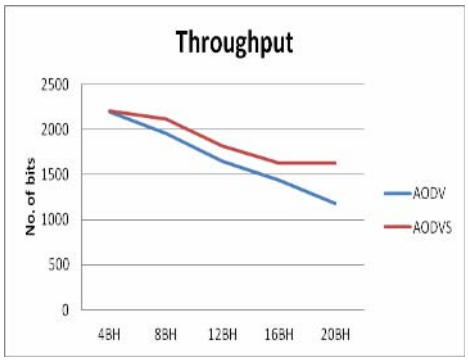


Fig. 4: Throughput

Fig. 5: Avg. End-to-End delay

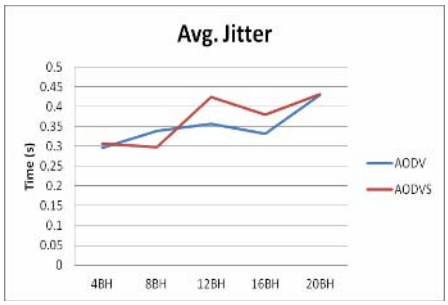


Fig. 6: Avg. Jitter

The above results distinguish that in the increase of 4% black hole node in network the First Packet Received, Total Packet Received, Throughput will be increased 50%, 13.81% and 13.88% respectively than the AODV protocol.

The Average Jitter will be found 4.98% lower that original AODV and the Average End-to-End will be decreased due to overhead of key mechanism.

VI. CONCLUSION AND FUTURE WORK

Finally after doing various comparisons, it can be concluded that the various authors have given various proposals for detection and prevention of black hole attack in MANET but every proposal has some limitations and their respected solutions. It is clear that malicious node is the main security threat that affects the performance of the AODV routing protocol. The approach leads to prevent the inducer that carry black hole node in very fast. Nobody will listen to malicious node's Hello message packet.

Every parameter has shown tremendous improvement except avg. jitter and avg. end-to-end delay due to the overhead of key mechanism. It will be extended such that the value of these parameters can be enhanced.

ACKNOWLEDGEMENT

I would like to take the opportunity to thank people who guided and supported me during this process. Without their contributions, this project would not have been possible. I have a great pleasure in expressing my deep sense of

gratitude and indebtedness to Mr. Ashok Kumar Sahoo(Associate Professor), Mr. Gouri Shankar Mishra(Assistant Professor) in Sharda University, my supervisors for their continuous guidance and invaluable suggestions at all time during research work. My special thanks to Mr. Rajiv Kumar, Assistant Professor in Sharda University, Mr. Ankur Tyagi and to all my friends for their support with me. Finally, many thanks to my parents and family members for their love, blessings, support and encouraged me at every instant of time.

References

[1] Poongothai T. and Jayarajan K., "A non-cooperative game approach for intrusion detection in Mobile Ad-hoc networks", International Conference of Computing, Communication and Networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4

[2] E. Cayirci, C.Rong, "Security in Wireless Ad Hoc and Sensor Network", vol. I. New York: Wiely 2009, pp.10.

[3] D. Djenouri, L. Khelladi and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks", IEEE Communication Survey & Tutorials, Vol. 7, No. 4, 4th Quarter 2005.

[4] E. M. Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Person. Commun., Vol. 6, no.2, Apr.1999.

[5] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", Proceedings of the SIGCOMM '94 Conference on Communication Architectures, Protocols and Applications, pp 234-244, Aug 1994.

[6] C. E. Perkins, E. M. B. Royer and S. R. Das, "Ad-hoc On-Demand Distance Vector (AODV) Routing", Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv -00.txt, Feb.2003.

[7] D. B. Johnson, D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, edited by Tomasz Imielinksi and Hank Korth, Chapter 5, pp 153-181, Kulwer Academic Publishers, 1996.

[8] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad-hoc Network", IEEE Communications Magazine, Issue 40, pp 70-75, 2002.

[9] S. Sreepati, V. Vengalla, and A. Lal, "A Survey paper on Security Issues Pert to Ad-Hoc Networks". www4.ncsu.edu/sssreepa/Adhoc-networks-Security-Survey.doc.

[10] J. Gronkvist, A. Hansson, and M. Skold, "Evaluation of a Speccification-Based Intrusion Detection System for AODV", di.ionio.gr/medhocnet07/wp-content/uploads/papers/90.pdf, 2007.

[11] L. Junhai, X. Liu, and Y. Danxia, "Research on multicast routing protocols for mobile ad-hoc networks", Cmput Netw., vol. 52, no.5, pp. 988-997, 2008.

[12] M. Khalili, H. Taheri, S. Vakilinia, "Preventing black hole attack in AODV through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, pp. 1-6, 2011.

Authors:

Golok Panda is currently a M.Tech. Scholar in Computer Science and Engineering, Sharda University, India. He received his B.Sc. degree from Uttkal University, and MCA from Manipal University. His research interests in Network security and Mobile Ad-hoc networks.

Mr. Ashok Kumar Sahoo joined as Associate Professor in the Dept. of Computer Science and Engineering, Sharda University, India. His primary research interests in security, networks, Mobile Ad-hoc networks and Image reorganization.

Mr. Gouri Shankar Mishra joined as Assistant Professor in the Dept. of Computer Science & Enggineering, Sharda University, India. He has interest in Network Security, Mobile Ad-hoc networks and in Information systems.