INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Eliminating black hole attack with authenticated Diffie Hellman algorithm

Nitika Sharma[1], Sukhwinder Sharma[2]

[1]Research Scholar, Department of Computer Science, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India
[1]nsnitu88@gmail.com
[2]Assistant Professor, IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab, India
[2] sukhwinder.sharma@bbsbec.ac.in

Abstract: *The. Mobile ad hoc networks (MANETs) are complex distributed systems comprising wireless mobile nodes that can self-organize dynamically into arbitrary and temporary, ad-hoc network topologies. Since the mobile devices are free to move randomly, the network's wireless topology may change rapidly and unpredictably. The communication in a mobile ad hoc network can occur directly between mobile nodes or through intermediate nodes acting as routers. Each organization needs to effectively deal with this major security concerns, making a security policy according to its requirements and objectives. An effective security policy must be proactive in order to provide sufficient defense layer against a variety of known and unknown attack classes and cases. In our proposed work we have compared RSA algorithm and Diffie Hellman Digital Signature. We will also conclude the algorithm which will perform best.*

Keywords: *Mobile Adhoc Network, Protocol, RSA, Network security, Wireless Devices, Routers.*

1. INTRODUCTION

The innovation in mobile computing technology and the proliferation of communication devices (e.g., cell phones, laptops, personal digital assistants, or wearable computers) are revolutionizing our way of sharing information. We are at the verge of entering the ubiquitous communication era in which a user utilizes numerous devices through which he can access all the required information whenever and wherever needed. The mode of ubiquitous communication advocates wireless networks as the most appropriate solution and as a consequence, the wireless networking realm has undergone exponential growth in the past decade. Mobile ad hoc networks are autonomous distributed systems that comprise a number of mobile nodes connected by wireless links forming arbitrary time-varying wireless network topologies. Mobile links or nodes performed as hosts and routers. As hosts, they presented source and destination nodes in the network while as routers, they presented intermediate nodes between a source and destination, providing save-and-forward services to neighboring nodes. Nodes that mainly constitute the wireless network architecture are free to move randomly and manage themselves in arbitrary fashions. Therefore the wireless topology that interconnects mobile hosts/routers can change rapidly in unpredictable ways or remain relatively static over long periods of time. Also, mobile ad hoc networks are now beginning to play an important role in the civilian realm (e.g., campus recreation, conferences, electronic classrooms, and in the form of various mesh networks). [1]

1.1 ADVANTAGES OF MANET

- They represent access to information and services respective to geographic location.
- These networks can be managed at any place and time.
- These networks operate without the help of any pre-existing infrastructure.
- They can be used in emergency services [2].

1.2 APPLICATIONS OF MOBILE ADHOC NETWORKS

Military battlefield- Military equipment now routinely contains some sort of computer equipment. Through ad-hoc networking, the military could take the advantage of commonplace network technology to maintain an information network among the vehicles, soldiers and military head quarters. Basically the techniques of ad-hoc networks came from that field [3][4].

Commercial sector- Ad hoc can be used in emergency/rescue operations for natural calamities relief efforts, e.g. in fire, flood, or earthquake. Rescue operations must perform where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is delivered from one rescue team member to another [5][6].

Local level- Ad hoc networks could autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a conference

Personal Area Network (PAN) - Short-range MANET can simplify the intercommunication between various mobile devices (such as a mobile phone, laptops, and wearable computers). MANET can also extend to access the Internet or other networks by mechanisms e.g. Wireless LAN [7].

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

1.3 MANET PROTOCOLS:

Destination Sequenced Distance Vector (DSDV) Protocol: The destination sequenced distance vector routing protocol is a proactive routing protocol which is a updating of conventional Bellman-Ford routing algorithm. This protocol injects a new attribute, sequence number, to each route table entry at every node. Routing table is maintained at every node and with this table, node exchange the packets to another nodes in the network [8].

Ad-hoc On-Demand Distance Vector (AODV) Protocol: AODV algorithm was motivated by the limited bandwidth that is available in the media which are used for wireless communications. It brings in most of the advantageous concept from DSDV algorithm. The required route discovery and hop-by-hop routing, management of node sequence numbers from DSDV make the algorithm cope up with topology and routing information.

Dynamic Source Routing Protocol (DSR): The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node provide routing table containing information about the routes to destination. The nodes modify entries in the route cache as it learns about new routes [9].

Associativity Based Routing (ABR): The Associativity Based Routing (ABR) protocol is a new scheme for routing. It defines a new metric for routing called as the degree of association stability. It is free of loops, deadlock, and packet delicacy. In ABR, a route is selected on the basis of associatively states of nodes [10].

Temporally Ordered Routing Algorithm (TORA): The Temporally Ordered Routing Algorithm is one of the efficient and expandable distributed routing algorithm based on the idea of link reversal. TORA is used for highly dynamic mobile network and multi-path wireless networks [11].

1.4 ATTACKS IN MANET:

There are various kinds of attacks in ad hoc network:

Location Disclosure- Location disclosure is an attack that targets the confidentiality requirements of an ad hoc network. By using traffic analysis techniques, simpler astute and monitoring approaches, an attacker is able to detect the section of a node, or the structure of the whole network.

Black Hole- In a black hole attack a malicious node add false route responses to the route requests, announcing it as having the smallest path to a destination. These fraudulent replies can be fabricated to alter network traffic through the malicious node for simply to attract all traffic towards it in order to perform a denial of service attack by abandon the received packets.

Wormhole- The wormhole attack is one of the most powerful presented here since it involves the cooperation between two nasty nodes that participate in the network. The connection between the nodes that have established paths over the wormhole link is completely under the control of the two connive attackers. The packet strap is the solution to this attack.

Blackmail- This attack is relevant against routing protocols that use mechanisms for the identification of nasty nodes and propagate messages that try to blacklist the attacker. An attacker may construct such reporting messages and try to confine legitimate nodes from the network.

Denial of Service- Denial of service attacks aim at the complete disruption of the routing function and therefore the complete operation of the ad hoc network. In a routing table format overflow attack the malicious links floods the network with fraudulent route creation packets in order to consume the resources of the participating nodes and disturb the establishment of legal routes.

Routing Table Poisoning- Routing protocols maintain tables that provide information regarding routes of the network. In these kind of attacks, the malicious links generate and send fabricated signaling traffic, or update legitimate messages from other nodes, in order to injects false entries in the tables of the participating nodes[12] [13].

1.5 SECURITY REQUIREMETS AND OBJECTIVES:

Security means the protecting privacy, availability, integrity and non-repudiation. Security implies the recognizing of potential attacks from unauthorized access, use, modification or destruction. A security attack is an action that compromises the security of information in an unauthorized way. Security is the combination of processes, procedures and systems used to confirm confidentiality, authentication, integrity, availability, access control, and non-repudiation. Our main objectives are to ensure Integrity authentication and Security.[14]

2. PRELEMNERIES

In this section we will discuss some basic concepts that are related to our research work.

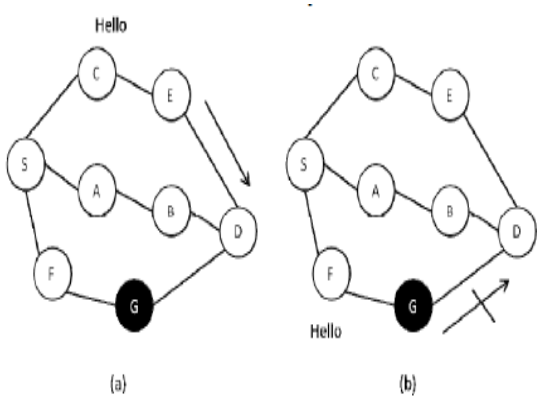

Figure 1: Black hole attack

2.1 PREVIOUS TECHNIQUE FOR BLACK HOLE ATTACK DETECTION

The previous method uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety, in other words, promiscuous

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

mode means that if a node *A* within the range of node *B*, it can overhear communication to and from B even if those communication do not directly involve *A*.[15]

The following is a detailed process. Consider a scenario as shown in Fig. 1; node S needs to communicate to node D and node G is a malicious node. Node S floods a RREQ packet in the network and waits for the RREP packet to obtain a fresh route to the destination node D. Now, there are two possibilities; the RREP packet may be received either from the destination node itself or from an intermediate node. In case 1, when the RREP packet is received from the destination node itself, a route is established. In case 2, when the RREP packet is received from an intermediate node, a node preceding to the node which sent RREP packet switches on its promiscuous mode and sends a hello message to the destination node through this node. If the hello message is forwarded by this node to the destination, the node and hence the route is safe; otherwise, the node is a malicious node. In latter case, the preceding node floods an alarm message to the network about the malicious node to isolate it.

2.2 PROPOSED APPROACH FOR BLACK HOLE ATTACK DETECTION

In our proposed work we have analyzed the performance of AODV protocol after implementing Diffie Hellman Digital Signature. The proposed technique authenticates the attacker and prevent network from black hole attack.

SIMULATION ASSUMPTIONS

- Radio Propagation Model: - Two Ray Ground
- Antenna type:- Omni Antenna
- Max packet size:- 512
- Number of Mobile Nodes: - 30
- Routing protocol:- AODV
- Simulation duration:- 30 sec

Description in steps:-

Suppose Alice = A and Bob = B

1. After calculating R_1, A sends R_1 to B.
2. After calculating R_2, and session key, B concatenates A's ID, R_1 and R_2. He then signs the result with his private key. B now sends R_2, the signature and his own public key certificate to A. The signature is encrypted with the session key.
3. After calculating the session key, if B's Signature is verified, A concatenates B's ID, R_1 and R_2. He then signs the result with his own private key and sends it to B. The signature is encrypted with session key.
4. If A's Signature is verified, B keeps the session key.

The use of digital signature assures that the malicious node should not enter the network with proper authentication. In this way the proposed algorithm prevent the network from black hole attack.

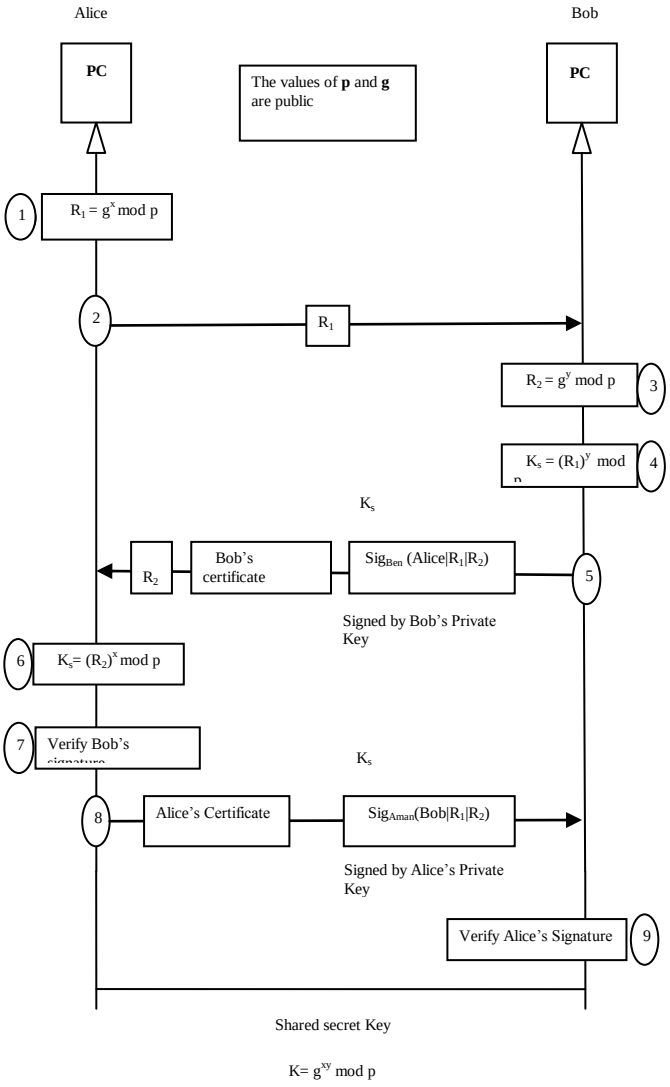

Figure 2: Diffie Hellman Digital Signature Scheme

3. RESULTS AND FUTURE SCOPE

The performance of proposed technique has been compared with existing technique using following parameters:-

- Throughput
- End to End Delay
- Packet Delivery Ratio

Throughput: Throughput refers to how much data can be transferred from one location to another in a given amount of time. The table below shows the percentage of throughput obtained in case of proposed digital signature scheme.

Table 1: Throughput

AODV without black hole	AODV with black hole	Digital Signature scheme with black hole
92	47.56	92.56

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

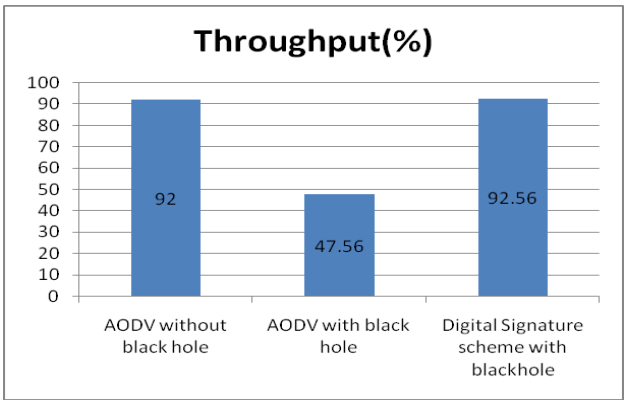

Figure: 3 Throughput

End-to-end delay: End-to-end delay or One-way delay refers to the time taken for a packet to be transmitted across a network from source to destination.

Table 2: Average end to end delay

AODV without black hole	AODV with black hole	Digital Signature scheme with black hole
0.08	0.055	0.045

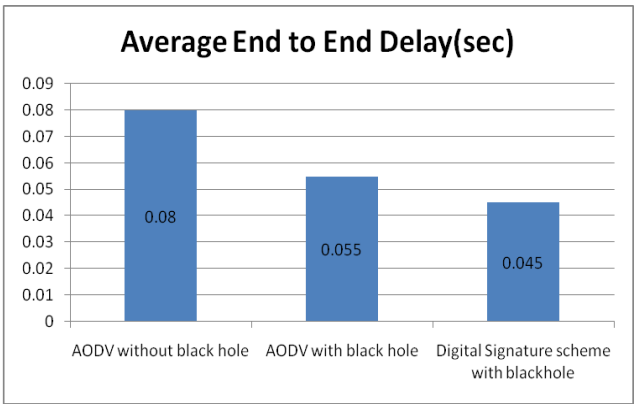

Figure 4: Average end to end delay

It is concluded that the proposed digital signature scheme has better throughput and average end to end delay as compared to the existing technique. In future this work can be extended further by considering other methods for dealing with black hole attack.

REFERENCES

[1] **A. Bechtsoudis and N. Sklavos (2012) "Aiming at Higher Network Security Through Extensive Penetration Tests" IEEE LATIN AMERICA TRANSACTIONS, VOL. 10, NO. 3, APRIL 2012.**

[2] **Priya Shrivastava, Sushil Kumar Manish, Shrivastava (2014) "Study of Mobile Ad hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 86 – No 3, January 2014.**

[3] **Kemal Akkaya , Mohamed Younis (2005) "A Survey on Routing Protocols for Wireless Sensor Networks"**

[4] **Gurpinder Singh , Jaswinder Singh (2012) "MANET: Issues and Behavior Analysis of Routing Protocols" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012 ISSN: 2277 128X**

[5] **Yogendra Kumar Jain, Nikesh Kumar Sharma (2012) "Secure Trust Based Dynamic Source Routing in MANETs" International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 ISSN 2229-5518**

[6] **B.Ruxanayasmin , B.Ananda Krishna (2013) "Minimization of Power Consumption in Mobile Ad hoc Networks" I.J.Computer Network and Information Security, 2013, 2, 38-44 Published Online January 2013 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2013.02.06.**

[7] **Stephen Mueller, Rose P. Tsang, and Dipak Ghosal (2012) "Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges".**

[8] **Guoyou He "Destination-Sequenced Distance Vector (DSDV) Protocol" Helsinki University of Technology .**

[9] **Parvathavarthini, A. Dr.Dhenakaran S.S (2013) "An Overview of Routing Protocols in Mobile Ad-Hoc Network" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 2, February 2013 ISSN: 2277 128X.**

[10] **Atul Yadav, Parag Joshi "Performance of Flat Routing Protocols in MANET' International Journal of Electronics and Computer Science Engineering 2035 ISSN 2277-1956/V1N4-2035-2041.**

[11] **Vincent D. Park and M. Scott Corsonb (1997) "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks" 0-8186-7780-5/97 $10.00 1997 IEEE.**

[12] **Jagtar Singh, Natasha Dhiman (2013) "A Review Paper on Introduction to Mobile Ad Hoc Networks" International Journal of Latest Trends in Engineering and Technology (IJLTET) Vol. 2 Issue 4 July 2013 143 ISSN: 2278-621X.**

[13] **Jawandhiya, Pradip M. Mangesh M. Ghonge. PROF. Deshpande J.S. DR. Ali M.S. (2010) "A Survey of Mobile Ad Hoc Network Attacks" International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071**

[14] **Abdulrahman H. Altalhi, (2012) "A Simple Encryption Keys Creation Scheme in Wireless Ad Hoc Networks", Scientific Research Publishing.**

[15] **Jain Shikha (2014) "Security Threats in Manets: A Review" International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.**