International
Journal
Of Advanced Research in Engineering & Management (IJAREM)
ISSN: 2456-2033 || PP. 58-64

Mitigating black hole attack using Public Key Infrastructure

[1]Umme-Haani, [2]Syeda Fareesa Naaz, [3]Arshia Sultana, [4]C. Atheeq
[1,2,3]Student, CSE, DCET, Hyderabad.
[4]Assistant Professor, CSE, DCET.

Abstract: Multi-hop wireless ad hoc network composed of wireless mobile devises communicate by relaying on intermediate node. This network characterized by lack of infrastructure, without central coordinator and constrained resources. Routing is possible by assumption that nodes in a network are cooperative, but it is not always true in distributed constrained resource environment. Attacker can perform the malicious activities by not following routing protocol stipulations, one such attack is black hole attack. In which attacker node manipulate the control message and attract the communication information towards it and then drop the information. Prior work detect and remove the black hole attack by monitoring the nodes, which is not feasible solution in hostile environment. We mitigate the black hole attack by PKI. Simulation results shows that our proposed method accurately prevent the black hole attack and hence extend the network performance.

Keywords: MANETs, Security, Black hole attack, PKI

1. INTRODUCTION

Mobile Ad Hoc Network (MANETS) is a collection of multi-hop wireless mobile nodes that communicate with each other without centralized communication. It is a dynamic network topology which changes frequently and unpredictably. Nodes can perform the role of both hosts and routers. One of the important characteristics of a MANET node is neighbour discovery. It also has some data routing abilities that the data can be routed for a source node to a neighbouring node[8]. It has flexible network architecture and variable routing paths to provide communication in case of the limited wireless connectivity range and resource constraints.

When a new network is to be established, the only requirement is to provide a new set of nodes with limited wireless communication range because a node has limited capability, that is, it can connect only to the nodes which are nearby and thus consumes limited power. MANETS have limited wireless connectivity range which require that a node should move in the region of at least one nearby node within the wireless communication range, else the node should be provided with the access-point of wired communication.

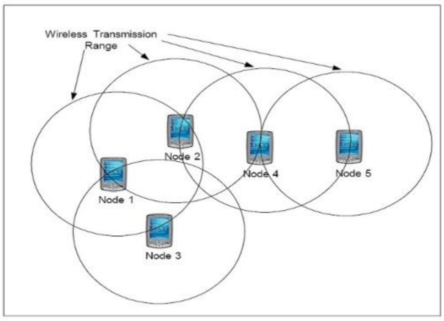

Figure 1. Mobile Ad Hoc Networks

The fundamental weak point to security attacks is peer-to-peer network characteristics. Therefore, it needs a security solution to address various types of attacks on MANETS. Another challenge of MANETS is that nodes are equipped with constrained energy and it is highly difficult to recharge the batteries of nodes during the mission.

The objective of paper is to provide security to MANET‟s environment by mitigating attacks on AODV routing protocol of MANET‟s[9], and to present its design and implement in wireless ad hoc networks. Through real implementations, we identify important design issues and propose an approach, to reduce the loss of data and to avoid declaring trusted nodes as black hole nodes by considering the public key infrastructure.

AODV:

AODV[1] is a well-known and most widely used protocol in MANETs. It is reactive and on demand protocol, in which routing information is exchanged only when communication needs to take place between nodes and only as long as the communication occurs this information is updated. AODV protocol uses three control messages that are RREP (Route Reply), RREQ (Route Request), and RERR (Route Error). RREQ packet is broadcasted by source, to find a path, to the nodes in the network and all the nodes which receive RREQ packet keep transmitting it until it finds a fresh enough route to the destination. On receiving RREQ, if the node is destination or if the node has fresh route to destination then it sends RREP packet. Hop count of every node increases by one on receiving RREQ message and route entry is updated with new data by intermediate nodes on receiving RREP message. After a node increases its sequence number each time a new RREQ, RREP, RERR messages are sent. A route discovery process is initiated whenever a node wants to communicate with other node.

AODV Route Discovery:

To establish a route from source S to the destination D, RREQ packet is broadcasted from S. On receiving RREP packet nodes G, H and I do one of the following:

(i) RREP packet is sent back, if it is the destination node or if it has a fresh enough node to destination.
(ii) Routing table is updated and RREQ is again broadcasted.

RREP is sent back to the source when RREQ is received by the destination. The source node receives RREP message through the intermediate nodes, which update their routing tables. RREP is accepted by source node if:

(i) The destination sequence number of this node is higher than the one in the routing table.
(ii) Destination sequence numbers are equal and the hop count is lesser with the one in routing table.

Black hole [1][3] attack is one of the active attacks possible on MANETs. On receiving a RREQ message the black hole node[7], without checking for a fresh route, immediately sends false RREP with high sequence number to the source node. On receiving this RREP, the source node establishes a route to this node assuming that it has fresh route to destination and sends its data packets over this route. However, when the packets are sent on this route the black hole node[5] absorbs the packets without relaying them further. Thus, black hole attack takes place.

2. RELATEDWORK

In [10,11,12,13,14,15,16,17,18,19,20,21] various method are proposed for secure data transmission and resolving attacks in MANETs, every node in a network listens to its neighbouring nodes promiscuously. In promiscuous mode, every node monitors the packet being forwarded by its neighbours in order to observe the behaviour of neighbour regarding packet operation. Every node compares the neighbour information with the information it stores in its knowledge table. If both are same the node assumes that the packet is forwarded further, otherwise node waits for particular amount of time and checks the reasons for packet dropping. In order to confirm packets are sent to its neighbour, the nodes monitor the control packets as well as data packets to prevent selective dropping, as black hole attack drops selected packets. In order to monitor the forwarded packets, every node has to maintain knowledge tables. If node does not forward the packet than the node at the instance checks the other reason for packet dropping, specified in the algorithm. If the packet dropping reaches to a threshold value the node is identified as malicious node and is removed from route selection. It first checks, whether the next node is destination node or not, and also checks the TTL, if its same then it checks node properties such as residual energy(ce).

Knowledge table contains the information about the packet which is most recently transmitted. When any node detects a black hole node in a network, it broadcasts the node's id to other nodes so as that the malicious node can be avoided in routing process.KSA algorithm is based on AODV, where the path is based on minimum hop and maximum sequence number. When source wants to send the information to destination, it broadcast the control packet RREQ to its entire neighbouring node. RREP is generated by destination through trusted nodes only, if any node is found malicious during route discovery process, its information is transmitted to all other nodes. If already a route is established and later it learns that one of the nodes of its route is a black hole node[4] than the source node removes that node and re initiates the routing process. However the KSA algorithm for mitigating black hole attack in AODV protocol monitors the data packets that are being forwarded in promiscuous mode to ensure that the packets are delivered to destination node. If any node drops a packet the algorithm checks for the packet drop reasons first before declaring it as a black hole node, thereby preventing a trusted node from becoming a black hole node.

The existing system put on trust values on its neighboring nodes based on the number of packets forwarded by that node. Packet drop can be due to many reasons i.e; packet properties such as destination address, time to live (TTL) etc, and node properties such as energy of the node. Since this system does not consider the other packet drop reasons, it may happen that packets that are dropped due to the above mentioned reasons also affect the trust value calculated on a node. Due to which the trust vale of a node may be lowered and thus it results in trusted node being taken as a malicious or black hole node that causes avoiding a trustable node in the data transmission route.

3. PROPOSED WORK

Every node in a network receives a public key infrastructure from trusted third party by securely using RSA algorithm. Black hole attack initiates the malicious activity by giving false route reply message. In order to get integrity of route replay message, destination node needs to replay the route reply by using proposed algorithm.

Proposed Algorithm:

Step 1: Destination get the RREQ packets from different node.
Step 2: Node selects a best route based on metric less hop count, and prepare the route replay packet.

Step 3: Node adds the route replay packet with its secrete key got from the PKI

$$\{RREP\}\text{ XOR }\{S_k\}$$

Step 4: Node calculate the message digest using the digest algorithm according to PKI instruction (In our method it is MD5)

$$\text{H}\{\text{RREP XOR } S_k\}$$

Step 5: Node append the calculated digest information with original route replay packet.
Step 6: RREP unicast towards the source node.
Step 7: Source node remove the H{RREP XOR S_k}from the RREP packet and adds the secrete key got from the PKI and perform the following task

{RREP} XOR {S_k}
H{RREP XOR S_k}

And compare the calculated information with obtained information if both matches, then source node conclude that the information did not tamper during the communication.

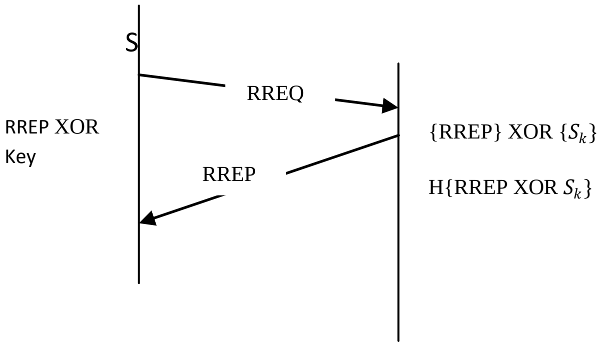

Figure 3:Request and reply of packet transfer

4. PERFORMANCE ANALYSIS

Using ns2, to calculate simulation with existing extension in ns2 libraries and compared our work with

- AODV without black hole attack.
- AODV with black hole node in network.
- Proposed algorithm/work with black hole node in network.

4.1 simulation Results

Network parameters:

PARAMETERS	VALUES
Nodes	10-40
Channel	Wireless channel
MAC	802.11
Routing	AODV, Proposed(SAODV)
Querying	Priority queue
Simulation time	0.9
Network area	1000x1000 meters
Packet size	512
Traffic	CBR(constant bit rate)

Figure 2:RREP Packet format of proposed protocol

The x-axis represents the number of nodes and the y-axis represents the throughput measured in terms of MBPS. For 10 and 20 nodes throughput remained same but increased for 30 nodes.

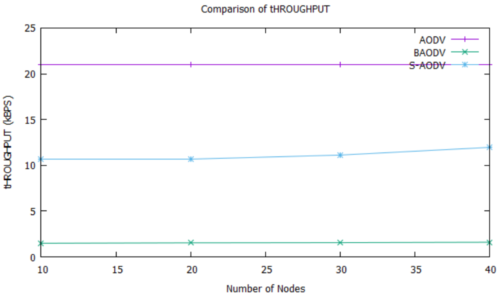

Figure 4: Throughput versus number of nodes

In the above graph we are measuring throughput. Throughput is a measure of how many units of information a system can process in a given amount of time. The throughput is more as compared to the existing system. It is applied broadly to systems ranging from various aspects of computer and network systems to organizations. Generally, it is the maximum rate of production or the maximum rate at which something can be processed.

The x-axis represents the number of nodes and the y-axis represents the packet delivery ratio measured in terms of number of packets. For 10 and 20 nodes packet delivery ratio remained same but increased for 30 nodes.

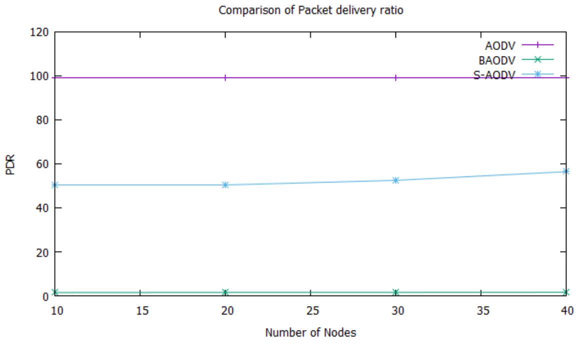

Figure 5: Packet Delivery Ratio versus number of nodes

In the above graph we are calculating the packet delivery ratio. The packet delivery ratio is more when compared to the existing system. The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. The x-axis represents the number of nodes and the y-axis represents the overhead measured in terms of number of packets. The overhead increases as the number of packets increases

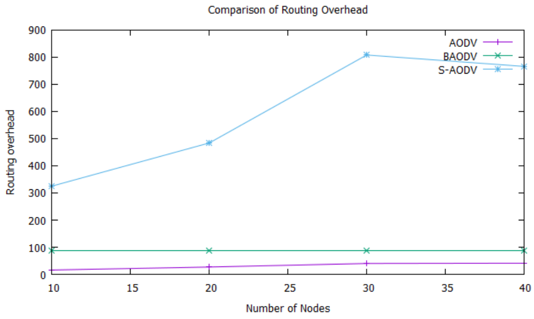

Figure 6: Overhead versus number of nodes

In the above graph we are calculating the overhead. The overhead is more when compared to the existing system. The time it takes to transmit data on a packet-switched network. Each packet requires extra bytes of format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces the overall transmission speed of the raw data.

The throughput is more when compared to the Black hole AODV and SKA AODV, The packet delivery ratio of the proposed PKI AODV is more when compared to the Black hole AODV and SKA AODV, with more overhead.

4.2 Comparative Study Of Existing Approaches And Proposed Approach

Existing System	Proposed System
Secure Knowledge Algorithm(SKA)	Proposed Algorithm
Based on monitoring.	Based on message digest.
Remove the black hole attack in dropping information phase, which is the second phase of black hole attack.	Removes the black hole attack in attracting information phase, which is the initial phase of black hole attack.
Overhead is more.	Less overhead when compared to existing system.
Need to maintain knowledge table.	No need to maintain knowledge table.
Packet dropping nodes are not always black hole nodes.	Here, black holes are removed at initial phase so, no packet loss or packet drop will occur.

5. Conclusion:

In MANETs, security is important and it plays a major role. In this work a "PKI based algorithm" for mitigating black hole attack in AODV protocol[6] has been proposed, which is used to provide security to the MANETs. This algorithm prevent the black hole attack at initial stage. The main goal of existing system(SKA) is not only to mitigate black hole attack but also to increase the throughput thereby reducing the packet loss due to black hole node In the existing work, the black hole node are removed based on packet drop count bit and, In the proposed work we are removing black hole nodes in the initial stage. However, in the work we have removed single black hole attack. In our future work we will be focusing to remove multiple black hole attack by using PKI. Black hole attack is malicious activity in network layer and its aim is to drop the packet which is one type of Denial Of Service(DOS).

References:

[1]. Thachil, F. and Shet, K.C., 2012, September. A trust based approach for AODV protocol to mitigate black hole attack in MANET. In *Computing Sciences (ICCS), 2012 International Conference on* (pp. 281-285).IEEE.

[2]. Kshirsagar, D. and Patil, A., 2013, July. Blackhole attack detection and prevention by real time monitoring. In *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on* (pp. 1-5). IEEE.

[3]. Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on* (pp. 421-425). IEEE.

[4]. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A. and Nemoto, Y., 2007. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *IJ Network Security*, *5*(3), pp.338-346.

[5]. Banerjee, S., 2008, October. Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In *proceedings of the world congress on engineering and computer science* (Vol. 2008).

[6]. Raj, P.N. and Swadas, P.B., 2009. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. *arXiv preprint arXiv:0909.2371*.

[7]. Rachh, A.V., Shukla, Y.V. and Rohit, T.R., 2014. A Novel Approach for Detection of Blackhole Attacks. *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, pp.2278-0661.

[8]. Rajaram, A. and Palaniswami, S., 2010. Malicious node detection system for mobile ad hoc networks. *International Journal of Computer Science and Information Technologies*, *1*(2), pp.77-85.

[9]. Hu, Y.C.P.A., 2002. Johnson D& A SEAD; Secure Efficient Distance Vector Routing for Mobile W ireless Ad Hoc Net—works1, A. In *Proc of the 4th IEEE Workshop on Mobile Com—puting Systems and Applications [-q. 2002.3-13. I-3] Yi S. Naldurg P, Kravets RA Security Aware Routing Pro—toeol for Wireless/\ d Hoc Networks* (pp. 15-149). Proc of the 6th W orld Muhi—Conference on Systemics. Cybernetics and In—formatlcs1, C].

[10]. Hu, Y.C., Johnson, D.B. and Perrig, A., 2003. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad hoc networks*, *1*(1), pp.175-192.

[11]. Castelluccia, C. and Montenegro, G., 2002. Protecting AODV against Impersonation attacks. *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(3), pp.108-109.

[12]. Papadimitratos, P. and Haas, Z.J., 2002. Secure routing for mobile ad hoc networks. In *the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002* (pp. 193-204).

[13]. Mohammad, A.A.K., Mirza, A. and Razzak, M.A., 2015. Reactive Energy Aware Routing Selection Based on Knapsack Algorithm (RER-SK). In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 289-298). Springer International Publishing..

[14]. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. *Indian Journal of Science and Technology*, *9*(26).

[15]. Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on* (pp. 421-425). IEEE.

[16]. Sana, A.B., Iqbal, F. and Mohammad, A.A.K., 2015, January. Quality of service routing for multipath manets. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on* (pp. 426-431). IEEE.

[17]. Mohammad, A.A.K. and Atheeq, C., MUTUAL AUTHENTICATED KEY AGREEMENT SCHEME FOR INTEGRATED INTERNET MANETS..

[18]. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Energy Aware Routing For Manets Based On Current Processing State Of Nodes. *Journal of Theoretical and Applied Information Technology*, *91*(2), p.340.

[19]. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Analytical Model for Evaluating the Bottleneck Node in MANETs. *Indian Journal of Science and Technology*, *9*(31).

[20]. Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data Transmission in Integrated Internet MANETs Based on Effective Trusted Knowledge Algorithm. *Indian Journal of Science and Technology*, *8*(1).

[21]. C.Atheeq, M.MunirahamedRabbani "Effective cluster key mechanism for integrated internet MANETs " *International journal of applied engineering research vol.10 No.44, 201*