Volume 3, Issue 2, February 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Preventing Black hole and IP spoofing attack using Diffie-Helman Algorithm

Satish Kumar, Vijay Raju, Arun
Lovely Professional University, Jalandhar
Punjab, India

Abstract:**The wireless ad hoc network is the self configuring type of network. The wireless enable nodes can join or leave the network as they want. In this type of network many type of internal as well as external attacks are possible. When the source nodes want to transmit data to the destination nodes, shortest path will be established between them. The secure and shortest path between sender and receiver ensures the reliable data transmission. AODV is the reactive routing protocol which is used to establish the shortest path, on the basis of hop counts .But in the self configuring type of network many malicious nodes may exits which are responsible for packet dropping. Diffie helman is the algorithm which is used to set up the secure path between the sender and receiver before transmitting the data. In this paper, we propose the novel approach to prevent black hole and IP spoofing attack. In our work, a secure channel is established between sender and receiver for reliable data communications, it will prevent black hole attack. A random number is used with the IP address for the prevention of IP spoofing attack.**

Keywords:**Black hole, IP Spoofing, Malicious, Diffie-Helman, Black hole**

I. INTRODUCTION

Wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. In ad hoc networks, the mobile nodes on the network dynamically establish the routing process by themselves. There is the possibility of more security threats in case of mobile and ad hoc networks (MANET) as compare to centralized wireless networks. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust. The AODV is the reactive routing protocol which is used to establish a shortest path between the source and destination for data transmission. On the basis of hop count and sequence number shortest path is selected. The route with the minimum number of hop counts are selected as the best route and sequence number tells the freshness of the route .The whole network will be flooded with the route request packets and the node which is having route to the destination will respond back with the route reply packets. The black hole is the most common type internal attack which is trigged by the malicious nodes, malicious node is responsible for packet dropping it is the denial of service attack .Many algorithms had been proposed for the prevention of black hole attack. In MANET we use the location based information for packet routing. The previous research proved that it is the inefficient approach and we use the IP address instead for location information for packet routing. In this approach IP spoofing attack will be possible, it will give arise to cross loop attack.

Literature Review will present in the section 1.Black hole in Ad hoc network will discussed in the section 2.In section 2 Diffie helman key exchange algorithm will be presented .New proposed scheme will written in section 4 .In the last section 5 future work and conclusion will be written.

II. LITERATURE REVIEW

Hongmei Deng, Wei Li, and Dharma P.Agarwa proposed the method for detecting the single black hole node. In this proposed method,each intermediate node send backs the next hop information when it sends back an RREP message. When the source node receives the reply message from intermediate node, it does not send the data packets quickly, but it extracts

the next hop information and then sends the Further-Request to the next hop to verify that it has the route to the intermediate node. If the next hophas no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hopto the destination. At the same time, send out the alarm message to the whole network to isolate the malicious node [1].

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto proposed the solution emphasis on the dynamically changing conditions of ad hoc networks. In AODV, the destination sequence is used to determine the freshness of the routing information contained in the message from originating node. The attacker must generate its RREP with the destination sequence number greater than the destination sequence number of the destination node. It is possible to for the attacker to find the destination sequence number from the RREQ packet. But if other nodes attempts to construct the route to the destination node other than the source node, then the destination node's sequence number will be significantly different from the current destination sequence number. So the effect of the attack may also change depending on the increased amount of destination sequence number [2].

Payal N. Raj and Prashant B. Swadasproposed DPRAODV (detection, prevention and reactive AODV) to prevent the black hole attack by informing the other nodes about the malicious node. As the value of RREP sequence number is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. [3].

Hesiri Weerasinghe proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) [4].

E.A.mary anita proposed a scheme to prevent black hole attack. They had used the threshold cryptography scheme to detect black hole attack. The certificate chaining or we can say authentication can use in term of digital signature every node in the network can issue certificate to other node within the radio communication range of each other certificate can bind the node every node have the repository consisting of certificate issue by the node and send to particular node it means certificate store twice one by issuer and other for whom by doing this periodically certificate from neighbor are requested and origin is update by adding certificate if any certificate conflicting it means there is the malicious node[5].

1. Black Hole attack in MANET

When a node requires a route to a destination, it initiates a route discoveryprocess within the network. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. In this process the intermediate node can reply to the RREQ packet only if it has a fresh enough route to the destination. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route isnolonger desired. A RERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred.A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D', 'M' receives the message. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'. The Node 'M' will responsible for packet dropping and black hole is created at node M. This is denial of service attack as F will not able to get the data from the A. The black hole problem discussed above will be shown the figure 1.

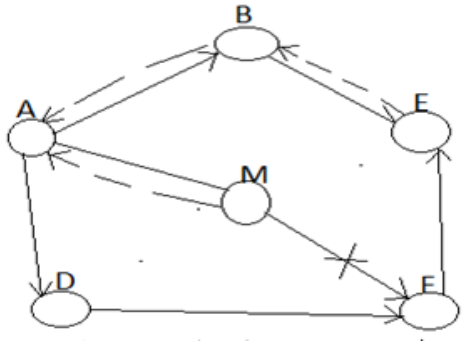

Fig1: Black Hole attack

2. Diffie Hellman Key exchange Algorithm

Diffie Helman is the popular key exchange and secure path establishment algorithm. In this algorithm we use asymmetric key cryptography to establish secure path between the sender and receiver. Both the communicating parties select the private and publish keys to establish secure channel for communication. Secure channel establishment procedure by using Diffie Helman algorithm will be shown in figure 2

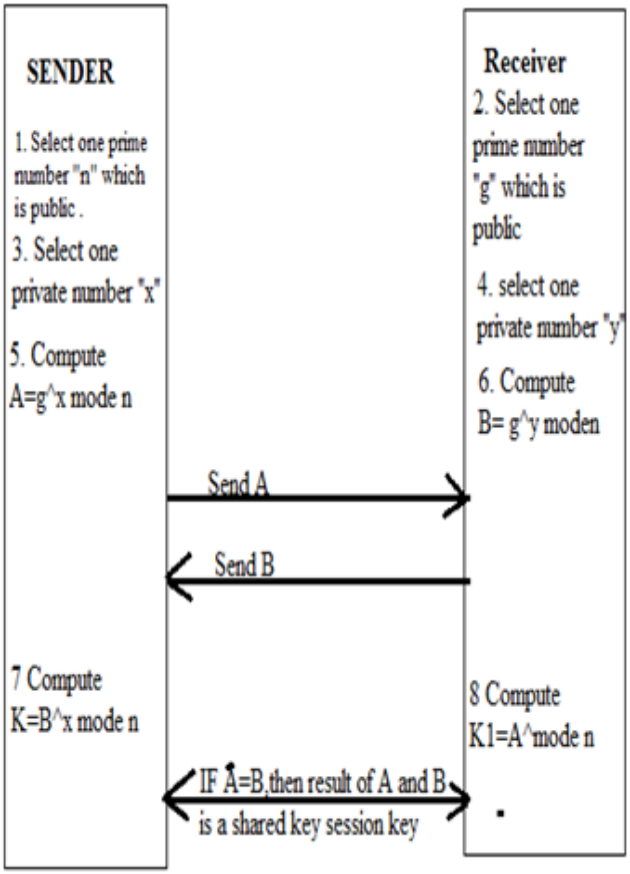

Fig2: Diffie Hellman Key exchange Procedure

III. NEW PROPOSED SCHEME

The Black hole attack is possible in the AODV protocol .The new proposed scheme will prevent the black hole attack in the AODV protocol .This proposed scheme will be based on the Diffie Hellman key exchange algorithm. In the previous schemes ,mobile nodes use the location based information of the mobile nodes for data routing .But in our scheme we use the IP address for data routing .In this type of schemes IP spoofing is possible to prevent spoofing attack. we use the random number and XOR operation is performed on the IP address to generated the unique identity of the node .Every node maintain the hashed table for the unique numbers. It prevents the IP spoofing .To migrate the black hole attack we use the Diffie Helman algorithm, in secure channel is established between the sender and the receiver before the data transmission .

IV. FUTURE WORK AND CONCLUSION

In our work, we propose the novel approach to prevent IP spoofing and Black hole attack. The new proposed scheme will be different from the previous schemes. In our Future work, we will implement this scheme in the network simulator NS2 and compare the results with the existing schemes, which are used to prevent Black hole attack.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[2] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.

[3] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[4] Hesiri Weerasinghe "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2008, pp 362-367

[5] K. Selvavinayaki, Dr. E. Karthikeyan "A Reliable Data Transmission Approach to Prevent Black Hole Attack in MANET" International Journal of Computer Science and Telecommunications, [Volume 3, Issue 3, March 2012].

[6]http://books.google.co.in/books?id=_VkTzFLnwD4C&pg=PA22&lpg=PA22&dq=basic+architecture+of+ns2&source=bl&ots=_Z12nk6Alg&sig=iimmx3xIwR97Z4gqNaLu_Ou87RA&hl=en&sa=X&ei=4CmvUMOtA4OMrgfJ7oHQDg&ved=0CDgQ6AEwAg#v=onepage&q=basic%20architecture%20of%20ns-2&f=false

