# Detection and Prevention of Black hole Attack in MANET

**Mangesh A. Suryawanshi, Priyanka G. Bharude, Harish B. Mahale, Bhagyashri A. Hiwarale**

*Abstract*— **A Mobile Ad-Hoc Network (MANET) is an autonomous collection of mobile nodes and wireless communication link used to connect those mobile nodes. Each device in a MANET is free to move independently. MANET is an infrastructure less network in which no anyone fixed Base Station for communication. Security is one of the major issues in Mobile Ad-hoc Network (MANET) because of its inherent liabilities. Black hole is a one type of data traffic attack of MANET. In this, one of the malicious node acts like a Black hole attack, indicating itself as a shortest path to destination in a network by sending fake route reply to the source node. As the data packets do not reach at the destination and data loss occurs therefore performance of network decreases. Proposed approach is used to prevent black hole attack in the network, which isolate malicious node on selective path in AODV routing protocol and secure the channel uses the Diffie Hellman key exchange and advance encryption standards (AES) algorithm**

*Keywords*

**MANET, Black Hole attack, AODV, Diffie-Hellman Algorithm, AES algorithm.**

## I. INTRODUCTION

An Ad-Hoc network is an autonomous collection of mobile nodes and wireless communication network is used to connect these mobile nodes. This type of network is known as Mobile Ad-Hoc Network (MANET). Each device in a MANET is free to move independently. Intermediate mobile nodes act as router to deliver the packets between the two nodes [4]. So, MANET is a highly dynamic network and hence more vulnerable to attack. Nodes in an Ad-hoc networks are computing and communication devices, which can be laptop computers, mobile phones, or even sensors that communicate with each other over wireless links and works in a distributed manner in order to provide the network functionality. Applications of Ad-hoc networks include military communication, emergency relief operations, commercial and educational use in remote areas, and in meetings and other situations where the networking is mission oriented and communication based [3].

## II. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

Security in MANET is the most imperative concern for today. Integrity, confidentiality of data and availability of network services are the issues that has to be achieved to provide a secure data transfer. MANET exhibit some features like dynamic topology, open medium, lack of central management, due to which it suffers from many attacks. A significant amount of research has been devoted to study security issues as well as preventive to various attacks in MANET. However, there is still much research work needed to be done in this area. The aim of the study is to detect and isolate the Black Hole attack using fake destination ID. The proposed work focuses on finding a secure route for communication by detecting and isolating all the malicious nodes in mobile Ad hoc network. The detection of the collective black hole nodes will provide more security and stability to MANET. Previously many of the researchers have worked on the security issues in MANET. Black Hole is one of the security attack which is studied under the AODV routing protocol and its effects are detail by specifying how this attack trouble the performance of MANET.

AODV is an on-demand routing protocol that creates routes only when source node required a specific route. When node requires a route to a destination, it starts a route discovery process within the network. It broadcasts a route request (RREQ) packet to its neighbours, which send the request to their neighboring nodes in the network, and the process is repeated, until either the destination or an intermediate node with a new route to the destination is identified. In this process the intermediate node can reply to the RREQ packet only if it has a new route to the destination. When the RREQ reaches the destination or an intermediate node with a fresh enough route to the destination, it responds by unicasting a route reply (RREP) packet back to the neighbour from which it first received the RREQ. After selecting and accepted a route, it is kept by a route maintenance method until either the destination becomes unreachable along every path from the source or the route is no longer have a need. A RERR (Route Errors) message is used to notify other nodes that the loss of that link has occurred. Fig. A black hole problem means that a malicious node utilize the routing protocol to declare itself of being the shortest path to the destination node, but drops the routing packets and does not forward packet to its neighbouring node.

## III. BLACK HOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to indicate itself for having the shortest path to the destination node. This malicious node advertises its availability of fresh routes irrespective of checking its routing table. Attacker node will always ready for replying to the route request and thus catch the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it depends on to the node whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies.

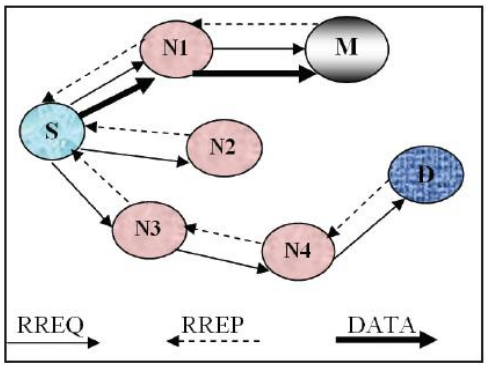



Figure: Black Hole Attack

Black hole attack is one of the attack in ad-hoc network due to it harms the security of MANET because now a day mostly the people

can use the ad-hoc network to transmission of data so it is very important to avoid the MANET from attacks. In MANET, when source node wants to communicate with destination node before the communications route will be establishing between them during the route establishing source node will send the route request to the destination node will send the reply but in during the communication black node or malicious node will also the reply shortest path to the source node. Source node know that this reply is send by the original node. As the malicious node receives data packets, it drops them instead of sending them to the destination, as a result the source and the destination nodes became unable to communicate with each other. In proposed solution we are using the AODV protocol for route establishing because this protocol is on demand protocol and for detection of black hole attack we are using random number, it broadcasts a route request (RREQ) packet across the network, receiving packets returns route reply(RREP) if it is original destination node otherwise it returns fake route. After the detection we can use the Diffie-Hellman algorithms to create the secure communication between the source and destination. 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 public keys to establish secure channel for communication. This algorithm to check the reliability of the selective path. In this way, we will isolate black hole attack [7].

## IV. Diffie- Hellman Key Exchange Algorithm

The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel in real time. The point is to agree on a key that two parties can use for a symmetric encryption. Today, D-H algorithms are used by protocols such as Internet Protocol Security (IPSec), Secure Shell (SSH), and Secure Sockets Layer. Diffie Hellman key exchange is the cryptographic protocol that allows two parties that have no previous knowledge of each other to jointly establish a shared secret key over an insecure communications channel. Diffie-Hellman is basically not an encryption algorithm it's a key-exchange algorithm. Diffie-Hellman Key exchange Procedure.

*Steps in the algorithm:*

1. Alice and Bob agree on a long prime number 'x' and a base 'y' which is public.
2. Alice chooses a secret number 'a', and sends Bob the value of 'A' by computing A= (y^ a mod x).
3. Bob chooses a secret number 'b', and sends Alice the value of 'B' by computing B= (y ^ b mod x).
4. Alice gets 'B' from Bob, and calculate shared key 'K' by computing K= (B^a mod p).
5. Bob gets 'A' from Alice, and calculate shared key 'K' by computing K= (A^b mod p). Both Alice and Bob can use the K-value as their key.

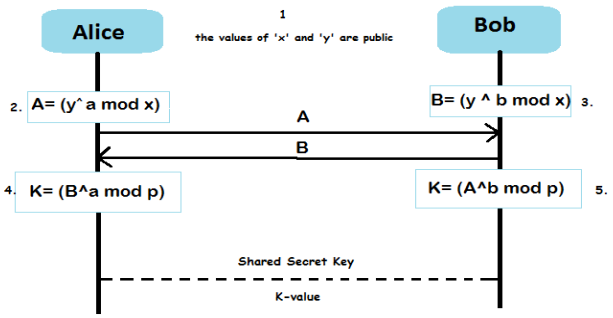



Figure: Diffie-Hellman Algorithm

## V. Advanced Encryption Standard (AES)

The more popular and widely symmetric encryption algorithm is to be an Advanced Encryption Standard (AES). It is found at least six time faster than triple DES. AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It has series of linked operations, some of which involve exchanging inputs by specific outputs (substitutions) and others involve dragging bits around (permutations). AES performs all its calculation on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are organized in four columns and four rows for processing as a matrix − DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a contrast 128-bit round key, which is counted from the original AES key.

The schematic of AES structure is given in the following figure:

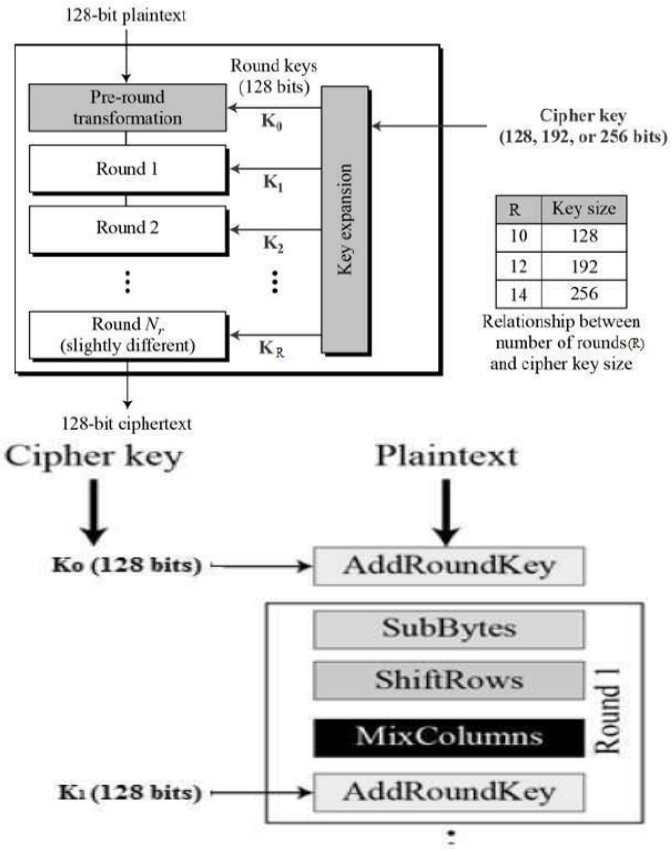



Figure: AES Encryption Process

AES contains three block ciphers, AES-128, 192 and 256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits respectively. For encryption and decryption, Symmetric or secret-key ciphers use the same key, so both the sender and the receiver must know and use the same secret key. All key lengths must be sufficient to protect secret data up to the authorized level. If data is Top Secret then it requires either 192- or 256-bit key lengths. There are 14 rounds for 256-bit keys, 12 rounds for 192-bit keys, and 10 rounds for 128-bit keys as shown in Fig. Each round consists of multiple processing steps that include substitution, transposition and mixing of the input plaintext data and transform it into the final output of cipher text data [8].

## VI. Related Work :

**Gayatri Wahane et. al. [1]** proposed a research work that suggests the modification of AODV Routing Protocol.in this paper, routing security issues in MANETs are discussed in general, and in particular the cooperative black hole attack has been described in

detail. A security protocol has been proposed that can be utilized to identify multiple black hole nodes in a MANET and thereby identify a secure routing path from a source node to a destination node avoiding the black hole nodes.

**Neetika Bhardwaj et. al. [2]** presented a new solution to detect and prevent the Black hole which does not increase routing or computation overhead and increases the performance metrics like packet delivery ratio, throughput by a huge margin. Also the false detection ratio of the approach is negligible. Black hole Attack is one of the most severe attacks because the attacker embeds itself into the route from source to destination by sending false RREP messages giving an impression that it has the freshest route to destination. Seeing its severity many researchers have addressed the problem of detecting and defending against black hole attack but the solutions presented so far suffered from one problem or the other.

**Nitesh Funde et. al. [3]** in this paper, they attempt to provide a solution to detect the multiple black hole nodes present and prevent them from the network. In particular , they are focusing on AODV protocol in MANET .The solution are not only provide protection mechanism against black hole attack but also consequently improve the performance of the network comparing with the existing approaches after detection and prevention of attack. The analysis shows that how severe the attack is and its effects on MANET.

## VII. Proposed Solution :

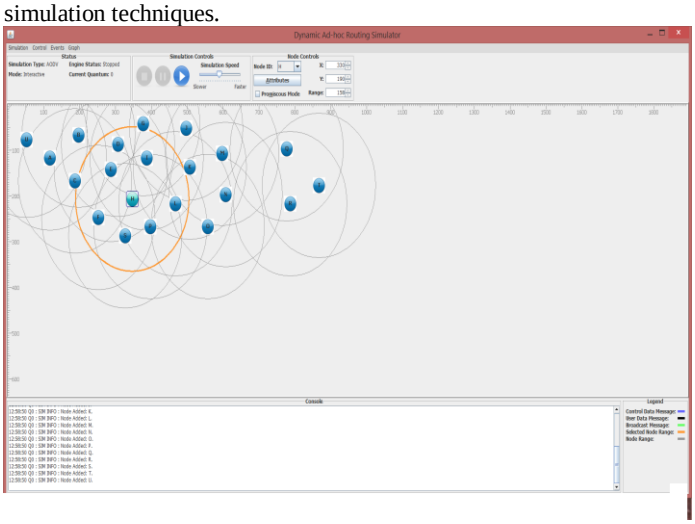
Ad-Hoc On-Demand Distance Vector Routing (AODV) has been used and implemented Black Hole attack to this protocol. AODV [7] Routing Protocol is used for finding a path to the destination in an ad-hoc network. When a node "A" wants to initiate transmission with another node "G", it will generate a route request message (RREQ). This message is propagated through a limited flooding to other nodes. This control message is forward to the neighbors, and those node forward the control message to their neighbors' nodes. This process of goes on until it finds a node that has a fresh enough route to the destination or destination node is located. Once the destination node is located or an intermediate node with enough fresh routes is located, they generate control message route reply message (RREP) to the source node. When RREP reaches the source node, a route is established between the source node "A" and destination node "G". Once the route is establish node "A" and "G" can communicate with each other. The following diagram show exchange of control messages between source node and destination node.

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbors nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node i.e. from node "A" to the neighbors nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error.

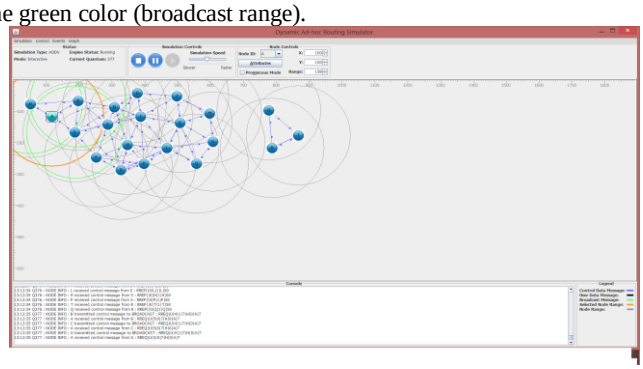
The working of ad-hoc on demand distance vector routing protocol is describe as above. After the processing in AODV the black hole is detected by using three parameters such as sequence number, tick counter and state. In which state has three types like valid, invalid and repaired. If the black hole detect in the network the state becomes valid otherwise it will be invalid. After detection of black hole, the black hole will be prevent by using two algorithms such as Diffie-Hellman key exchange and advanced encryption standard algorithm (AES). In prevention the firstly the Diffie-Hellman generate a key which is symmetric and then it will send to advanced encryption standard algorithm and the AES will doing the encryption and decryption and prevent the black hole.

## VIII. Simulation Result

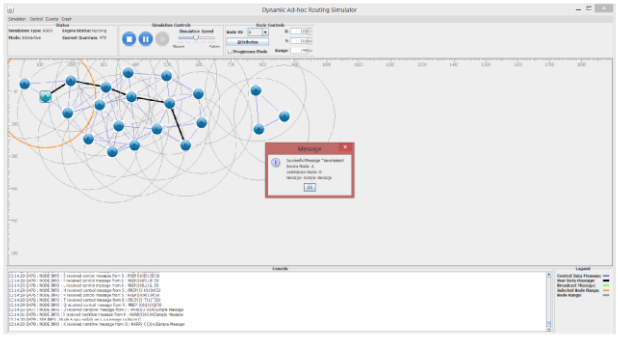
*Case 1:* Figure shows the nodes in the network without applying the simulation techniques.



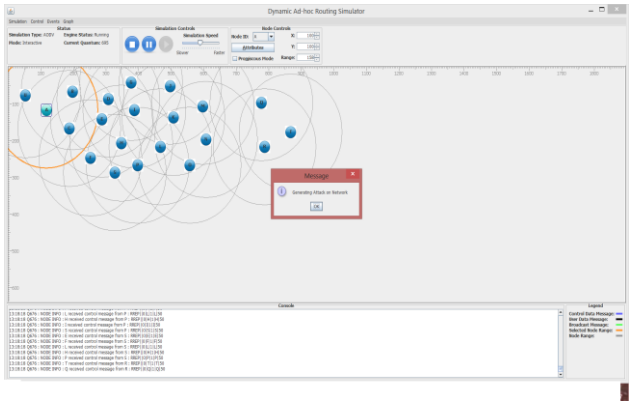
*Case 2:* Figure shows the scenario in which after sending the packets, first it will broadcast the RREQ in the network which has the green color (broadcast range).



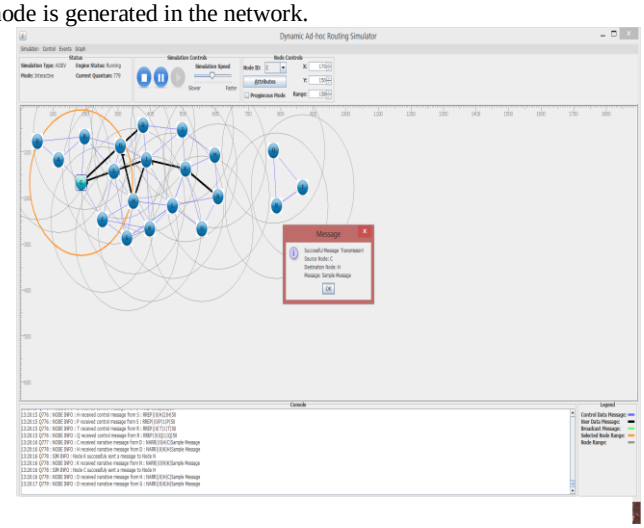
*Case 3:* Figure shows after broadcasting RREQ it will send the packet from source node A to Destination O successfully.



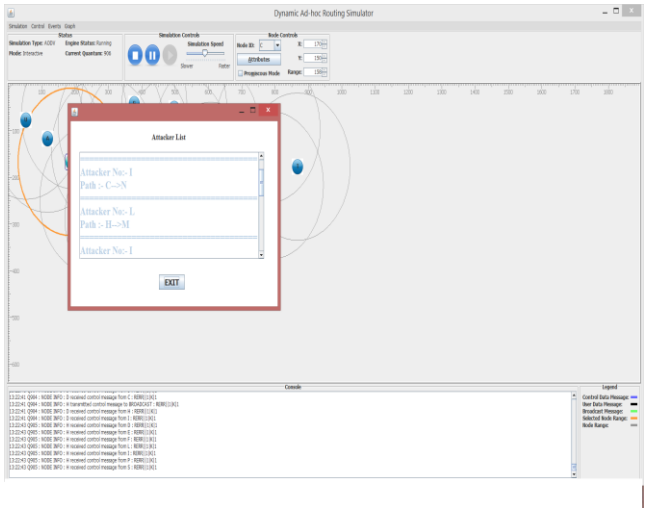
*Case 4:* Figure shows after sending the packets the attack is generated.



*Case 5*: Figure shows after generating the attack the black hole node is generated in the network.



*Case 6*: Figure shows the attacker list of black hole nodes in the network.



## IX. Conclusion And Future Scope

Our proposed solution is to detect and isolate the black hole nodes by using Diffie-Hellman (DH) Key Exchange and Advance Encryption Standard (AES) Algorithm. The proposed work will probably detect the malicious nodes in the route, and as any malicious node is not participating in any route discovery the communication will be attack free. Ultimately, proposed methodology detects malicious nodes, and repairs of such nodes, and multipath to destination and decrease the route discovery time, packet drop therefore the performance of network increase and secure communication is done in MANET.

## REFERENCES

[1] Gayatri Wahane, Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack in MANET", 2014 (ICAET-2014 IOSR Journal of Computer Science (IOSR-JCE) pp. 59-67.

[2] Neetika Bhardwaj, Rajdeep Singh, "Detection and Avoidance of Blackhole Attack in AODV Protocol in MANETs", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, Issue 5, pp376-383, 2014.

[3] Nitesh Funde, P. R. Pardhi, "Analysis of Possible Attack on AODV Protocol in MANET", International Journal of Engineering Trends and Technology (IJETT) – Vol. 11, No. 6, pp. 306-309, 2014.

[4] Aware A. Anand, Kiran Bhandari, "Prevention of black hole attack on AODV in MANET using hash function", 8-10 Oct.2014 IEEE.

[5] Chavda, K.S. Nimavat, A.V., "Removal of black hole attack in AODV routing protocol of MANET", IEEE 4-6 July 2013,

[6] Shashi Gurung, Dr. Krishan Kumar Saluja,"Mitigating Impact of Blackhole Attack in MANET", 2014 Association of Computer Electronics and Electrical Engineers (IACEEE) 2014, pp. 229-237.

[7] Jeevan Kumar Yumnam, Maninder Kaur, "Detection and Avoidance of Black hole Attack in MANETs using Diffie-Hellman Algorithm", 2015 (IJCST/63/1/A-0548).

[8]https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

**Author Details:**

**Mangesh A. Suryawanshi** B.E. in Computer Engineering (pursuing). SSBT's COET, Jalgaon-425001, North Maharashtra University.

**Priyanka G. Bharude** B.E. in Computer Engineering (pursuing). SSBT's COET, Jalgaon-425001, North Maharashtra University.

**Harish B. Mahale** B.E. in Computer Engineering (pursuing). SSBT's COET, Jalgaon-425001, North Maharashtra University.

**Bhagyashri A. Hiwarale** B.E. in Computer Engineering (pursuing). SSBT's COET, Jalgaon-425001, North Maharashtra University.