# Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm

G.Vennila, Dr.D.Arivazhagan, N. Manickasankari
Department of Information Technology
AMET University, Chennai.

**Abstract**

The Mobile ad-hoc network (MANET) is a collection of wireless mobile node in which each node can communicate with other node without use of predefined infrastructure. Currently, a lot of efficient protocols have been proposed for MANET. All of these efficient Routing protocols are depends only conviction and supportive environment. Conversely, the networks are more vulnerable to various kinds of routing attacks with the presence of malicious nodes. Black hole attack is one of network layer attack. In this attack, A malicious node make use of routing protocol to advertise itself that has a shortest path to reach destination, drops at the cost of original routing packets. In our work, the proposed algorithm is used to secure the DSR protocol. This will help to improve the performance of Mobile Ad hoc network due to the attack. There are several prevention mechanisms to eliminate the Black Hole attack in MANET. The aim of the paper is to provide better prevention of Co-operative Black hole attack in MANET and how it affects the performance metrics in terms of throughput and delay of the network by comparing the network performance with and without black hole nodes.

**Keywords:** Mobile ad-hoc networks, Routing protocol, DSR, Black hole

## INTRODUCTION:

The MANET is a collection of wireless mobile nodes that communicate with each other without use of network infrastructure. Each mobile node in wireless network function as a host as well as router [1]. MANET is susceptible to all types of attacks because of the dynamic topology and lack of centralized management. The principal of a MANET routing protocol is to establish the efficient route between nodes. So, the message may be delivered in timely manner. If routing can be misdirected, the entire network can be collapsed. Consequently routing security plays a most important role in the security of the complete network [3]. One of the routing protocols used in ad-hoc network is DSR (Dynamic Source Routing Protocol). The security of the DSR protocol is cooperated by one of the network layer attack called 'black hole' attack. In this attack, a malicious node uses routing protocol to advertise itself that has shortest path to reach destination. So it drops all the routing packets and act as a black hole. The proposed algorithm is used to prevent Co-operative Black hole attack in Manet using DSR protocol and also improve the performance in terms of throughput and delay. The rest of the paper is organized as follows: The DSR protocol is described in section 2.In section 3, there is a detailed analysis of black hole attack and their types. Related works has been discussed in section 4.The study of Proposed Algorithm in section 5.Performance analysis in section 6.the final one is conclusion in section 7.

## II. DSR PROTOCOL:

Dynamic Source Routing Protocol is a reactive routing protocol and is called as on demand routing protocol [12].It is also called as source routing protocol .This efficient routing protocol used in wireless ad-hoc network. The DSR commonly updates the available routes in its route cache. If there is any new available route, it will send the packet through that route if it is efficient. Basically, it is composed of two parts namely Route Discovery and Route Maintenance.

Route Discovery:

When the source node wants to communicate with destination, first it checks its route cache that whether it has a route to reach destination [5]. If there is a route to reach destination, then it sends the packet through that path. But if the node does not have a route, then it initiates the route discovery process by broadcasting a Route Request Packet (RREQ).Each intermediate node checks its route cache whether it has a route to the destination. If the intermediate node does not have a route, it appends its address to the route request of the packet and forwards the packet to its neighbors until reach destination. When the RREQ packet reaches to the destination, it generates RREP (Route Reply) with route information. After getting the RREP from destination, the source node sends the packet through the route.

Route Maintenance:

The DSR uses two mechanisms for route maintenance: Route Error packet and Acknowledgements (ACK). When a destination node receives packet successfully, it send ACK message to the source. If there is any

problem in the communication link [5], it sends Route error packet message. When a node receives the route error packet, it removes the hop from its route cache.

## III. BLACK HOLE ATTACK

The black hole attack is one type of network layer attack in Mobile ad-hoc Network .In this attack , a fake node advertise itself that has shortest path to reach destination[3]. So it collects the entire packet from source and drops it. The Black hole attack can be classified into two categories:

Single Black hole attack:

In Single Black hole attack, only one node act as a fake node that collects all the packet from source and drops the packet [6].The single Black hole problem is shown in Fig.1. The source node S wants to communicate with destination D. First, it sends RREQ to the neighbor node. If it has a valid route to reach destination then it sends the packet through the path. If it does not have a route then it forwards the RREQ to the neighbor's node until reach destination. The node F act as a Fake node that sends RREP with highest sequence number before any other node responds, even if any intermediate node sends RREP to the source. The Source node S discards the reply and it assumes that the F node has shortest path to reach Destination and it. It sends the packet through that path .So, the node F collects all the packets coming from source which creates black hole problem.

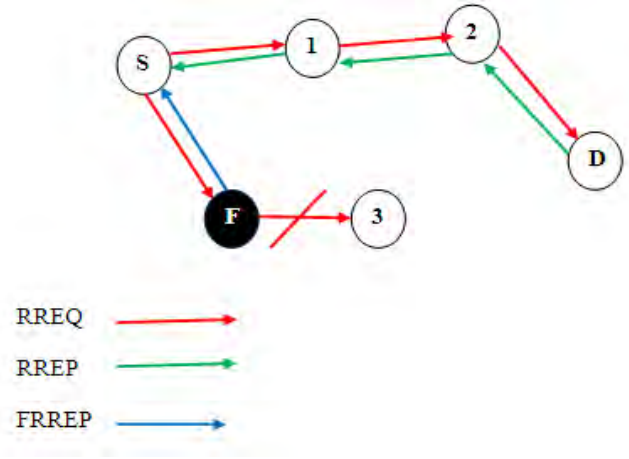



Fig.1.Single Black Hole attack

Co-operative Black hole attack:

In Co-operative Black hole attack, more than one node combined mutually and act as Fake node is called as Co-operative Black hole attack[11]. This will affect the network performance than the Single Black hole attack. The Co-operative Black hole attack is shown in Fig.2.

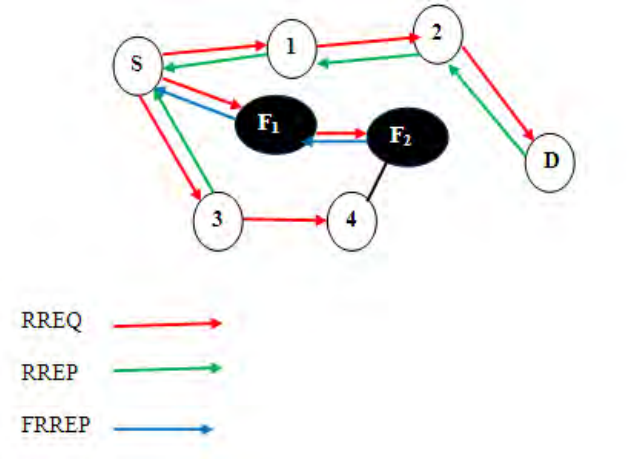



Fig.2.Co-operative Black Hole Attack

## IV.RELATED WORKS:

A lot of different approaches have been implemented to prevent black hole attack. Some of the approaches are described below;

Rashid Sheikh, Mahakal Singh Chandel et al [2], developed one solution SMC used to Secure Multiparty computation. The anonymization technique is used to find the solution to SMC problem.

Saurabh Gupta et al [7], proposed one protocol namely BAAP (Black hole Attack Avoidance Protocol for wireless network)] used to avoid black hole attack. In this protocol, every node keeps the authority of all neighbors' nodes in order to find the path to reach destination. The performance evaluation of this protocol based on the parameters such as Packet Delivery Ratio, Route Formation Delay, Node Speed, Pause Time. The packet losses in AODV (Ad-hoc On-demand Distance Vector) are more than 90% and it is only 15.6% - 21.3% with the presence of malicious nodes. This protocol requires little more time without presence of the fake node.

Maitha Salem Al Mazrouei et al [8], used Intrusion Detection System and Watchdog & Path rater in MANET. The performance evaluation is based on availability and integrity factor. The result of availability of the Intrusion Detection System is better than Watchdog and Path rater. The results of integrity of Watchdog and Path rater is better than Intrusion Detection System

Elhadi M. Shakshuki et al [9] proposed Enhanced Adaptive Acknowledge (EAACK) to prevent black hole attack in MANETs. In this EAACK, the authors are implemented both RSA (Rivest Shamir Adelman) and DSA (Digital Signature Algorithm) and compare the performance in terms of Packet Delivery Ratio and Routing Overhead. The DSA algorithm is more suitable algorithm in Manet Environment than RSA algorithm.

Sunil kumar yadav et al [10], developed one Black hole Prevention algorithm identify a secure routing path from a source node to a destination node avoiding the black hole nodes. The performance evaluation is based on Packet Drop Ratio and Delay. The Delay is minimized as compared to previous black hole detection mechanisms, packet dropped ratio is reduced significantly.

## V.PROPOSED SOLUTION:

The proposed solution use one cryptographic algorithm RSA and sequence number calculation to eliminate the black hole node. Initially, the two large prime numbers has been taken and calculate the d and e value. The RREQ is considered as M. The RREQ is encrypted at the sender side and it forwards the RREQ to the neighbor's node. If the node knows key value then the node can able to decrypt the RREQ and it generates RREP to the source. After receiving the RREP in source, it computes the threshold_diff in which the RREP come from legitimate node or malicious node. Base on the threshold_diff, it sends the packet from source to destination. If the difference of sequence value is below the threshold_value, then the node is considered as legitimate node. Suppose, if the difference of Sequence number is greater than the threshold_value, then the node is considered as malicious node. The proposed algorithm is described as follows;

Step 1:

Select any two prime numbers namely p and q (p! =q)

Calculate the followings

$n=p*q$

$Ø(n) = (p-1)*(q-1)$

gcd (e, n)=1 and find e

$(d*e)\% Ø(n) =1$ and find d

Step 2:

M= RREQ

Step 3:

To encrypt the RREQ by using following

For i =0 till i<e

C=C*M mod n Where C=1

Step 4:

Forward the RREQ to neighbor's node.

Step 5:

If the RREQ is received by the legitimate node, then decrypt the RREQ by using following

(i). Decrypt RREQ using the followings,

For i =0 till i<d

M = M*C mod n

Step 6:

Generate RREP based on RREQ

Step 7:

Forward RREP to source node

Step 8:

If RREQ is received by a black hole then decrypt as in Step 5,

Step 9:

Generate RREP

Step 10:

Forward RREP to source node

Step 11:

Check RREP at source on receiving RREP. This is done as follows:

(i). Decrypt the received RREP as in step 5.

(ii). If the RREP has come from a legitimate node, then RREP will be decrypted correctly. Set BHI (Black hole Indicator) to 0 to indicate that RREP has come from a legitimate node.

(iii). Else, the RREP has come from a black hole. Then Set BHI to 1

Step 12: Compute the Threshold_diff by using the following formula:

Threshold_diff = Current Sequence number – Previously received sequence number

If the difference is below the threshold value then the packet is forwarded Else if the difference is above the threshold_diff, then the value of threshold_diff is incremented and the packet is dropped.

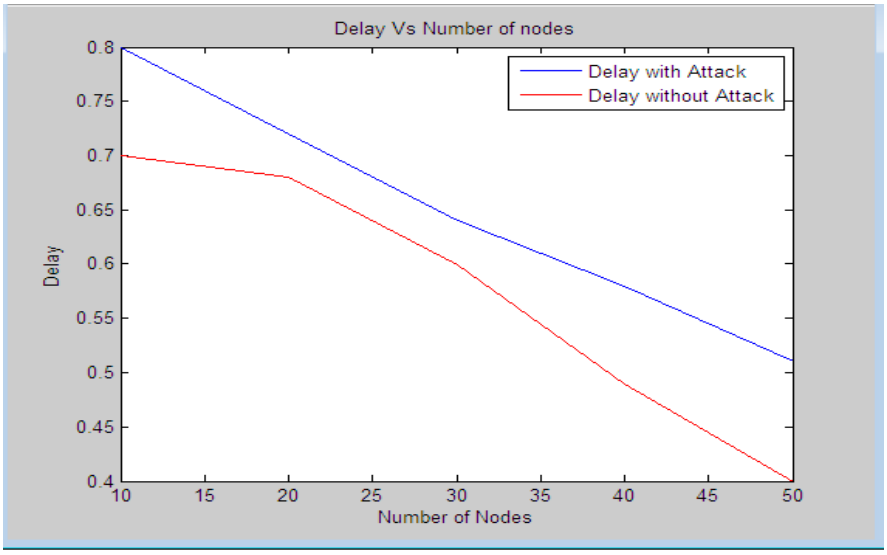
## VI.SIMULATION RESULTS:

The simulation was carried out using MATLAB. The MATLAB is a simple tool for simulation. The number of nodes from 10 to 50 with 8 malicious nodes has been taken during simulation within the area 1000 X 1000. The following performance metrics are considered to evaluate the performance of the network with black hole attack and without black hole attack.

Delay:

The process of time taken by the packets to pass throughout the network is called delay [4].

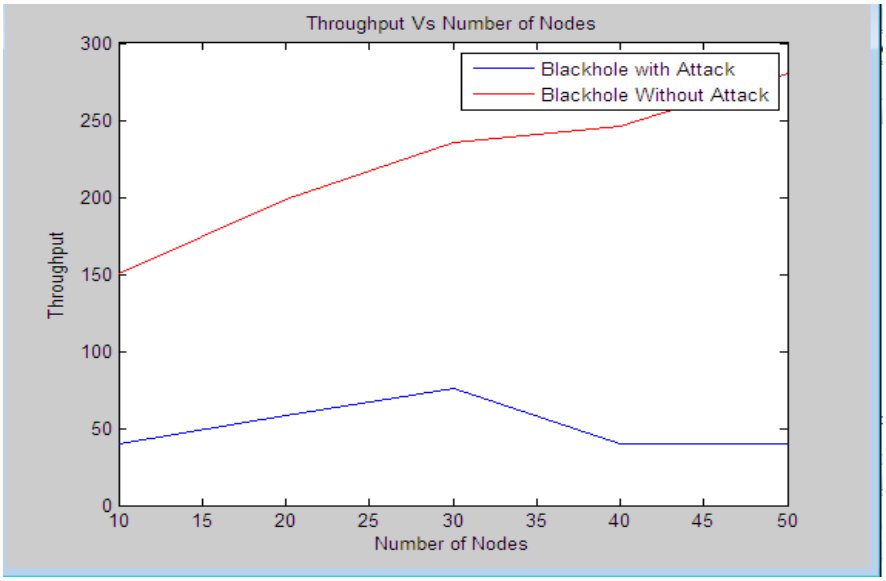
The following graph shows that the delay with the presence of Black hole node and without presence of Black hole node.




Throughput:

The Throughput is defined as the total number of packets delivered over the total simulation time. It is represented in packets per second or bits per second [4].

The following graph shows that the throughput with the presence of Black hole node and without presence of Black hole node.




## CONCLUSION:

This paper proposed one algorithm that uses both the concept of RSA and sequence number calculation to remove the black hole attack. It provides security to transfer the packets from source to destination. This algorithm was tested in MATLAB. It is shown that the proposed model can be utilized for eliminating the black hole nodes effectively. The performance of proposed algorithm graph is provided for achievement of better results in terms of delay and throughput. In future work, the proposed algorithm may be apply to other types of attack such as Worm hole, Gray hole etc.

## REFERENCES:

[1] Vishnu K, Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22, 2010

[2] Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra,"Security Issues in MANET: A Review",IEEE 2010.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati,"Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine0163-6804/02/$17.00 © 2002 IEEE.

[4] Ramanpreet Kaur, Anantdeep Kaur,"BLACKHOLE DETECTION IN MANETS USING ARTIFICIAL NEURAL NETWORKS", International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014

[5] D. B. Jagannadha Rao ,Karnam Sreenu, Parsi Kalpana,"A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks", International Journal of Advanced Research in Computer and Communication Engineering,Vol. 1, Issue 8, October 2012

[6] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao," A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences 2011.

[7] Saurabh Gupta, Subrat Kar, S.Dharmaraj, "BAAT:Black hole Attack Avoidence Protocol For Wireless Network",International Conference on Computer and Communication Technology (ICCCT)-2011.

[8] Maitha Salem Al Mazrouei, Dr Sundaravalli Narayanaswami,"Mobile Adhoc Networks: A Simulation based Security Evaluation and Intrusion Prevention", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011

[9] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami,"EAACK—A Secure Intrusion-Detection System for MANETs",IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS,VOL. 60, NO. 3, MARCH 2013

[10] Sunil kumar yadav,shiv om tiwwari,"An Efficient approach for prevention of co-operative black hole attack on DSR protocol", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. V (Jan. 2014), PP 56-62

[11] Ankur Thakur, Anuj Gupta ,"Single and Co-Operative Black Hole Problem in Aodv Protocol in MANETS: A Review", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 4 Issue 1 June 2014

[12] Ms. Sonal R. Jathe ,Prof. D.M. Dakhane "Detection of Sinkhole Attack against DSR Protocol MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012