# Implementation and Removal of co-operative blackhole and wormhole Attacks on manet with DSR

**[1]Manisha, [2]Dr. Mukesh Kumar**
**[1]M.Tech, banasthali vidyapith, banasthali**
**[2]Associate Professor, TITS, Bhiwani**

**Abstract: When the network is an open access network like mobile network, the criticality or the security challenge increases. These challenges are in terms of different kind of communication attacks over the network. These attacks include the blackhole and wormhole attacks. In this paper, we have designed a two level neighborhood analysis approach to generate effective preventive path in case of black hole and wormhole attacks. The proposed approach is divided in two main stages. In first stage, the analytical study is performed to identify the criticality of these attacks under different performance parameters. After identifying the node criticality, the next work is to provide the safe communicate route over which the communication is performed.**

**Keywords: MANET, Black Hole, wormhole attack, security.**

## I. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats. The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In internal attack, the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks. Such kind of attacks includes the blackhole and wormhole attacks.

In this paper, a communication analysis based node criticality identification approach is suggested. Section II of this paper includes the related work done by various authors in this field. In section III novelty of proposed idea is given. Section IV includes the proposed technique in detail. Experiment design for the simulation is present in section V. The work is concluded in section VI.

## II. RELATED WORK

Sun B[1] et al. use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. A. Shurman et al.[2] propose two techniques to prevent the black hole attack in MANETs. The first technique is to find at least two routes from the source to the destination. Tamilselvan L et al.[3] proposed a solution based on an enhancement of the original AODV routing protocol. The major concept is setting timer for collecting the other request from other nodes after receiving the first request. It stores the packet's sequence number and the received time in a table named Collect Route Reply Table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value. The simulation shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. Wu Chang et al.[7] propose a distributed and cooperated "blackhole" node detection mechanism which composes four sub-steps: (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction. Wang W et al. in 2009[12] proposed a technique for detection of collaborative packet drop attacks on MANETs. This mechanism is for audit based detection of collaborative packet drop attacks. Firstly the vulnerability of the REAct system is studied and then illustrated that Collaborative adversary can compromise the attacker identification procedure by sharing Bloom filters of packets among them. To defend against such attacks, Wang proposed mechanism to generate node behavioral proofs. Every intermediate node needs to conduct only a hash calculation on the received packet. A collaborative attacker cannot generate its node behavioral proofs if an innocent node before it does not receive the data packets correctly.

## III. NOVELITY AND PROPOSED TECHNIQUE

One of the critical problem of mobile network is the open network communication, because of this network can be infected with number of attacks. These attacks include the blackhole and wormhole communication attacks. To perform the effective communication over the network, we have suggested a preventive secure path identification approach in case of wormhole and blackhole attacks. The presented approach will improve the communication over the network in terms of better throughput, less network delay and the loss rate over the network.

## IV. PROPOSED APPROACH

A Mobile is an open area dynamic network because of this security is one of the critical issue in such network. A Mobile network suffers from different kind of attacks. These attacks affect the network at node level as well as at network level. These crucial attacks include the Wormhole attack and Blackhole Attack.

Blackhole attack: is the attack performed by a node to hijack the communication. It means all the communication will be diverted to the attacker node.

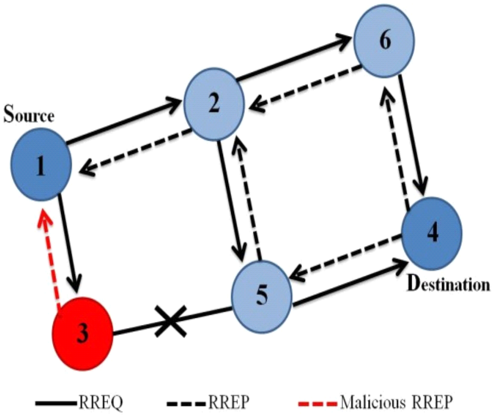


Fig1. Black hole attack

Black hole Attacks are classified into two categories:-

Single Black Hole Attack: In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node.

Cooperative Black Hole Attack: In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

Wormhole attack: is done by two or more nodes in cooperation and they form a tunnel to perform the communication and hijack the bandwidth. So that the communication over that particular path get disturb.

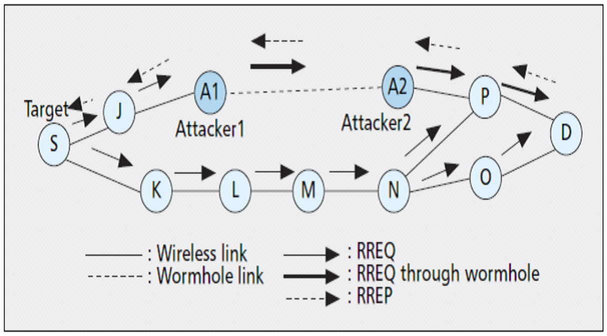


Fig2 wormhole attack

Proposed approach:

The presented approach is divided in two main stages. In first stage, the analytical study is performed to identify the criticality of these attacks under different performance parameters. After identifying the node criticality, the next work is to provide the safe communicate route over which the communication is performed. Communication analysis based node criticality identification is done. This analysis is based on the current communication analysis under the effect of average aggregative communication analysis. The aggregative analysis is periodic and based on it average communication parameters is obtained over the node. The current communication is compared with aggregative average communication and if the performance is lower, the node will not be elected as the next hop. The node that provides the communication performance average or above average is identified as the effective next hop.

Hence, a comparative analysis on these two attacks is performed. The work will not only analyze the effect of these attacks over the network but also it will provide the effective solution so that reliable communication will be drawn over the network. In this section, a statistical analysis based approach is suggested to identify the attack severity by performing the communication analysis. As the attack situation is identified, the communication is diverted to some reliable node. Therefore this presented approach is defined on two layers:

1) the current communication – for effective next node identification.
2) the period based analysis - aggregative communication analysis is performed

Later on, the weightage is assigned to these two layers to perform the effective communication over the network. The reliability or the effectiveness of nodes is here identified in terms of delay analysis and the loss rate analysis. The presented approach is implemented on DSR protocol. The approach is implemented on the routing scheme so that the effective network communication is drawn over the identified route. The basic flow of implementation is shown here under

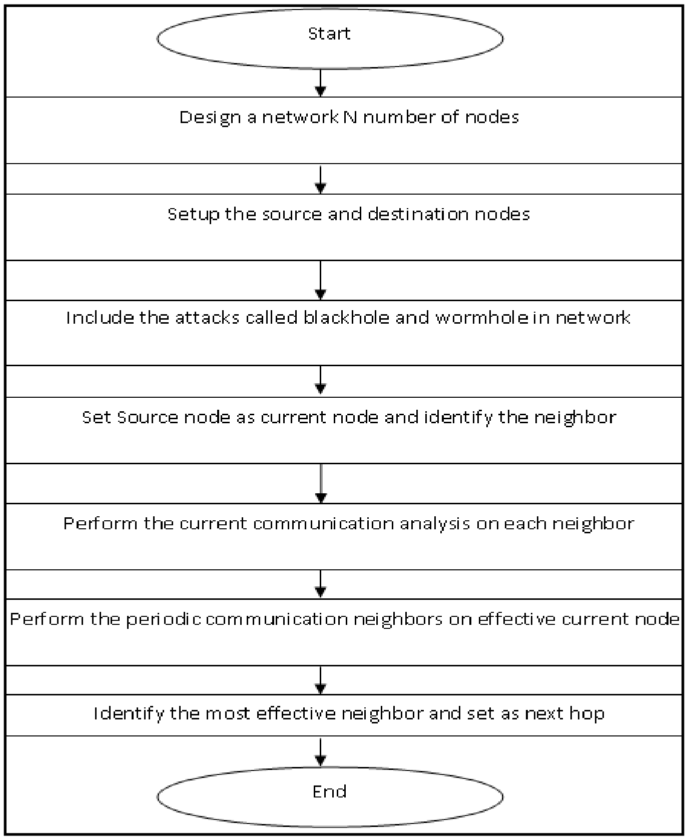

Start
Design a network N number of nodes
Setup the source and destination nodes
Include the attacks called blackhole and wormhole in network
Set Source node as current node and identify the neighbor
Perform the current communication analysis on each neighbor
Perform the periodic communication neighbors on effective current node
Identify the most effective neighbor and set as next hop
End

Fig3 flow of implementation

## V. RESULTS

To calculate the impact of the proposed approach, simulation of MANET is done using NS2. The simulation scenario consists of 25 mobile nodes. Protocol used for simulation is DSR. Common parameters used in simulation are shown in table 1 below:

Table 1Common parameters used in simulation

| Parameters | Values |
|---|---|
| Number of Nodes | 25 |
| Protocol | DSR |
| Simulation Time | 100 Sec |
| Packet Size | 512 |
| MAC protocol | 802.11 |
| Topology | Random |
| Attack | Blackhole/Wormhole |
| Communication Delay | .05 |

1. Delay analysis

As the communication is performed, both the delay over a node and the throughput is analyzed over the communicated nodes and data is transmitted over a safer path. Figure 4 shows comparative analysis of delay in case of DSR & blackhole attack. As can be seen from figure that there is gradual increase in delay in presence of blackhole attack.

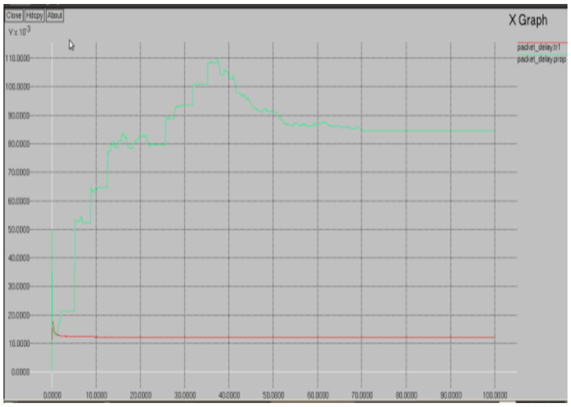


Fig 4 Comparision of DSR & Blackhole Attack for Delay

Figure 5 shows comparative analysis of network in terms of delay under DSR, & wormhole attack. It can be seen that delay, in presence of wormhole attack is comparatively lower than in presence of blackhole attack as was shown in fig 4.

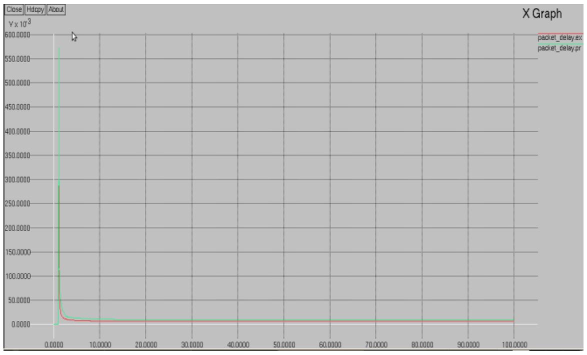


Fig 5 Comparison of DSR & wormhole Attack For Delay

2. Packet loss analysis: the total number of packets dropped during the simulation.

Packet lost = Number of packet send – Number of packet received.

The lower value of the packet lost means the better performance of the protocol**.**

Figure 6 shows no. of packets lost in case of DSR & cooperative blackhole attack and figure 7 also shows comparative loss analysis in case of DSR & wormhole attack.

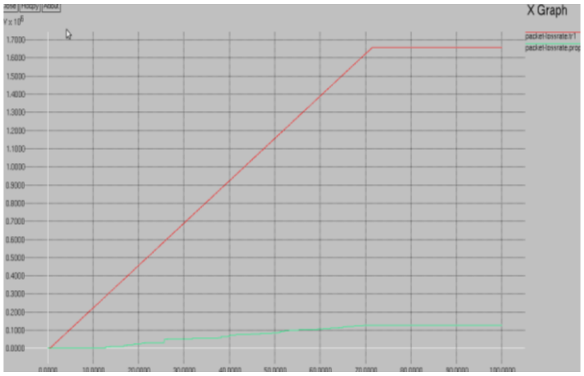
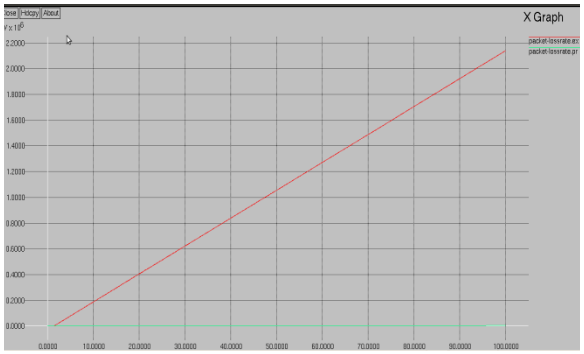


Fig 6 comparision of DSR & cooperative Blackhole attack for Packet lossrate



ISSN: 2278 – 1323

Fig 7 comparision of DSR & Wormhole attack for Packet lossrate

## VI. CONCLUSION

Wireless mobile ad hoc networks present difficult challenges to routing protocol designers. Mobility, constrained bandwidth, and limited power cause frequent topology changes. The very basic nature of the mode of communication is the main concern because anything that moves over the open air medium is susceptible to be picked up by unauthorized access. We discussed various activities of nodes which they are shown during the MANET operation and these activities are grouped into modes along their working. We also discussed the packets that are going to be exchanged in different mode of nodes. We have compared the two attacks namely blackhole, wormhole on the basis of their performance using different parameters. This is also to identify the effective preventive path so that effective communication can be drawn over the network.

## VII. REFERENCES

[1] Sun B, Guan Y, Chen J, Pooch UW, "Detecting *Black-hole Attack in Mobile Ad Hoc Networks*". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[2] Al-Shurman M, Yoo S-M, Park S , " *Black Hole Attack in Mobile Ad Hoc Networks*". 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[3] Tamilselvan L, Sankaranarayanan V, "*Prevention of Blackhole Attack in MANET*", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.

[4] Djenouri D, Badache N, "*Struggling Against Selfishness and Black Hole Attacks in MANETs",* Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.

[5] Hesiri Weerasinghe and Huirong Fu, "*Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation*", Intenation Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.

[6] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, " *Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks*", Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003 .

[7] Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "*A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network*", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.

[8] Kozma W, Lazos L , "*REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits*".Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.

[9] Raj PN, Swadas PB, "*DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET*", International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.

[10] Wang W, Bhargava B, Linderman M, "*Defending against Collaborative Packet Drop Attacks on MANETs*". 2nd International Workshop on Dependable Network Computing and Mobile Systems, New York, USA, 27 September 2009.

[11] Mistry N, Jinwala DC, IAENG, Zaveri M, "*Improving AODV Protocol Against Blackhole Attacks",* International MultiConference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19 March, 2010.

[12] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, " *Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs*". Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011.

[13] Prof. Sanjeev Sharma, Rajshree, Ravi Prakash, Vivek ,"*Bluff-Probe Based Black Hole Node Detection and prevention*", IEEE International Advance Computing Conference (IACC 2009), 7 March 2009.

[14] Jaisankar N, Saravanan R, Swamy KD (2010)" *A Novel Security Approach for Detecting Black Hole Attack in MANET.*"Paper presented at the International Conference on Recent Trends in Business Administration and Information Processing, Thiruvananthapuram, India, 26-27 March 2010

[15] Su M-Y (2011)" *Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems*". IEEE Computer Communications 34(1):107–117. doi:10.1016/j.comcom.2010.08.007