Detection and Removal of Black Hole Attack in Mobile Ad hoc Network

Harmandeep Kaur, Mr. Amarvir Singh

***Abstract*—A mobile ad hoc network consists of large number of inexpensive nodes which are geographically distributed over a specific area. Nodes in mobile ad hoc networks are small, cheap and light weight with limited computing capability and often deployed in dangerous or inaccessible areas where securing the mobile ad hoc network usually adds to the complexity. These types of networks are prone to various security attacks; in which black hole attack is a kind of denial of service attack which is quite common and harmful attack affecting the network layer. In this type of attack, the adversary controls the node and drops the entire set of packets forwarded to it. In this paper, DelPHI technique combined with geographical detection is used for detection and removal of malicious nodes from the network which are responsible for triggering the attack. Simulation results show a significant increase in throughput while the packet loss ratio and delay is reduced considerably by using the proposed mechanism.**

***Index Terms*— Black hole attack, Delay Per Hop Indicator (DelPHI) technique, Mobile Ad hoc Network (MANET)**

I. INTRODUCTION

A Mobile ad-hoc network (MANET) is a type of ad-hoc network comprising of wireless units that communicate with each other without any central control. The network is called *ad-hoc* because it does not require any additional routers or access points. It is a self-organizing and infrastructure-less network. Due to lack of infrastructure in MANETs, information that is exchanged among mobile devices depends on the cooperation of each node in the network [8]. Thus, a main requirement for achieving communication among participating nodes is that they should cooperate with each other. Today, mobile ad-hoc network is widely used technology in regions where it is difficult to deploy networks that rely on infrastructure. However, the distinguishing characteristics of MANETs from wired networks such as openness, decentralization, dynamic topology make it susceptible to various attacks which result in information loss along with energy expenditure. Hence, ensuring security in these types of networks becomes a primary concern. In black hole attack, an attacker captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them to the intended destination. As a result, any information that enters the black hole region is captured and does not reach the destination. Due to this attack, high end-to-end delay is introduced in the network and performance of the network is degraded. The main aim of this research is to propose a technique for detection and removal of black hole attack in mobile ad hoc network.

Manuscript received Aug, 2017.

***Harmandeep Kaur**, Department of Computer Science, Punjabi University Patiala, India.*

***Mr. Amarvir Singh**, Assistant Professor, Department of Computer Science, Punjabi University Patiala, India.*

II. LITERATURE SURVEY

Sun [1] described mobile ad-hoc networking as an important technology which has become quite popular with time. This paper gives a brief introduction about two types of wireless network and the main focus is on mobile ad-hoc network. The basic concept of mobile ad-hoc network, features and few of its applications are discussed. It also presents various challenges posed by MANET. The paper concludes with certain important research issues in mobile ad-hoc network such as security schemes, internetworking mechanisms etc.

Rajakumar et al. [2] emphasized on various security attacks that are prevalent in ad hoc network and schemes for the detection of these attacks. This paper summarizes the attacks and their classifications and also an attempt has been made to explore the corresponding detection schemes widely used to avoid those attacks.

Chang et al. [3] proposed a cooperative bait detection approach for defending against collaborative black hole attacks in MANETs. This paper attempts to combat the problem of non-cooperative nodes by designing a security mechanism called dynamic source routing (DSR)-based routing, which is referred to as the cooperative bait detection scheme. This scheme combines the benefits of both reactive and proactive defense architectures. Simulation results show that in the presence of malicious-node attacks, the performance of proposed approach is better than the DSR, 2ACK, and best-effort fault-tolerant routing protocols.

Jain and Khuteta [4] proposed a method for handling black hole attacks in mobile ad hoc networks. In this method, the base node is deployed in the network so that the probability of detecting multiple malicious nodes is increased. After the detection of these malicious nodes, these are further isolated from participating in any future transmissions. This paper also presents the simulation results and determines the performance of the proposed method based on the observed results.

Kumar and Kumar [5] proposed an adaptive approach for the detection of black hole attacks in mobile ad hoc network. This detection scheme is more efficient in terms of cost and security as compared to various other solutions for the detection of black hole attacks. Its performance is also compared with standard AODV routing protocol using NS-2 simulator and it is shown that the proposed approach is better by using the experimentation results.

Abdelshafy and King [6] demonstrated a new concept of Self-Protocol Trustiness for accomplishing the detection of a malicious node. A black hole Resisting Mechanism is described to withstand such attacks that can be introduced into any reactive routing protocol. This approach relies on locally applied timers and thresholds for identifying the black hole nodes. There is a little overhead and no extra communication because no changes to the packet formats are required. By analyzing the simulation results, it is concluded in the paper that the proposed mechanism is successful in the detection of malicious nodes within a shorter period of time irrespective of the number of misbehaving nodes and the amount of time for which they are active in the network.

Arathy and Sminesh [7] proposed a novel approach to detect both single and multiple black hole attacks in wireless mobile ad-hoc network. The lack of security in the design of Ad hoc On Demand Distance Vector Routing protocol increases the risk of attacks in this protocol. This paper discusses in brief about the black hole attacks in Ad hoc On Demand Distance Vector Routing. The paper proposes two algorithms. First is the Detection of Multiple Black Hole Attack and another is the Detection of Collaborative Black Hole Attack. These algorithms are analyzed with the existing Data Routing Information, trust based and fidelity scheme. It is observed that the routing and computational overhead was reduced considerably whereas no such improvement is analyzed in storage overhead.

Dangare and Mangrulkar [8] proposed a trust based approach to reduce the effect of various attacks in mobile ad-hoc network. This paper lists various security attacks. Two attacks are considered in this paper. First are the vampire attacks which are not any protocol specific and second are the denial of service attacks which use up all the resources available to a network. Simulation results shows that the two attacks under consideration are mitigated using a cluster based technique.

III. PROPOSED METHOD

In this paper, DelPHI (Delay Per Hop Indicator) technique is used to solve the proposed problem. The aim of the proposed scheme is to detect the malicious behavior of nodes and prevent the black hole attack by removing those nodes from the network. The benefit of using this scheme is that it does not need clock synchronization and position information. Another benefit is that it provides higher power efficiency as it does not require the mobile units to be equipped with specific hardware.

The disadvantage of Delphi method is that it cannot identify the location of malicious node that triggers the attack. This disadvantage can be overcome by using Geographical Detection. The proposed solution works in two phases:

Phase 1: Network deployment

- Firstly, we set up a mobile ad-hoc network consisting of fixed number of nodes in a fixed area. The network deployed is independent of any central control and each node has the capability to move freely.
- After deploying the MANET, an Ad-hoc On demand Distance Vector (AODV) routing protocol is used to establish a route from source node to destination node. AODV utilizes the control packets to find the path to the destination.
- In order to establish route to the intended destination, the source node broadcasts the route request (RREQ) packet to its neighboring nodes in the network. Upon receiving the RREQ, the intermediate nodes containing an active path to the intended node reply back with the route reply (RREP) packets to the source node.
- After receiving the route reply packets, the best route is chosen from the multiple paths for carrying out further communication between source and the destination.

Phase2: Malicious node detection and removal

- The existence of malicious node along the path will generate the black hole attack and is responsible to change the delay between the source and destination node.
- The delay per hop value is computed for each node existing in the path which acts as an indicator to detect the presence of the black hole node.
- Then, we trace the neighbor of each node in the network and compute its distance from the source node. This enables us to determine the location of the node responsible for the black hole attack.
- Finally, the malicious node is removed from the mobile ad-hoc network by forming a new path from the source node to the destination node for transmitting the data packets.

After this, we further plotted three graphs of throughput, delay and packet loss for both the scenarios that are with and without the proposed solution of the black hole attack in the network. We observed that the results showed the great differences.

Algorithm for the proposed scheme

Step 1: Deploy finite number of nodes to form mobile ad-hoc network.

Step 2: Define the source and destination nodes in the network.

Step 3: The source node transmits the route request packets in the network to establish the path from source to destination node.

Step 4: On the basis of hop count and sequence number, shortest path will be set up from source to the destination.

Step 5: Calculate the delay per hop in the network.

Step 6: If (delay < defined delay), calculate Euclidian distance of each node.
Step 7: Using the ping point technique of Delphi, detect the malicious node in the network and isolate it from the network.
Step 8: Else, communication continue between source and destination.

IV. RESULTS AND ANALYSIS

In order to evaluate the performance of mobile ad-hoc network under black hole attack, simulations are performed using NS-2 simulator. It has been used as a simulation tool since it supports simulating an ad-hoc mobile environment.

Simulation of the problem and proposed solution

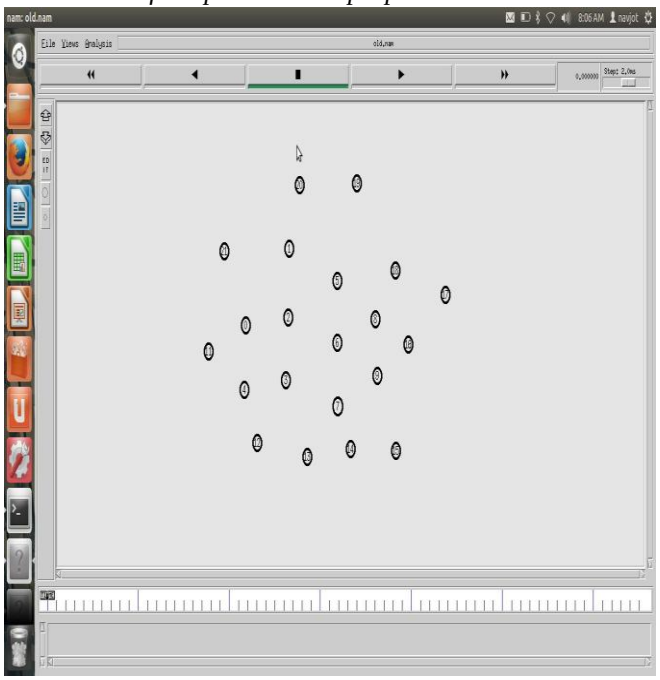


Fig. 1 Deployment of MANET

As shown in Fig. 1, the mobile ad-hoc network is set up in the fixed area with fixed number of nodes. There is no central authority that controls the entire network. The network functions are distributed among the mobile nodes.

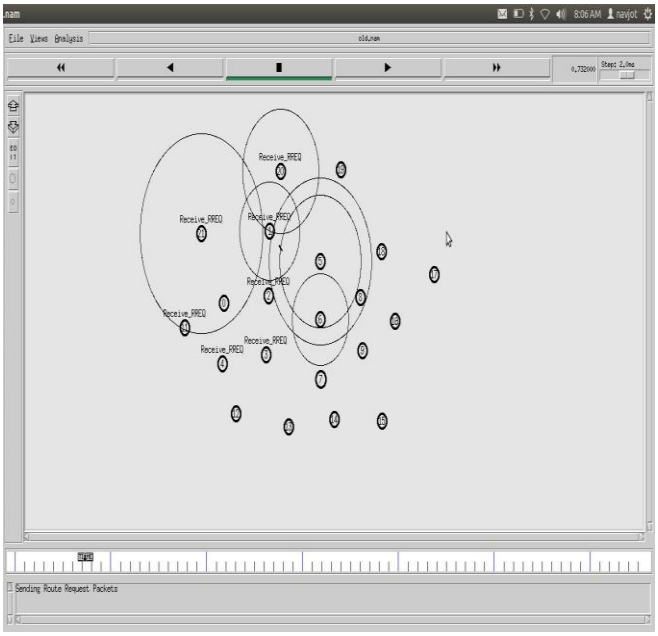


Fig. 2 Path establishment using AODV routing proocol

As illustrated in Fig. 2, the AODV routing protocol is used to establish path from source to destination. The source node broadcast route request packets to its neighboring nodes in the network for establishing route to the intended destination.

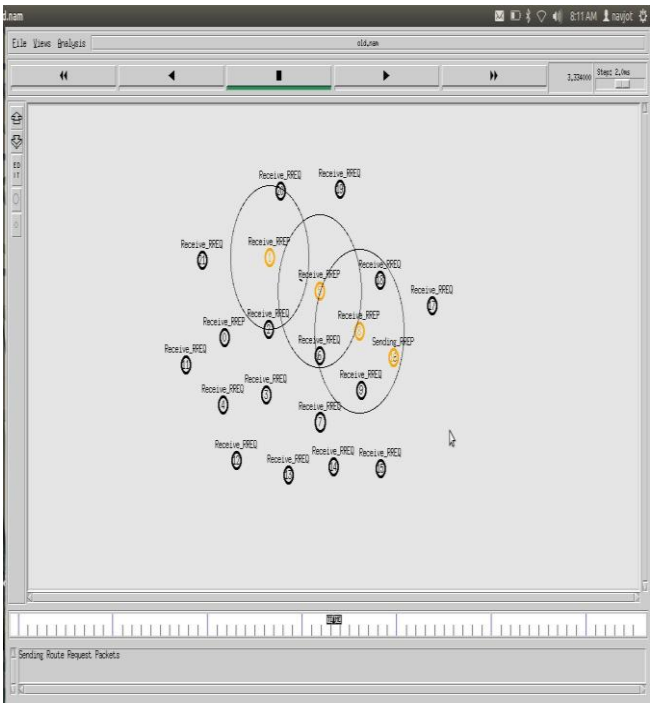


Fig. 3 Adjacent nodes reply with RREP

As shown in Fig. 3, the intermediate nodes having an active route to the destination will reply back to source node with the route reply packets (RREP). Using RREP source is able to maintain the best route from itself to the destination node.

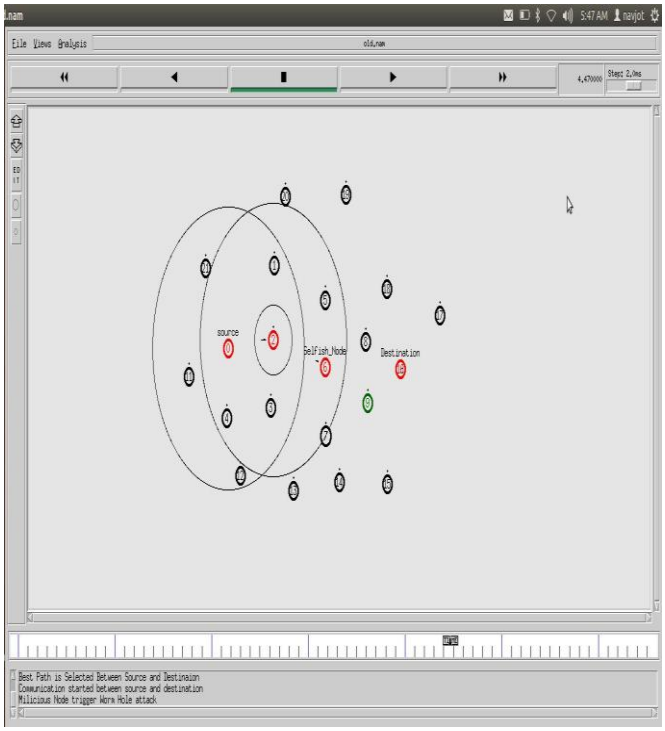


Fig. 4 Depiction of malicious node in the path

The malicious node exists along the path which will trigger black hole attack in the network as depicted in Fig. 4. The data packets forwarded through this path will be dropped by malicious node.

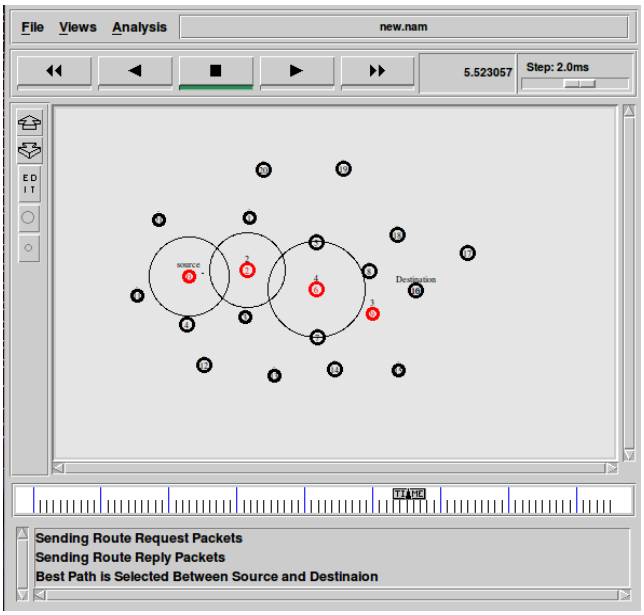


Fig. 5 Detection of malicious node

As shown in Fig. 5, using Delay per hop value we can figure out that some malicious node is present in the network. To isolate the malicious node position based technique is used which is defined through next simulation graph.

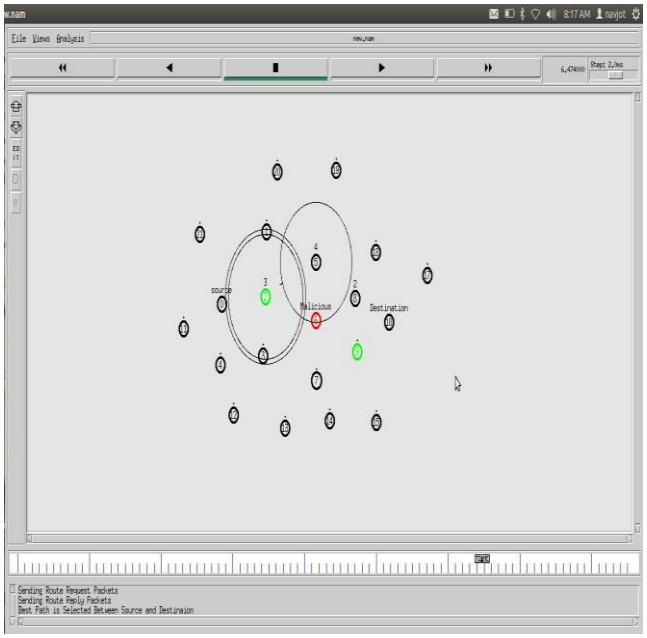
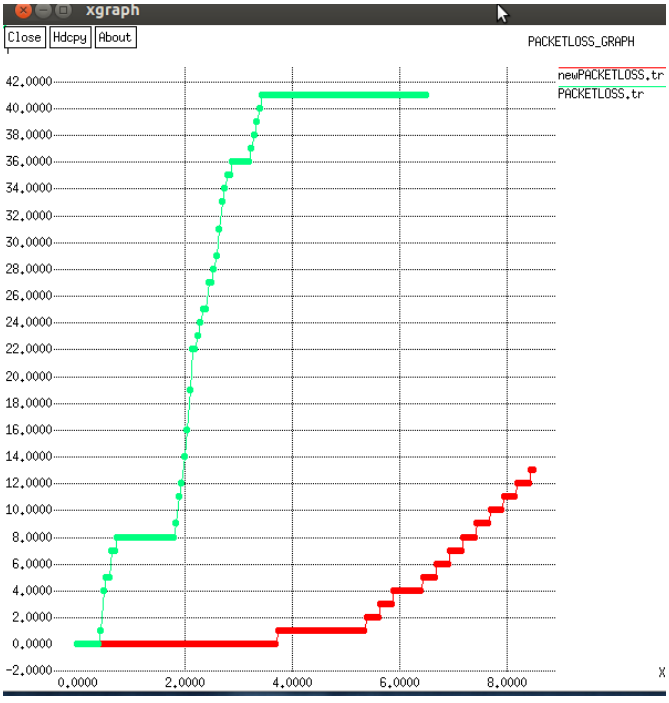


Fig. 6 Isolation of malicious node

Fig. 6 represents the isolation of malicious node in the mobile ad-hoc network. By computing the distance of each node from the source node, we can isolate the malicious node. The new path will be formed between source and destination to carry out the further transmission of data packets.



Simulation Results

Packet Loss: It is a phenomenon in which a packet traveling from a source fails to reach the destination. It is inversely proportional to performance, that is, the lower is the value of packet loss, better is the performance of network.

$$Packet\ Loss = \frac{\sum Number\ of\ packet\ sent}{\sum Number\ of\ packet\ received} \quad (1)$$

Fig.7 Packet loss

As illustrated in Fig. 7, large number of packets fails to reach the destination under attack scenario. Packet loss under isolated scenario is depicted by the red line. It is reduced when the malicious node is removed from the network.

Throughput: It is defined as the total number of bits transmitted per second. In other words, it measures the number of packets that have been delivered successfully from source node to the destination in a given time period. In MANET, factors that affect throughput include dynamic topology, limited resources and unreliable communication.

$$Throughput = \frac{\sum Data\ received}{\sum Data\ transmission\ period} \quad (2)$$

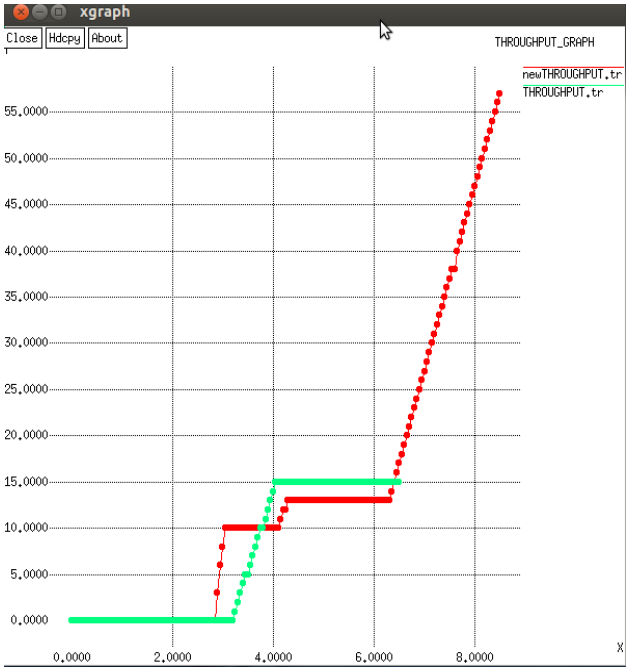


Fig. 8 Throughput

In Fig. 8, green and red lines depict the throughput of attack scenario and isolated scenario respectively. It is clear from the graph that the throughput increases when the attack is isolated from the network.

Delay: It is defined as the average time taken by a data packet to reach the destination node. It may be caused due to the presence of malicious nodes in the network.

$$Delay = \frac{\sum(arrival\ time - send\ time)}{\sum Number\ of\ connections} \quad (3)$$

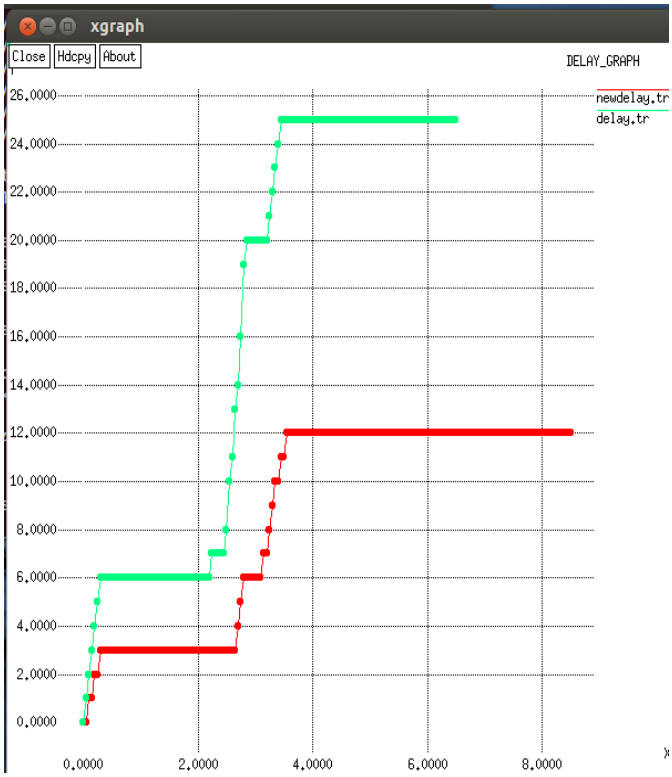


Fig. 9 Delay

The green line and red line in the above graph denote the delay of attack scenario and isolated scenario respectively. As illustrated in Fig. 9, the delay in the attack scenario is found to be more as compared to the delay in the new scenario. The delay reduces significantly in the absence of black hole attack.

ACKNOWLEDGEMENT

With profound gratitude and due regards , I whole heartedly and sincerely acknowledge the efforts, encouragement and proper guidance by Mr. Amarvir Singh Assistant Professor, Department of Computer Science, Punjabi University, Patiala .

V. CONCLUSION

The proposed study has broader scope. When the nodes are mutually loyal, it leads to the reliable data transmission between the nodes, but the problem arises when some malicious node sits in between the path and start dropping the packets. Drop of the packets can be due to black hole attack which leads to lower down the throughput of the transmission. Delay (Del) - Per (P) - Hop (H) – Indicator (I) – (DelPHI) technique is used to count the delay occurred to reach each node in the path. As malicious node enters in the source destination path, it changes the delay which helps to identify the presence of selfish node. Further, neighbors of each node are identified by distance calculation to identify the exact location of selfish node. Attack degrades the performance of the system by dropping the packets. Solution is designed to find out the packet drop nodes and those nodes are then isolated from the path forming a new path for sending the packets to its destination. This work will help to reduce the problem occur in link failure and packet lost. The

simulation results show the improvements in the performance of the network.

REFERENCES

[1] J.Z. Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing," *IEEE International Conference on Info-Tech and Info-Net*,pp. 316-321, 2001.

[2] P.Rajakumar, T.P.Venkatesan, and A. Pitchaikkannu, "Security attacks and detection schemes in MANET," *IEEE International Conference on Electronics and Communication Systems (ICECS)*, pp. 1-6, 2014.

[3] J. M. Chang, P .C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE systems journal*, vol. 9, no. 1, pp. 65-75, 2015.

[4] S.Jain, and A. Khuteta, "Detecting and overcoming black hole attack in mobile Ad hoc Network,"*IEEEInternational Conference on Green Computing and Internet of Things (ICGCIoT)*,pp. 225-229, 2015.

[5] V. Kumar, and R. Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network,"*Procedia Computer Science*, vol. 48, pp. 472-479, 2015.

[6] M.A.Abdelshafy, and P.J.B. King, "Resisting black hole attacks on MANETs," 13th*IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1048-1053,2016.

[7] K.S.Arathy, and C.N. Sminesh, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET,"*Procedia Technology*, vol. 25, pp. 264-271., 2016.

[8] N.N. Dangare,and R.S. Mangrulkar,"Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad hoc Network,"*Procedia Computer Science*, vol. 78, pp. 342-349, 2016.

Harmandeep Kaur is a student of M.Tech (CSE) in Department of Computer Science, Punjabi University, Patiala carrying out her research work under the guidance of Mr. Amarvir Singh.

Mr. Amarvir Singh is presently serving as Assistant professor in Department of Computer Science, Punjabi University, Patiala.