# An Implementation of Black hole Detection and Prevention Method using AODV Routing Protocol in MANET Environment

Devendra Kumar
PG scholar,
CSE Department,
Shri Vaishnav
Institute of Technology and
Science, Indore,
Madhya Pradesh, India.

Rupali Bhartiya
Reader, CSE Department
Shri Vaishnav
Institute of Technology and
Science, Indore,
Madhya Pradesh, India

## ABSTRACT

Network security is a pathetic link in wired and wireless network systems. A mobile ad hoc network (MANET) is a compilation of self-sufficient nodes that converse with every further by forming a multi-hop radio network and maintaining associations in a decentralized manner. Security remains a main challenge for these networks owing to their features of open medium, animatedly changing topologies, confidence on accommodating algorithms, absence of federal monitoring points, and lack of clear lines of protection. Mainly of the routing protocols for MANETs are therefore susceptible to dissimilar kind of attacks. Ad hoc on-demand detachment vector routing (AODV) is a much admired routing algorithm. Though, it is susceptible to the recognized black hole attack, where a malevolent node incorrectly advertises good pathway to a purpose node throughout the route discovery process. This attack becomes additional sever while a group of malevolent nodes assist every other. In this paper, a security mechanism is offered against a corresponding attack by multiple black hole nodes in a MANET. The reproduction approved out on the proposed scheme has produced results that establish the efficiency of the mechanism in discovery of the attack as maintaining Constant Network Performance.

## Keywords

AODV, Black-hole, NS2, MANET, Routing Protocol

## 1. INTRODUCTION

The rapid growth in communiqué technology has known rise to strong research interest on Wireless Networks. Malicious attacks include reason tremendous loss by impairing the functionalities of the computer networks. Therefore, security is a major concern for protected communiqué among mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and submissive attacks next to intercept capable routing in embed in routing message and data packets [1]. Mobile ad hoc network (MANET) is one of the most up-and- coming fields for investigate and review of wireless network. Necessary condition in MANET is security. In ad hoc network the converse nodes sets new challenges for the security architecture since it doesn't essentially feed on fixed infrastructure.

Mobile ad hoc network (MANET) is one of the mainly up-and- coming fields for research and review of wireless network. Necessary condition in MANET is security. In ad hoc network the converse nodes sets new challenges for the security architecture because it doesn't necessarily feed on fixed communications. The ad-hoc network is additional susceptible to black-hole attack forcefully initiate through malicious nodes or attacker. In networking, Nodes can be anything like systems or devices i.e. mobile phone, laptop, individual digital assist, MP3 player and individual computer that are participating in the network and free to moving in and out in the network. At the similar time nodes can act as host as well as router and form conflicting topologies turn on their comparability with each other in the network. As of their self-alignment aptitude these nodes include the capability to reconfigure itself [2].

Wireless links in addition makes the MANETs additional probable or liable to be partial or harmed by a particular thing, which make it, trouble free for the intruder to go inside the network and gain access to the existing communication.

A Mobile Ad-Hoc Network (MANET) is a network where additional than two self-sufficient mobile hosts (mobile devices i.e. mobile phone, laptop, iPod, PDAs etc.) can converse with no some mean of communications i.e. on the fly. When source (S) node want to send some data toward the purpose (D), if they are in the similar broadcast range can directly communicate with each other or else in-between nodes help to relay data from resource to destination. In MANETs individual node can leave and join the network on it possess, consequently the physical organization of the network frequently changes dynamically. Battery power of mobile device is as well significant feature, since depletion of battery power may affect the lifetime of a node. Node movements be different for mobile nodes are dissimilar, the topology also depend on the speed and direction of nodes. Due to vibrant topology of the network routing in MANET is a challenging problem. Particular pathway routing is not always sufficient to disseminate data to the purpose. Consequently; multipath routing comes into existence to overcome the problem of single path routing [3].

MANET preserve provide rapid connection among self-governing mobile users. Examples include establishing survivable, resourceful, vibrant communication for emergency/rescue operations, disaster relief efforts, military networks, convention or property networks, car networks, personal networks, etc.

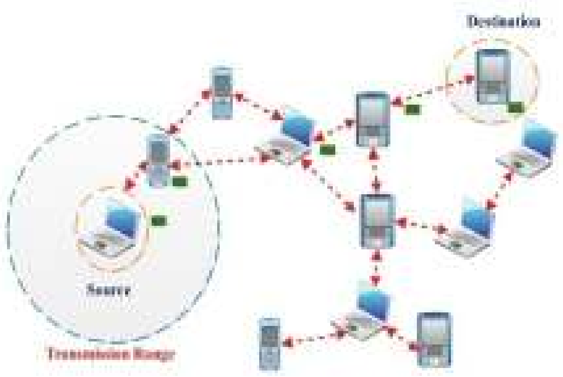


**Figure 1 Mobile Ad-hoc Network [4]**

## 1.1 MANET Security Challenges

Some security challenges in MANET are hereditary from ad hoc networks that were investigating interests since 1999 [5]. Services refer to various defensive policies in order to create a secure network, even as attacks use network vulnerabilities to defeat a security service. Some of the security challenges are as follows [6].

### *1.1.1 Security Services*

The aim of a security service is to secure network before some attack happened and made it harder for a malevolent node to breaks the security of the network. Owing to particular features of MANET, providing these services faced lots of challenges. For securing MANET a trade-off among these services should be supply, which means if one service guarantees with no noticing additional services, security system resolve fail. Providing a trade-off among these security services is depended on network request, but the difficulty is to provide services one by one in MANET and there a method to guarantee every service. We converse five significant security services and their challenges because follows:

- **Availability:** According to this service, every certified node should have admittance to all data and services in the network. Accessibility challenge arises owing to MANET's vibrant topology and open boundary. Admittance time, which is the time, required for a node to admittance the network services or data is important, because time is one of the security parameters. By with lots of security and verification levels, this service is disregarded as transitory security levels wants time.
- **Authentication:** The goal of this service is to supply trustable communications among two dissimilar nodes. While a node receives packets from a resource, it should be sure regarding identity of the source node. One method to present this service is using certifications, whoever in absence of central control unit, key distribution and key management is challengeable.
- **Data confidentially:** According to this service, every node or submission should have admittance to particular services that it has the authorization to access. Most of services that are provided by data confidentially use encryption technique but in MANET because there is no central management, key distribution faced lots of challenges and in some cases not possible.
- **Integrity:** According to reliability security service, just authorized nodes can create, edit or delete packets. As an instance, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then eliminates or transforms them.
- **Non-Repudiation:** By using this service, neither source nor destination can disclaim their performance or data. In previous words, if a node receives a packet from node 2, and sends a reply, node 2 cannot renounce the packet that it has been sent.

The remainder of paper is organized as follows. Section 2 describes related work and Section 3 is short note about Black hole Attack. In Section 4, proposed scheme is discussed for making MANETs free from the Black hole attack. Implementation of the proposed scheme is covered in Section 5 and Result Section is 6. Finally conclusion and future directions are given in Section 7.

## 2. LITERATURE SURVEY

Numerous Researchers have worked on manifold discovery and avoidance of wormhole attacks in wireless sensor network, based on the detection mechanism, the accessible method of perceive and preventing wormhole attacks can be illustrate in this section.

Patel and Dadhaniya [7] proposed a 3-step host based Intrusion detection technique in which each node acted as IDS node. It detects a malicious node based on sequence number generated by it. If sequence number generated by replying node is greater than the sequence number generated by source node, then the replying node is considered as malicious node and the messages sent by it are also blocked, by transmitting node id to all other nodes. The simulation results of the paper showed that there was an increase in PDR and average throughput.

Deng et al. [8] presented a solution for solving problem of Black Hole Attack. In this technique, along with the RREP message, information regarding the neighbor of replying node is also asked and when RREP message reaches source, source instead of sending message immediately sends another message to neighbor of replying node asking whether the intermediate node which is replying for RREQ message really has path to destination or not. But it had limitation that it increased the message overhead so it can be used to verify identity of node which is under doubt of being malicious and it also assumed that Black hole nodes cannot work in group.

Raj and Swadas [9] proposed a method DPRAODV to detect black hole node based on RREP sequence number and threshold value. If the value of RREP sequence number comes out to be greater than the threshold value then the node sending this RREP will be considered as malicious. Further this malicious node is isolated from network by sending a control message ALARM to all other nodes and a list of blacklisted nodes is created. The simulation results showed that there was an increase in packet delivery ratio but also an increase in routing overhead and delay in message delivery.

Mistry et al. [10] did a modification in working of source node by the addition of new function for storing RREP messages for some specified time, a table which stores these RREP messages, a timer and Mali_node id for detecting black hole node and to keep record of all malicious nodes present in network. This technique discards the RREP message stored in table which has highest value of destination sequence number and node sending this RREP will be considered as malicious and its identity will be stored as malicious id. This method leads to an increase in memory and time overhead but increase in packet delivery ratio compensated for that overhead.

Bhosle et al. [11] proposed a watch dog mechanism in which an additional information is stored in tables at all nodes to detect the presence of attacking node. In this the nodes keep track of the packets they send and packets they drop, and if the value of packet drop ratio increases from threshold the node will be considered as an attacking node.

Bansal and Baker [12] have proposed a scheme that relies on first-hand observations. Directly observed positive performance increases the rating of a node, while honestly observed depressing behavior decreases it by an amount larger than that is used for optimistic increments. If the rating of a node dips below the faulty threshold, the node is added to a defective list. The faulty record is appended to the route request by each node distributing it to be used as a list of nodes to be avoided. A route is rated superior or awful depending on whether the next hop is on the faulty list. If the next hop of a path is in the faulty record, the route is rated as bad. As a response to misbehavior of a node, all traffic from that node is discarded. A second chance means for release employs a break after an idle period. After a break, the node is removed from the defective list with its rating remaining unchanged.

Deng, Li and Agarwal [13] have suggested a method of security against black hole attack in ad hoc networks. In their proposed scheme, as soon as the Route Reply packet is received from one of the middle nodes, another Route Request is sent from the source node to a neighbor node of the middle node in the path. This is to ensure that such a path exists from the middle node to the destination node. For instance, let the source node S send Route Request packets and receive Route Reply through the intermediate malicious node M. The Route Reply packet of M contains information about its next hop neighbor node. Let it contain information about the neighbor E. Then, the source node S sends Further Route Request packets to this neighbor joint E. Node E responds by sending a Further Route Reply packet to source node S. Since node M is a malicious node, and thus not present in the routing list of node E, the Further Route Reply packet sent by node E will not contain a route to the malicious node M. But if it contains a path to the destination node D, then the new path to the destination through node E is selected, and the earlier selected route through node M is rejected. While this scheme totally eliminates the black hole attack by an only attacker, it fails completely in identifying a cooperative black hole attack linking multiple malicious nodes.

## 3. BLACK HOLE ATTACK

The Black hole Attack in MANETs can be categorized into several type in terms of the approach adopted by the malevolent node to launch the attack. In particular the malicious node can intentionally drop all the forwarded packets going through it (packet drop attack), or it can selectively drop the packets originated from or destined to certain nodes that it dislikes. In order to launch a Packet Drop Attack, the first step for a malicious node is to find a manner that allows it to find involved in the route forwarding path of data or control packets. To do so, it exploits the vulnerabilities of the causal routing protocols which are generally designed with strong hypothesis of credibility of all the nodes participating in the network. Thus, any node can easily misbehave and provide a severe damage to the network by targeting together data and control packets. Dropping data packets leads to suspend the on-going communication among the start and the goal node. More seriously, an attacker that captures the arriving control packets can avert the associated nodes from establishing routes between them [14].

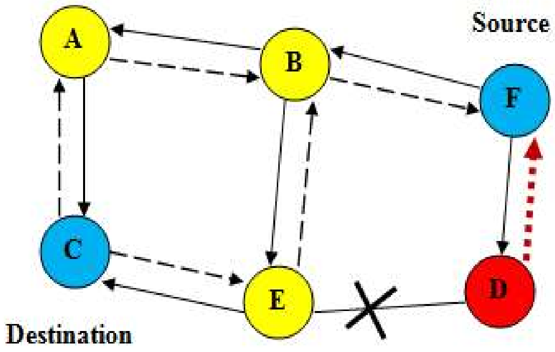


**Figure 2 Black hole Attacks**

In Black whole attack, using routing protocol to an invader promotes itself as the shortest path to the objective device [15]. An attacker watches the routes appeal in an overflow based routing protocol. When the attacker receives an application for a route to the purpose node, it forms a react connecting of actually short route. If the naughty respond reaches the initiate node previous to the reply from the authentic node, a false route gets formed. Once the malicious device joins the network itself among the converse nodes, it is forceful to do the whole thing during the packets passing through them. It can crash the packets between them to implement a denial-of-service attack, or on the beforehand use its situation over the route is the first step of man-in-the-middle attack [16].

## 4. PROPOSED SYSTEM

The proposed work is intended to find an adoptable security algorithm formulation by which the mobile ad hoc network becomes secure.

### 4.1 Domain Overview

The mobile ad hoc networks having the various vital properties by which the numerous applications are getting the advantages of these properties. The network is a kind of distributed network technology by which the network information is not handled with the centralized control. The routing protocols are used to discover routes between two parties those are going to communicate. But due to the changing network topology the intermediate nodes are frequently changing their positions a new node can join the active communication sessions.

### 4.2 Solution Strategy

In a MANET when we using ad-hoc types of routing ,if nodes want to communicate then the route search have be start, there are dissimilar kind of packets in a MANET such because data packets and routing packets routing packets are which is used for pathway searching from resource to purpose so the resource send a routing packets recognized as RREQ packets which in addition recognized as application packets contain all the information about source and destination and these packets flood to his neighbours nodes then they send it to their neighbors nodes thus these packets travel hole network and next while they discover out the purpose they reply message were start to sending form purpose ends and a route has been ascertain .The additional kind of packets are data packets which contains data .

### 4.3 Proposed Algorithm

```
Algorithm for Black hole Attack
1: Initialize the Network, with N nodes where
   $N = 1,2,3,.....,$ , in ideal condition.
2: Initialize Route Discovery by Source Node $N_s$
3: $N_s$ sends RREQ Packets to Destination $N_d$
4: Wait Until all Route Replies not received
5: Calculate Packet Drop Ratio
   $PacketDropRatio = \frac{TotalForwardedPacketByEachNode}{TotalSentPacket}$
6: Calculate Average PDR Value for each Node i.e. Threshold Value
   $\alpha = \frac{1}{N} \sum_{i=1}^{N} PDR\,i$
7: Compare PDR Value of each node to Average Threshold $\alpha$
        $if(PDR > \alpha)$ {
        set as Trusted Node
          }
          else {
         Untrusted Node
          }
8: Apply Neural Network for all untrusted node
9: Select number of parameter for node training as input Pattern
      a. Number of Packet Send
      b. Number of Packet forwarded by nodes
      c. PDR
      d. Node ID
   Output: Class Level
10: $If\ Class\ Level = 0 \wedge ¿ Node = Untrusted$ , then
      Set Node as Malicious
      Stop Communication
11: End Process
```

Neural network uses the number of training cycles for correcting the error in output omitted.

## 5. IMPLEMENTATION

The simulation is being implemented in the Network simulator [16]. Protocol used here is AODV.

Table 2 Simulation Scenarios

| *Parameters* | *Values* |
|---|---|
| **Antenna Model** | Omni Antenna |
| **Dimension** | 1000 X 1000 |
| **Radio-Propagation** | Two Ray Ground |
| **Channel Type** | Wireless Channel |
| **Traffic Model** | CBR |
| **Routing Protocol** | AODV |
| **Mobility Model** | Random Waypoint |
| **Simulation Time** | 50.0 sec |

### 5.1 Simulation of AODV Routing under Attack

In this network simulation the network is configured with the traditional AODVrouting protocol and the network performance is evaluated. That simulation also contains a malicious attack which demonstrates the effects of Black hole attack in normal network. The simulation of the discussed technique is given in the given figure. In this diagram the green nodes show the client nodes involved in the network and the sender and receiver for the network is demonstrated using the pink color.

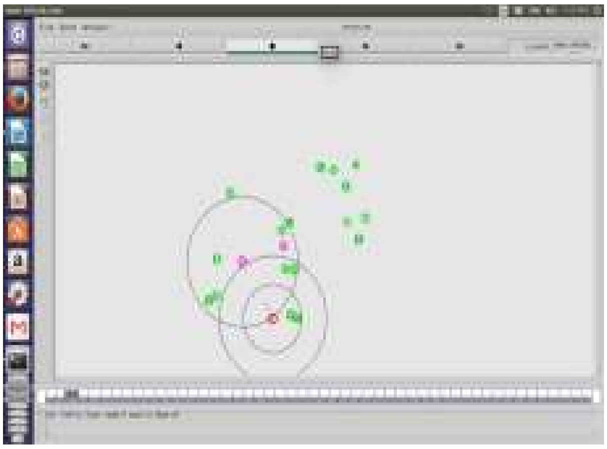


Figure 3 Network under Attack condition

### 5.2 Simulation using Proposed Routing Method

In this phase, of proposed secure routing method is simulated when attack prevention is established. Therefore the second simulation is prepared which is demonstrated in given figure. In this simulation screen the green nodes demonstrate as normal legitimate node in network. The given simulation is developed using the proposed secure routing technique. When the proposed method is deployed network performance is improve and large number of packet is delivered to the destination. Communication is happened between source node 9 and destination node 18.

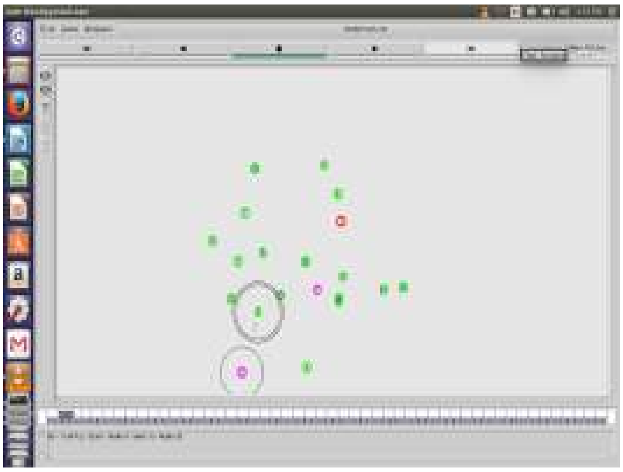
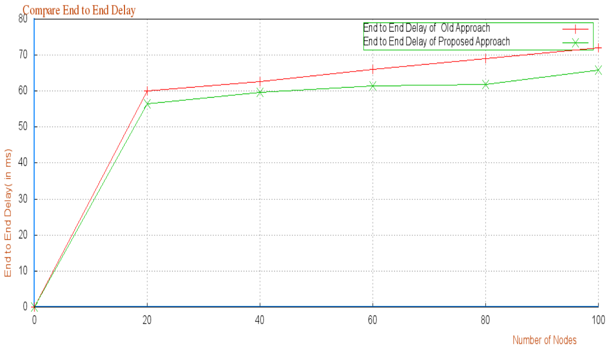


**Figure 4 Proposed Solutions for Attack Prevention**

# 6. RESULT ANALYSIS

End to end day on network refers to the time taken, for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2E\ Delay = Receiving\ Time - Sending\ Time$$



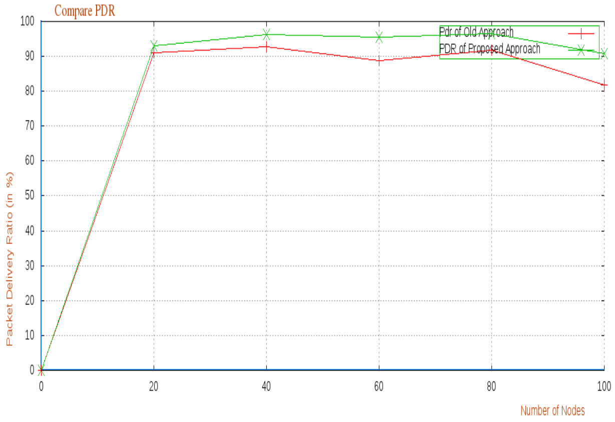
**Graph 1 End to End Delay**

Graph 1 shows the comparative End to End Delay of the traditional AODV routing and the proposed secure routing technique. In this figure 5.1 the X axis contains the number of nodes in network and the Y axis shows the performance of network in terms of milliseconds. According to the obtained results the proposed technique is produces less end to end delay as compared to traditional routing technique under attack conditions. Therefore the proposed technique is an efficient technique and produces less amount of time.

## 6.1 Packet Delivery Ratio

The performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully delivered packets to the destination, where PDR can be estimated using the formula given:

$$Packet\ Delivery\ Ratio = \frac{Total\ Delivered\ Packets}{Total\ Sent\ Packets}$$

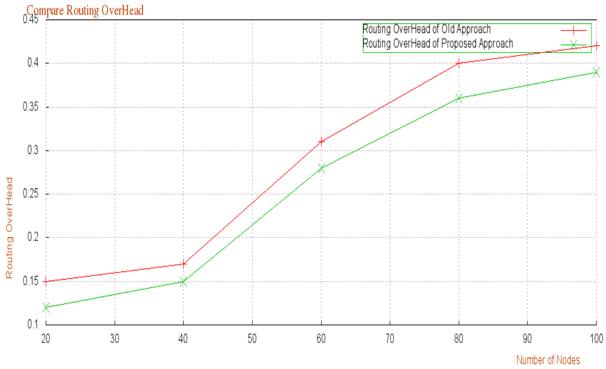


**Graph 2 Packet Delivery Ratio**

The comparative packet delivery ratio of the networks is given using Graph 2, in this graph the X axis shows the number of nodes in the network and the Y axis shows the amount of packets successfully delivered in terms of the percentage. According to the obtained results the proposed technique delivers more packets as compared to the traditional technique even when the network contains the attacker node therefore the proposed technique able to escape the attack effect and improve the network performance.

## 6.2 Routing Overhead

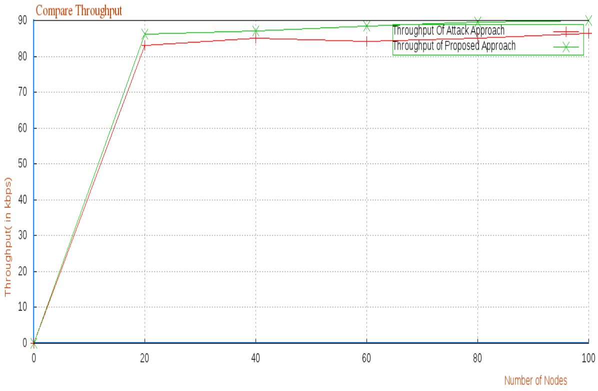
During the communication scenarios it is required to exchange the packets for different tracking and monitoring purpose. Therefore the additional injected packets in network is termed as the routing overhead of the network. The comparative routing overhead of both the routing protocols i.e. traditional AODV and the proposed secure routing technique is in graph. In this diagram for demonstrating the performance of the proposed technique the green line is used and for traditional technique the red line is used. According to the obtained performance of the techniques the proposed technique produces less routing overhead as compared to the traditional AODV routing under attack conditions. Therefore the proposed technique offers higher bandwidth consumption as compared to the traditional routing technique under attack situations.



**Graph 3 Routing Overhead**

## 6.3 Throughput

Network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

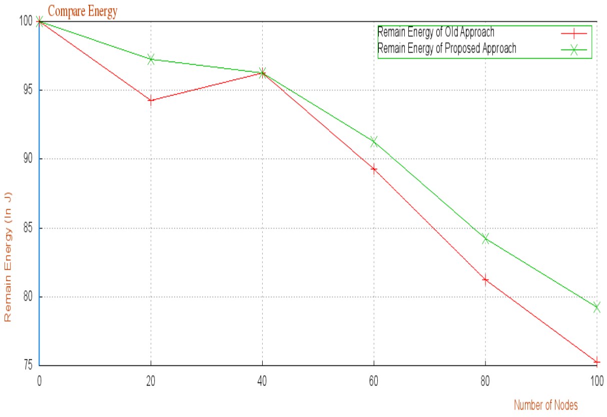


**Graph 4 Compare Throughput**

The comparative throughput of the network is demonstrated in graph, in this diagram the X axis shows the number of nodes in network and the Y axis shows the throughput of the network in terms of KBPS. According to the obtained performance the proposed technique improve the throughput of the network during the attack conditions also therefore the technique is effectively avoid the attack effect as compared to the traditional routing technique.

## 6.4 Energy consumption

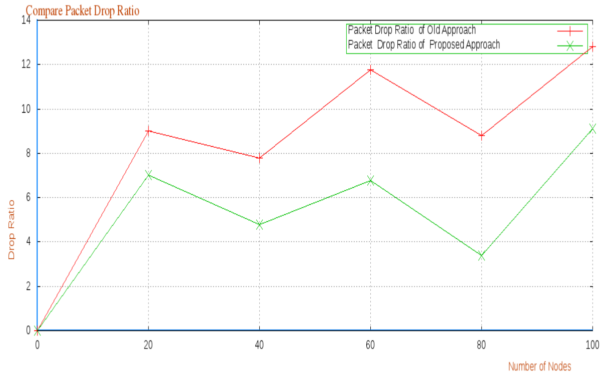
The energy consumption of the node demonstrates the rate of change in energy level of the node from its initial energy level. The low energy consumption demonstrates the higher performance of network. The network consumes energy at the every event of node such as packet forwarding and others. Therefore the energy consumption is measured with the respect of initial energy of the network node. Additionally the X axis of the graph shows the number of nodes in the network during the experiments and the Y axis shows the energy consumed in terms Jules. According to the obtained performance of the routing techniques the proposed technique is consumes less energy as compared to the attack condition. Therefore the proposed technique is more energy efficient as compared to the traditional approach.



**Graph 5 Energy Consumption**

## 6.5 Packet Drop Ratio

The packet drop ratio shows the amount of packets failed to deliver in destination device, thus the percentage amount of data dropped in network is termed as the packet drop ratio



**Graph 6 Packet Drop Ratio**

In a given graph the performance of the proposed technique is simulated using green line and red line shows the performance of traditional scheme. In addition of that in the given graph the X-axis shows the number of nodes and the Y-axis shows the amount of packet dropped. According to the obtained performance the proposed technique drops fewer amounts of packets as compared to the traditional algorithm. Thus the proposed technique is more adoptable than the traditional approach of secure routing.

# 7. CONCLUSIONS

Generally in MANET the design of Routing protocols are very important criteria because the performance of network depends on the design of routing protocols. Due to the unspecified design there are many limitations of routing protocol in MANETs; many researchers have conducted various techniques to suggest different types of prevention mechanisms from black hole problem under MANET scenario. We concentrated on how black hole can be prevented by developing a solution with the help of Wireless Communication Algorithm and In this paper we have implemented a new algorithm to detect and prevent black hole attack using AODV routing protocol in MANET. We calculate the performance of old proposed method with attack and our new proposed method with attack The other proposed method which is reactive detection method eliminates the routing overhead problem from the on demand way of route generation. Our complete implementation reveals that the proposed method of trust mechanism when applied on AODV protocol gives better results in all the cases for MANET as compared with normal AODV in case of black hole attack.

# 8. FUTURE WORK

Future work includes following points: In our proposed work, we control the malicious activity in efficient way and evaluated performance consideration of various factors and compare to existing methods. Concluded that our proposed method give better results and degrade packet drops due to malicious activities and due to error in transmission that’s why network end to end delay, routing overhead are degrades and packet delivery ratio, system throughput are increases. But we have some limitations that’s may be resolve in future to removing security threats.

In our proposed work , algorithm extendable for more than one attacks that's why we can prevent MANET from other type of attacks by further use of proposed algorithm.

## 9. ACKNOWLEDGMENTS

After the completion of this paper, work are not enough to express my feeling about all those who helped me to reach my goal; feeling above this my indebtedness to The Almighty for providing me this moment in life.

It's a great pleasure and moment of immense satisfaction for me to express my profound gratitude to Mrs. Rupali Bhartiya, Reader, Computer Science and Engineering Department SVITS Indore, whose constant encouragement enabled me to work enthusiastically. Their perpetual motivation, patience and excellent expertise in discussion during progress of the dissertation work have benefited me to an extent, which is beyond expression. Their depth and breadth of knowledge of Computer Engineering field made me realize that theoretical knowledge always helps to develop efficient operational software, which is a blend of all core subjects of the field. I am highly indebted to them for their invaluable guidance and ever-ready support in the successful completion of this dissertation in time. Working under their guidance has been a fruitful and unforgettable experience.

I wish to acknowledge my deep sense of gratitude for Dr. V.N. Walivadekar, Principal SVITS Indore for providing necessary infrastructure and help to complete the project work successfully.

I express my sincere thanks and gratitude to Dr. Anand Rajavat, Head, Computer Science and Engineering Department, SVITS Indore, who took care about imparting expert knowledge for design and development of project.

## 10. REFERENCES

[1] Priyanka Goyal, Sahil Batra and Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, Volume 9– No.12, November 2010

[2] Khushboo Sawant and Dr. M.K Rawat, "Survey of DOS Flooding Attacks over MANET Environment", International Journal of Engineering Research and Applications, Volume 4, Issue 5, Version 6, PP.110-115, May 2014.

[3] Pradip M. Jawandhiya and Mangesh M. Ghonge, "A Survey of Mobile Ad Hoc Network Attacks", / International Journal of Engineering Science and Technology, Vol. 2(9), PP. 4063-4071, 2010.

[4] Indrani Das and D. K Lobiyal, "Effect of Mobility Models on the Performance of Multipath Routing Protocol in MANET", Computer Science & Information Technology (CS & IT) Computer Science Conference Proceedings (CSCP), PP. 149–155, 2014

[5] Vaibhav, "Mobility Models and traffic Pattern Generation Based Optimization of Reactive Protocols", International Journal Intelligence Engineering Informatics, 2012.

[6] Y. Z.a and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks," presented at the 6th annual international conference on Mobile computing and networking, PP. 275-283, 2000.

[7] N. Patel, A. Dadhaniya, "Detection of Black Hole Attack in MANET using Intrusion Detection System", International Journal of Advance Engineering and Research Development (IJAERD, Vol 1, Issue 5,May 2014.

[8] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazines, vol. 40, no. 10, October 2002.

[9] P.N. Raj, P.B. Swadas, "DPRAODV: A Dyanamic Learning System against Black Hole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009.

[10] N. Mistry, D.C. Jinwala, M. Zaveri, "Improving AODV Protocol against Black hole Attacks", in Proc. of the International Multi Conference of Engineer and Computer Science, Vol. 2, 2010.

[11] A.A. Bhosle, T.P. Thosar and S. Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, No.1, February 2012.

[12] S. Bansal and M. Baker, "OCEAN: Observation based cooperation enforcement in ad hoc networks", Technical Report, Stanford University, 2003

[13] H. Deng, H. Li and D. Agrawal, "Routing Security in Wireless Ad hoc networks", IEEE Communications Magazine, Volume 40, No. 10, Oct 2002

[14] Juan-Carlos Ruiz, JesúsFriginal, David de-Andrés, Pedro Gil, "Black Hole Attack Injection in Ad hoc Networks".

[15] Fan-Hsun Tseng1, and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Tseng et al. Human-centric Computing and Information Sciences 2011

[16] Neetika Bhardwaj, Rajdeep Singh, "Detection and Avoidance of Black-hole Attack in AOMDV Protocol in MANETs", International Journal of Application or Innovation in Engineering & Management (IJAIEM), PP. 376 – 383, Volume 3, Issue 5, May 2014.Quansheng Guan, F. Richard Yu, Shengming Jiang and Victor C.M. Leung, "A Joint Design for Topology and Security in MANETs with Cooperative Communications", 978-1-61284-231-8/11/$26.00 ©2011 IEEE.