Improving the QoS Routing Algorithms of the IEEE 802.11 based Reliable Mesh Networks

Abhishek Kumar Fenin[1] Dinesh Choudhary[2]
[1,2]Department of Computer Science and Engineering
[1,2]Shekhawati Institute of Engineering & Technology, Sikar, India

Abstract— A wireless mesh network (WMN) is a particular type of Mobile Ad Hoc Network (MANET), which plans to give pervasive high transmission capacity access to an expansive number of clients. An unadulterated MANET is powerfully shaped by cell phones without the prerequisite of any current foundation or earlier system design. Like MANETs, a WMN likewise has the capacity of self-association, self-finding, self-mending, and self-setup. Nonetheless, a WMN is regularly an accumulation of stationary work switches with each utilizing various radios. A few MRs has wired associations and go about as the Internet entryways (IGWs) to give Internet availability to different work switches. These new highlights of WMNs over MANETs empower them to be a promising option for high broadband Internet get to. In this part, we expand on the advancement from MANETs to WMNs and give an extensive comprehension of WMNs from hypothetical angles to useful conventions, while contrasting it and MANETs. Specifically, we center on the accompanying basic issues as for WMN organization: Throughput, End to End Delay, Packet Delivery Ratio and Routing Overhead. Toward the end some open issues and future headings in WMNs talked about.

Keywords: WMN, MANET, Routing, QoS, PDR, E2E Delay, Throughput

I. INTRODUCTION

An unadulterated MANET is progressively settled by cell phones gathered together as required with no help from existing framework as appeared in Fig. 1. The cell phones in the system speak with one another through single or multi jump remote connections [1]. The key advantage of MANET correspondence is that it empowers us to frame a system unexpectedly without the need of having any foundation, which is both costly and tedious [2].

The main MANET was introduced around 30 years back by Defence Advanced Research Projects Agency (DARPA). In spite of unconventional favourable circumstances related with MANETs, they have not been generally acknowledged for regular citizen applications. This could be principally a result of two reasons (1) a few constraints of MANETs, for example, the security and restricted throughput frustrate MANETs from non-military personnel applications [3] and (2) the military and development applications command the exploration heading in MANETs with the goal that the majority of the works target how to meet the interesting prerequisites for these applications, for example, the dynamic topology, which may not be determinedly essential for regular citizen applications.

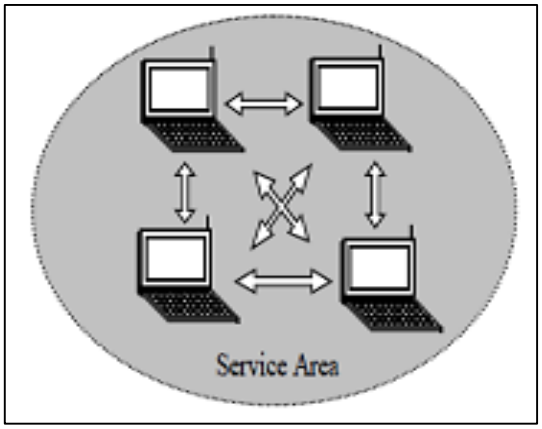

Fig. 1: Step by Step Digital Signature process.

In the ongoing years WMNs rise as logical multihop specially appointed systems to give the high transfer speed Internet administration to networks, ventures, or whole urban areas [4]. A WMN is a specific multihop specially appointed system, comprising of two sections: work spine and work customers. The stationary remote work switches (MRs) interconnecting through single/multi jump remote connections structure the spine. A couple of MRs with the wired associations go about as the IGWs to trade the traffic between the Internet and the WMN. The work customers can be the portable remote gadgets, for example, phones and workstations [5]. The portable customers associate with any MRs to get to the Internet by means of the IGWs in a multihop style. Contrasted with unadulterated MANETs, a WMN has a various levelled structure and the topology of the remote [6].

Instinctively, the system limit is relied upon to increment with the system estimate in light of spatial reuse of remote channel. Truth be told, the hypothetical examination [7][8] has demonstrated that the limit of MANETs diminishes with the development of the system measure. We consider a MANET with n MR hubs self-assertively situated in a plate R. Every hub picks a self-assertively goal to which it wishes to send traffic at a self-assertive rate by single bounce or multihops.

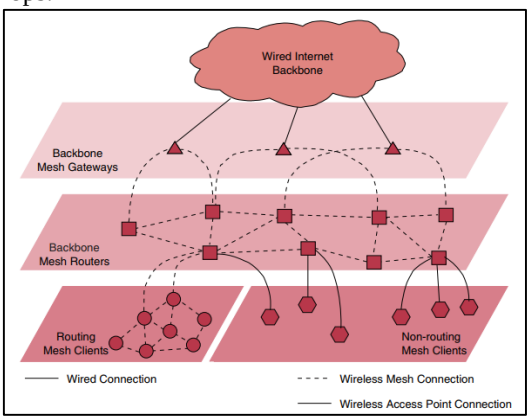

Fig. 2: Architecture of wireless mess network

II. LITERATURE SURVEY

The writing review concentrates on remote work systems, especially to examine the steering issue in the system, limit and recoup the system from connection disappointments and enhance the use of assets accessible in the system. In remote work arrange, IEEE 802.11 [9] [10] experienced adaptability issues brought about by connection level convention, for example, information preparing in the system. Wired Ethernet utilizes transporter sense different access to identify Ethernet crashes, which is impossible with RF flag (Tran A H and Mellouk A 2011). Likewise, Ethernet has a few requests of greatness more transmission capacity to explain this test. In any case, taking all things together remote condition, there is far less data transmission than a wired system and the AODV convention forces limit restrictions, particularly in single-radio Access Points (APs). Resulting remote work arrangements utilized separate radios for access and backhaul to relieve the impacts. Some item utilizes numerous radios for backhaul and directional receiving wires to limit self-obstruction, which can drastically build the quantity of impacts in expansive systems [11][12].

A Wireless Mesh Network is a framework comprises of broadcasting hubs arranged in an interconnect topology. Remote work systems comprise of work customers, work switches and portals [13] [14]. The work customers are as often as possible workstations, mobile phones and extra remote plans. The work switches exchange the information to and from the entryway which may yet require not being joined the Internet. Specially appointed On-Demand Distance Vector (AODV) directing is an unaware steering convention for work systems and different remote impromptu systems (Dana An and Ghalavand G 2011). A similar convention is utilized in fluffy rationale however it performs contrastingly on the work arrange. (Sharma S and Kumar S 2013). It is an on-request and separation vector steering convention, implying that a course is built up by AODV from a goal, since AODV convention Route Discovery is connected when a source hub wishes to send a bundle to the goal hub. The greater part of the responsive directing methodologies utilizes full flooding plans to find ideal courses. In these methodologies, a functioning source starts a course revelation process by communicating a Route Request parcel (RREQ) to the entire system (Luo H 2009). All hubs, aside from the source and the goal, are required to rebroadcast the primary got RREQ's, or potentially the RREQ's spread from better courses. Much of the time, just the middle of the road hubs between the source and the goal are the possibility for the ideal courses, the hubs in far locales pointlessly take an interest in the course revelation [15][16].

III. PROPOSED METHODOLOGY

The proposed network model consisting of 10, 20, 30, 40 and 50 nodes having a gateway, intermediate nodes and destination. All the nodes in the network have assigned a certificate through mutual exchange form the certification authority (gateway) that makes the node authentic and reliable. Any node in the network can behave abnormally and act as an intruder by advertising its field value to maximum, so all the traffic will divert to those selfish nodes.

A. Routing

Ever node calculates its field value from their neighbours. Ever node in the network has the information about their neighbour's field value. The node always forwards the packet having highest field value and hence the packet reaches to its destination.

B. Node Types

There are three types of nodes present in the proposed network. Gateway that route the traffic from internet to the network, the intermediate nodes that perform the routing operation, and the destination nodes that receives the packets.

C. Selfish Node Detection

As every node advertises its field value and node always forwards the traffic towards highest field value node so any node having wrong highest fled value can be the selfish node.As ever node have record of field values of each of their neighbors node so whenever any node advertises its field value, the node compare that value with its saved value in the array if there is a difference between the two values is greater than an acceptable threshold value than the node is considered to be the selfish node and labeled as intruder. The specified node will be removed from the forwarding list.

D. Performance Evaluation

The proposed scheme has been implemented and analyzed in the network simulator NS3.25. In the proposed network the traffic is analysed and shows some comparative results. Figure 4 shows a comparative result of secure field based routing approach and proposed selfish node detection mechanism on the basis of advertised field value. The comparison shows number of packets captured by the intruders. The SFBR only deals with the external intruders and hence shows that how much packets store by these external intruders, but on the other hand the proposed selfish node detection mechanism deals with the internal intruders and hence more chances to store the packets and misuse it. The graph shows number of packets received by internal and external intruders as SFBR approach only deals with the external intruder hence total number of packets received by these intruders are relatively smaller than selfish node detection because internal intruders are more dangerous as compared to external.

The analysis results of both these approaches shows that internal attacks are more powerful and the ratio of receiving the packets by internal intruders are more as compared. The packet delivers analysis of SFBR and selfish node detection approach.

Earlier SFBR is an external intruder's detection approach, after securing the network using SFBR approach the packet delivery ratio is not better than the proposed Selfish node detection approach, the Selfish node detection approach captured the intruder node and never send the packet towards that node who shows the field value to maximum in the network and all the traffic route towards that node. Figure 5 shows a comparative result between two approaches, as selfish node detection approach is more efficient mechanism to detect the intruders hence achieve relatively more packet delivery ratio. Figure 6 shows the graph of packet delay between these two approaches as in

secure routing packet always cover a longer distance to avoid the intruders, so face more delay as compared to traditional routing having shortest path to deliver the packet.

E. Watchdog Technique

The watchdog [9] method allows detecting misbehaving nodes. At the point when a hub advances a parcel, the watch dog set inside the hub ensures that the accompanying hub inside the course also driving the bundle. The watch dog does this with the guide of being mindful to all hubs inside transmission assortment indiscriminately. In the event that the consequent hub does never again forward the bundle, at that point it's miles labelled as got rowdy. A fit support that the parcel has been usefully sent, delivering the neighbour's reliability to be expanded. On the off chance that a parcel isn't sent inside a timeout period, at that point a disappointment count for the hub chargeable for fundamental the bundle is increased. In the event that this count surpasses a foreordained limit, at that point the hub is named as noxious. The watch dog strategy distinguishes getting rowdy hubs.

F. Algorithm

```
1:  Start
2:  Initialize Field Value of Each Node
3:  Find Neighbor of Every Node
4:  Store Field Value of Each Node in the Array
5:  Calculate Field Value of Neighbor
6:  If (Field Value of Neighbor is < Stored Field Value) then
7:  {
8:      Forward the packet to Next hop having Highest Field Value
9:  }
10: Else if
11: {
12:     Node is an Malicious
13:     Remove this from Neighbor List
14: }
15: if (Destination reached) (Termination condition) then
16: goto 5
17: end if
```

IV. SIMULATION RESULTS

Simulation and analysis of the proposed scheme was performed in NS3.25. Network simulator is an event driven discrete simulator where all communication operations between nodes in a network can be monitored carefully.

General Parameters	
Number of Nodes	10,20,30,40,50
Topology	Dynamic
Simulation Time	1000 Sec
MAC Layer	802.11
Range	200 meters
Simulation Area	1000 x 1000 meter2
Routing Protocol	AODV
Traffic Model Parameter	
Traffic Model	Constant Bit Rate
Packet Size	512 Bytes
Interval	1 Sec

Table 4.1: Simulation Parameter

The simulation parameters used to test the AODV protocol in the network are listed in Table 1 below. The results obtain from the simulation analysis include some of the QoS parameters like Packet Delivery Ratio, Packet Loss Ratio, Delay and the Overhead produced by the proposed work.

A. Simulation Results on Routing Protocols

1) Throughput:

Its community throughput is the slight fee of successful message shipping over a verbal exchange channel. This statistics can be introduced over a physical or logical hyperlink, or pass thru a positive network node. The throughput is usually calculated in bits in line with 2nd (bit/s or bps), and every so often in data packets in keeping with second or records packets in step with time slot.

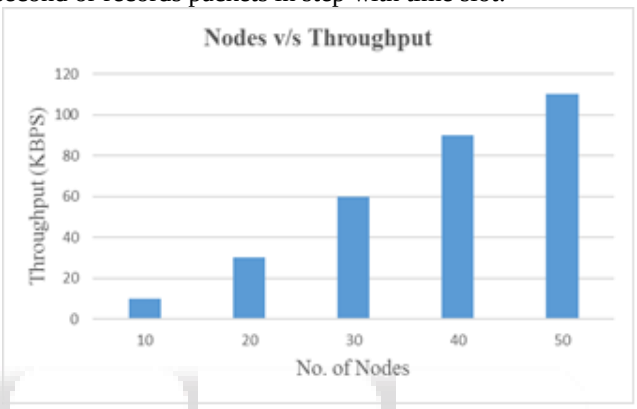

Fig. 2: Nodes Vs Throughput

Above determine suggests the graph of number of nodes Vs throughput. From graph we are able to examine as number of node growth in community throughput gets higher.

2) Packet Delivery Ratio:

Packet transport ratio may be figuring out by using the ratio among the range of statistics packets which might be sent by way of the source and the number of records packets which are obtained with the aid of the sink. Graph shows as the range of node growth it receives better because possibility of course breakage decrease.

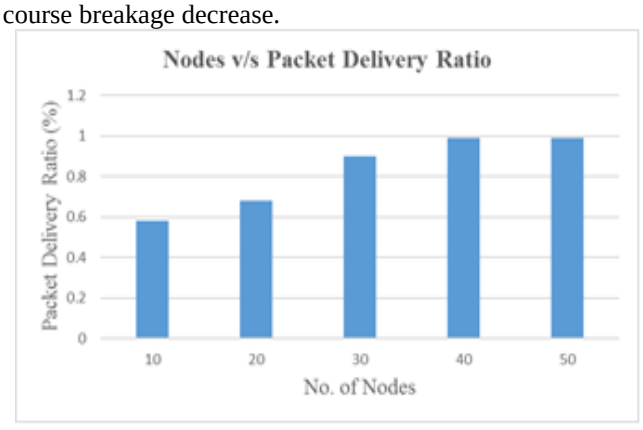

Fig. 4: Nodes Vs Packet Delivery Ratio

3) Normalized Routing Load (NRL):

Normalized routing load is the range of routing packets transmitted in keeping with facts packet dispatched to the vacation spot. Also every forwarded packet is counted as one transportation. This metric is likewise relatively correlated with the variety of route modifications came about inside the simulation.

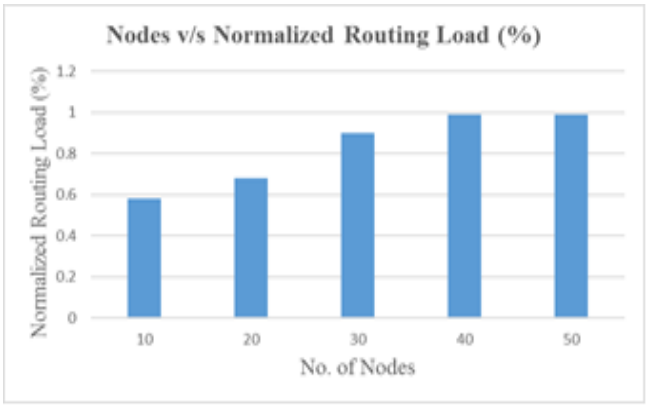

Fig. 5: Nodes Vs NRL

4) Average end-to-end delay of Data Packets:

There are feasible delays as a result of buffering for the duration of course discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and relocation times. Once the time difference among each CBR packet dispatched and received become recorded, dividing the overall time distinction over the full quantity of CBR packets obtained offer the average give up-to-quit put off for the obtained packets. This metric describes the packet transport time: the decrease the stop-to-give up postpone the higher the application overall performance.

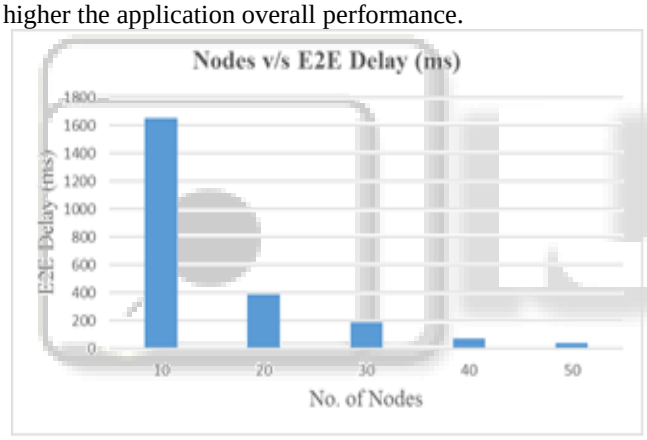

Fig. 6: Nodes v/s E2E-delay

B. Simulation Outcomes with Grey hole attack

The proposed method is compared with the existing algorithm of efficient route method based upon the ant colony based routing algorithm by packet delivery ratio (PDR), throughput, end-to-end delay (E2E), etc. The results of the simulation as detailed below:

1) Throughput:

It defined as the ratio of number of bytes received per second at the destination end. As we can see that in the following fig 7 that performance of the network is decreasing while black hole attack is performed. A simulation outcome reflects that comparison between Normal AODV, AODV with black hole attack and AODV based on proposed method.

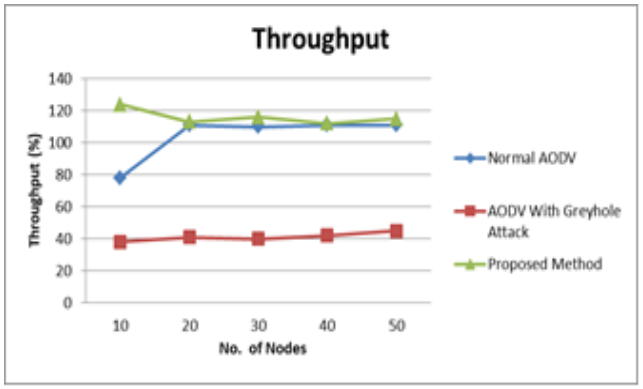

Fig. 7: Throughput under Grey Hole Attack

$$T=\frac{\sum_{i=1}^{n} A_i^r}{\sum_{i=1}^{n} A_i^S} * 100\%$$

Where,

A^r = average receiving node for the i^{th} application,

A^S = average sending node for the i^{th} application, and

n = number of applications.

In Fig. 7 shows that the proposed algorithm improved good throughput compared to AODV with black hole attack.

2) Packet Delivery Ratio

It can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node as shown in the following equation.

$$T=\frac{\sum_{i=1}^{n}(A_i^S - A_i^r)}{\sum_{i=1}^{n} A_i^S} * 100\%$$

Where, A^s node sent by the sender, A^r means number of application data node received by the receiver, i^{th} represents application number, and n is the number of applications. If describing about the original AODV working it decreases delivery of packet with an increase in the number of nodes.

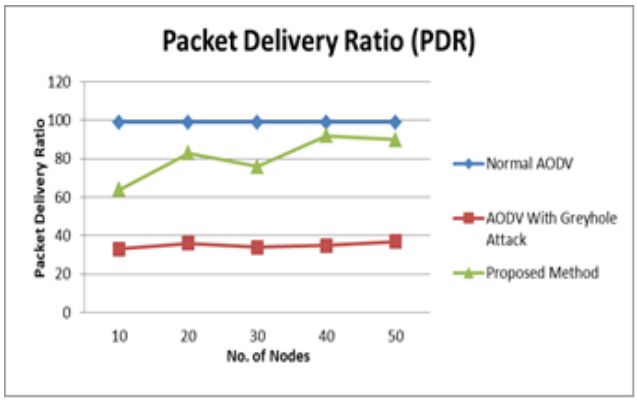

Fig. 8: Packet Delivery Ratio under Grey Hole Attack

3) End-to-End Delay

It represents the time required to move the packet from the source node to the destination node.

$$D=\frac{\sum_{i=1}^{n} d_i}{n} * 100\%$$

Where, d_i means average end to end delay of node of i^{th} application and n represents number of application. Fig. 9 shows that the proposed algorithm provided minimum end-to-end (E2E) delay compared with original AODV with black hole attack.

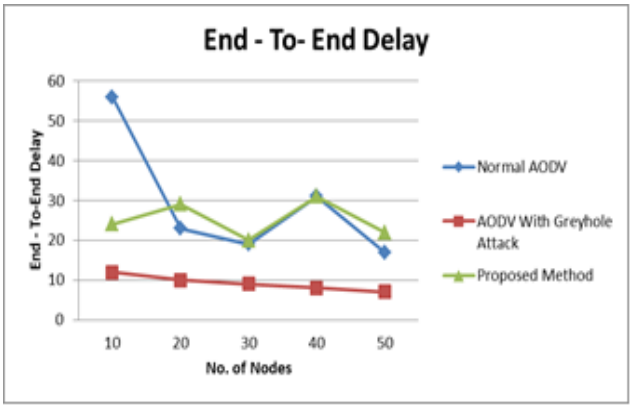

Fig. 9: End to End Delay under Grey Hole Attack

4) Dropped Packets

Dropped packets as shows in fig. 10 the number of nodes that sent from the source and fail to reach to the destination.

$$T = \sum_{i=1}^{n} (A_i^S - A_i^r)$$

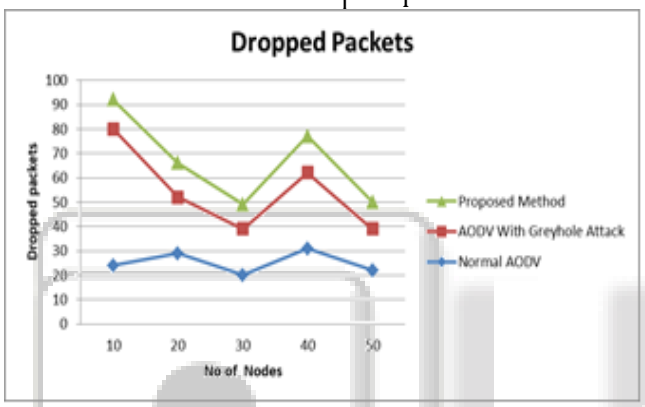

Fig. 10: Dropped Packets under Grey Hole Attack

V. CONCLUSION AND FUTURE SCOPE

In the Wireless Mess Network performed Greyhole assault and prevention on Ad hoc On-Demand Distance Vector (AODV) Routing. The simulation of AODV has been achieved the usage of NS3.25. Simulation is performed for 10, 20, 30, until 50 nodes in Mobile advert hoc community. As a visitors parameter we've got used Constant Bit Rate. As a ways as mobility difficulty we're using Random Way Point Model. A commonplace of 10 simulations is taken to make result more appropriate. An AODV protocol is analyzed in terms of throughput, Delay, Routing Overhead and Packet Delivery Ratio.

It is likewise observed that in Grey hollow assault, based at the number of nodes, the Packet Delivery Ratio is low. If the quantity of them increases, the Packet Delivery Ratio is low, due to the fact we are losing records packets. As a long way as throughput challenge, as variety of malicious node growth our throughput decreases due to the fact nodes aren't capable of gain at the holiday spot and that motives dropping. Delay is also increasing due to constantly detection of the course the simulation is operating. It is likewise found that in case of Grey hollow, the routing overhead is reduced. This is because this attacker does not forward routing packets and that lessen ordinary routing overhead.

A. Future Work

In this work, simulation of greater Static and Dynamic routing protocols using Bayesian Filtering and Collaborative Message Passing Interface. Future work entails the have a look at of certain assaults on community below stochastic modeling for nodes taking part in the routing path, and its impact on routing protocol by using evaluating various community parameters. It is also aimed to find the analytical expression for the same.

WMNs provide a new paradigm for high bandwidth wireless community that tightly integrates multiradio and multichannel MANET with the Internet. On the opposite to the constrained civilian software of MANETs, within the past few years no longer handiest many nonprofit WMNs have been deployed, but also many industrial giants have launched their business WMN solutions. However, there are nonetheless some of open troubles before the benefits of WMNs can fully take effect. These challenging problems involve all seven Open Systems Interconnection (ISO) protocol layers. Specifically, the critical troubles associated with above discussion are summarized as below:

- Capacity development. The contemporary implemented WMNs are nevertheless far from the theoretical capability due to the fact those implementations couldn't efficaciously combat the interference problem, channel assignment problem, and many others.
- Efficient routing protocols. Multihop, Multiradio, and Multipath routing protocols are required for efficiently deploying a WMN.
- Fairness. Most of works pertain to fairness are nonetheless within the experimental phase and require similarly assessment.

REFERENCES

[1] Gurung, Shashi, and Krishan Kumar Saluja. "Mitigating Impact of Blackhole Attack in MANET." Int. Conf. on Recent Trends in Information, Telecommunication and Computing, ITC. 2014.

[2] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. "A survey of black hole attacks in wireless mobile ad hoc networks." Humancentric Computing and Information Sciences 1.1 (2011)

[3] Vu, Cong Hoan, and Adeyinka Soneye. An Analysis of Collaborative Attacks on Mobile Ad hoc Networks. Diss. Master Thesis at School of Computing, Blekinge Institute of Technology, 2009.

[4] Dhurandher, Sanjay Kumar, et al. "GAODV: A Modified AODV against single and collaborative Black Hole attack in MANETs. " Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE, 2013.

[5] J.Sen, S. Koilakonda, A. Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Networks" IEEE Second International Conference on Intelligent Systems, Modeling and Simulation, 2011.

[6] Bindra, Gundeep Singh, et al. "Detection and removal of co-operative blackhole and grayhole attacks in MANETs." System Engineering and Technology (ICSET), 2012 International Conference on. IEEE, 2012.

[7] Hiremani, Vani, and Manisha Madhukar Jadhao. "Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET."Green Computing, Communication and Conservation of Energy (ICGCE), 2013 International Conference on. IEEE, 2013.
[8] Wahane, Gayatri, and Savita Lonare. "Technique for detection of cooperative black hole attack in MANET." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.
[9] Biswas, Santosh, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." Applications and Innovations in Mobile Computing (AIMoC), 2014. IEEE, 2014.
[10] Nishu kalia, Kundan Munjal, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, Issue-3, February 2013.
[11] S. Arezoomand, "Prolonging Network Operation Lifetime with New Maximum Battery Capacity Routing in Wireless Mesh Network," vol. 4, pp. 319–323, 2010.
[12] F. T. Bin Muhaya, Fazl-e-Hadi, and A. Naseer, "Selfish node detection in wireless mesh networks," ICNIT 2010 - 2010 Int. Conf. Netw. Inf. Technol., pp. 284–288, 2010.
[13] G. A. Cabral and G. R. Mateus, "Simulation-based optimization for Wireless Mesh Network planning," Proc. - 3rd Int. Conf. Adv. Mesh Networks, MESH 2010, pp. 28–34, 2010.
[14] M. Camelo, C. Omaña, and H. Castro, "QoS routing algorithms based on multi-objective optimization for mesh networks," IEEE Lat. Am. Trans., vol. 9, no. 5, pp. 875–881, 2011.
[15] J. M. Castillo-Secilla, P. C. Aranda, F. J. B. Outeiri??o, and J. Olivares, "Experimental procedure for the characterization and optimization of the power consumption and reliability in ZigBee mesh networks," Proc. - 3rd Int. Conf. Adv. Mesh Networks, MESH 2010, pp. 13–16, 2010.
[16] Y. Chai and W. Shi, "Access-enhanced hybrid routing protocol for hybrid wireless mesh network," 2017 9th IEEE Int. Conf. Commun. Softw. Networks, ICCSN 2017, vol. 2017–Janua, pp. 138–141, 2017.

