Advanced Technique Using Trust Based Approach for Prevention of Black Hole Attack in Mobile Ad Hoc Network

Ankita Gupta, M.Tech Student, NITM, Gwalior & India, 19ankita92@gmail.com

Abhishek Dubey, Assistant Professor, NITM, Gwalior & India, abhishek2be1989@gmail.com

Abstract: The present Mobile Ad hoc Networks known to be (MANETs) develop into well-liked matter for researchers, and typical studies have been prepared to lift introduction of ad hoc networks. In the MANET nodes are bargain to promote packets for each other impart more distant than to their scope of transmission. The mobile node is conveying through each other without some kind of foundation. MANET is an alluring technology for some applications, for example, protect and strategic tasks, because of the adaptability gave by their dynamic infrastructure. In this propose work we created Black hole attack on DSR (dynamic source routing) protocol, and for avoidance and detection we initially we performed the trust calculation of the nodes in the network which established the secure path for the transmission of data from source to destination. At first flood the network with route request packet which ought to be gotten by each neighbor node. We find the multiple routes for the data transmission but the path should be shortest. Then send the data by finding the secure and trustful path which makes them more efficient and reliable for data transmission.

Keywords — MANET, Wireless Local Area Networks (WLANs), DSR, Blackhole Attack, RREQ and RREP.

I. INTRODUCTION

The Wireless Local Area Networks (WLANs), created back in the 1990s, are a standout amongst the most imperative permit excluded get to arrange advancements these days. They permit information, voice and video interchanges over a wireless channel. A specific class of norms which have obviously ruled the market is the IEEE (Institute of Electrical and Electronics Engineers) 802.11 wireless LAN, otherwise called Wireless-Fidelity (Wi-Fi).

Fig. 1 Structure of MANET [2], [3], [4]

These systems can work in two modes; (I) foundation, which utilizes a wireless access point, and (ii) ad-hoc mode, which permits the making of a self- configuring system comprising of mobile routers (for instance workstations, advanced smart phones) which are interconnected by wireless links. The last are called MANETs [1] and their degree is to empower routing functionalities into the mobile nodes. A MANET, as portrayed by the Internet Engineering Task Force (IETF) MANET Working Group (WG), is a transitory or changeless independent system included free roaming nodes aiming to build up wireless interchanges without network infrastructures.

II. BLACK HOLE ATTACK

A Black Hole attack for the most part called the packet drop attack is a sort of DOS attack where a malicious node attracts in all packets by dishonestly asserting that a new route to the goal and after that holds them without sending the packets to the goal, thusly achieving all advantages of catching all the message packets for the benefit of the destination node. A black hole attack is alluded to as a node dropping all packets and sending routing packets, to course parcels from the source to itself. In this category of attack, a malicious node spuriously reports a small and a new route to the sink node (i.e., the destination) to draw in supplementary traffic to the malicious node and after that drops them. In this sort of attack, a malicious node falsely reports a short and another course to the sink node (i.e., the goal) to attract extra activity to the malicious node and after that drops them. A source node that needs to send data packets to the destination node starts the routing discovery process in an AODV protocol. Imagine a malicious node M. Right when a node P conveys a RREQ packet, each one of the nodes as well as Q, R and the malicious node M get it. Node M, being a malicious node does not check up with its routing table for the requested course to node T which is the destination. Henceforth, it promptly sends back a RREP packet, asserting that it has a course to the goal. Node P gets the RREP from M even before Q and R could send one. Node P misconstrues that the course through M is the briefest course and sends any packet to the destination

 DOI : 10.18231/2454-9150.2018.0126

through it. Exactly when the node P sends data to M, it pulls in and gets each one of the data without sending them to the destination and subsequently acts like a Black hole.

Along these lines a malicious node M can completely modify the packet and produce false data which causes the network traffic to be occupied or dropped. The black hole attack has two attributes. Initially, the node abuses the mobile ad hoc routing protocol, for example, AODV, to promote itself as having a substantial course to the coveted destination node. Furthermore, the aggressor utilizes the caught packets for its own particular advantage without sending it. Be that as it may, the attacker faces the likelihood of a peril that the neighbor nodes will screen and uncover the continuous attacks to every single concerned nodes. There is a more sensitive type of these attacks where an attacker can specifically modify packets, i.e., an attacker can smother or alter packets beginning from a few nodes, while unaffecting the data from other nodes, which limits the uncertainty of its attack [5, 11].

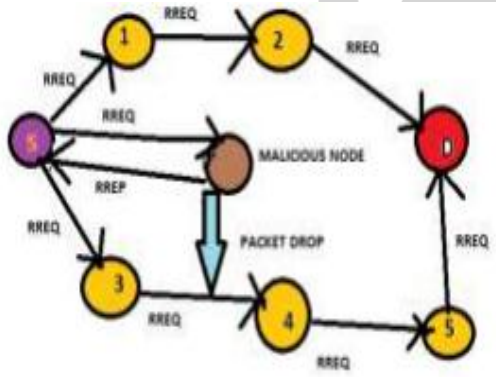

Fig.2. Black hole attack in AODV

Two types of black hole attack

A. Internal black hole attack

Here the faulty node is accessible inside the system. It takes part successfully in the correspondence of source and destination. This is called as internal attack on the grounds that the malicious node has a place with the network inside. This attack is more extreme as the malicious node effectively partakes in the network.

B. External black hole attack

Here the flawed hub stays outside the system and deny access to network traffic This attack can wind up plainly inside attack when it takes control of internal malicious node and control it to attack different nodes in the network [6].

III. LITERATURE SURVEY

Elbasher Elmahdi et al. [7] In this paper we propose a new approach to provide reliable and secure data transmission in MANETs under possible blackhole attacks based on ad hoc on-demand multipath distance vector (AOMDV) protocol and homomorphic encryption scheme for security. Simulation results show the improvement of packet delivery ratio and network throughput within the sight of blackhole nodes in our proposed plot.

Swapnil Bhagat et al. [8] in this study, the behavior of blackhole attack is discussed and has proposed a lightweight solution for blackhole attack which uses existing functions. Simulation results of proposed system are discussed at the end of the paper. Mobile Ad Hoc Network (MANET) technology is emerging technology in recent year. Many researchers find future of networking in it. MANET is simple and effective wireless technology which depends on mutual trust for communication. Due to limited processing and energy power, developers used the lightweight protocol to build it. This made developers concentrate on basic functionality (like routing, route discovery) and less on security aspects. One of its examples is mutual trust between nodes. In MANET, nodes are interdependent for communication as well as data transmission which need mutual trust between nodes. This mutual trust flaw is exploited by attackers to perform a different kind of attacks by injecting malicious node in the network. One of these attacks is blackhole attack.

Shashi Gurung et al. [9] In the paper, we have exhibited diverse classes for black hole attack relief strategies and furthermore introduced the rundown of different systems alongside its disadvantages that should be considered while planning a efficient protocol. Mobile Ad-hoc Network (MANET) is an prominent technology in the wireless networking field in which the movables nodes works in disseminated way and teams up with each other keeping in mind the end goal to give the multi- hop correspondence between the source and destination nodes. By and large, the primary presumption considered in the MANET is that every node is confided in hub. Be that as it may, in the genuine situation, there are some unreliable nodes which perform black hole attack in which the misbehaving nodes pull in all the movement towards itself by giving bogus data of having the base way towards the goal with a high destination sequence number and drops every one of the data packets.

Mohammed Baqer et al. [10] In this paper a safe and trust construct approach based with respect to specially appointed on demand distance vector (STAODV) has been proposed to enhance the security of AODV routing protocol. The approach confines the malicious nodes that endeavor to attack the network relying upon their past data. A trust level is connected to each partaking hub to recognize the level of trust of that hub. Every approaching packet will be analyzed to keep the black hole attack.

 DOI : 10.18231/2454-9150.2018.0126

Nikhil G. Wakode et al. [12] This paper is used to solve malicious nodes by using Ad hoc demand distance vector (AODV) routing by cooperative bait detection approach (CBDA) with malicious node detection algorithm. The CBDA alluded reactive and proactive routing mechanism. Malicious node detection algorithm indentifies the malicious nodes in the network. It executes an invert following way to deal with accomplish the coveted objective. Simulation comes about have specified, AODV, presence of malignant hubs in AODV and securing malicious nodes in AODV by utilizing CBDA with Malicious hub detection calculation as far as packet delivery ratio,end-to-end delay, standardized routing overhead and packet dropped ratio (taken as execution networks) .

IV. PROPOSED WORK

D-MBH algorithm detects single and multiple black hole nodes using an additional route request with nonexistent target address, computes a threshold ADSN, makes a black hole list and conjures the proposed D-CBH calculation. Utilizing ADSN, black hole list and next bounce data removed from RREP, the D-CBH calculation makes a rundown of cooperative black hole nodes. This method is not efficient to detect malicious nodes accurately as it has to maintain the list of malicious nodes which require large amount of memory and processing time. So to overcome this drawback we have proposed another technique which is applied when the true positive results come.

Initially, fake request generated by sender node to find the blackhole node using ADSN value of each malicious node. then genuine request are broadcast to calculate the trustful route. We performed the trust calculation of the nodes in the network which established the secure path for the transmission of data from source to destination. initial trust value of each node is 1 and there we consider ith node which calculate trust and their neighbor nodes are taken as jth node. so the trust calculation between i and j node is performed. At first surge the network with route request for packet which ought to be gotten by each neighbor node. We find the multiple routes for the data transmission but the path should be shortest. Then send the data by finding the secure and trustful path which makes them more efficient and reliable for data transmission.

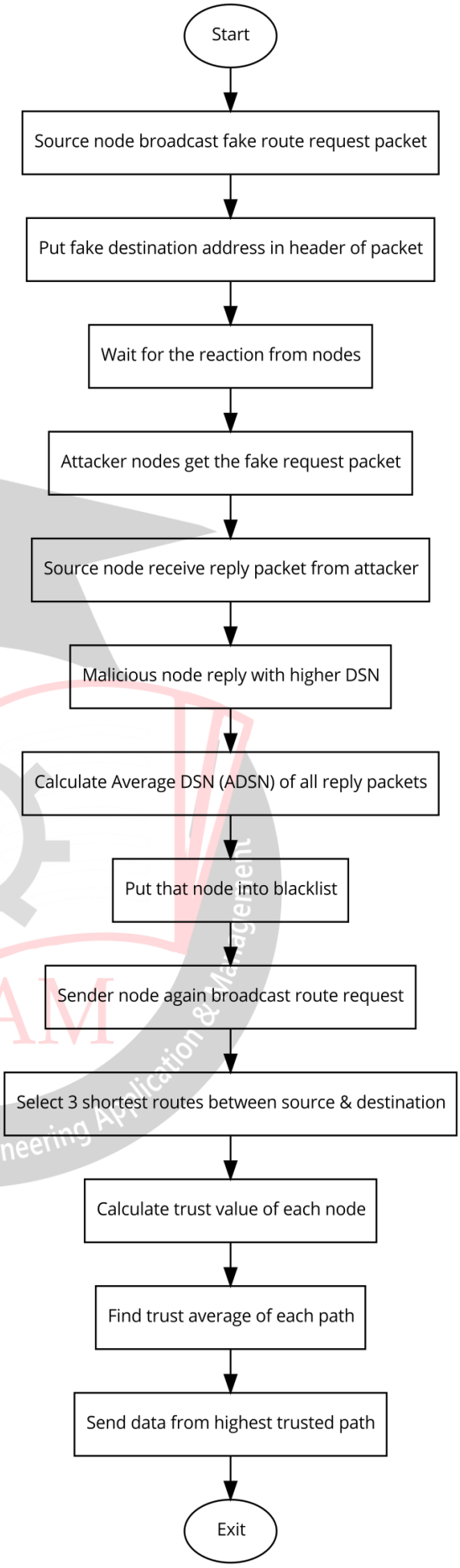

Fig.3. Flowchart of Proposed Algorithm

 DOI : 10.18231/2454-9150.2018.0126

The fake request is initiated in the first approach for selecting attacker nodes and then genuine request is generated to find the trustful nodes in the selected routes. The proposed algorithm with the detailed steps is given below:

Proposed Algorithm:

Step:1 Start
Step:2 Source node broadcast fake route request packet in the network
Step:3 Put fake destination address in the header of the packet
Step:4 Wait for the reaction from the nodes
Step:5 Attacker nodes get the fake request packet then it respond with the shortest path
Step:6 Source node receive reply packet from attacker
Step:7 Malicious node reply with higher DSN
Step:8 Calculate Average DSN (ADSN) of all reply packets
Step:9 Put that node into the blacklist
Step:10 Sender node again broadcast route request
Step:11 Select 3 shortest routes between source and destination
Step:12 Calculate the trust value of each node

Trust(i,j) = packet forward/(packet sent - packet forward)

Step:13 Find the average trust calculation of each path performed as:

$$\text{Avg(Trust)} = [\sum_{n=1}^{k} Trust(i,j)]/k$$

Step:14 Send the data from the highest trusted path
Step:15 Exit

V. RESULT ANALYSIS

A. *Network Animator*

Network Animator is an activity tool which is based on for performance of actual world packet traces and network simulation traces. It shows the succession of the packets through the network. It supports topology outline, packet level simulation, and various data examination tools.

For the implementation of the proposed work, we used NS2 for the simulation and the above mentioned techniques are applied to show the work.

Table 1: Parameter Table with their Values

Parameters	Values
Simulation Used	NS2
Network Size	1500m x 150m
Number of Nodes	50
Simulation Time	50s
Antenna Used	Omni directional Antenna
Packet Size	1KB
MAC Protocol	IEEE 802.11

B. *Trace file*

The record composed by an application to store data or general system data and whole network details, it is known as Trace File. It logs each bundle, each occasion that happened in the activity and are utilized for investigation.

Output:

s 0.000000000 _0_ AGT --- 0 tcp 40 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [0:0 3:0 32 0] [0 0] 0 0

r 0.000000000 _0_ RTR --- 0 tcp 40 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [0:0 3:0 32 0] [0 0] 0 0

s 0.000000000 _0_ RTR --- 0 AOMDV 52 [0 0 0 0] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

s 0.000235000 _0_ MAC --- 0 AOMDV 110 [0 ffffffff 0 800] [energy 100.000000 ei 0.000 es 0.000 et 0.000 er 0.000] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

r 0.001115374 _4_ MAC --- 0 AOMDV 52 [0 ffffffff 0 800] [energy 99.999296 ei 0.000 es 0.000 et 0.000 er 0.001] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

r 0.001115476 _8_ MAC --- 0 AOMDV 52 [0 ffffffff 0 800] [energy 99.999296 ei 0.000 es 0.000 et 0.000 er 0.001] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

r 0.001115531 _1_ MAC --- 0 AOMDV 52 [0 ffffffff 0 800] [energy 99.999296 ei 0.000 es 0.000 et 0.000 er 0.001] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

r 0.001115667 _11_ MAC --- 0 AOMDV 52 [0 ffffffff 0 800] [energy 99.999296 ei 0.000 es 0.000 et 0.000 er 0.001] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

r 0.001115667 _13_ MAC --- 0 AOMDV 52 [0 ffffffff 0 800] [energy 99.999296 ei 0.000 es 0.000 et 0.000 er 0.001] ------- [0:255 -1:255 30 0] [0x2 0 1 [3 0] [0 4]] (REQUEST)

C. *AWK file*

AWK Scripts are great in handling the information from the log which we acquire from NS2.

D. *Result in graphical form*

XGRAPH is a universally useful x-y information plotter with intelligent catches for printing, panning, expanding and selecting show choices. It will plot information from any number of documents on a similar chart and can deal

 DOI : 10.18231/2454-9150.2018.0126

with boundless information set sizes and any number of information records.

1) Packet Delivery Ratio:

It is known as the aggregate number of packets received per add up to number of packets sent. It is shown from the below figure that our proposed work has better PDR value than the existing work.

Packet Delivery Ratio = Number of packet received / Number of packets sent

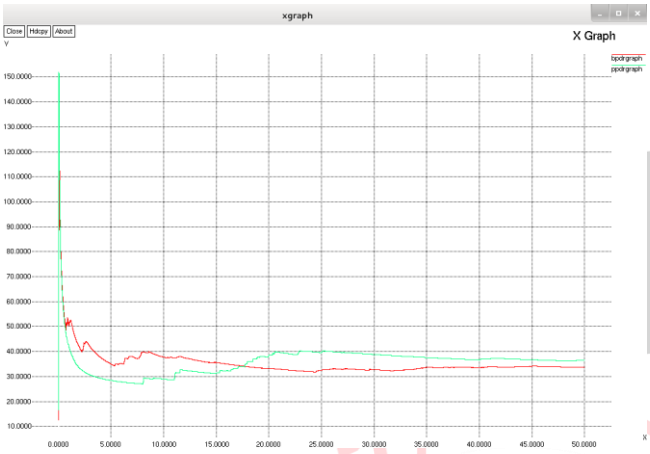

Fig.4. PDR Graph

Table 2: Packet Delivery Ratio

Time (in ms)	Base paper	Propose paper
5	35.75	29.32
10	36.68	28.9674
15	34.76	31.1504
20	32.43	38.5031
30	31.84	38.8381
35	31.34	37.6035
40	32.56	36.6301
45	34.43	36.7176
50	35.32	36.4076

2) Throughput

It is the aggregate number of packets received by the destination node which is conveyed by the sender at a specific time. In the graph below it is shown that our proposed throughput is better than the existing work.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

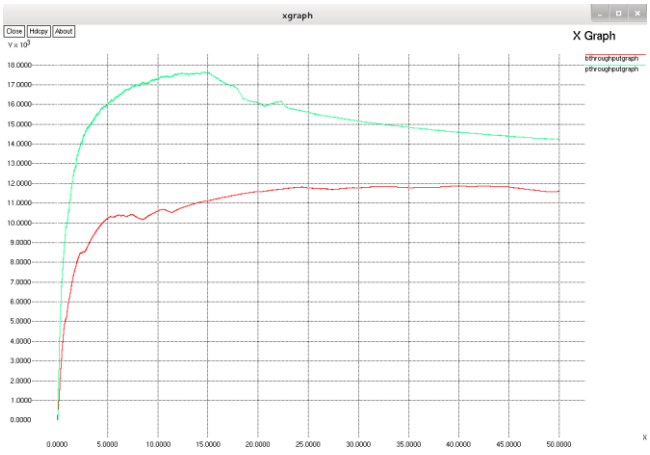

Fig.5. Throughput Graph

Table 3: Throughput

Time (in ms)	Base paper	Propose paper
5	10218.7	15969
10	10602.3	17072.7
15	11118.4	16336
20	11576.5	16065.9
25	11773	15452.1
30	11775.7	14601.9
35	11772.7	14155.8
40	11877.2	13944.9
45	11819.2	13838.5
50	11601.7	13737.8

3) Routing Overhead:

It is the total number of packets which is required to perform the communication of the sender and receiver nodes in the network. It is shown from the graph that our routing overhead is less in our proposed work which is good for our network.

Routing overhead = Total number of control packets in the network

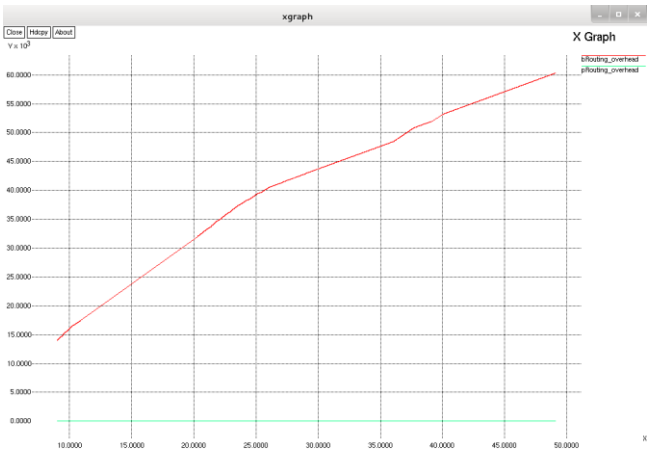

Fig.6 Routing Overhead Graph

 DOI : 10.18231/2454-9150.2018.0126

Table .4: Routing Overhead

Time (in ms)	Base paper	Propose paper
10	16012	7.739
20	32016	16.438
30	43711	22.636
40	53150	28.593
50	60326	34.131

VI. CONCLUSION

In many situations where the wired networks or even the straightforward wireless networks could not be used, but MANET due to its various significant properties are useful in those situations. But as it is having adaptive environment it is more likely to be vulnerable by amount of attacks. A few protocols for secure routing in ad hoc networks have been proposed in the literature. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks.

This theory exhibits the trust based secure routing protocols for mobile ad hoc networks. Distinctive trust based secure routing protocols are discussed and analyzed in the paper alongside their qualities, shortcomings and future improvements. Some of them are black hole attack, change, Gray Hole attack, flooding attacks and so forth. With the assistance of our proposed component we ensure our system against blackhole strike in MANET and we recently developed network which give greater security and give progressed results in a variety of system parameters like end in the direction of end hindrance, throughput, PDR. In the future work, we can use other techniques which provide the more efficiency and security in the network.

REFERENCES

[1] Meenakshi Yadav, Nisha Uparosiya "Survey on MANET: Routing Protocols, Advantages, Problems and Security" International Journal of Innovative Computer Science & Engineering Volume 1 Issue 2; Page No. 12-17, ISSN: 2393-8528.

[2] Pallavi Agarwal and Neha Bhardwaj, "Vehicular Ad Hoc Networks: Hashing and Trust Computation Techniques", International Journal of Grid and Distributed Computing 9, no. 7 (2016): 301-306.

[3] Rakesh Kumar Yadav, Deepika Gupta and Richa Singh "Richa Singh" International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Special Issue March 2015.

[4] Wenjia Li and Anupam Joshi "Security Issues in MANETs - A Survey"2012.

[5] Wenjia Li and Anupam Joshi "Security Issues in MANETs - A Survey"2015.

[6] Bessy M Kuriakose, M S Annie Ramya "A Survey on Prevention of Black Hole Attack in an Ad-Hoc Network" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013.

[7] Elbasher Elmahdi, Seong-Moo Yoo and Kumar Sharshembiev "Securing Data Forwarding against Blackhole Attacks in Mobile Ad Hoc Networks" 978-1-5386-4649-6/18/$31.00 ©2018 IEEE.

[8] Swapnil Bhagat, Puja Padiya, Nilesh Marathe "A Generic Request/Reply Based Algorith For Detection Of Blackhole Attack In Manet : Simulation Result" 8th Icccnt 2017.

[9] Shashi Gurung and Siddhartha Chauhan, "A Review of Black-Hole Attack Mitigation Techniques and its Drawbacks in Mobile Ad-hoc Network" 2017 IEEE.

[10] Mohammed Baqer "STAODV: A Secure and trust based approach to mitigate black hole attack on AODV based MANET" 2017, IEEE

[11] Pallavi Agarwal. Technical Review on Different Applications, Challenges and Security in VANET. Journal of Multimedia Technology & Recent Advancements. 2017; 4(3): 21–30p.

[12] Nikhil G. Wakode "Defending Blackhole Attack by Using Acknowledge Based Approach in MANETs" 2017 IEEE.

 DOI : 10.18231/2454-9150.2018.0126