Vol.VII / Issue XIII March-2018 ISSN:2278-4187

Anusandhan

Science Technology & Management Journal

Approved by UGC Indexed by Copernicus
Online version (eISSN 2457-0656) http://aujournals.ipublisher.in/Default

Published by
Rabindranath TAGORE UNIVERSITY
MADHYA PRADESH Where aspirations become achievements.
(Formerly known as AISECT University)

Rabindranath TAGORE University: Village-Mandua, Post-Bhojpur, Distt.-Raisen (M.P.)
India Pin-464993, Ph-0755-6766100, 07480-295707
E-mail-aisectjournal@rediffmail.com, info@aisectuniversity.ac.in
Web site : www.aisectuniversity.ac.in

RABINDRANATH TAGORE UNIVERSITY

UGC Approved Journals

Anusandhan (AUJ-AN)

- Technology & Management

Indexing and Impact Factor :

INDEX COPERNICUS : 48609 (2018)

ANUSANDHAN- AISECT University Journal
Vol. 06, Issue No. 13, March-2018, P-ISSN 2278-4187, E-ISSN 2457-0656

Detection Black Hole and Sybil Attack in GPCR-MA VANET based on Road Network

Naziya Hussain[1]* Dr. Priti Maheshwary[2] Dr. Piyush Kumar Shukla[3] Anoop Singh[4]

[1]IPS Academy, Indore (M.P.) India

[2]RNTU, Bhopal (M.P.) India

[3]UIT , Bhopal (M.P.) India

[4]Director, CMCC, Mhow, Indore (M.P.) India

Abstract – Vehicles can be directly communicated with each other if this Vehiclescomes in transmission range; the sender vehicles which send packets to the receiver's vehicle.We focused on enhancedand modified Vanet protocol Greedy Perimeter Coordinator Routing with mobility awareness (GPCR-MA) and presented the security for Blackhole and Sybil Attacks in the GPCR-MA. The solutions of blackhole and Sybil attack are verified with the help of implementation and simulation using network simulator (NS-2.35). Our investigation demonstrates the comparison between GPCR-MA, blackhole GPCR-MA (BH-GPCR-MA) and Sybil GPCR-MA (Sybil-GPCR-MA) attack in the network. This comparison carried between the simulation time and number of nodes established on QOS parameter presentation of network delay, Delivery Ratio (PDR), Average throughput and energy consumption. The packet deliver ratio performances are decreased in BH-GPCR-MA and Sybil-GPCR-MA with respect to rapidly change network state and network density of the network. The simulation results show that GPCR-MA is better than BH-GPCR-MA and Sybil-GPCR-MA.

Keywords—GPCR-MA, BH-GPCR-MA, Sybil-GPCR-MA, Vanet, Security.

----------♦----------

I. INTRODUCTION

VANET incorporate, vehicle to vehicles, Networks-on-Wheels and security Communication pool (Yan, et. al., 2010). Although, all at once for these advances to create them to the arrangement organize, potential security and protection problems (Hussain, Rasheed, et. al., 2013. Rostami, et. al., 2014), should be address. Since protection may be a twofold edge weapon thanks to its rivalry with different security requirements, a restrictive and exchange arrangement ought to be at the place keeping in mind the top goal to regulate the impact of rivalry. For example, if there ought to be an incident of Sybil attack and security preservation, simply associate exchange off arrangement is feasible to discourage the impact of the Sybil attack and moderate the contingent protection of the shoppers within the meanwhile (Ismail, et. al., 2007). while not tending to those problems, client loyalty are going to be a tested, which is able to foursquare influence the chance of those advances.

In this manner, on the receipt of various RREPs, the one with the most noteworthy devotion level is chosen. In any case, if numerous nodes have a similar dedication level, the RREP with the insignificant is picked. At last, directing is refined through the chosen way. Upon information delivery, the node sends an affirmation to the neighbor node inside the boundary. Next, the constancy level of RREP node is augmented as an honor for legit vehicular routing for both RREP node.Anyway, it is considered as a dark opening and the nearness of attacks is implied to all utilizing caution packets. In spite of the way that this technique handles both single and community dark opening attacks, it includes expanded capacity overhead, directing overhead and deferral.

II. METHODOLOGY

There is a form of attacks like part Attack and Sybil Attack. Black Attack is a miscalculation node procedure; it's defeating protocol to market itself taking the shortest path towards the destination node. On purpose route is about up, then the error node forwards it to the malicious attacks needs addressing (Zeadally, Sherali, et. al., 2012. Bibhu, Vimal, et. al., 2012). Nodes decline to understand the system or once a group of node drops out. The system traffics

are occupied by a random node, that doesn't exist to makes those knowledge be lost. Since this vehicle taking part in out the routing task, varied vehicles were associated with it because the switch client in (figure 1)

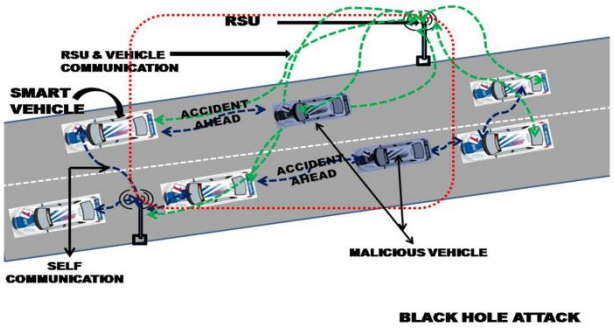


Fig. 1– Black Hole Attack (Hussain, Naziya, et. al., 2016).

The Black Hole Attack should build RREP with Destination arrangement additional noteworthy than the destination arrangement of the receiving node and sender node trusts that part node and extra interconnects with a black hole node in its place of the real destination node. This mischievous, often hurt node's interface and so waning all quality usage in accumulation to losing packets (Rawat, et. al., 2012. Bhoi and Pabitra, 2013).

Blackhole has been a dynamic zone of research and modified 'next hop information' (Hiremani & Jadhao, 2013). Many researchers proposed blackhole attack with different algorithms and security system for recognizing and handle a black hole attack. However, only a couple of researches are identifying multiple black holes in the wireless sensor or vehicular network. In (Wahane & Lonare, 2013) proposed network system thought the 'Loyalty Table. In the vehicular network, every vehicle is allotted a specific constant level, and measure the dependability of the vehicle in the network. At that point when source vehicle communicates a RREQ and carry the acknowledgement, the approach of acknowledgement (RREPs) are assembled in its routing Response Table. When average of dependability level of RREP forsource vehicle and its destination vehicleon the available routehigher than the prearranged threshold, than RREP vehicle is shownresponsible.

In Sybil attack, malicious vehicletransmitnumber of messages to other vehicles and each message comprehends asubstituteproduced source behavior is not known source or predefined source in the network. The basic destinations of the attacker vehicle are offered confusion to different nodes by sending incorrectly messages and to approve unique or (smart vehicle) headed straight on road to leave the street for the benefits of the attacker vehicle. Numerous messages containing an alternate source vehicle of created character sending by attacker vehicle to another vehicle. The attacker vehicle make numerous vehicles out and about by utilizing incorrectly messages with same personality and illusions of network traffic overload position. It's upholding another vehicle to leave the street for the advantage of the attacker vehicles shown in (figure 2).

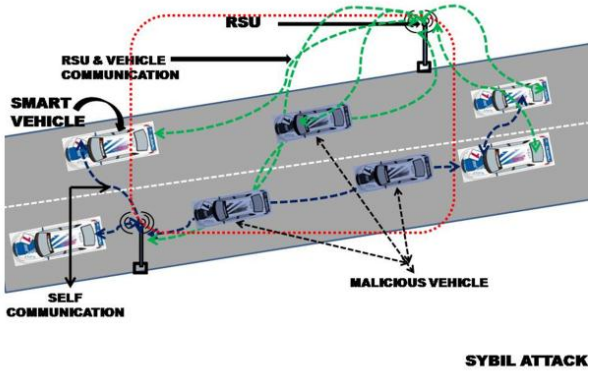


Fig. 2- Sybil Attack (Hussain, et. al., 2016).

III. RESULTS AND ANALYSIS

After the mathematics, integration and algorithms, simulated the performance of BH-GPCR-MA, Sybil-GPCR-MA and GPCR-MA with the help of network simulator 2 (NS-2.35) [13]. Here used a real road network topology. The scenario consists of 100, 200, 300, 400 and 500 numbers of Vanet nodes which is shown in figure. The movement of presenting road network nodes was generated with Vanet network simulator (Hussain, et. al., 2016). For the evaluation considered two protocols of the Vanet networks-GPCR-MA, BH-GPCR-MAand Sybil-GPCR-MA Protocol with black hole attack is developed and design for comparative study of the basic of QOS performance parameter (Hortelano, et. al., 2010).

Table 1:

Simulation parameter

Parameters	Values
Operating System	Linux (Ubuntu 12.04)
NS-2 version	NS-2.35
No. of Node	20, 40, 60, 80, 100
Packet Size	512
Traffic Type	UDP/CBR
Simulation Time	100, 200, 300, 400, 500 Second
Antenna Type	Omni-Antenna
Transmission Range	1000*1000 m
Mobility Model	Reference Point Group Mobility (RPGM)
Routing Protocol	GPCR-MA [18-19], BH-GPCR-MA, Sybil-GPCR-MA

(a) Performance Metrics

(i) Average end-to-end delay: The mathematical formula of average end-to-end delay (D) and total number of packet delivery successfully (n) in this scenario shown in equation (1).

$$\text{Average end2end delay} = \frac{\sum_{i=1}^{n}(\text{Received Packet Time} - \text{Send Packet Time}) * 1000(ms)}{\text{Total Number of Packets Delivery Successfully}} \quad (1)$$

(ii) Average network throughput: The average network throughput expressed the total amount of data packets which successfully arrived at final destination as per given simulation time. The mathematical calculation of throughput shown in equation (2).

$$\text{Throughput} = \frac{\text{PacketSize}}{(\text{PacketArrival} - \text{PacketStart})} \quad (2)$$

(iii) Packet Delivery Ratio (PDR): Packet Delivery Ratio expressed the ratio of total packets positively reached at the destination nodes source nodes. The network performance is high, when packet delivery ratio is high in the network. The mathematically calculation of packet delivery ratio shown in equation (3)

$$\text{Packet Delivery Ratio} = \frac{\sum \text{Total packets received by all destination node}}{\sum \text{Total packets send by source node}} \quad (3)$$

Average Energy Consumption: The Average spent energy is calculated by total number of energy is consumed for transmitted and received packets during the simulation in the networks. The total energy consumption is the summation of spend energy of overall nodes in the network, where the spend energy of node is the summation of energy spend for communication, packet transmit (Pt), received packet (Pr), and idle packet (Pi).

(b) Simulation Results

Several simulations scenarios on the different approaches were done. Here represent two different comparison scenarios of the present work.

Table 2:

Delay comparison table for GPCR-MA, blackhole attacks and Sybil using GPCR-MA with respect to Simulation Time and No. of Node respectively.

Simulation Time	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
100	126.09	111.74	168
200	127.14	118.73	174
300	122.9	119.74	169
400	126.66	118.73	175
500	122.45	118.73	168

No. of Node	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
20	125.82	120.73	159
40	129.94	121.73	163
60	124.55	123.74	169
80	128.01	125.74	171
100	121.29	123.73	167

Table 3:

PDR comparison table for GPCR-MA, blackhole attacks and Sybil using GPCR-MA with respect to Simulation Time and No. of Node respectively.

Simulation Time	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
100	98.75	62.99	58
200	48.78	65.7	51
300	48.86	66.46	53
400	98.71	66.9	50.6
500	48.86	68.79	56

No. of Node	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
20	98.59	70.78	61
40	98.71	72.02	59
60	98.68	73.38	57
80	98.66	71.86	59.8
100	98.7	71.98	62

Table 4:

Throughput comparison table for GPCR-MA, blackhole attacks and Sybil using GPCR-MA with respect to Simulation Time and No. of Node respectively.

Simulation Time	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
100	59.58	51.66	1.8
200	56.87	51.44	0.82
300	72.21	52.31	1.94
400	57.65	51.52	0.92
500	71.24	52.31	1.86

No. of Node	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
20	60.36	51.61	1.02
40	76.33	55.92	2.04
60	161.76	55.38	5.81
80	215.53	55.57	6.53
100	229.45	58.08	8.67

Table 5:

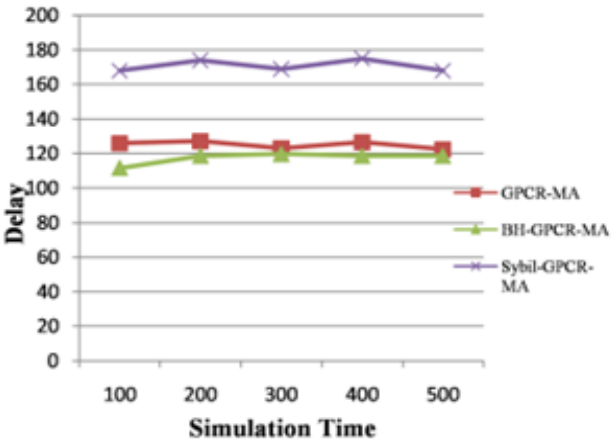
Energy comparison table for GPCR-MA, blackhole attacks and Sybil using GPCR-MA with respect to Simulation Time and No. of Node respectively.

Simulation Time	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
100	19.8	40.5	9
200	19.8	40.5	9
300	19.8	40.5	9
400	19.8	40.5	9
500	19.8	40.5	9

No. of Node	GPCR-MA	BH-GPCR-MA	Sybil-GPCR-MA
20	19.8	10.5	9
40	19.8	12.6	4.5
60	19.8	13.5	3
80	19.8	10.12	2.25
100	19.8	8.1	1.8

Average end-to-end delay: The average delay of GPCR-MA lesser the Sybilattack and higher that blackhole attack because both attach have differed behavior. Blackhole attack chose shortest route to pretend a perfect destination so average delay to setup routing is less on other side Sybil attack sends various messages to other network in network and created the a source to provide a misconception for all other nodes by this wrong messages in (Figure 3).

(Table 2) clearly indicate the performance difference between these three routing. Average delay values clearly indicating Sybil-GPCR-MA>GPCR-MA>BH-GPCR-MAwith respect to number of nodes variation or simulation time.



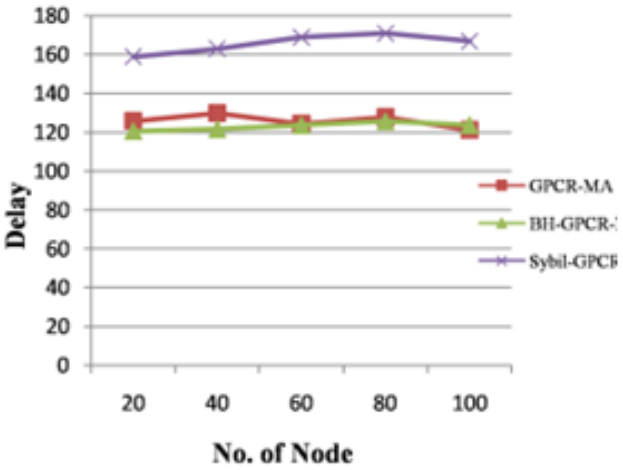


Fig.-3 Delay comparison for GPCR-MA, blackhole attack on GPCR-MA (BH-GPCR-MA) and Sybil attack on GPCR-MA (Sybil-GPCR-MA) with respect to number of node variations.

Packet Delivery Ratio: The Performance of packet delivery ratio of black hole-GPCR-MA is increased with 200 second simulation time and 20 nodes. With the variation of number of node GPCR-MA routing protocol packet delivery ratio is similar same as black

hole GPCR-MA but with respect to simulation time, GPCR-MA is better the BH-GPCR-MA

(Figure 4).

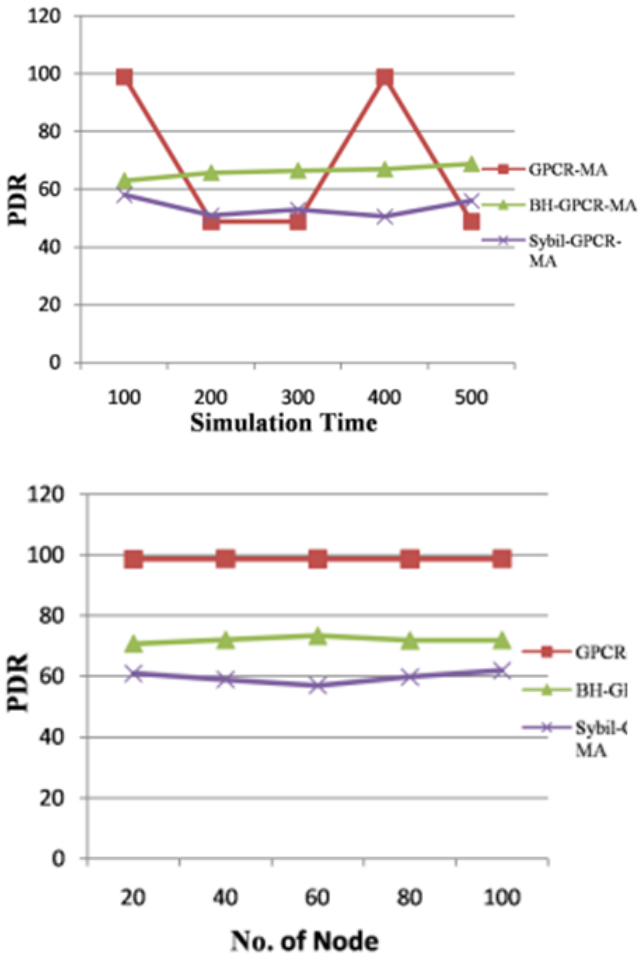


Fig.-4 Packet Delivery Ratio comparison for GPCR-MA, blackhole attack on GPCR-MA (BH-GPCR-MA) and Sybil attack on GPCR-MA (Sybil-GPCR-MA) with respect to number of node variation.

(Table 3) shows the packet deliver ratio among these three Vanet routing. GPCR-MA have highest packet delivery ratio as compare to BH-GPCR-MA and Sybil-GPCR-MA. Table-3 indicate GPCR-MA >BH-GPCR-MA>Sybil-GPCR-MA> with respect to number of nodes variation or simulation time.

Throughput: The performance of throughput for BH-GPCR-MA and BH-GPCR-MA almost same for nodes 40, 60 and 300, 400 simulation time but throughput at 20 nodes is showing the different performance as GPCR-MA decreased (Figure 5).

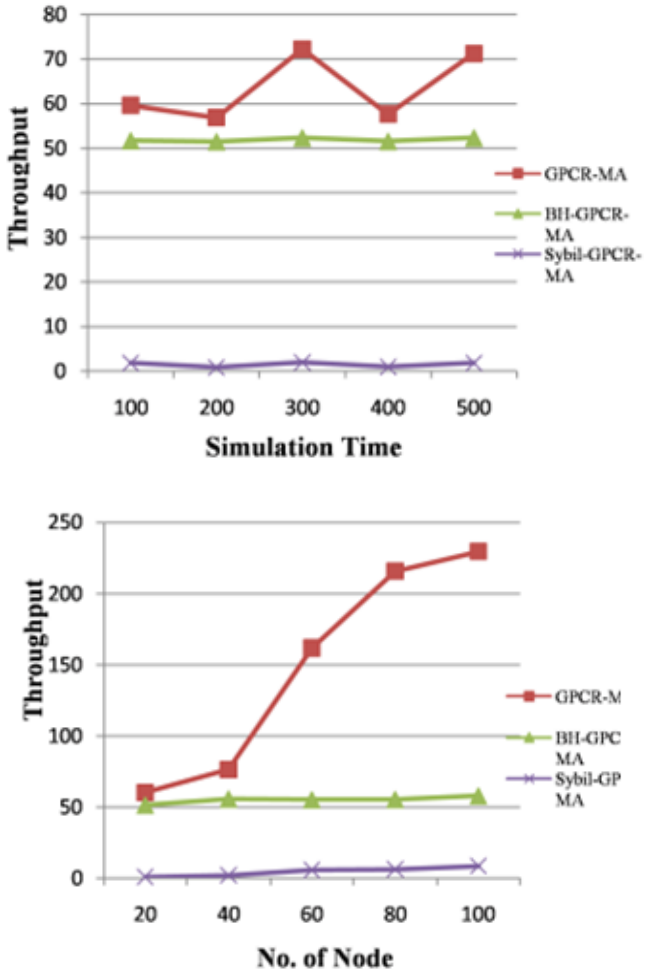


Fig.-5 Throughput comparison for GPCR-MA, blackhole attack on GPCR-MA (BH-GPCR-MA) and Sybil attack on GPCR-MA (Sybil-GPCR-MA) with respect to number of node variation.

(Table 4) shows the throughput state the amount of data message which arrived at destination as per given simulation time and number of node in Vanet Network. GPCR-MA have highest average network throughput as compare to BH-GPCR-MA and Sybil-GPCR-MA. Average network throughput for GPCR-MA >BH-GPCR-MA>Sybil-GPCR-MA> with respect to number of nodes variation or simulation time in table 4.

Energy Consumption: The Performance of energy consumption of black hole in GPCR-MA network is continuously increased as compare to GPCR-MA and Sybil-GPCR_MA have constant energy consumption (Figure 6). Each vehicle maintain the route from source to destination inside the network area with the transmission process for every data packets consumed the unit energy so based on that consumed energy increased. If traffic density and network range increase then energy consumption

also increased but BH-GPCR-MA consumed more than ten times energy as compare to the GPCR-MA.

(Table 5) energy consumption presented the total consumed energy during the network transmission during the network simulation based on the given scenarios. The total consumed energy in the network is calculated based on the all nodes, based on the transmitting, receiving and dropped packet energy.

BH-GPCR-MA consumed higher energy as compare to the Sybil-GPCR-MA and GPCR-MA routing in both the scenarios.Consumed energy in these scenario represent this combination for BH-GPCR-MA >Sybil-GPCR-MA>>BH-GPCR-MA with respect to number of nodes variation or simulation time in table5.

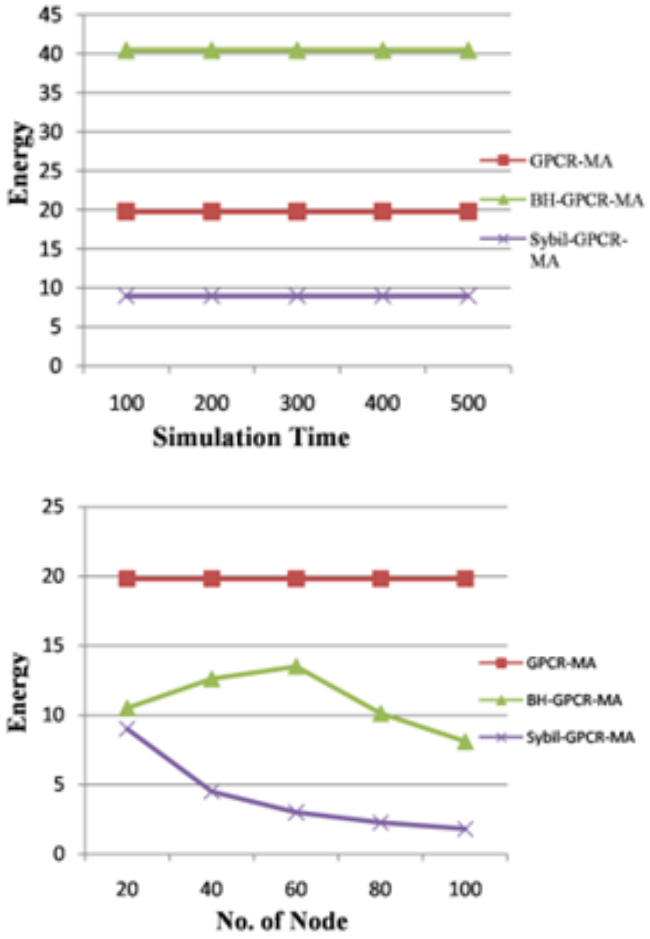


Fig.-6 Energy Consumption comparison for GPCR-MA, blackhole attack on GPCR-MA (BH-GPCR-MA) and Sybil attack on GPCR-MA (Sybil-GPCR-MA) with respect to number of node variation.

CONCLUSION

A Black Hole attacks is one of the genuine security issues in Any Vanet Network. It is an attack where a vindictive hub imitates a goal hub by sending fashioned RREP to a source hub that starts course disclosure, and therefore denies information movement from the source hub. In this paper a review on various existing strategies for identification of dark opening attacks in Vanet with their deformities is displayed. The discovery methods which make utilization of responsive directing conventions have low overheads, yet have high parcel misfortune issue. In light of the above execution correlations, it can be presumed that black Hole attacks influences organize adversely. The recognition of Black Holes in impromptu systems is as yet considered to be a testing errand. Future work is expected to a productive Black Hole attacks discovery and disposal calculation with least postponement and overheads that can be adjusted for impromptu systems helpless to Black Hole attacks. The overall performance of average end to end delay, packet delivery ration, and throughput for blackhole attack with respect to number of nodes variation are -GPCR-MA performance better to BH-GPCR-MA protocols.

IV. REFERENCES

Ariyakhajorn, J., Wannawilai, P., & Sathitwiriyawong, C. (2006, October). A comparative study of random waypoint and gauss-markov mobility models in the performance evaluation of manet. In Communications and Information Technologies, 2006. ISCIT'06. International Symposium on (pp. 894-899). IEEE

Bhoi, Sourav Kumar, and Pabitra Mohan Khilar (2013). "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services." Communications and Signal Processing (ICCSP), 2013 International Conference on. IEEE.

Bibhu, Vimal, et. al. (2012). "Performance analysis of black hole attack in VANET." International Journal Of Computer Network and Information Security 4.11: p. 47.

Hiremani, V. A., & Jadhao, M. M. (2013, December). Eliminating co-operative blackhole and grayhole attacks using modified EDRI table in MANET. In Green Computing, Communication and Conservation of Energy (ICGCE). International Conference on (pp. 944-948). IEEE.

Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni (2010). "Evaluating the usefulness of watchdogs for intrusion detection in VANETs." Communications Workshops (ICC), 2010 IEEE International Conference on. IEEE.

https://www.isi.edu/nsnam/ns

Hussain, Naziya, Anoop Singh, and Piyush Kumar Shukla (2016). "In Depth Analysis of Attacks & Countermeasures in Vehicular Ad Hoc

Network." International Journal of Software Engineering and Its Applications 10.12: pp. 329-368.

Hussain, Rasheed, et. al. (2013). "Privacy-aware route tracing and revocation games in VANET-based clouds." Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on. IEEE, 2013.

Ismail, Datuk Prof Ir Ishak, and Mohd Hairil Fitri Ja'afar (2007). "Mobile ad hoc network overview." Applied Electromagnetics, 2007. APACE 2007. Asia-Pacific Conference on. IEEE.

Liang, B., & Haas, Z. J. (2003). Predictive distance-based mobility management for multidimensional PCS networks. IEEE/ACM Transactions on Networking, 11(5), pp. 718-732.

Rawat, Ajay, Santosh Sharma, and Rama Sushil (2012). "VANET: Security attacks and its possible solutions." Journal of Information and Operations Management 3.1: 301.

Rostami, Masoud, Farinaz Koushanfar, and Ramesh Karri (2014). "A primer on hardware security: Models, methods, and metrics." Proceedings of the IEEE 102.8 (2014): pp. 1283-1295.

Wahane, G., & Lonare, S. (2013, July). Technique for detection of cooperative black hole attack in MANET. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-8). IEEE.

Yan, Gongjun, Nathalie Mitton, and Xu Li (2010). "Reliable routing in vehicular ad hoc networks." Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on. IEEE.

Zeadally, Sherali, et. al. (2012). "Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems 50.4: pp. 217-241.

Corresponding Author

Naziya Hussain*

IPS Academy, Indore (M.P.) India

E-Mail – naziyahussain@gmail.com