International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 3 (2018) pp. 1613-1622

Attack Resilient & Efficient QoS based GPCR-ARE Protocol for VANET

Naziya Hussain[1]
Research Scholar, AISECT University, Bhopal 464993, India;
Assistant Professor, School of Computers, IPS Academy, Indore 452012, India.
E-Mail: naziyahussain@gmail.com

Dr. Priti Maheshwary[2]
Associate Professor, AISECT University, Bhopal 464993, India.
E-mail: pritimaheshwary@gmail.com

Dr. Piyush Kumar Shukla[3]
Assistant Professor, Department of Computer Science and Engineering,
University of Institute of Technology, Bhopal 462023, India.
E-Mail: pphdwss@gmail.com

Anoop Singh[4]
Director, CMCC, Mhow, Indore 453441, India.
E-Mail: cmccmhow@gmail.com

Abstract

A VANET is observed an adequate solution to the cooperative driving among communicating cars on road. Organizing road network and testing these networks, typically known as (VANETs), contains a high cost in real world, so the simulation is valuable alternative in research. Our investigation demonstrates the comparison between the GPCR-MA routing networks and attack resilient and efficient protocol (GPCR-ARE) routing network based on different parameter of mobility model that is Freeway, Gauss Markov, Manhattan, Random Waypoint Mobility Model (RWMM) and Reference Point Group Mobility (RPGM) for simulation and analyzed the performance results. The solution of GPCR-ARE are verified with the help of implementation and simulation using network simulator (NS-2.35). Here demonstrate the two scenarios 1) GPCR-MA network scenario. 2) GPCR-ARE network scenarios. This comparison carried between the GPCR-MA and GPCR-ARE based on QOS parameter performance in the presence of attack resilient and efficient protocol. The QoS performances are low in GPCR-ARE as compare to GPCR-MA with respect to network traffic density, and variation of simulation time, its decrease the performance of the network. The simulation results show that RPGM Mobility-Model with GPCR-MA and GPCR-ARE in Vehicular Network.

Keywords: GPCR-MA, GPCR-ARE, QoS Performance, RPGM, VANET.

INTRODUCTION

A Vehicular Network technology used for communication between vehicles and with the development of intelligent transport systems applications, the number of accidents and waste of energy of fossil fuels in expected to diminish. VANET's utilizing short-range wireless communication within vehicles moving on the highway.

VANET incorporate Networks to infrastructure (V2I), vehicle to vehicles (V2V) and safety transmission Association[1]. Although, all together these advances to variety them the arrangement organize, security and protection issues must address[2, 3]. The security is twofold edge because of its routing with security necessities, a restrictive and tradeoff arrangement should be at the place keep in mind this goal to adjust a impact of routing. [4] Without tending to these issues, consumer loyalty will be a tested, which will straightforwardly influence the possibility of these advances.

Nodes decline to appreciate the system, when setup node dropout. The system traffics engaged with specific node, that specific node does not happen, which makes those data be lost.

Here are two prospects in VANET [5] of black hole attack.

1) Correspondence of original client with another client decline communicate and messages transmission too bad. At that point original client tried with another client, however both client position still same.

2) The correspondence begins with another client, all of a sudden dropout and communication interface with neighbor client aggravation will happen. Since vehicle moved out from routing boundary then it associated through switched with another inside vehicle (figure 1).

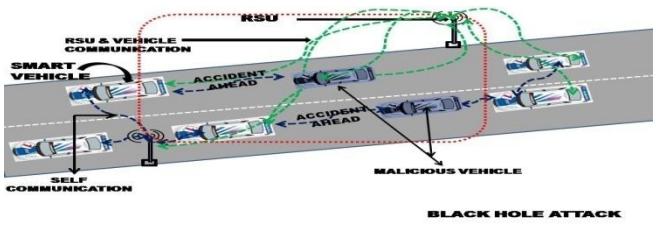

Figure 1– Black Hole Attack [5]

There is a sort of attack like Sybil, Denial of Service and Black hole Attack. An Attack is an error node procedure, it's defeating protocol to promote itself taking the shortest path towards the destination node. At point route is set up, then the error node forwards it to the malicious attacks wants address [6, 7].

The Black Hole Attack must make RREP with Destination arrangement more noteworthy than the destination arrangement of the receiving node and sender node trusts that black hole node and additional interconnects with a black hole node in its place of the real destination node. This mischievous frequently harm node's interface and thus waning all asset usage in accumulation to losing packets [8, 9].

RELATED REVIEW

VANET facilitate various other applications [10] in the domain of vehicular communication. Vehicular ad hoc network has many unique features [11]. The distinctive characteristics [12] of a VANET atmosphere are an area under discussion of significance for many. Thus the characteristics of VANET create both network design challenges [13] and opportunities in achieving security goals. These are the self-motivated wireless network, in which wireless nodes interchange randomly. Every node can come and move in and outside of the network in a dynamic manner. Vehicular network is used for communication and transmission media without a safety. This makes it more complex and also makes it more prone to attacks. If network traffic increases over the VANET then it's having more number of vehicles, RSU, after communication and transmission, packet loss increased and congestion too. The congestion control[14] and loss the packet occurs presence of attack in VANET. Black hole attack is one of the security threats where the black hole node collected all packets which falsely declare a different route to the destination node without forwarding them to the destination. So due to this attack node some packet loss over the network during the communication.

In which present the performance of GPCR-MA routing network and attack resilient and efficient protocol (GPCR-ARE) based on Freeway, Gauss Markov, Manhattan, RPGM and RWM Model mobility model for simulation of QOS matrices like Generated packets, Received packets, Dropped packets. In VANET networks different application based routing protocol [15] is recommended. These parameters are compared to AODV routing protocol both using with black hole and without black hole attack. The security requirements for VANETS [16] [17] are also considered.

METHODOLOGY

VANETs confront diverse security threats like attack that are completed against them to disturb the ordinary performance of the systems. Black hole attack occurs in the vehicular network (VANET).

In black hole attack, A malicious node vehicle has used it for VANET routing keeping in mind destination and have shortest distance from source to destination or can say that packet want to interrupt. Along this way malicious node have the accessibility to reply request route in this manner to capture the data packet. In vehicle routing based on the malicious node, flooding reply by destination node before assembly of acknowledge from real node; consequently malignant and artificial route is established.

To detect a malicious vehicle in this scenario in vehicular data rates in figure 2. Which shows that how an attacker node to communicate with the vehicle. In this figure, indication three different types of communication like malicious to vehicle communication (M2V), V2V and V2I communication. When a real Vehicle sends a data packet to another real vehicle and recruit route discovery process, so if any, malicious vehicle claim that have active route and its pretend that it's a specified destination, vehicle and its received RREQ packets, then malicious to vehicle communication happen between them and its send an acknowledgement to the initial real vehicle before getting the response from the other real vehicle. So based on this initial node that is active route and it's discovered the active route completely. Initial node refuse all replies and all data messages from other rail vehicles [1] and those data packets lost.

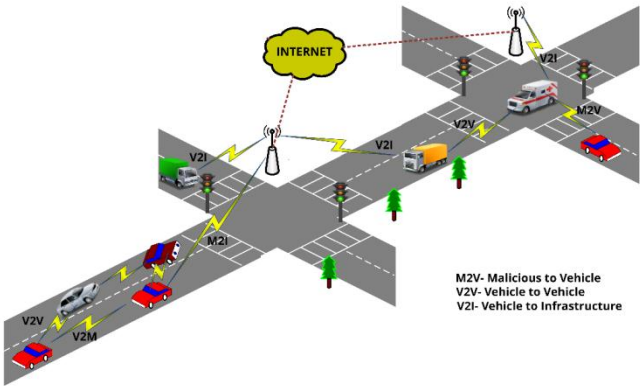

Figure 2– Black Hole Attack scenario with network topology.

In the above scenario, black hole attacks communication topology are represented, attack vehicles acts as malicious vehicles within the above shown networks topology. This attack can be external or internal black hole attack basically this attack physically out of the vehicular network or generating congestion vehicular networks by disorderly entire network [2]. It takes controller of internal malicious vehicle in VANET. Black hole attack can brief in following points.

1. Malicious vehicle setup an active route from source vehicle to destination vehicle.
2. Malicious vehicle sends RREP with destination, vehicle pretended to a real destination, vehicle and at same hop count and sequence value is set to lowest to highest value.
3. Malicious vehicle sends reply route packet to shortest distance vehicle which totally goes to this active router. This data packet transferred to the direct data vehicle node if any route is exist.

4. The route reply data packet received by the shortest distance vehicle for the malicious vehicle will reply by established route discovery to source vehicle. So that the new data packet received by route reply and it's allow to source vehicle to update information in routing table.
5. The malicious vehicle dropped data packets which belonged to this malicious set up a route.
6. Source and destination, vehicle did not have position anymore to interconnect the of black hole attack scenario.

EXPERIMENTAL ANALYSIS: -PERFORMANCE METRICS

Simulation scenario used in this paper constructs for GPCR-MA routing network and attack resilient and efficient protocol (GPCR-ARE) routing network VANET topology with no of vehicles which is located inside network topology dimension. The vehicles following the patterns based on giving mobility model such as Freeway, Gauss Markov, Manhattan, RPGM and RWP Model. The network parameter which is used in this simulation to generate the valuable and analyzed the performance results.

Table I: Scenario Parameter for Mobility Model [18]

Parameters	Values
Network Simulator	NS2.35
Routing protocols	GPCR-MA and GPCR-ARE
Node number	20, 40, 60, 80, 100
Simulation district	900 ×900
Mobility paradigm	Freeway, Gauss-Markov, Manhattan, RPGM and Random Way Point
Simulation time	100, 200, 300, 400 and 500 Second
Application Layer	TCP
Traffic type	CBR
Antenna type	Omnidirectional
Channel mode	Wireless channel
Radio-propagation pattern	Two ray ground
Network interface mode	Phy / WirelessPhy
Performance Metrics	Average Delay, Average Energy, Packet Delivery Ratio and Throughput

Based on the data obtained from the simulation can we measured, average delay, energy consumption, throughput and packet deliver ratio using the following formula.

1. ***Average end-to-end delay***

Mathematical formula of average delay (D) and total number of packet delivery successfully (n) in this scenario shown in equation (1).

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

1. Average Energy Consumption

The total energy consumption is summation of spending energy of overall nodes in the network, where spend energy of the node is a summation of energy spend for communication.

2. Average network throughput

The mathematical calculation of throughput shows, here PacketSize is size of a packet of its packet reaching to the destination, PacketArrival is the time when the last packet arrived and PacketStart is the time when first packet arrived to destination.

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

3. Packet Delivery Ratio (PDR)

The mathematical calculation of PDR shown in equation (3)

$$\text{Packet delivery ratio} = \frac{\text{received packets}}{\text{generated packets}} \quad (3)$$

SIMULATION RESULTS ANALYSIS

In this paper, Highway based road network, Freeway, Gauss Markov, Manhattan, RPGM and random way point mobility models are simulated for GPCR-MA routing network and attack resilient and efficient protocol (GPCR-ARE) routing network and NS2.35 simulator to evaluate the performance of these five mobility models in VANET network. Simulation is carried using Network Simulator (NS2.35). An introduction of resilient and efficient protocol (GPCR-ARE) in VANET with NS2.35 is done.

The comparative analysis of GPCR-MA attack resilient and efficient protocol (GPCR-ARE) based on number of node and simulation time over the mobility models. The GPCR-MA and GPCR-ARE routing performance presented in a table(II,III,IV,V & X,XI,XII,XIII) and (VI,VII,VIII,IX & XIV,XV,XVI,XVII) respectively for a variety of simulation and increased network density. With respect, graphical representation in GPCR-MA (Figure 3-6), which is comparing respectively, with the performance of GPCR-ARE(Figure 7-10) protocol, examined the effect of VANET model of mobility. If we look previous published research paper based

on the comparison of VANET routing protocol with attack effect on vehicle, attack in network reduced the performance overall performance of that system because it pretend a shortest routing discover for source vehicle so data packet never received by a network destination vehicle, its at malicious vehicles and its dropped that data packet and information lost.

Here we examined two different following points 1) how does GPCR-MA VANET routing protocol work with attack or malicious vehicle in the network? 2) How does GPCR-ARE performance dissimilar from GPCR-MA?

Figure 3-4 & 7-8 indicate that the average delay for GPCR-MA, and GPCR-ARE presented respectively, GPCR-ARE routing protocol have the lowest value because of the shortest routing path as compared to GPCR-MA routing. In GPCR-ARE packet dropped ratio is very high that's why the packet delivery ratio is very low in GPCR-ARE (Figure 9-10 & 17-18) as compared to the GPCR-MA (Figure 5-6 & 13-14).

The performance over the model of mobility between GPCR-MA and GPCR-ARE, as analysis of model of mobility indicate that Manhattan performance is worst over other mobility model and RPGM is very good performance in the network in term of average delay. The simulation shows that GPCR-MA has high performance based on these parameters over the attack resilient and efficient protocol (GPCR-ARE).

Figure (3-4, 11-12 and 7-8, 15-16) with respect to their performance table indicating the energy consumption because which is showing much change over the routing and model of mobility's in the GPCR-ARE, its value changed by network traffic density and network running time. GPCR-MA took less energy consumption for packet transmission over the GPCR-ARE routing protocol.

Comparative analysis of GPCR-MA and GPCR-ARE VANET Protocol based mobility models on the Simulation Time variation

Table II: Average End-End Delay for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on Simulation time.

Simulation Time	Average End-End Delay				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	124.51	199.69	121.78	126.09	122.51
200	192.58	194.8	683.7	127.14	127.71
300	206.36	216.66	208.58	122.9	130.39
400	122.95	203.67	217.2	126.66	127.17
500	206.37	126.39	110.09	122.45	122.36

Table III: Average Energy Consumption for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on Simulation time.

Simulation Time	Average Energy Consumption				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	19.8	19.8	19.8	19.8	19.8
200	19.8	19.8	16.2	19.8	19.8
300	19.8	19.8	19.8	19.8	19.8
400	19.8	19.8	19.8	19.8	18
500	19.87	19.8	16.2	19.8	19.8

Table IV Average Throughput for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on Simulation time.

Simulation Time	Average Throughput				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	69.47	61.66	60.53	59.58	66.08
200	70.02	63.53	15.45	56.87	70.3
300	64.47	64.79	60.56	72.21	71.35
400	71.1	64.46	62.79	57.65	74.44
500	66.22	52.09	17.74	71.24	64.71

Table V Packet Delivery Ratio for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on Simulation time.

Simulation Time	Packet Delivery Ratio				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	98.75	48.38	98.71	98.75	98.75
200	48.78	48.86	16.66	98.63	98.63
300	48.86	48.78	48.88	98.71	98.59
400	98.71	48.86	32.22	98.61	98.64
500	48.86	98.76	16.66	98.75	98.64

Table VI: Average Delay for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on Simulation time.

Simulation Time	Average End-End Delay				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	128.76	146	129.77	111.74	128.77
200	134	138	110	118.73	129.76
300	124	131	170	119.74	128.75
400	129.76	124	150	118.73	130.17
500	145	128.77	143	118.73	129.75

Table VII: Average Delay for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on Simulation time.

Simulation Time	Average Energy Consumption				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	40.5	90	40.5	40.5	40.5
200	40.9	90	45	40.5	40.5
300	40.9	90	49	40.5	40.5
400	40.5	90	90	40.5	36
500	40.9	90	40.9	40.5	40.5

Table VIII: Average Throughput for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on Simulation time

Simulation Time	Average Throughput				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	51.94	35.96	51.58	51.66	52.2
200	76.64	54.44	25.47	51.44	51.66
300	22.58	56.94	53.94	52.31	53.66
400	51.74	62.93	53.44	51.52	54.18
500	43.62	52.71	52.45	52.31	51.26

Table IX: Packet Delivery Ratio for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on Simulation time

Simulation Time	Packet Delivery Ratio				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
100	61.78	67	63.34	62.99	62.3
200	59	70	65.6	65.7	63.65
300	63	70.9	67	66.46	62.71
400	62.84	73	69	66.9	62.22
500	69.8	62.34	71.96	68.79	62.76

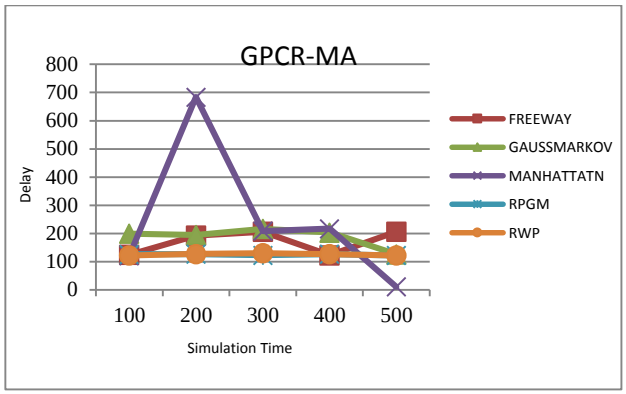

Figure 3: Comparison of the Average Delay between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-MA protocol.

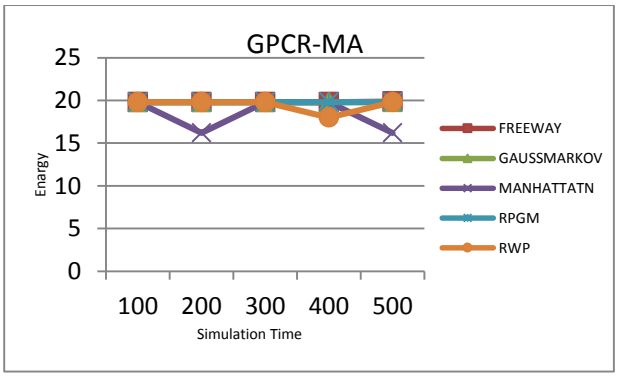

Figure 4: Comparison of the Energy consumption between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-MA protocol.

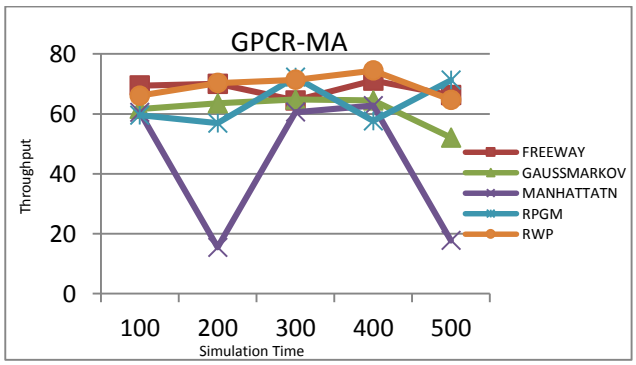

Figure 5: Comparison of the Average Throughput and Packet Delivery Ratio between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-MA protocol

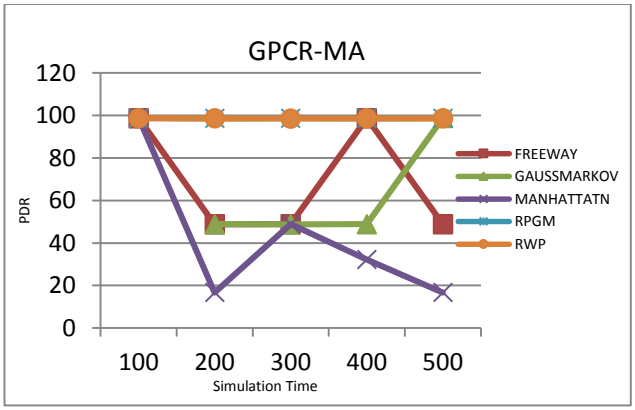

Figure 6: Comparison of the Average Throughput and Packet Delivery Ratio between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-MA protocol

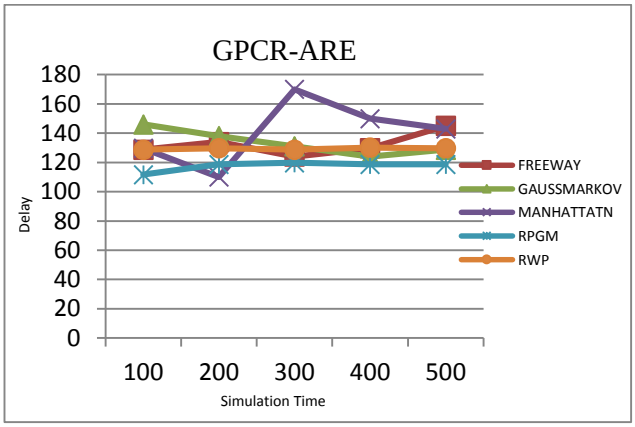

Figure 7: Comparison of the Average Delay and Energy Consumption between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-ARE protocol.

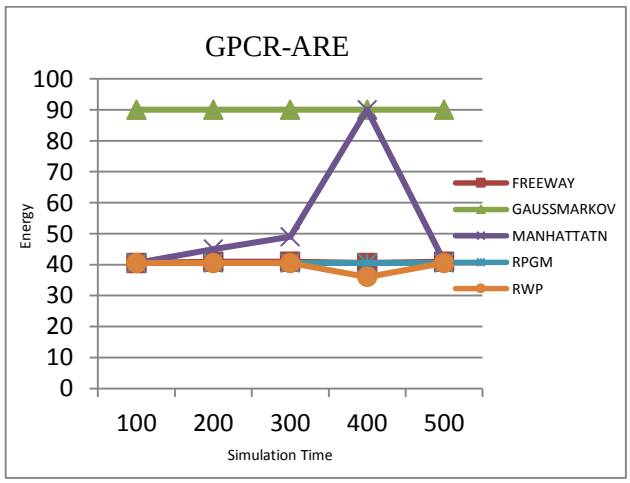

Figure 8: Comparison of the Average Delay and Energy Consumption between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-ARE protocol.

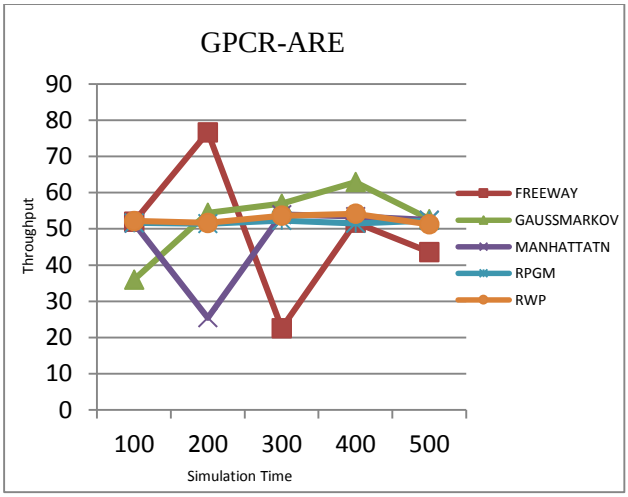

Figure 9: Comparison of the Average Throughput and Packet Delivery Ratio between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-ARE protocol.

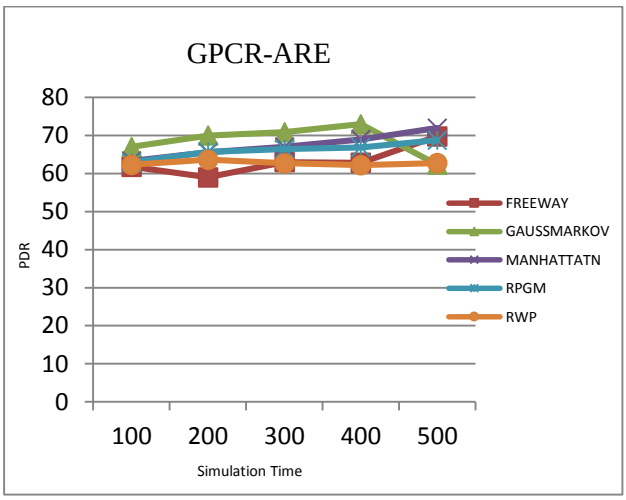

Figure 10: Comparison of the Average Throughput and Packet Delivery Ratio between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on the simulation time using GPCR-ARE protocol.

Comparative analysis of GPCR-MA and GPCR-ARE VANET Protocol based mobility models on the number of node variation

Table X: Average Delay Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on network traffic density

Number Of Nodes	Average End-End Delay				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	183.1	234.52	129.57	125.82	123.24
40	118.87	199.48	118.73	129.94	127.13
60	3854.02	126.67	199.48	124.55	124.58
80	683.52	3858.54	688.42	128.01	130.34
100	126.94	123.22	193.48	121.29	123.18

Table XI: Energy Consumption Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on network traffic density

Number Of Nodes	Average Energy Consumption				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	19.8	19.8	19.8	19.8	19.8
40	19.8	19.8	19.8	19.8	19.8
60	16.2	19.8	19.8	19.8	19.8
80	16.2	16.2	16.2	19.8	19.8
100	19.8	19.8	19.8	19.8	19.8

Table XII : Average Throughput Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on network traffic density.

Number Of Nodes	Average Throughput				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	67.01	60.93	64.27	60.36	69.5
40	107.35	89	86.17	76.33	95.85
60	43.03	150.02	111.19	161.76	146.79
80	153.45	44.57	129.26	215.53	169.44
100	224.97	185.92	202.37	229.45	178.51

Table XIII: Packet Delivery Ratio Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-MA based on network traffic density.

Number Of Nodes	Packet Delivery Ratio				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	48.75	32.4	48.78	98.59	98.7
40	98.66	98.71	98.66	98.71	98.66
60	25	98.66	48.86	98.68	98.68
80	50	16.66	25	98.66	98.63
100	98.64	98.75	32.14	95.7	98.75

Table XIV: Table 8: Average Delay Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on network traffic density.

Number Of Nodes	Average End-End Delay				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	81	141	121	120.73	128.73
40	129.75	128.75	129.76	121.73	128.77
60	123	128.77	126	123.74	129.75
80	129.77	189	190	125.74	129.75
100	129.76	128.76	140	123.73	128.76

Table XV: Table 8:Energy Consumption Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on network traffic density.

Number Of Nodes	Average Energy Consumption				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	9	9	9	10.5	40.5
40	20.25	20.25	20.25	12.6	20.25
60	3	13.5	3	13.5	13.5
80	10.12	2.25	2.25	10.12	10.12
100	8.1	8.1	1.8	8.1	8.1

Table XVI: Average Throughput for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on Simulation time

Number Of Nodes	Average Throughput				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	11.29	30.97	53.94	51.61	52.04
40	53.44	55.22	51.82	55.92	52.89
60	30.97	52.89	60.44	55.38	58.62
80	56.1	27.97	35.46	55.57	55.22
100	56.67	52.8	45.15	58.08	57.72

Table XVII: Packet Delivery Ratio for Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model performance comparison using GPCR-ARE based on Simulation time

Number Of Nodes	Packet Delivery Ratio				
	Freeway	Gauss-Markov	Manhattan	RPGM	RWP
20	78	72	70	70.78	62.55
40	63.5	59.91	68.43	72.02	62.1
60	66	61.61	71	73.38	63.85
80	63.3	69.8	69	71.86	63.81
100	63.07	61.53	73	71.98	62.75

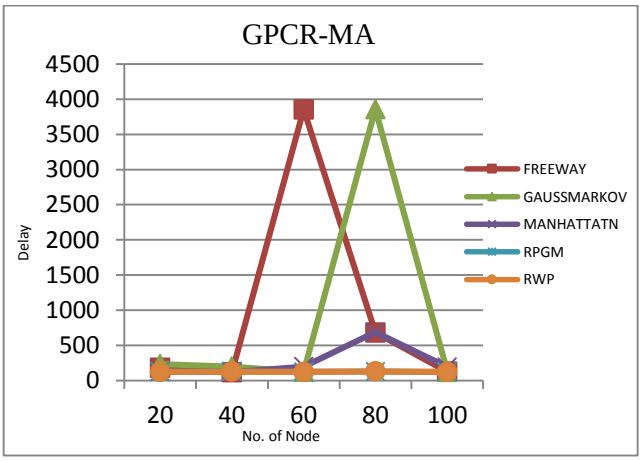

Figure 11: Comparison of the Average Delay between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density using GPCR-MA protocol.

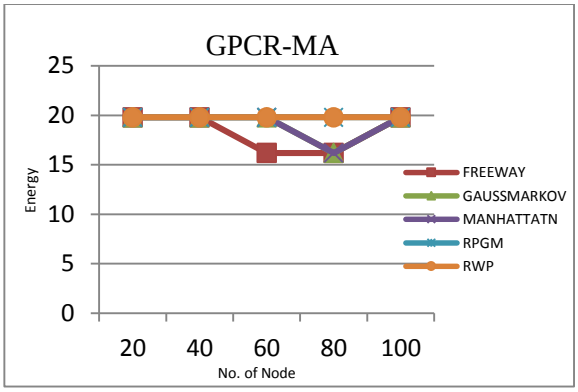

Figure 12: Comparison of the Average Energy Consumption between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density using GPCR-MA protocol.

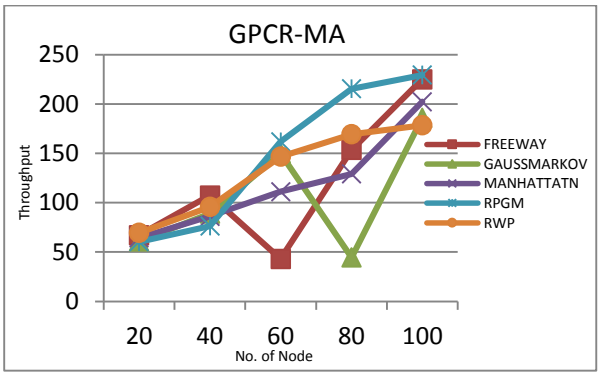

Figure 13: Comparison of the Average Throughput between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density using GPCR-MA protocol.

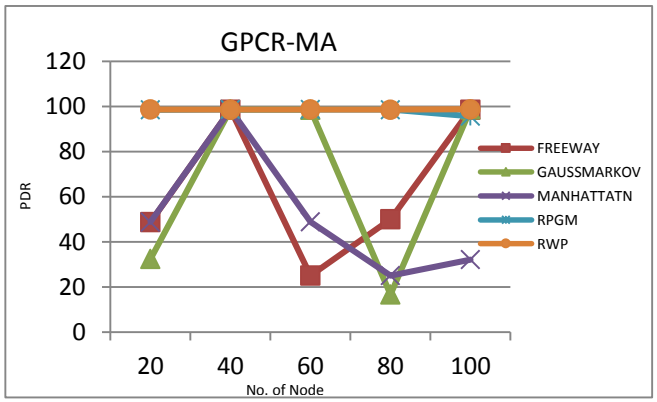

Figure 14: Comparison of the Packet Delivery Ratio between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density using GPCR-MA protocol.

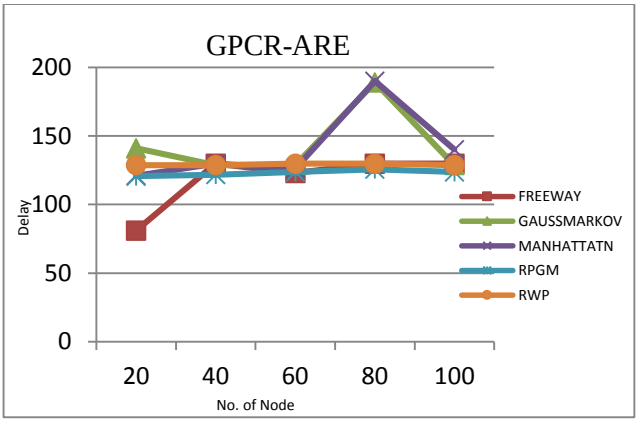

Figure 15: Comparison of the Average Delay between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density time using GPCR-ARE protocol.

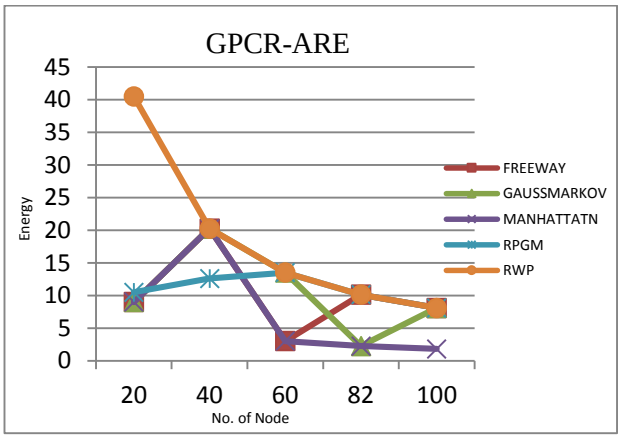

Figure 16: Comparison of the Average Energy Consumption between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density time using GPCR-ARE protocol.

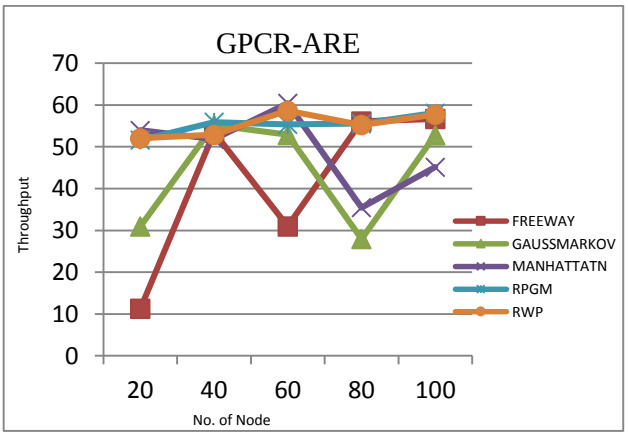

Figure 17: Comparison of the Average Throughput between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density using GPCR-ARE protocol.

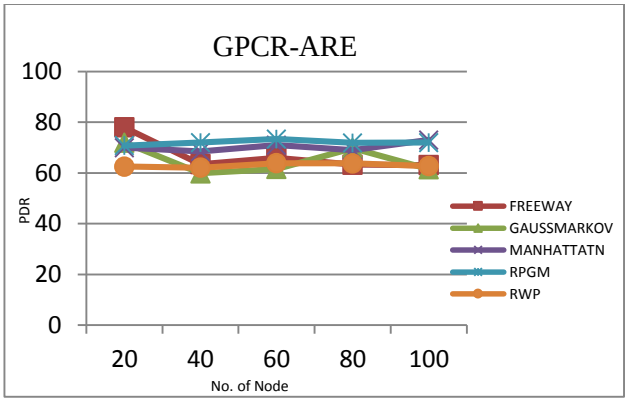

Figure 18: Comparison of Packet Delivery Ratio between Freeway, Gauss-Markov, Manhattan, RPGM and RWP Mobility Model based on network traffic density using GPCR-ARE protocol.

CONCLUSION

Vehicular Ad Hoc Network Routing Protocol such as GPCR-MA and GPCR-ARE are performed based on the various models of mobility Freeway, Gauss-Markov, Manhattan, RPGM and RWP based on the above network scenario. The analyzed results indicate that RPGM performed better than other three models of mobility in both the scenarios. GPCR-MA vehicular ad-hoc routing protocol performed best with the rapidly changing network state time, increased network traffic density and high relative speeds of the vehicles in network topology. The average delay was quite low and packet delivery ratio is also very low in GPCR-ARE as compare to GPCR-MA. As compared among the routing in VANET GPCR-MA is the highest performer over the GPCR-ARE. RPGM model of mobility worked in the group with the group leader so that it's not covered entire network at once, its divide network into server part and then start working over these so that RPGM suggestively enhanced performance in heavy traffic density over Freeway, Gauss Markov, and Manhattan and RWP models of mobility.

REFERENCES

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

[2] Hussain, Rasheed, et al. "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.

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

[4] Ismail, Datuk Prof Ir Ishak, and Mohd Hairil Fitri Ja'afar. "Mobile ad hoc network overview." Applied

Electromagnetics, 2007. APACE 2007. Asia-Pacific Conference on. IEEE, 2007.

[5] Hussain, Naziya, Anoop Singh, and Piyush Kumar Shukla. "In Depth Analysis of Attacks & Countermeasures in Vehicular Ad Hoc Network." International Journal of Software Engineering and Its Applications 10.12 (2016): 329-368.

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

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

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

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

[10] Schoch, Elmar, Frank Kargl, and Michael Weber. "Communication patterns in VANETs." IEEE Communications Magazine 46.11 (2008).

[11] Luo, Jie, et al. "MI-VANET: A new mobile infrastructure based VANET architecture for urban environment." Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd. IEEE, 2010.

[12] Tee, C. A. T. H., and Alex CR Lee. "Survey of position based routing for inter vehicle communication system." Distributed Framework and Applications, 2008. DFmA 2008. First International Conference on. IEEE, 2008.

[13] Nuri, Mohd Diana, and Halabi Hasbullah Nuri. "Strategy for efficient routing in VANET." Information Technology (ITSim), 2010 International Symposium in. Vol. 2. IEEE, 2010.

[14] Wischhof, Lars, and Hermann Rohling. "Congestion control in vehicular ad hoc networks." Vehicular Electronics and Safety, 2005. IEEE International Conference on. IEEE, 2005.

[15] Trivedi, Harsh, et al. "Routing mechanisms and cross-layer design for vehicular ad hoc networks: A survey." Computers & Informatics (ISCI), 2011 IEEE Symposium on. IEEE, 2011.

[16] La Vinh, Hoa, and Ana Rosa Cavalli. "Security attacks and solutions in vehicular ad hoc networks: a survey." International journal on AdHoc networking systems (IJANS) 4.2 (2014): 1-20.

[17] Papadimitratos, Panagiotis, et al. "Secure vehicular communication systems: design and architecture." IEEE Communications Magazine 46.11(2008).