I.J. Modern Education and Computer Science, **2015, 11, 20-27**
Published Online November 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2015.11.03

Movement Abnormality Evaluation Model in the Partially Centralized VANETs for Prevention Against Sybil Attack

Mandeep Kaur
Computer Science Department, CGC Landran, Mohali, India
E-mail: mandeepcheema6@gmail.com

Manish Mahajan
Computer Science Department, CGC Landran, Mohali, India
E-mail: cgccoe.hodcse@gmail.com

***Abstract*—**The VANETs carry many security concerns. One of the popular and dangerous attacks can be launched in the form of Sybil or Prankster attack, where an attacker inserts a fake position within in the cluster. The inserted fake node information can be utilized by the hackers in the case of selfish driver, traffic jams, selective collisions and other similar hazardous situations. To avoid such things the VANETs must be protected against such attacks. In this paper, a novel solution has been proposed to overcome the Sybil and prankster attacks on the VANETs. The new solution is capable of detecting the fake information injections by verifying the VANET node behaviour in the cluster. The behaviour of the node includes the direction, speed, pattern, etc. In case a node is found malicious, the whole cluster is reported against that node, and node is ordered to stop by the central control system. The proposed model has been developed using the random waypoint model. The random way point model is much closer to the real time VANETs. The random waypoint model has been compared against the reference point group model. The experimental results have shown the effectiveness of the proposed model.

Index Terms—Random way point mobility, Reference point group mobility, VANET, Sybil, Prankster.

I. Introduction

Vehicular ad-hoc network (VANET) is an ad-hoc network which is recognized as a subclass of the mobile ad- hoc network (MANAET). It is one of the auspicious approaches of the intelligent transportation system (ITS). VANET offers the number of features such as quick changes in the network topology, high mobility, recurrent or periodic portioning etc. Vehicular ad-hoc network allow inter-vehicle communication to enhance driving experience and road safety. Communication in the vehicular ad-hoc network depends on the transfer of messages between several nodes in the network. It helps to enhance the safety, driving effectiveness and relief on the course for the travelers [1]. In the vehicular network, the messages collected from other nodes make use of to build the most of the decisions.

Still, a node may function as malicious or selfish in order to take the benefit from other vehicular nodes. Security of the VANET has been identified as a big challenge. The applications of the VANET compromise with life critical information and support the real-time communication. To do it properly, it's essential to follow some security requirements like integrity, confidentiality, non-repudiation, authentication and privacy across attackers and malicious attacker nodes. There are the no. Of attacks such as black hole, timing, illusion, DOS, Sybil which not only influences the vehicles and deriver's privacy but also affects the traffic safety [1]. In some cases, it may leads to loss of life. To ensure the traffic safety the VANET needs some suitable security techniques that will assure protection across distinct misbehaviors and malicious nodes that influence the security of the VANET.

Information distribution in the VANET takes place through the joint behaviour of the vehicular nodes. The messages that are broadcast hold the essential information like road condition, traffic jam, and bad weather condition, emergency break events and accidents notifications etc. In these case, when a vehicle interfere or alter the messages then the results will be very hazardous. Hence, misbehaviour in the VANET is very important concern. Normally, the misbehaviour indicates the abnormal behaviour. Thus, the detection of the misbehavior and malicious nodes includes a misconducts i.e. greatly crucial. A lot of work has been lugged out to identify the misbehaviour and malicious node in the vehicular ad-hoc network. Generally, the misbehaviour detection strategies can be of two types: data centric and node centric misbehaviour detection strategy [8][9][11].

The data-centric scheme examines the data broadcasts between the nodes to identify the misbehaviour. It is interested in relationship among messages rather than the identities of single node. The information distributed by the nodes in the network is examined and compared

with the information collected by other nodes. Hence, any node in the vehicular network which transmits some false information about the several events in the VANETs such as fake traffic messages, false location, fake emergency events, road conditions, accidents etc. is recognized to be as misbehaving. This kind of behaviour is determined through data centric misbehaviour schemes [1] [3].

Non-centric techniques are used to characterize between the nodes using authentication. Digital signatures, security credentials are used to validate the node that transmitting the messages [3]. Such techniques are focus on the node that transmitting the messages rather than the data transmits. Non-centric schemes can be further classified as behavioral and trust based non-centric schemes. Behavioral techniques works by monitoring the node's behaviour by uses a metric helps to examine the how efficiently a node works. Trust based node-centric techniques are used to judge the nodes by its behaviour in the past and present. This behaviour also used to access the wonted behaviour in the future [9].

Vehicular networks have been developed to improve the safety, security and efficiency of the transportation systems and enable new mobile applications and services for the travelling public. Vehicular networks are becoming a crucial component for the future intelligent road traffic management system. Future intelligent road traffic management systems are expected to offer several key advantages compared to the current traffic management systems.

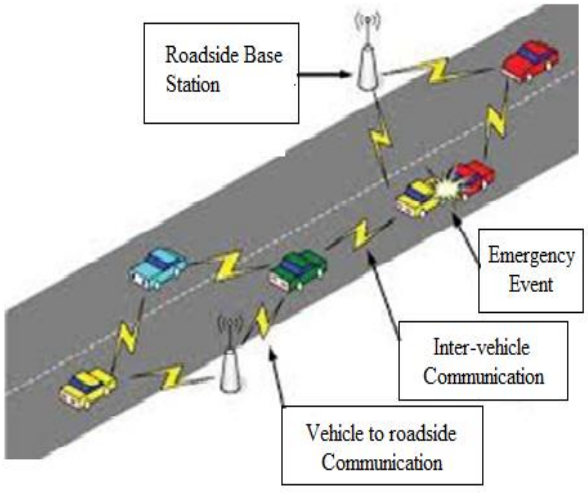

Fig.1. Vehicular ad-hoc network

The key advantages are improved knowledge based real time traffic signaling systems, improved safety of vehicular traffic and reduced vehicular emissions. Researchers in communications engineering and traffic management systems are engaged for more than a decade to develop suitable Vehicular Ad hoc Networks (VANET) for traffic safety systems. VANET is evolving as one of the practical applications of MANET in the future. This vehicular network is interconnected with vehicles which have wireless interface. The vehicle can easily provide the required power for wireless communication, and adding antennas or additional communication hardware does not cause major problems. The goal of VANET is to develop a vehicular communication system to provide quick and cost-efficient distribution of data for the benefit of passenger safety and comfort. Vehicular delay-tolerant networks rely on opportunistic contacts between network nodes to deliver data in a store carry – and - forward DTN paradigm that works as follows. A source node originates a data bundle and stores it using some form of persistent storage, until a communication opportunity (i.e., a contact) arises. This bundle may be forwarded when the source node is in contact with an intermediate node that can help bundle delivery.

Afterwards, the intermediate node stores the bundle and carries it until a suitable contact opportunity occurs. This process is repeated and the bundle will be relayed hop by hop until reaching its destination (eventually and over time).VANETs can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UMTS, LTE and Wi-MAX networks. Main advantages are low cost of implementation and maintenance, self- organization and lower local information dissemination time. VANETs can be seen as self-organizing autonomous system which can distribute traffic and emergency information to vehicles in a timely manner. VANETs have several advantages over the conventional wireless networks such as UMTS, LTE and Wi-MAX networks. Main advantages are low cost of implementation and maintenance, self- organization and lower local information dissemination time.

Vehicular ad-hoc network is also called as intelligent transportation system (ITS). In this the vehicles communicate with each other called vehicle to vehicle communication (V2V) or inter vehicular communication and vehicles communicate with the road side equipments called as vehicle to road communication (V2R). In intelligent transportation systems, each vehicle takes on the role of sender, receiver, and router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic. Each vehicle broadcast the message to another one.

Vehicular ad-hoc network have achieved a lot of concentration as it can incredibly enhance the safety on the roads and the driving conditions. Discovering the misbehaviour in the VANET is very important as it can be dangerous. The node centric and data centric misbehaviour detection techniques have a no. Of issues which demands to eliminate to make the VANET more reliable and safe. The non-centric techniques can be enhanced by choosing the node as observer after appropriate validation. These techniques need great observations to find out the abnormal misbehaviour [8][3]. Hence, to do this there is great need of high speed computation and processing hardware on the on board unit (OBU) to build the decisions more rapidly and

correctly. Some misbehaviour detection techniques use the result of short term misbehaviour. In data centric schemes, the misbehaviour is detected by using the safety alert messages, beacons etc. To decrease the overburden associated in the communication of the messages. It has been found out that no one misbehaviour detection scheme can detect all types of the misbehaviour efficiently in the vehicular networks (VANETs).

II. Literature Survey

The literature review has been conducted in detail over the adequate number of techniques to know their advantages and shortcomings. The motivation behind the literature study is to find and remove the appropriate shortcoming in the existing models, while keeping the advantages intact in order to build the robust system. We have conducted the literature review on as many as similar papers we found similar to our research. The literature review has been defined as following:

Ghosh et al. [8] proposed a strong and powerful scheme to determine the malicious vehicles for post crash notification application. Firstly, it recognizes the driver's actions establishing a crash alert message. Examined mobility and predicted trajectory of the vehicular node for the crash mobility model is computed. If the difference among two surpass the threshold value then the alert is taken to be false. This technique efficiently decreases the false positions and the false negatives while efficiently discovering the misbehaviour.

Kim and bae [7] have suggested a novel misbehaviour based reputation management scheme (MBRMS). It contains the three components (a) Misbehaviour detection (b) event rebroadcast (c) global eviction algorithms to discover and filter the false information in the vehicular networks. Every vehicular node manages the information system of the events and equivalent actions for determining of misbehaving node. The current system uses the outlier detection scheme. MBRMS efficiently discovers and ejects the misbehaving node.

Daeinabi and Rahbar [2] have proposed a detection of malicious vehicles (DMV) algorithm through examination to detect the malicious nodes that duplicate the received packets greater than the threshold value. Vehicles are labeled using a apparent value and are guided by the allocated verifier nodes. Black and white lists are managed in order to separate the malicious vehicles from the truthful vehicles. The analysis of the performance indicates that this misbehaviour detection technique is able to identifying the malicious vehicles at high speeds.

Wahab et al. [12] have proposed a quality of service-optimized link state routing (QoS-OLSR) is a clustering algorithm to discover the malicious vehicles in the vehicular network. Some vehicles may over the highest speed limits or under the lowest speed. Hence may prove to be in-cooperative in packet forward results in the reducing performance of the network. Authors have suggested a two phase model: a) incentive and b) detection.

III. Experimental Design

The above figure describes the traffic in the two directions. Each direction has two lanes the vehicles in the first lane are marked with green and the second lane vehicles have been marked with the orange color. The red colored vehicle in the bottom lane has been defined as the attacker node, which inject the false information in the cluster to launch the prankster attack to take the

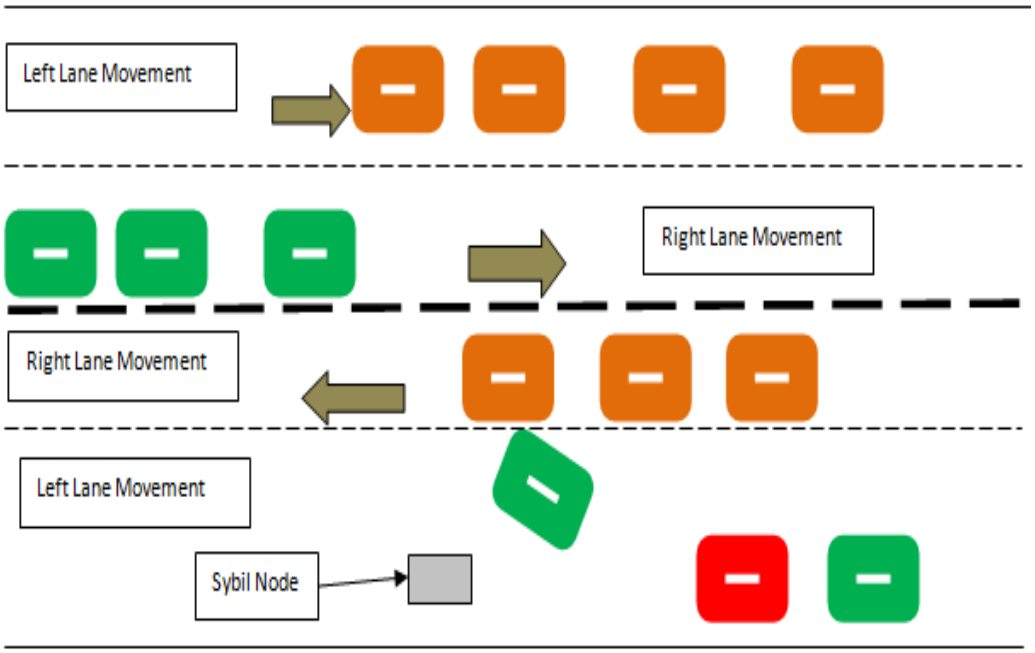

Fig.2. The demonstration of the prankster or Sybil attacks with single node

advantage by making its way clear in order to facilitate the hassle free movement by forcefully amending the driving direction or lane of the other vehicles in the cluster. The red node have plotted the gray colored Sybil node in the front of the green vehicle and have slowed down the speed, which forced the green vehicle to change its lane to obtain the obstacle free movement, which directly gives the way to the red vehicle in the fast lane.

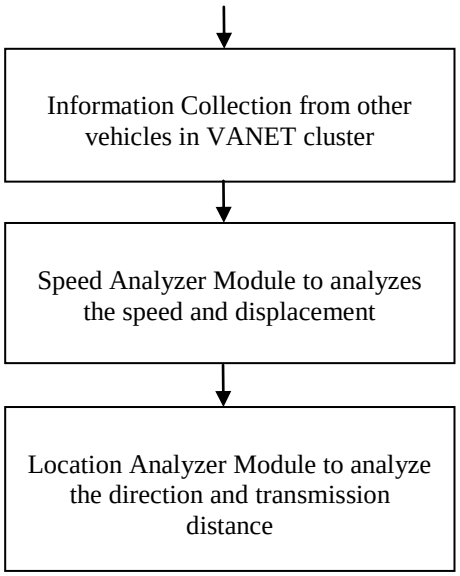

Fig.3. The System Components

In this research, we have worked upon the VANET security issue of prankster attack. In this attack one to more VANET nodes propagates their false location and direction to other nodes in the cluster, which may cause accident or traffic jam. This attacking mechanism can be utilized by terrorist or selfish driver to mandate their intensions. In this paper, the solution suggested is applicable to the VANET cluster without any traditional setup of Road Side Units. The proposed solution will be utilized by the VANET nodes individually or in the cluster.

The aim of the proposed model is to protect against the fake information injection because the fake information injection attacks (Eg. Prankster Attack, Sybil Attack, etc.) are dangerous and can cause various false implications in the VANET cluster.

The false information injection attacks can be the reason behind the massive traffic jams, terrorist attacks, targeted accidents and selfish driver. The proposed model is the amalgamation of various kinds of mathematical equation to calculation the actual position of the vehicle irrespective of its inserted information. The minimum criteria has been defined to protect the vehicular network from the false information injection attacks. The false information injection attacks are initially found with the minimum originality criteria, which verify the behavior of the vehicular node in the VANET cluster. If the minimum originality criteria are met, the node is declared as the authentic and permitted to join the VANET cluster. In case the originality criteria is not met, the vehicular node is verified more deeply for its movement, speed, displacement, direction or driving, which gives us the better perspective about the authenticity of the vehicular node.

Assumptions:

a. All VANET nodes must be aware about its own location and direction of movement.
b. VANET nodes may be the part of VANET cluster.
c. VANET nodes must have processing power on their own. (Nodes should not depend on centralize node for the decision logic).
d. Nodes must be capable of sharing its information in step a with other nodes in the neighborhood or cluster.

Work Flow:

1.) Prankster node P sends its location information $(X, Y\ co-ordinates)$ to node A.
2.) Node A receives the location coordinates X and Y of node P.
3.) Node A assumes its own location coordinates X and Y as central point i.e. X_c and Y_c.
4.) Now it will assume the location coordinates by node P as X_p and Y_p.
5.) In this simulation, each node's transmission radius is of 250 meters.

$$\text{i.e.} r = 250 \quad (1)$$

6.) It will perform the trigonometric formulas to find the location of the point in a circle with the formula

a. $(X_p - X_c)^2 + (Y_p - Y_c)^2 < r^2$ if this equation is satisfied then the point is within the circle.
b. $(X_p - X_c)^2 + (Y_p - Y_c)^2 = r^2$ If this equation is satisfied then the point is on the circle boundary
c. $(X_p - X_c)^2 + (Y_p - Y_c)^2 > r^2$ If this equation is satisfied then the point is out of the circle.

7.) If a point is within circle then, direction is calculated.

a. If

$$X_p < Y_p \quad (2)$$

then perform $(N - y + x)$ and return counterDistance where N is the point on circumference.
b. Otherwise perform $(x - y)$ and return counterDistance
c. If counterDistance is less than $N/2$, direction is counter clockwise
d. Otherwise direction is clockwise.

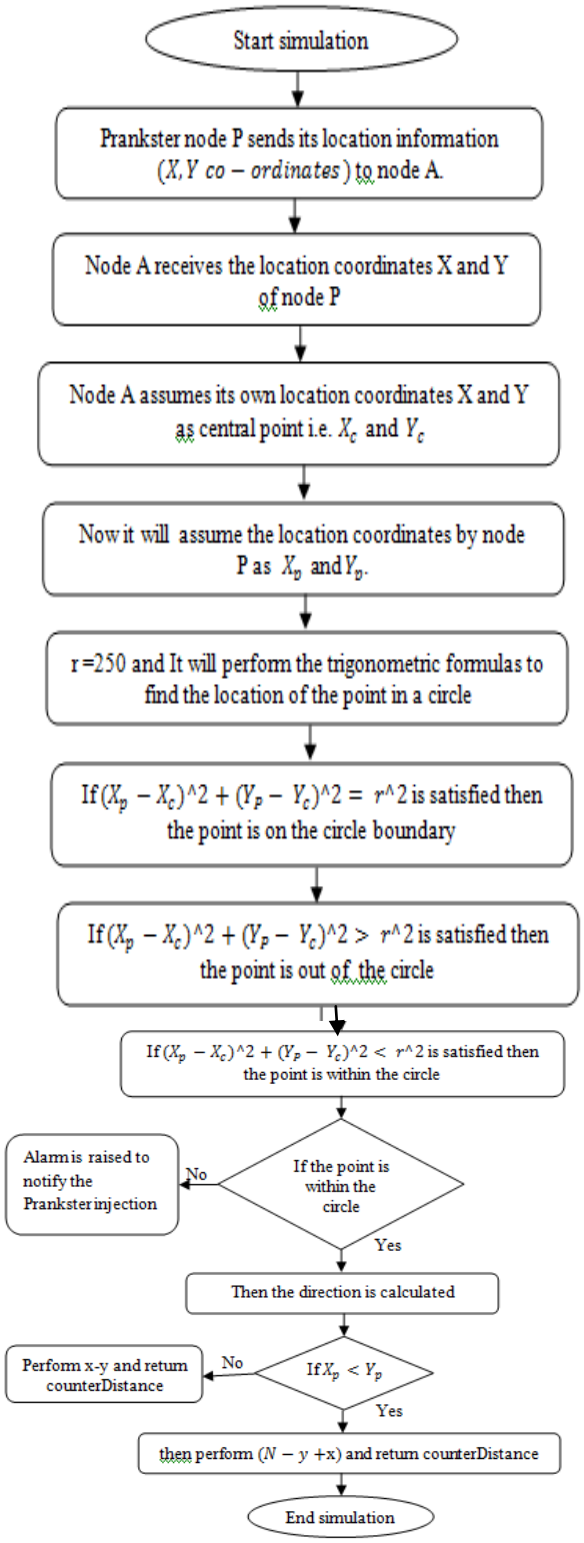

Fig.4. The Detailed System Flow Chart

IV. Result Analysis

The results have been obtained in the form of various performance parameters. Our major focus is to reduce the energy consumption as well as to improve the performance of the vehicular network. The energy consumption based evaluation has been done on the basis of energy level tracking on the given node for both proposed and existing models. The performance of the proposed model has been also evaluated on the basis of network performance parameters. The network performance parameters of end-to-end delay, network load and packet loss has been obtained from both of the simulation experiments and compared to evaluate the performance comparison. This section clearly defines the performance evaluation of the proposed model in comparison with existing model.

Comparison of energy and throughput of both mobility models is made. The output of terminal which shows comparison of energy and throughput of both mobility models:

A. Throughput

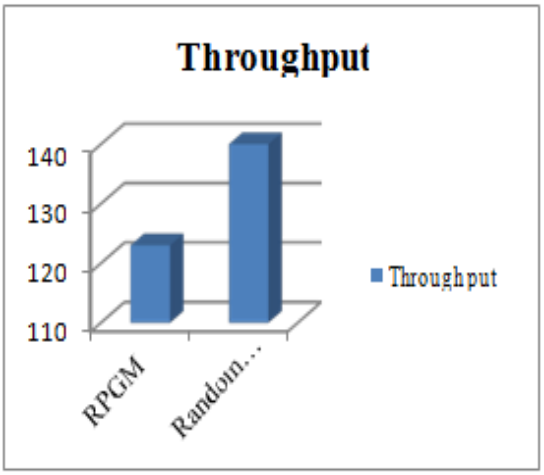

Fig.5.Comparison graph of throughput

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations. It is expressed in packets per second or bytes per second. Higher throughput demonstrates the better performance of the network.

B. Energy Comparison

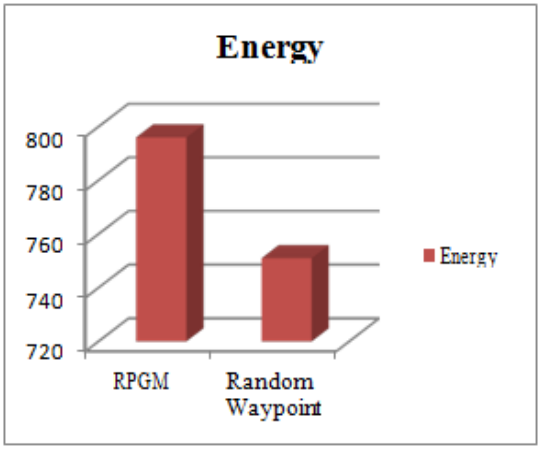

Fig.6.Comparison graph of energy

The energy consumption is the parameter of measuring the consumption of the energy on the basis of the data transfer, network load and other similar parameters. The proposed model has been designed with two different mobility models in the vehicular ad-hoc networks (VANETs). The reference point group model has been found consuming more energy than the random way point model in the proposed model simulation.

The proposed system consumes 751 Joules which is much lesser than the existing system i.e. 794 Joules. We have computed this to check that proposed system consumes less energy than existing. There is a difference of almost 43 Joules, which prolong the lifetime of proposed system.

C. End to end delay

It is the total time taken to transmit the packets from the source to destination. It is also known as transmission delay. The delay is represented in seconds. It gives the review about the performance of the network to deliver the packets from one end to another end. Lower delay is directly proportional to the lower performance.

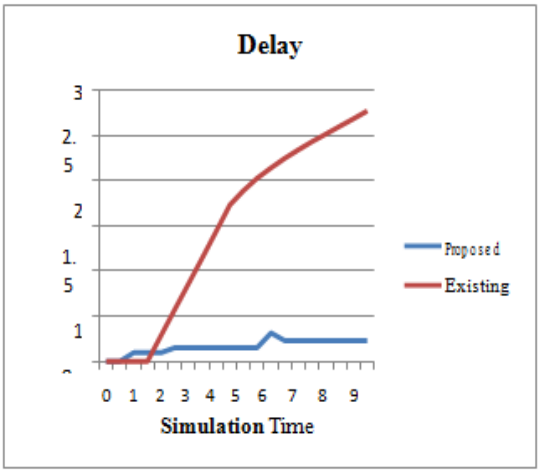

Fig.7. End-to-End delay

From figure 6 & 7 and Table 1 it showed the result comes from RPGM model is weaker than Random way point model in all parameters.

Table 1.Comparison of Random way point &RPGM Mobility Model

Parameters	Reference Point Group Model	Proposed Random Way Point Mobility Model
Energy	794 Joule	751 Joule
Throughput	123 kbps	140kbps

D. Packet Loss

Packet loss is the number of packets that are not successfully transmits from source to destination.

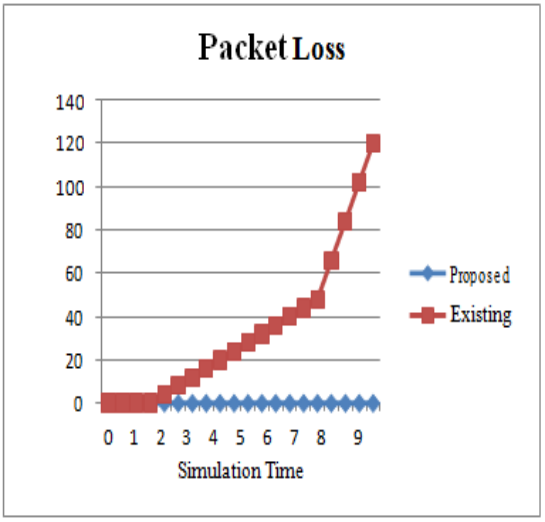

Fig.8. Packet Loss

Both of the mobility models for the VANETs have been tested for their performance on the basis of various performance parameters. The delay, load and lost are the primary parameter in-focus in this research paper. In the delay, load and lost, the random way point model has performed far better than the reference way point model, while enabled with the same security model for the VANET Sybil and Prankster attack prevention. The VANETs more near to the random way point movement than the reference point group model, unlike the movement patterns followed in the MANETs. The Random Way Point models have proved its efficiency in case of delay, load and lost as presented in the following graphical representations:

E. Network Load

It is the bulk of data that is carried out by the network at a specific time. It is expressed in packets per second or bytes per second. It is varies from time to time.

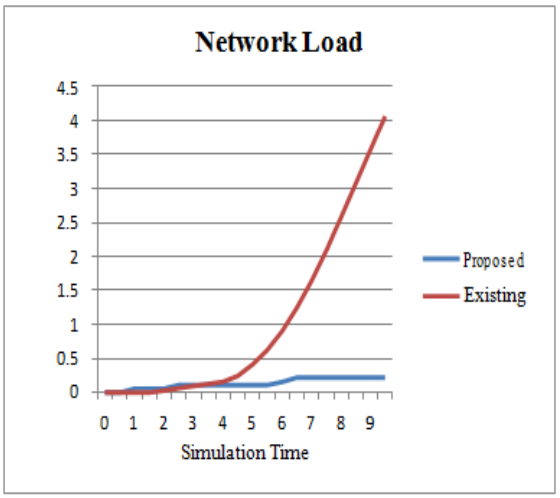

Fig.9. Network Load

V. Conclusion and Future Work

The proposed model has been deployed using the random way point mobility in the VANET. The performance of the proposed model has been has been evaluated against the existing model implementation using the Reference point group model. The VANET mobility is more similar to the random way point mobility (RWPM) mobility model, as the vehicle are always changing their location and lane according to the driving patter than the reference point group model (RPGM), which is clearly indicated by the result analysis. The proposed model has been found consuming less energy than the existing model by almost 7%, which is handful conservation of the energy. Sybil and Prankster attacks in VANET significantly degrade network performance and threat to public security. For that our proposed model with the Random way point mobility model, which makes the VANETs immune to such attacks. To prevent from Sybil or prankster attack, it helps the nodes to change the path or stop their activity.

The proposed model has been found effective than the existing model in mitigating the Sybil attack, which can be clearly indicated from the network performance parameters of delay, packet loss and network load. We have compared the proposed model results with the existing model based upon reference point group model. Our simulation results have shown the effectiveness of the proposed model with Random way point group model in the form of lowered energy consumption, network load, delay and packet loss in comparison with reference point group model. So we conclude that Random way point model has performed better than Reference point model for VANETs. Moreover, it is practical and easy to implement. In future, the present work may be extended with the proposed model extension development to detect and prevent the denial of service and selective jamming attacks. Also the proposed model can be enhanced with more dynamic mobility model than the random way point mobility model.

Acknowledgement

This research paper is made possible through the help and support from everyone including teachers, parents, family and friends. Especially I would like to dedicate my acknowledgement of gratitude towards the following significant advisors and contributors. First and foremost, I would like to thank Mr. Manish Mahajan and Miss Dapinder Kaur for his esteemed guidance and support. Secondly I would like to thank Mr. Ajitpal Brar for his kind help in carrying out this research. Finally, I sincerely thank my family for their patience and support. The product of this research paper would not be possible without all of them.

Refrences

[1] S. RoselinMary, M. Maheshwari, “Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)”, vol. 1, issue 1, IEEE, 2013.

[2] Daeinabi, A., Rahbar, A.G.: Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. Multimedia Tools Appl. 66(2), 325–338 (2013).

[3] Khan, Uzma, Shikha Agrawal, and Sanjay Silakari. "A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks."Information Systems Design and Intelligent Applications. Springer India, 2015. 11-19.

[4] Constantinos Kolias, Georgios Kambourakis, Stefanos Gritzalis, “Attacks and Countermeasures on 802.16: Analysis and Assessment”, CST, vol. 1, pp. 487-514, IEEE, 2013.

[5] Vulimiri, A., Gupta, A., Roy, P., Muthaiah, S.N., Kherani, A.A.: Application of secondaryinformation for misbehavior detection in VANETs. IFIP. LNCS, vol. 6091, pp. 385–396.Springer, Berlin (2010).

[6] Sonali Swetapadma Sahu, Manjusha Pandey, “Distributed Denial of Service Attacks: A Review”, vol. 1, pp. 65-71, IJMECS, 2013.

[7] Kim, C.H., Bae, and I.H.: A misbehavior based reputation management system for VANETS.LNEE 181, 441–450 (2012).

[8] Ghosh,M.,Varghese,A.,Kherani,A.A.,Gupta,A.: Distributed misbehavior detection inVANETs.In:Wireless Communications and Networking Conference,WCNC IEEE, pp. 1–6 (2009).

[9] Ghosh, M., Varghese, A., Gupta, A., Kherani, A.A., Muthaiah, S.N.: Detecting misbehaviors in VANET with integrated root-cause analysis. Ad Hoc Netw. 8, 778–790(2010).

[10] Ms. Poonam Barua, Mr. Sanjeev Indora, “Overview of Security Threats in WSN”, vol. 2, issue 7, pp. 422-426, IJCSMC, 2013.

[11] Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi, “SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks”, ETFA, vol. 1, pp. 1-8, IEEE, 2013.

[12] Wahab, O.A., Otrok, H., Mourad, A.: A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles. Comput. Commun. 41, 43–54 (2014). Elsevier.

[13] Md. Monzur Morshed, Md. Rafiqul Islam, “CBSRP: Cluster Based Secure Routing Protocol”, IACC, vol. 1, pp. 571-576, IEEE, 2013.

[14] Bibhu, V., Roshan, K., Singh, K. B., & Singh, D. K. (2012). Performance Analysis of black hole attack in VANET. International Journal of Computer Network and Information Security (IJCNIS), 4(11), 47.

[15] Joe, M. M., Shaji, R. S., & Kumar, K. A. (2013). Establishing Inter Vehicle Wireless Communication in Vanet and Preventing It from Hackers. International Journal of Computer Network and Information Security (IJCNIS), 5(8), 55.

Authors' Profiles

Mandeep Kaur, she is pursuing the master of technology from the CGC college of engineering (COE), Landran, PTU. She received her B.Tech in computer science from CGC Landran in 2013. Her main research area is vehicular network security.

Manish Mahajan, He received his B.Tech in computer science from Kurukshetra University in 2004 and his M.Tech in 2006 from Punjab technical university (PTU). He is now a head of department, professor in CGC College of engineering, Landran, Mohali, India. He has 11 years teaching experience and 6 years research experience. His total publications are more than 50. His research interests include image processing and information security.

