Performance Analysis of Multi Phase Abnormal Node Detection Model for Sybil Attack in VANET

Ashish Ranjan[1] Mukesh Kumar Choudhary[2]
[1,2]Department of Computer Science and Engineering
[1,2]Rajasthan Institute of Engineering & Technology, Jaipur, India

Abstract— Vehicular Adhoc Networks (VANET) is a special type of adhoc networks. VANET uses vehicles as mobile nodes in the network. VANET turns the every participating vehicle into a wireless router or node allowing vehicles approximate 100 to 300 meters of each other. The police and fire brigade are connected with each other of safety purpose by VANETS. There are many security issues in VANET but in this work dealing with one of its major security issue i.e. the Sybil attack. Sybil attack is a malicious attack in which the attacker creates multiple identities and uses them to gain a disproportionately large influence. Sybil attack is very dangerous in which the attacker can play any kind of attack with the system and down the efficiency of VANET to a larger extent. These forge identities creates an imaginary appearance that there are additional vehicles on the road. For the prevention of Sybil attacks various strategies have been developed to prevent intruders from attacking the system. In this dissertation work the Multi Phase Abnormal Node Detection Model (MAND Model) is proposed to detect the malicious node. Model is in biphasic which detect malicious node by RSU at entry in the network as well as by the node at packet transmission time. The model is designed and implemented. The results are obtained. The results show that the MAND model gives very good results at low load on each node than the higher load on each node. At the low load model is capable to identify the 57.6% malicious nodes. The whole simulation is performed in MATLAB environment.

Keywords: Wireless Network, VANET, DTN, ERDV, FFRDV, Sybil attacks

I. INTRODUCTION

A. Vehicular Ad Hoc Networks (VANET)

Ad hoc networks are characterized by infrastructure free, wirelessly connected and distributed systems with no central administration for controlling different operations in network. Every node has capabilities of a router which helps in providing multi hop communication among nodes which don't have direct link. There are constraints in ad hoc networks i.e. limited battery backup, radio range, and heterogeneity of devices. Mobile ad hoc network (MANET) is a sub class of ad hoc networks with mobile nodes. Vehicular ad hoc networks (VANETs) are special class of MANETs which are characterized as, distributed, self-organized networks formed by moving vehicular nodes with no central administration. VANETs are different from MANETs because of high mobility and predictable mobility patterns. Vehicular ad hoc network is becoming a popular area of research where researchers from all over the world are devoting their extensive time to provide safe (providing required information in advance about dangerous situations like accident) and enjoyable (real time game/file sharing between two user in different vehicles) drive over crowded roads.

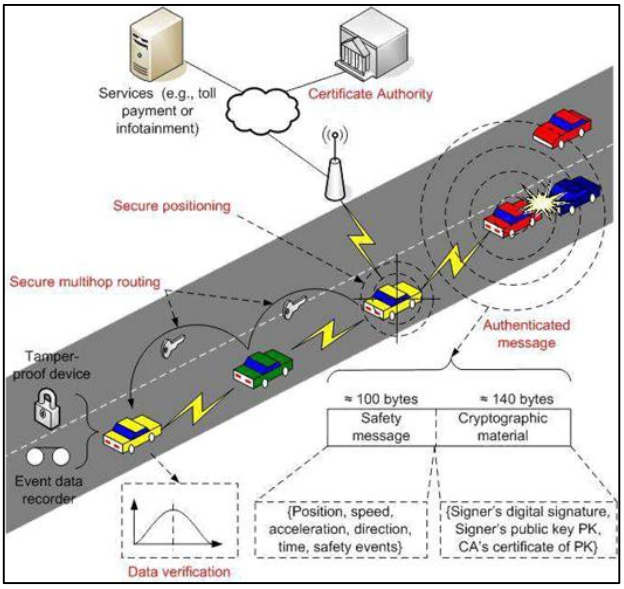

Fig. 1: Vehicular Ad-hoc Network [4]

The roads are very crowded now a day due to increase in number of vehicles in last few years. On congested roads, vehicles speed is low due to large number of vehicles which causes interference in communication among vehicles. Intelligent transportation systems (ITS) is a group which looks after safety of vehicles on roads and traffic management in USA. All the intelligent vehicles can follow the schedule provided by ITS system, which allows vehicles to reach their destination timely. Government security agencies and vehicle owners can track the vehicles if required. ITS uses infrastructure-to-vehicle (I2V) and vehicle-to-vehicle (V2V) communication system. This system also helps in the situations, when an accident occurs on the road, and the vehicles coming in the direction of accidental place should be aware of incident so that vehicles can choose alternate path to avoid congestion on the road [3].

Vehicular Ad Hoc Networks (VANETs) face highly variable density of traffic, which affects drastically to connectivity and coverage of the ad hoc networking. During the rush hours, ad hoc networking attains high probabilities for successful data delivery. Unfortunately, when the traffic quiets down, end-to-end connections via intermediate nodes cannot be established any more [5].

A vehicular ad hoc network (VANETs) is an ad hoc wireless communication system setup between multiple vehicles in a neighbourhood. The communication may be only vehicle-to-vehicle (V2V) or may also involve some roadside infrastructures. Some other applications have been proposed on VANETs for different purposes such as infotainment, safety, financial and navigational aid [6].

1) Application of VANET

The VANET is very useful in the vehicle communication. It has the following applications [

– Safety applications:

- Car speed warning:
- Traffic signal violation warning:
- Collision risk warning:
- Lane change warning:

2) Major Issues in VANET

There are some issues in VANET. These are as follow [5A]:
High Mobility:

- Real-time Guarantee:
- Privacy and Authentication:
- Location Awareness:
- Delay in VANET

B. Delay Tolerant Networks (DTNs)

Vehicular networks belong into one of the most challenging class of DTNs due to vehicles autonomous motion. In ordinary DTNs opportunities to communicate with other intermediate nodes are scheduled or can be predicted with high probabilities. In vehicular DTNs contacts between nodes appear without any a priori knowledge, and therefore routing protocols do not have any certain information available for means to make routing decisions. There have been efforts to utilize scheduled and fixed movement in vehicular networks in purpose to offer limited communication capabilities for peripheral areas, for example by using public transportation vehicles as digital couriers or utilizing existing postal services for data delivery. These systems, however, cannot employ autonomously moving vehicles as mobile routers [4].

Delay tolerant networks (DTN) are those networks which do not require immediate data delivery and can wait for a specific time period before the delivery of data. DTN uses the concept of store and forward. The DTN can be considered as overlay network. DTN network uses bundle protocol over IP network. Bundle protocol wraps up data of applications and transfers it as a bundle to lower layers of overlay network. There may be multiple copies of a bundle simultaneously in a DTN network because of store and forward strategy. Bundle can be fragmented by overlay networks if required during transmission. DTN vehicular ad hoc network uses store and forward strategy because of frequent network partitioning due to high speed of vehicles [3].

C. FFRDV

The fastest-ferry scheme for DTN [17] enable vehicle ad hoc network. It is assumed that each vehicle can get its current location information by Global Positioning System (GPS). Based on the geographic information, i.e. x-axis and y-axis coordinates, the road is divided into logical blocks, shown in Figure 1(a). The velocity of vehicles is compared within one block. At the initialization of the network communication, every vehicle create one state-report, which include the current position and velocity. And the state report is updated periodically. The node (vehicle) is called message ferry only when it's carrying data. Once the bundles are forwarded and acknowledged, the ferry will discard the data and change to be normal mobile node. Within one block, the priority of vehicle selection is decided by maximum velocity. In our scenario, each vehicle in the network is assumed to be equipped uniformly; therefore every vehicle has equal opportunity to become a ferry.

The following steps describe, in details, that how a ferry is selected and message is transferred in our proposed scheme. We divided our scheme into two phases: the Ferry Selection Phase and the Message Forwarding Phase.

1) The Ferry Selection Phase:

- When urgent event occurs, the event sources are sensed by nearby vehicles based upon request/response mechanism. The first responding vehicle becomes the initial ferry (IF) and is responsible for choosing next ferry, shown in Figure 1(a). Differently, IF chooses the next ferry basing on speed-priority.

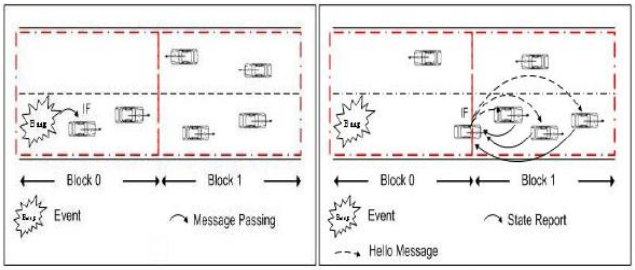

Fig. 2: (a) Mobile node sensing one urgent event becomes the initial ferry. (b) Ferry broadcasts hello messages upon entering into a new block [17].

- Once IF enters a new block, it broadcasts hello message and ask for state reports among neighbors within this block. Afterwards, any nodes that are able to accept new bundles send back current location Si, a timer ti, and its current speed vi, as depicted in Figure 1(b). IF has a waiting period: time-to-live (TTL). Within TTL, IF compares the speed values, and choose the fastest vehicle k. If the vk > vIF , IF predict the node k's location and forward the bundles, as it's described in Figure2. SNF is the location of new ferry.

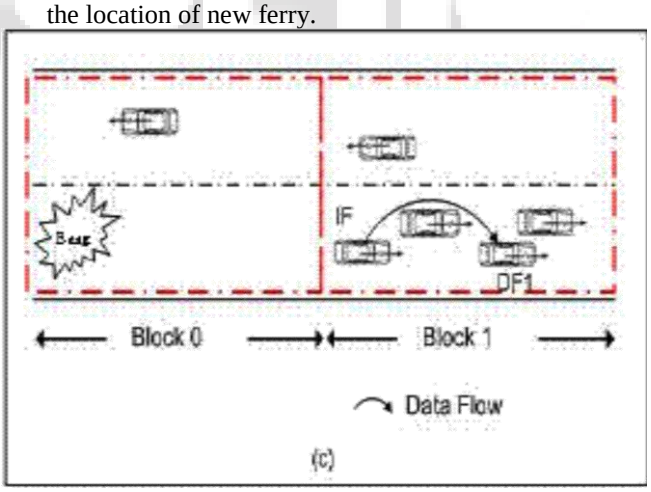

Fig. 3: The initial delivers data to the first dynamic ferry (DF1) [17].

After receiving acknowledge from node k, IF discards the data. If there is no vehicle offers vk > vIF , IF holds the data until next block and repeats the same selection.

$$SNF = Si + vi(t - ti) \quad (1)$$

- The vehicle holding data is called ferry. In our proposed scheme, it is called dynamic ferry (DF), because the ferry varies with the changeable blocks. Figure 2 shows the generation of DF1. Through the same procedure, DFi selects DFi+1. If DFi can't get the faster vehicle or the faster ones are not available, it keeps data until it finds a

new superior one in velocity vector. - The message is forwarded on the current road until it reaches an intersection. When DF reaches crossing, the data transmission direction is varied for shortest path. Because our protocol is designed for uncast application, the distances between crossings and the destination can be calculated basing on the geographic information. If the next intersection along the same road is nearer to the destination than the current one, the data will be relayed along same direction. Otherwise, the data transmission direction is changed for shorter path. The current DF chooses the next DF in the new transmission direction.

2) The Message Forwarding Phase

High data delivery rate can be achieved through the careful selection procedure of ferry in the algorithm of our routing. The velocity-based scheme results in minimum number of ferries, which contributes to lower delay and high bundle transmission rate. The total end- to- end delay comes from the processing time (Tp) and transmission time (Tt). DF is selected for the smallest sum of Tp and Tt among k mobile nodes within one block. The total delay Td equals to the sum of Np packets' delay which are transferred through N times delay of each packet. Every fastest ferry is deemed to successfully receive and transmit the packet to the fastest ferry in the next block or final destination.

D. ERDV

In the proposed scheme (ERDV), we are considering that each vehicle is equipped with Global Positioning System (GPS) and is able to get the information about its current location. The geographic information is used to generate logical blocks which divide the road into sections. These blocks are of variable size based on speed of vehicle. The size of block is inversely proportional to speed of vehicle. Each vehicle has its own logical block based on its velocity. Every vehicle broadcasts HELLO message every time it enters its own block. Each HELLO message has the information about, speed and direction of vehicle which has generated it. If there is a vehicle with high speed, it will broadcast HELLO message very frequently because increase in the speed of vehicle will decreases its block size. This helps in detecting the high speed vehicle quickly, rather than detecting in next block as in case of same block size [5]. In ERDV we have taken three steps of four cars with different speeds. To distinguish among cars of different speeds, these are numbered. The car with highest speed is numbered as car1 and slowest as car4. Similarly blocks of each car are also numbered with number of car. Each car follows the respective lane (numbered with car number). As there are four different cars, there will be four different blocks numbered as 1 to 4 for respective car. Car1 broadcasts HELLO messages while entering block 1, car2 while entering block2 and so on.

In first step, whenever an event (accident, query related to destination or road map etc.) occurs, any nearby ferry becomes CF and carries the message. As discussed in figure 2, car4 becomes CF and carries the message. Blocks have been shown as marked line in figure 2.

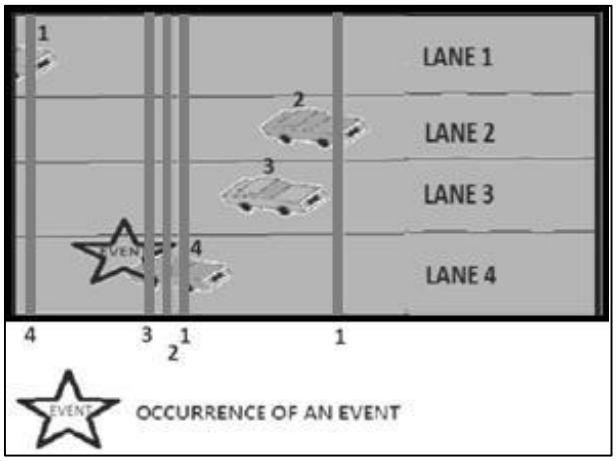

Fig. 4: Ferry becomes current ferry by sensing an event [3].

This CF (car4) will carry the data (in case of light load there are 100 packets to be sent as a bundle and 500 packets in case of heavy load) until it finds a ferry with greater speed. The blocks for specific car are numbered with respective numbers of cars. In second step, every vehicle sends HELLO packet at the starting of its block as shown in figure 3. Here car1 and car3 are entering their respective blocks. In such case CF will receive two HELLO packets broadcasted by car1 and car3. HELLO packet contains the information about velocity and direction of vehicle.

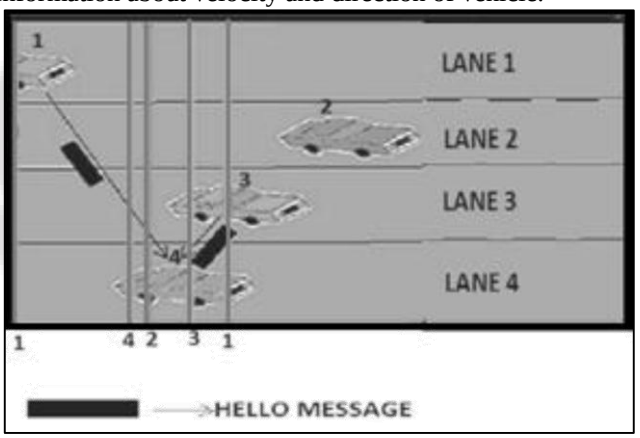

Fig. 5: Ferries send HELLO messages at the starting of their blocks [3].

In third step, CF compares its velocity with velocity in received HELLO packet and decides to send bundle. CF selects a ferry between cars if the velocity in any of received HELLO packets is greater than the velocity of CF and the direction is same as of CF. Here CF (car4) will compare the velocity of car1 and car3 and selects the ferry with highest speed among them which is car1 in this case. The ferry with greater velocity is called designated ferry (DF) and all ferries with lower speed than DF but greater than CF are called candidate ferry (CdF). In given scenario, DF is car1 and CdF is car3. After selecting DF (car1) the CF (car4) will send the data to DF as shown in figure 6.

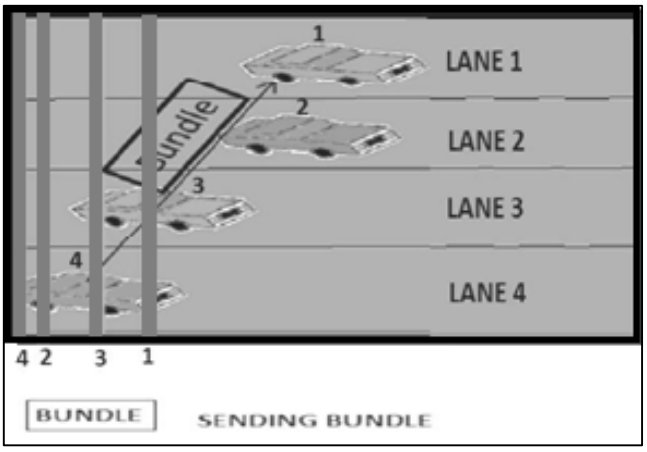

Fig. 6: Sending Bundle to Designated Ferry [3].

A ferry is called CF till it is carrying bundle. When the bundle is transmitted and acknowledged the CF discards stored bundles and becomes normal ferry. In this scenario, there is no boundary of blocks for receiving HELLO packets, but the block boundaries are strictly followed while broadcasting HELLO messages.

II. LITERATURE SURVEY

In [6] Mainak Ghosh et al. proposed a Misbehavior Detection Scheme (MDS) and analyze the dependence of its reliability performance on the micro-mobility model of the vehicles and its parameter estimation. The qualitative understanding gained from this exercise carries over to other related MDSs. This work helps in understanding the trade off in the two conflicting performance indicators of an MDS, namely, (a) detection delay, and (b) reliability. In this work, authors focus on the Post Crash Notification (PCN) application. The PCN application informs the driver when there is a crashed vehicle ahead on the same roadway. A PCN alert is normally sent by a car involved in a crash. Authors assume a misbehavior model in which a car can send a false PCN alert even if there is no crash. In this initial work, authors assumed that the position information sent in the alert is correct even if the alert is false. A method to identify false alerts in PCN application is proposed. The proposed method is based on observing the driver action after a crash alert is raised, and measuring the deviation between the drivers' observed behavior and the expected behavior on a crash. Detailed simulation results are shown to observe the behavior of the method under different mobility models. A secondary contribution of this work is to propose some mobility models for VANETs that try to model the driving habits of different types of drivers.

Authors have presented and evaluated a misbehavior detection scheme for PCN application. The results indicate that the scheme performs well in detecting misbehaviors while reducing the chance of false positives and false negatives. It is also quite robust with respect to small errors in estimating the parameters of the mobility model. This is important as in a practical setting; the model parameters assumed need to be estimated from observed data, and small errors in estimating the parameters should not significantly affect the performance of the system. Even though a Markovian model is assumed for mobility of vehicles, the basic approach of using the deviation between actual and expected trajectories for misbehavior detection is equally applicable for other mobility models also as long as an expected trajectory in the presence and in the absence of a crash can be derived. Finally, this initial work assumes that even in a false alert, the position information will be correct, which may not be true in practice.

In [14] Vimal Bibhu et al. present the performance analysis of the black hole attack in Vehicular Ad Hoc Network. Authors elaborate the different types of attacks and their depth in ad hoc network. The performance metric is taken for the evaluation of attack which depends on a packet end to end delay, network throughput and network load. The delay, throughput and load are simulated by the help of OPNET 14.5 modeler. The simulation setup comprises of 30 Vehicular nodes moving with constant speed of 10 meter per second. The data rate of Vehicular nodes is 11 Mbps with default transmitting power of 0.005 watts. With On Demand Distance Vector Routing and Optimized Link State Routing the malicious node buffer size is lowered to a level which increase packet drops.

Vehicular Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of VANET comparative to its vast potential it has still many challenges left in order to overcome. Security of VANET is one of the important features for its deployment. In this work authors have analyzed the behavior and challenges of security threats in Vehicular Ad-Hoc networks with solution finding technique. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches, authors concluded that the approach offered by Deng suit well with author's scenario. The intermediate reply messages if disabled leads to the delivery of message to the destination node will not only improve the performance of network, but it will also secure the network from Black Hole attack. In this work authors analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end-to-end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. Authors have analyzed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR. Based on research and analysis of simulation result, authors draw the conclusion that AODV is more vulnerable to Black Hole attack than OLSR.

In [15] S. Roselin Mary et al. proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial of Service) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET. The mechanism is attached with each RSU. Vehicles can send messages to RSU through APDA mechanism. It is to detect a certain position of the messaged vehicles. After detecting the position of vehicle

information it is stored in the certain RSU. Each vehicle has OBU and TAMPER PROOF device. These devices, store the detailed information about the vehicles. For example speed, position and etc. Vehicles positions are identified by the frequency and velocity of the vehicles and the use of OBU. APDA algorithm is detecting the position of the vehicle and detects the packet of vehicles send. If the packet is not attacked, vehicle will not track else track the particular vehicle. APDA can be applied, before the verification time and to increase the security. It is used to detect the invalid request and attacked packets and it is used to avoid the delay overhead. The APDA algorithm is used to improve the security of VANET system and to avoid the delay overhead in early time. The algorithm can be applied before the verification time delay overhead is minimized and will enhance the security of VANET.

In [16] Uzma Khan et al. proposed algorithm DMN-Detection of Malicious Nodes in VANETs improves DMV Algorithm in terms of effective selection of verifiers for detection of malicious nodes and hence improves the network performance. To effectively detect misbehaviors and malicious vehicular nodes in VANETs, authors have proposed a novel algorithm called DMN (Detection of Malicious Nodes in VANETs). DMN algorithm is designed to isolate the nodes showing abnormal behavior as well as enhancing the network performance. DMN optimizes the selection of verifier node which perform the work of monitoring node's behavior. DMN improves the pre - existing DMV algorithm which selects all the nodes as verifiers which have distrust value less than the vehicle to be monitored. It has been optimized by our proposed DMN algorithm taking into consideration three parameters for choosing appropriate verifiers that are load, distance and distrust value. Based on these parameters, a decision value is evaluated and compared to verifier selection threshold. Thus, optimal verifier selection improves the network utilization and in turn improves network performance. The simulation results indicates that DMN provides higher throughput, better packet delivery ratio and reduces the end to end delay, when compared to DMV algorithm.

In [17] Sonia et al. analyzed the performance of VANET in presence of black hole node by using different routing protocols AODV, DSR and AOMDV. Authors analyzed that which protocol is more vulnerable to the black hole attack and how much is the impact of attack on these three protocols. The main parameters considered are throughput, end-to-end delay and scalability. These parameters are compared for each routing protocol both using with black hole attack and without black hole attack. Simulation shows that DSR has high performance in terms of throughput, delay and scalability. DSR outperforms in terms of throughput and delay as compared to AODV and AOMDV. Results shows that DSR is much scalable than other routing protocols. DSR is better routing protocol to be deployed in VANET, Out of all three routing protocols, black hole node has high impact on AOMDV than AODV and DSR.

In [18] M. Milton Joe et al. proposed wireless inter vehicle communication will allow vehicles to inter change messages from one vehicle to another vehicle with the help of network communication and prevents the communication from the hackers. Authors modeled network communication between vehicles and also brought out network communication between vehicles and mobile phones. Authors studied the comprehensive characteristics of vehicles moving on the road and Bluetooth technology. Authors form the network communication among vehicles using Bluetooth technology. In order to provide securable communication between vehicles and prevent our network architecture from the hackers, authors have provided securable communication between vehicles by authenticating the vehicles in a securable manner. Our authentication process takes place by matching the master key and slave key shared by the vehicles. Authors have also provided background authentication mechanism to reduce the authentication delay. Their mechanism works well and it is evaluated by the metrics provided.

In [19] Omar Abdel Wahab et al. proposed a two-phase model that is able to motivate nodes to behave cooperatively during clusters‟ formation and detect misbehaving nodes after clusters are formed. This work addressed the problem of misbehaving nodes in Vehicular Ad Hoc Networks. Incentives are given in the form of reputation and linked to network's services to motivate vehicles to behave cooperatively during the first phase. A vehicle is considered as selfish or misbehaving when it over speeds or under-speeds the maximum/minimum road speed limit. Misbehaving vehicles can still benefit from network's services by behaving normally during the clusters‟ formation and misbehave after clusters are formed. Giving incentives will not stop such behavior but will ensure the clusters formation. Thus, the main challenge was the detection of misbehaving vehicles. To detect misbehaving vehicles, cooperative watchdog model based on Dempster–Shafer is modeled where evidences are aggregated and cooperative decision is made. Simulation results show that the proposed detection model is able to increase the probability of detection, decrease the false negatives, and reduce the percentage of selfish nodes up to 30% in the vehicular network, while maintaining the Quality of Service and stability.

In [20] Ravneet Kaur et al. proposed several solutions for securing safety messages. The significant below against the security of VANET is a Sybil attack. It is an attack in which an original identity of the vehicle is corrupted or theft by an attacker and creates multiple dummy identities for stealing the vehicle. This work presents various Sybil attack detection mechanism in VANET. This work include various types of attack involve in VANET and their detection mechanism. Authors showed that only certain areas may contain cheated nodes. There is no unique method for identifying and removing the Sybil attack in the VANET. Each method has its own advantages and disadvantages. The number of issues such as detecting the presence of Sybil attacks, localizing multiple adversaries and eliminating them are not solved effectively. The results given in this paper provide a good framework to elaborate realistic test suites for Sybil attack detection methods and to evaluate them from an objective point of view.

In [21] Mandeep Kaur et al. 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 behavior in the

cluster. The behavior 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. 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. Sybil and Prankster attacks in VANET significantly degrade network performance and threat to public security. To prevent from Sybil or prankster attack, it helps the nodes to change the path or stop their activity.

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.

In [22] Harsimrat Kaur et al. introduced genetic algorithm for optimization of fake nodes then again check the value on the basis of some specific parameters. VANETs is quiet unsafe as well as susceptible to numerous attacks so there is necessity of a dependable, proficient as well as a protected protocol which can be able to quickly organized and also utilize dynamic routing technique. Peer-to-peer systems play an ever-increasingly important part of our daily lives. However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In order to design more efficient and practical Sybil defenses, authors proposed an implementation based on Genetic algorithm. In this work, the issues related to security like Sybil attack has been reviewed. Then an Intrusion Detection System (IDS) especially for Sybil attacks is implemented using Genetic Algorithm, and then tested with networks of varied node configurations. The performance analysis will be done in terms network load, throughput of the algorithm as the node number is increased. Sybil attack prevention is achieved at greater rate when GA has been used. In [9], Amit Mane proposed received signal strength (RSS) based technique for detecting Sybil nodes in VANET. RSS represents the transmission power minus signal attenuation, which is related to both distance between the transmitter and receiver and environment conditions. Signal attenuation differs significantly from its theoretical expectation, due to many environment factors. Most existing detection approaches give inaccurate result due to the noisy channel and presence of obstacles between transmitter and receiver. These are based on statistical analysis and that is only for static networks. Since our network scenario is not static, existing position verification approaches cannot be directly applied for identification of malicious nodes. Proposed approach does not consider the inaccuracies of wireless channel instead it considers the similarity of RSS values of nodes.

III. Conclusion and Future Enhancement

Vehicular ad hoc networks (VANETs) are special class of Ad hoc Networks. Vehicular ad-hoc network (VANET) is an ad-hoc network which is an important approach used in the intelligent transportation system (ITS). Vehicular Ad Hoc Network is characterized by its highly mobile topology. The vehicles in the network move on the road and create the very high mobility of the nodes. VANET suffers the problem of malicious nodes that misbehaving by sending the false information either by their false location or false information packets. Dealing with these nodes in VANET is more challenging due to the increased ambiguity in the detection caused by the high mobility of vehicles. Lot of work is performed to identify these nodes. Different authors gave the algorithm to identify the misbehaving node.

In this work the MAND Model is proposed to overcome the limitations of previous work. The algorithm is proposed, designed and implemented. This algorithm detects the misbehaving node and does not communicate with these nodes. The model works in two phases. First phase detect the malicious node at the RSU and in second phase the node is again checked by the packet transferring node. The two phases tries to completely remove the malicious node. This model removes the extra packets from the network and congestion of the network decreases. The algorithm uses the routing protocol FFRDV for packet transfer in the network. The algorithm is implemented in the MATLAB 2013. The various experiments are performed and results obtained. The delay and attacked node percentage is obtained. From the analysis of result it is found that the delay is below the 70 ms for the maximum number of nodes for packet=1 and the delay is below the 89 ms for the maximum number of nodes for packet = 10. The MAND model detects approx 57.6 % attacked node in the network for packet = 1 while the attacked node identification percentage is from 12% to 12.64 % for packet = 10. The MAND Model gives better results for packet=1 for each node.

In this work FFRDV routing protocols is considered. Only packet =1 and packet =10 is taken. In future other routing model can be taken. Along with this number of packets can be increased. The behavior of model can be observed for different conditions. By using this network can be improved.

References

[1] Geetha Jayakumar and Gopinath Ganapathi, "Reference Point Group Mobility and Random Waypoint Models in Performance Evaluation of MANET Routing Protocols", Journal of Computer Systems, Networks, and Communications, Volume 2008.
[2] Jochen H. Schiller, "Mobile Communications", Second Edition, Pearson Education Limited, 2003.
[3] Arun Kumar, "Enhanced Routing in Delay Tolerant Enabled Vehicular Ad Hoc Networks", International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012.

[4] Archana Harit, N C Barwar, "Comparative Analysis of Identification of Malicious Node in VANET using FFRDV and ERDV Routing Algorithm", 6th International Conference on Recent Innovation in Science, Engineering and Management, IIMT College of Engineering, 20 August 2016.
[5] Jani Kurhinen, Jukka Janatuinen, "Delay Tolerant Routing in Sparse Vehicular Ad Hoc Networks", Acta Electrotechnica et Informatica, Vol. 8, No. 3, 2008, 7–13.
[6] Mainak Ghosh, Anitha Varghese, Arzad A. Kherani and Arobinda Gupta, "Distributed Misbehavior Detection in VANETs", WCNC 2009 proceedings, IEEE 2009.
[7] Mrs. M. Sivajothi & Dr. E.R. Naganathan, Analysis of Reference Point Group Mobility Model in Mobile Ad hoc Networks with an Ant Based Colony Protocol",
[8] Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong.
[9] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", Springer Science+Business Media, LLC 2010
[10] Amit Mane A., "Privacy Aware VANET Security: - Sybil Attack Detection in VANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 4, April 2017 ISSN: 2277 128X.
[11] Chaker Abdelaziz Kerrache, Carlos T. Calafate, Juan-Carlos Cano, Nasreddine Lagraa, Pietro Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview", IEEE Access, Received December 1, 2016, accepted December 20, 2016, date of publication December 26, 2016, date of
[12] Attacks in Vehicular Adhoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 167 – No.1, June 2017.
[13] Shivangi Nigam, Abhishek Bajpai, Neeraj Kumar, "Signal and Time Based Fuzzy Cluster Scheme to Detect Sybil Attack in VANET", International Journal on Computer Science and Engineering (IJCSE), Vol. 9, No.07, Jul 2017.
[14] Prachi Chauhan1, Hardwari Lal Mandoria2, , "An Empirical Study of Vehicles Communication in Vehicular Ad-Hoc Network", International Journal of
[15] Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 3, March 2017.
[16] Vimal Bibhu, Kumar Roshan," Performance Analysis of Black Hole Attack in VANET", I. J. Computer Network and Information Security, 2012, 11, 47-54
[17] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan, "Early Detection Of DOS
[18] Attacks In VANET Using Attacked Packet Detection Algorithm(APDA)", International Conference On Information Communication And Embedded Systems ICICES 2013
[19] Uzma Khana, Shikha Agrawala, Sanjay Silakaria, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks", Procedia Computer Science 46 (2015) 965 – 972
[20] Sonia, Padmavati, "Performance analysis of Black Hole Attack on Vanet"s
[21] Reactive Routing Protocols", International Journal of Computer Applications (0975 – 8887) Volume 73– No.9, July 2013
[22] M. Milton Joe, R.S. Shaji, K. Ashok Kumar, " Establishing Inter Vehicle Wireless Communication in Vanet and Preventing It from Hackers", I. J. Computer Network and Information Security, 2013, 8, 55-61
[23] Omar Abdel Wahab, Hadi Otrok, Azzam Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles", Elsevier, Computer Communications 41, (2014), 43–54.
[24] Ravneet Kaur, Nitika Chowdhary, Jyoteesh Malhotra, "Sybil Attacks Detection in Vehicular Ad Hoc Networks", International Journal of Advanced Research (2015), Volume 3, Issue 6, 1085-1096.
[25] Mandeep Kaur, Manish Mahajan, "Movement Abnormality Evaluation Model in the Partially Centralized VANETs for Prevention Against Sybil Attack", I.J. Modern Education and Computer Science, 2015, 11, 20-27.
[26] Harsimrat Kaur,Preeti Bansal, "Efficient Detection & Prevention of Sybil Attack in VANET", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9, September 2015.
[27] Danlei Yu and Young-Bae Ko," FFRDV: Fastest-Ferry Routing in DTN-enabled Vehicular Ad Hoc Networks" , Feb. 15-18, 2009 ICACT 2009
[28] Stephen J. Chapman, "MATLAB Programming for Engineers", ISBN-10: 81-315-0228-7, Cengage Learning India Private Limited, New Delhi, 2004

