Volume 3, Issue 12, December 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Self Designed Secured Mobility Pattern in VANET

Anjali Jain*, Ritin Behl, Manish Srivastava
Department of IT
India

Abstract— — As the traffic is increasing day by day. Security of VANET (Vehicular Adhoc Network) along with privacy of drivers is major challenging task. The behaviour of drivers is getting worst day by day and it is reflected in the mobility pattern of drivers on the road. Vehicles who behaved roughly are threat to the Safety Since, VANET is a form of ephemeral networks, mobility issues have to be taken seriously. Detection of those vehicles will lead to increase security and privacy. Mobility pattern will be changed to maintain security in VANET. In this paper the mobility pattern is introduced to detect misbehaved nodes in VANET. Algorithm is designed for vehicles to design its mobility pattern to reduced accidents and increased safety in VANET. Simulation is done using Qualnet 5.0.

Keywords— VANET, LAM, Sybil attack, OBU's, DynaBIP.

I. INTRODUCTION

VANET is like mobile ad hoc network with constitutes between neighbouring vehicles. VANET's consists of two types of nodes: Vehicles and Roadside Stations. VANET is of two types Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Vehicular communication Systems are emerging two types of network, in which vehicles and road side units are the communication nodes, providing each other with information, such as safety warnings and traffic information.

In VANET vehicles are equipped with On-Board Units (OBU's). On board means computing incorporated into the main circuit board of a computer or computerized device or we can say installed and functional with a device. Vehicles are smart and intelligent enough to communicate and compute. VANET suggest unlimited advantage to companies of any size. Vehicles access of fast speed internet which will change automobiles the onboard system from an effective widget to necessary productivity equipment, making nearly any internet technology accessing on cars. Safety related issues are real time and mission critical so strict guarantee of safety and reliability is required. Ssafety, infotainment, financial and navigational are application areas of VANET's. The safety related information should be reliable to rely on. As the mobility pattern is high in VANET and vehicular moving pattern is changing rapidly, so frequent disconnectivity is very common in VANET's. The network topology changes frequently due to movement of nodes in and out in range of other vehicles. In rush hours traffic density also changes highly, so traffic density changes over time. These make security of Vehicles a very challenging task.

Most of the drivers misbehave which reflects the mobility pattern of vehicles. Vehicles who misbehaved create threat to safety, VANET's security and privacy. Some vehicles issue false alerts due to some internal or some failure bus some vehicles misbehave intentionally due some personal reasons or they want to trouble other just to enjoy. These are also called malicious nodes. They may have some motives to cause accidents and may gather sensitive information about other nodes like, credit card number from RFID signals at an electronic toll station [2], [3], [5]. So it's an important task to detect misbehaving nodes drivers or vehicles. Lot of the work is done on misbehavior detection in VANET. Mostly done on data centric misbehavior detection in VANET rather than physical pattern based misbehavior detection. Our aim is to improve safety as well as privacy and security in VANET's on basis of physical mobility pattern. The paper is presenting mobility pattern based misbehavior detection in VANET's. The detection method is based on sharing of location and time and previous knowledge periodically among vehicles. On the basis of those data vehicles can itself decide whether behavior is normal and abnormal and hence can detect misbehavior node and can take decision. It exploits LAM, location anonymous vehicle, which help in improving privacy along with safety. The required information level and awareness can be achieved by exchange of periodic status of messages (beacons) among neighboring vehicles together with quick dissemination of information about potential hazards by identifying malicious nodes. In other section the paper will briefly describe relation between security misbehavior in VANET's. It also describes the importance of misbehavior node detection. The technology that provides each vehicle worth required information about its surrounding in order to assist the driver avoiding potential dangers. Other section will give brief overview of related work. The very other section will give overview of proposed work. Simulation result will show how justified the proposed approach is. Lastly,the work for some future.

II. MISBEHAVIOUR IN SECURITY AND PRIVACY OF VANET'S

In VANET's the misbehaviour nodes insider or outsider can be one. The authorized node is a insider node that intentionally or unintentionally take unauthorized or undesirable actions, like modify, fabricate, drop message in

© 2013, IJARCSSE All Rights Reserved

addition to impersonate other node identities. Insider can easily break safety rules and can lead to serious accidents as they can easily drop messages. Like Sybil attack is a serious type of malicious attack, it creates illusion of traffic congestion by claiming multiple existing identities. Side by side it can also disseminate critical time safety applications. It may leave serious and saviour effect on life of people. On the other hand outsider node is a kind of intruder that aims to intercept, misuse or denial of the communications among VANET's nodes. Outsider attack is limited and can be accessed using the cryptography mechanisms. Privacy can be ensured, as the vehicle must be able to resist the tracking, and a message must not be linked to the sender vehicle. Behavioural tendencies of drivers can be reflected by the movement of vehicles. A safe driver observes the behaviour of his/her drivers surrounding vehicles like left, right, rear and front then drives accordingly with safety. Smart driver always observes the neighbourhood carefully and keenly to estimate the safe location to keep him/herself away from danger in case of sudden mishap or accidents. But the drivers who want to create mishap might not take care of all misbehave selfishly.

In VANET one can see the misbehaviour in two perspectives 1) physical movement and 2) information security perspective. When physically vehicle with abnormal and greedy driver drive crazily, which reflect the mobility pattern. These are those drivers who want their benefit and maximize their gain, causing the safety threat to the system. In other case vehicles who want to break security or create security threat to other neighbouring nodes give false or wrong information. In such type of information two types of false information may hit each other. Hence, the detection of one will help detection of other. In information security attack "intelligent Collision" which works on convincing one vehicle to slow down while the vehicle behind it to speed up. This type of attack will result in physical movement. This false information may be generated intentionally or for selfish reasons or unintentionally by faulty sensor or loss of some signals. In congestion control a greedy driver may also convince other drivers that there is congestion ahead to clear his/her path. This will also result in physical mobility pattern.

Exploration of location/position, speed, RSU_id and information of time from surrounding vehicles can be used in generating the mobility pattern of vehicles, which may help us to detect and prevent security attacks related to false position information of vehicle. For detecting misbehaviour node information may be required UID (unique identification), like licence plate, as it can compromise privacy of drivers[8]. For privacy location or position information is required. Location Anonymous Message can be used to capture the location information without help of identification and it will perverse privacy.

III. RELATED WORK

Mostly work has been done on data centric misbehaviour detection. Less amount of research is done on physical pattern based misbehaviour detection in VANET. Golle et al [9] create a model to detect misbehaviour in VANET. This model consists of all possible events in the network. If at time instant any event observed by another node is checked with the model. Some details are in model if event is valid according to model then the message is considered to correct one, otherwise false one. The problem with this approach was it is not significant to real VANETs data and also not shown how that data may be taken or maintained. In VANET building global database is really a great job and that will not preserve privacy. Many solutions [10], [11], [12] have been proposed to detect Sybil attacks in VANETs. A malicious node can give false location information and defeat all schemes, although the precise location of a node is known. One author proposed a scheme to detect and revoke a malicious node. Certificates are revoked, to revoke a node. To each pseudonym correspondingly there is one public/private key pair and a certificate issued by certificate authority.

One more scheme to evaluate the behaviour of vehicles proposed by Robert. A framework is proposed to analyse the behaviour, it consists modules on the basis of that trustiness of vehicles is performed. A value is assigned as a trustworthy number to each vehicle which was exchanged among all vehicles, building up reputation. This scheme is dependent upon the previous knowledge, history of all other vehicles. As it is based upon history, privacy is not preserved since the vehicle can investigate the previous information or history of any vehicle. From security point of view vehicles cannot falsify their location, but can evaluate vehicles wrongly and can share wrong information. This totally disturbs the security and reliability of system reacting to safety messages. The key factor in VANET safety applications is time. Tviour has his process to analyse, evaluate and share trustworthiness value among vehicles is not much useful.

The detection of misbehaviour of vehicles with integrated root cause analysis is presented by Ghosh. They investigated post crash scenarios, in which they compared actual and expected trajectory to decide whether node is sending correct post crash alert correctly. Nodes possible behaviour is noted and than expected trajectory is modelled. Assuming that node always send the correct location information, which is not a valid assumption, as the nodes might send wrong information and can make other nodes to believe on the same. Small position change can lead to huge change in trajectory and that will result in lane change. Human behaviour also reflects in the movements of behaviour. Due to some failures vehicles can issue false alerts due to some internal and external faults. Malicious nodes might have some criminal motives to cause accidents or to disturb the mobility pattern or may also attempt to gather sensitive information about other nodes, e.g. credit card number from RFID signal at electronic toll station. It's not like our system like sensor enriched RSU's along with GPS, that mainly rely on faulty sensor can generate false alarm as it is not malicious intent and will wrongly fine and revoke security of node security credentials respectively. Anonymous Location-Aided Routing [5] in suspicious MANET's framework uses nodes correct location to construct a secure MANET map. In MANET node authentication, data integrity, anonymity and tracking resistance provided by Alarms. Alarm ensures privacy and security preserving state. Alarm also focuses on current locations of nodes to securely determine the topology and also construct topology to visualize node and similar graph connectivity. The security strength of alarm in routing protocol is that it provides secure forwarding by injecting some advanced cryptography mechanisms such as digital group signature.

© 2013, IJARCSSE All Rights Reserved

IV. OVERVIEW OF THE PROPOSED SOLUTION

Our proposed solution for VANET relies on the location, speed and corresponding time. Location coordinates will be used to represent the existence and identity of vehicle and at present where it is. Through its present location and speed other will be able to get the correct information and it will help to correct mobility pattern. Location, speed and information of time will be very important to preserve the accidents and for security in VANETs. Our detection/privacy or simulation method will rely on location coordinates of vehicles, speed along with RSU's information from where it is getting previous information.

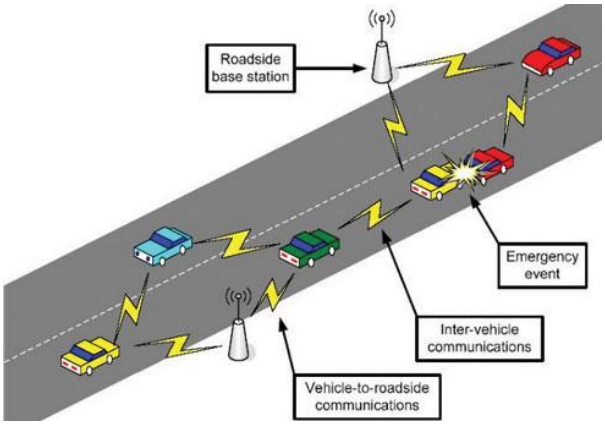

Figure1. VANET's Communication System

As the RSU's supposed to have all the information related to neighbouring one or other RSU's along with mobility pattern of the area. In this paper RSU signature scheme will be used so that any vehicle or RSU will be able to get the current information or previous information. On the basis of that vehicle may be able to judge or calculate the malicious vehicle itself or can be able to get the accidental prone lane or mobility pattern. So the node may be able to take decision to avoid that path to prevent from accidents. Also a change in location coordinates of vehicles behind other vehicle is treated as threat or faulty situation that can be due to some external attack of misbehaving node.

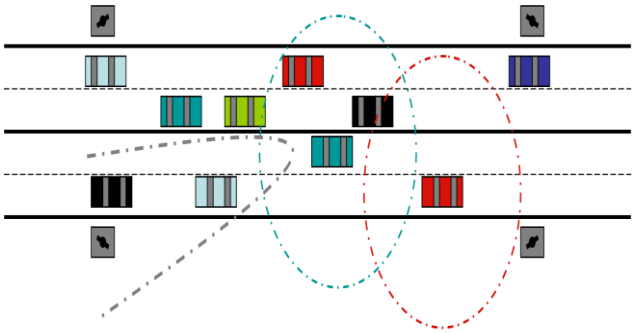

Figure 2: Nodes broadcasting its Location Coordinates

To maintain privacy of vehicle each node is communicating with its dynamic location so the location cannot be linked to any specific vehicle to be tracked. Location coordinates are captured time to time. For security in VANET, time slot is decided for broadcast, after each time slot location coordinates, speed, RSU_id, time will be broadcast with security message to preserve security in VANET. For broadcasting information and location coordinates, we will use DynaBIP (Dynamic Broadcast Incremental Power Protocol) to reduce cost of construction, less transmit power and also to avoid unnecessary flooding. Using DynaBIP broadcast reaches to as a maximum node as possible as broadcasting is done with its full power.

DynaBIP is used rather than flooding as flooding is too costly and it requires lots of transmits power and incurs high cost of construction. Also there is lots of redundancy in flooding.

Algorithm 1: DynaBIP(Dynamic Broadcast Incremental Power Protocol)

Minimum incremental cost link selection.
MinimumCost ← ∞
for all R_i € RouteCache do
incrementalCost ← C_{ij} - T_i
if incremental cost < MinimumCost then
MinimumCost ← incrementalCost
parent ← i
MinimumRoute ← R_i
end if
end for

© 2013, IJARCSSE All Rights Reserved

As discussed in, DBIP tree is constructed and it is based on the principles of BIP in a single sweep across the network. It is a centralized algorithm that uses a variation of MST (minimum spanning tree) to construct a broadcast tree with an approximation [12]. As there is lots of variation of BIP (broadcast incremental protocol) distributed version of Broadcast Incremental Power (BIP) is used to provide energy-efficient dissemination for dissemination phase. It allows minimum energy broadcast tree for dissemination of packets to all nodes in the network with least energy and minimum cost at least as possible. This process reduces contention with minimum packet loss due to collision. DBIP constructs distributed broadcast tree on the basis of received signal strength measurements to estimate link costs. BIP is constructed by selecting link with minimum incremental cost at each iteration. At each node and link provided with smallest incremental cost among the nodes are added to tree. The nodes or vehicles which have less transmission range will be selected first. Global information will be needed to select the order of nodes for iteration. So, overhear signals may be able to approximate the order in which they should be added.

The tree construction of DBIP can be completed with a single sweeping flood across the network. The source node (RSU) will initiate the tree construction by broadcasting the first packet. It will include in the header of the packet it's transmit power, Psrc and the route to this node (a null array for the source). After each time slot nodes broadcast its present location coordinates to RSU and other neighbouring nodes/vehicles. This broadcasting is done periodically. The message contains location coordinates, time, RSU_id within its range. Each node get the information and periodically update its table, which will be used as database for investigation of further movement and to analyse any incoming alert message or to prioritize alert message.

V. OVERVIEW OF THE PROPOSED SOLUTION

In VANET's nodes require location coordinates and they may constrain to a fixed physical pattern referenced to a road structure. Now, to find misbehaviour nodes, or to detect misbehaving nodes, some assumptions are made. Which are based on location coordinates as:

1. Each vehicle are obtaining its correct position via GPS reference to RSU.
2. All vehicle nodes should synchronize a time with road side unit.
3. Movement of node should be periodic; any change in movement or stop is an update for driver for some threat or any security measure.

A. Each node prepares and broadcast location coordinates along with current RSU and safety message. As proposed method relies on location coordinates. So, each node maintains a table for location coordinates message after each broadcast or each time updates table for mobility pattern. With the help of physical map and previous database, each node verifies its collected information and if location coordinates are not within the stored database or link table that vehicle can be a threat to the VANET's, as it is violating mobility pattern. The node and RSU will remove that location coordinates from the pattern and that node has to be investigated. Safety message will be broadcast for that location coordinate to avoid threat or accidents. Location coordinates will help node to build its mobility pattern and to evaluate safety and integrity of other nodes in network. A vehicle can periodically broadcast its location coordinates its current location, RSU information without any fear of being tracked.

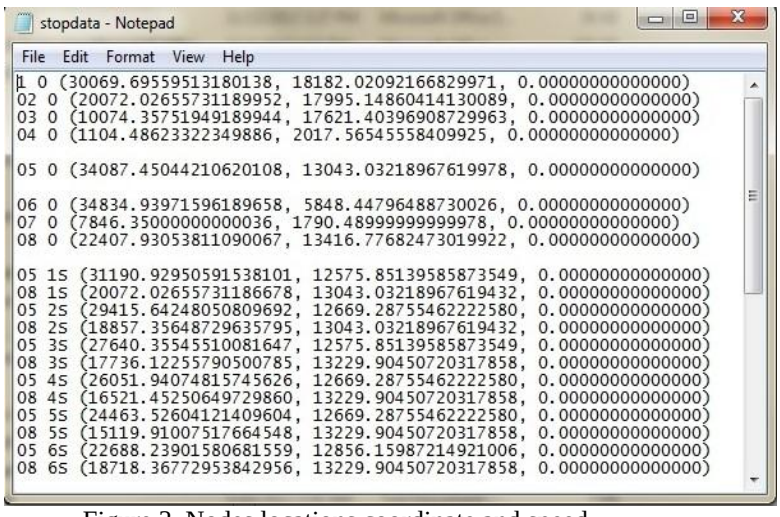

Figure 3. Nodes locations coordinate and speed.

B. Mobility pattern formation and detection of misbehaving nodes is the main focus of this paper. Every time each vehicle is assumed to gather the location coordinates of other nodes, but it might be possible that any of the node coordinates missed or any of them might not useful. As discussed above the table will be maintained with location coordinates, RSU_id, speed, location. To maintain table with real time, time slots will be divided into chunks. Time slot is less than frequency of communication in VANET. It is noted that well behaving nodes always follow speed regulations and maintain some standard range of speed. Any change in speed beyond threshold range means there must be some problem in that node. The problem can be natural or some intentional. Node uses location coordinates for creating mobility pattern of it and nodes ahead it.

© 2013, IJARCSSE All Rights Reserved

Algorithm for Mobility Pattern and Misbehaviour Detection.

ALGORITHM:

For each node **do**

Receive incoming signals \\(location coordinates with time and speed)
if received
validate node from table using signature
if valid
keep in database
else
remove from database \\ (vehicle\node not valid can be malicious node
compare time of database with time of vehicle
if different **then**
remove node \\ (node vehicle can be an insider)
end if
verify location coordinates **then**
if conflicts then
remove \\ (node could be misbehaving insider)
end if
compare node present coordinates with database
if available then
pass, store location in database
else **if**
remove **it** \\ (for maintaining vehicle that are in front or this node)
end for.

VI. SIMULATION

The simulation of this paper is done using Qualnet. It's a network simulator. During simulation, it is shown that the user observe the signals being transmitted and received at each node, which helps in understanding what is happening. The three main programs used in QualNet are the simulator, the analyzer and the packet tracer. The simulator runs the given simulation, the analyzer displays the results and the packet tracer allows us to follow the path of a packet through the network. And the protocol is developed from C++ coding. Then the user calculates the location coordinates. The vehicles than broadcast location coordinates, RSU_id, speed and time further using DynaBIP. After broadcasting neighbouring nodes receive signals and observe the location coordinates, speed and time of other vehicles. Location coordinates are compared with the previous maintained database, if coordinates are within the database then its ok, kept in database table. If coordinates are not within the database then that node is treated as malicious node and will be dropped. After checking the validity of received signals node behind the nodes can make their mobility pattern itself, as shown in figure. After that node will follow its mobility pattern. After each time slot mobility pattern will be created accordingly and will be followed for safety and to get safe and secure route without the threat of accident.

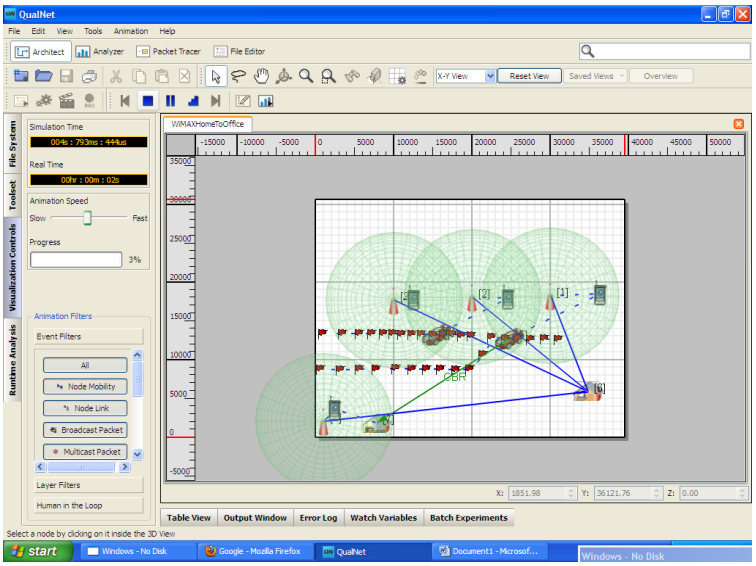

Figure 3. Vehicles broadcasting information to other node

Figure 3 shows that location coordinates are being calculated and broadcasted further to all other nodes/vehicles. As it is shown in the figure two vehicles broadcasting location coordinates, speed, RSU_id and time. The information is gathered at node and RSU to calculate or observe the pattern.

© 2013, IJARCSSE All Rights Reserved

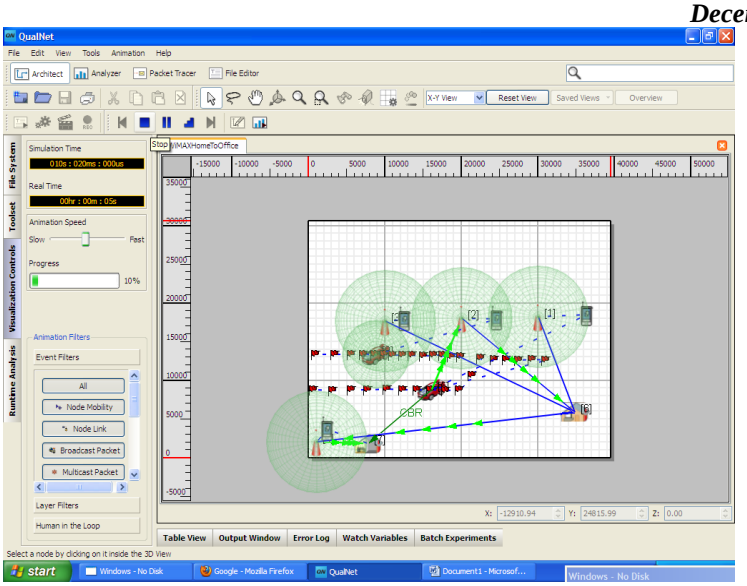

Figure 4. Vehicle changes its route accordingly

Figure 4 Shows that after observing that there is threat ahead in the path the vehicle moving behind designed or modifies its mobility pattern and change its path.

VII. RESULTS

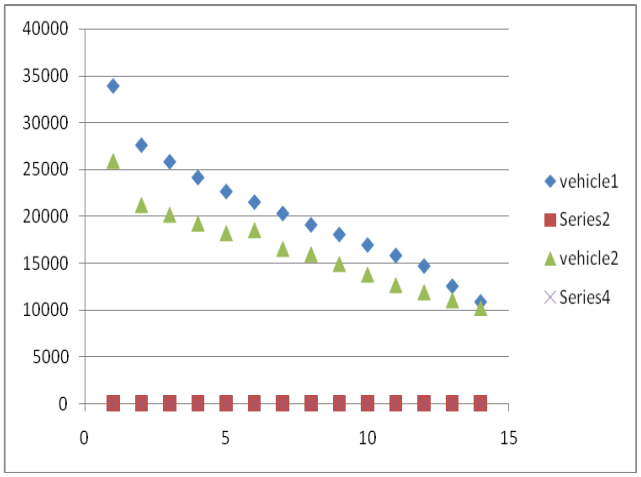

Figure 5. Vehicle compares information and observes the threat

First graph shows that vehicle1 and vehicle2 are exchanging information between nodes and preserve accidents.

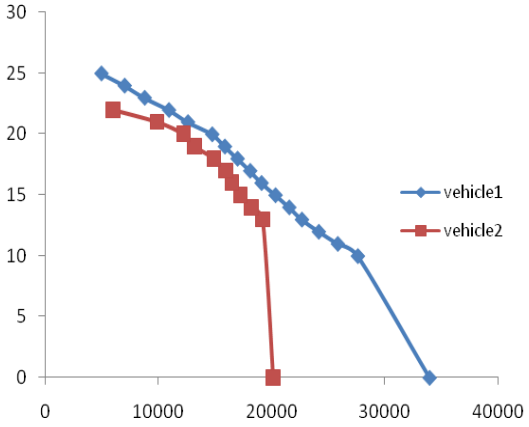

Figure 6. Vehicle changes its path modifies mobility pattern.

© 2013, IJARCSSE All Rights Reserved

First graph shows that vehicle1 and vehicle2 is creating its mobility pattern after getting location coordinates of other nodes.

VIII. CONCLUSION

This paper gives you the conclusion that the vehicle/node creates its mobility pattern on the basis of information e.g. location coordinates, RSU_id, speed and time. On the basis node takes the decision to avoid threat coming to it. The mobility pattern contributes in taking a vehicle to a secure location or making right decision at time instant. This approach helps a lot in VANET's to improve safety and security. As the only aim of Vehicular Adhoc Network to provide vehicle safe and secure environment.

REFERENCES

[1] A. Jain and D. Yadav, "Reprogramming in VANET", IJCEEE, vol 2, issue 1, pp. 2249-9997.
[2] J. Sun and Y. Fang, " Defence against misbehaviou anonymous vehicular ad hoc networks," Ad Hoc Networks, Vol.7, no.8, pp.1515-1525, 2009.
[3] M. Ghosh, A. Varghese, A.gupta, A.kherani and S.Muthaiah, "Detecting misbehavior in vanet with root-cause analysis," Adhoc Networks, vol.8, no.7, pp.778-790, 2010.
[4] S. Ruj, M.A. Cayennaghi, Z. Huang, A. Nayak, and I.Stojmenovic, " On data centric misbehavior detection in vanets," in Vehicular Technology Conference (VTC Fall), 2011 IEEE, IEEE,2011, pp.1-5.
[5] K. EI Defrawy and G.Tsudik, " Alarm: Anonymous location-aided routing in suspicious manets," IEEE Transactions on Mobile Computing, vol.10, no.9, pp.1345-1358, sept.2011.
[6] R. Vijayan, S. Singh "A Novel Approach For Providing Security in Vehicular Adhoc Through Vehicles Present in the Network," in IJARCS, vol.2, no.1, jan.2011.
[7] J. Champ, A. Elisabeth Baert, V. Boudet, "Dynamic localized broadcast incremental power prorocol and lifetime in wireless adhoc and sensor network," wireless and mobile networking, IFIP Advances in Information and communication Technology, vol 308, pp.286-296.
[8] F.Farnoud and S. Valaee, "Reliable broadcast of safety messages in vehicular ad hoc network," in Proc. IEEE INFOCOM, Apr.2009, pp. 226-234.
[9] Q.Xu, T. Mak, J. Ko and R. Sengupta, "Vehicle-to-Vehicle safety messaging in DSRC," in Proc. ACM VANET, Oct. 2004, pp.19-28(2002).
[10] A. Festag, A. Hessler, R. Baldessari, "Vehicle to Vehicle and road side sensor communication for enhanced road safety," Nec Laboratories European Shell.
[11] M.T.Moreno, J.Mittag, "Vehicle to Vehicle communication: Fair Transmit Power Control for Safety Critical Information",IEEE trans on vehicular technology, vol.58, no.7, sept.2009.
[12] F.Farnoud, S.Valaee, "Relaible Broadcast of safety Messages in Vehicular Adhoc Network", IEEE Communication Society, ieee infocom, 2009.
[13] P. Golle, D. Greene, and J. Staddon, " Detecting and correcting malicious data in vanets," in proceeding of the 1st ACM international workshop on vehicular ad hoc network, ACM, 2004, pp.29-37.
[14] T. Zhou, R.R. Choudhary, P.Ning, and K. Chakrabarty, "Privacy preserving detection of Sybil attacks in vehicular adhoc network," in MobiQuitous-2007. IEEE, 2007, pp.1-8.
[15] S. Park, B. Aslam, D.Turgut and C.C.Zou, " Defence against Sybil attack in vehicular adhoc network based on roadside unit support," in military communications conference, 2009. MILCOM, IEEE 2009, pp. 1-7.
[16] R.Hissain, S. Kim, and H.Oh, " privacy-aware vanet security: putting data-centric misbehavior Sybil attack detection schemes into practice," in information security applications, M.Y.Dong Hoon Lee, Ed. Springer, 2012.

© 2013, IJARCSSE All Rights Reserved