Detect the Sybil Attack by using GPSR Protocol

Sheenam Arora
SBSSTC, Ferozepur

Chakshu Goel
SBSSTC, Ferozepur

ABSTRACT

VANET is a vehicular ad hoc network. This is a part of mobile ad hoc network. VANETs also called as intelligent transportation system (ITS) in which vehicles convey to give auspicious data. Their point is to give security, information and management of network. Rather than of their numerous advantages vehicular network is inclined to various attacks. Like prankster attack, denial of service attack, black hole attack, alteration attack, fabrication attack, man in the middle attack, timing attack, illusion attack and so forth. In this research we will attempt to uproot Sybil attack in which node creates its multiple identities and it can be affected by various ways. In previous research researcher judge the estimated physical measurement on the bases of three parameter but it may also be the case that message delay occur due to various another reasons like queue problem, congestion problem, accidental problem, so this approach is not accurate due to absence of GPS. According to this work GPSR protocol will be used through which physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If GPS coordinate matched then there is no attack.

Keywords

DSR, Vanet’s, WSN, GPSR, GPS

1. INTRODUCTION

A (VANET) utilizes autos as mobile nodes in a MANET to create a moving network. A VANET turns turn participating car into a wireless node which allowing cars 100 to 300 meters of each other to connect and create a network with a wide range. As cars fall out of the sign range and drop out of the network, different cars can meet in, interlink vehicles to one another so that a moving network is created. It is estimated that first systems that will be this technology are fire and police vehicles to communicate with each other for the purpose of security.

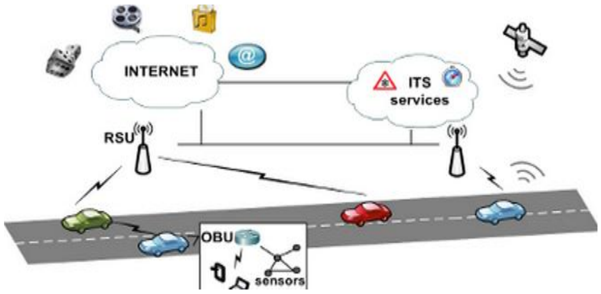


Fig 1.1: VANET

The connectivity is done among one vehicle to other vehicle and vehicle to road side infrastructure and vehicle or road side infrastructures to the central authority responsible for the network maintenance.

The basic method for message transfer is the short range radios that are being introduced in any of the nodes. The short transmission node is utilized by vehicular node. RSU's are spread sporadically or consistently relying upon the organization of the system in a specific locale. In reality spread sporadically. They act as a mediator node in between the Central Authority (CA) and Vehicular Node (VN). Vehicular Ad-Hoc Network is the mesh in which communication has been done between road side units to vehicles, vehicles to vehicles in a range of 100 to 300 m. Existing authentication protocols to secure vehicular ad hoc networks raise challenges like as certificate distribution and revocation, avoidance of communication and computation bottlenecks, and decrease of the strong reliance on tamper proof devices. In a VANET, vehicles will depend on the integrity of received data for deciding when to present alerts to drivers. This data may be on the basis of control decisions for autonomous vehicles. If this information is corrupted, vehicles may present unnecessary or erroneous warnings to their drivers, and the information based on the results of control decision could be even more disastrous. Information can be corrupted by two different mechanisms: malfunction and malice. Similarly, vehicles have two defense mechanisms: an external reputation information and internal filter.

1.1 Characteristics of VANET

- High Mobility: The nodes are moving quickly in VANETs. This makes hard to know a node's position and assurance of hub protection. As a result of this, VANETs tends to change frequently in network topology.
- Unbounded network size: VANET can be actualized for one city, several cities, one state and numerous states or for nations. This means that network size is geographically unbounded in VANET.
- Frequent exchange of information: The ad hoc nature of VANET stimulates the nodes to collect data from the other vehicles and road side units. Hence the data exchange among node gets to be visit.
- Wireless Communication: VANET is made for the wireless environment. Nodes are joined and exchange their information via wireless. Therefore, in communication, some security steps must be taken.
- Time Critical: Within time constrain, the information in VANET must be conveyed and received by the nodes. So that a decision can be taken by the node and take action accordingly.
- Sufficient Energy: The VANET nodes have no issue of calculation assets and energy. This allows VANET to use demanding techniques such as ECDSA, RSA implementation and also gives illimitable transmission power.
- Better Physical Protection: The VANET nodes are physically protected. Thus, VANET nodes are harder to compromise physically and decrease the impact of framework attack.

1.2 Various type of attackers

a) **Insiders Vs Outsiders:** In a network, a member node who can communicate with other node of the network is called as an Insider and can assault in diverse ways. Outsiders are those who cannot communicate directly with the alternate nodes of the network have a constrained ability to assault (i.e.., have less variety of attacks).

b) **Malicious Vs Rational:** A malicious attacker utilizes different methods to damage the member nodes and the network without searching for its personal benefit. On the contrary, a normal attacker expects individual benefit from the attacks. Thus, these attacks are more unsurprising and follow some patterns.

c) **Active Vs Passive:** A dynamic aggressor can make new parcels to harm the network whereas a passive attacker only eavesdrop the wireless channel but cannot create new packets (i.e.., less harmful).

1.3 Attacks

There are various kinds of attack that can affect the entire system or can degrade the performance of system. The attacks can be categorized into following types.

a) Denial of Service attack

This strike happens when the attacker additions control of a vehicle's advantages or jams the channel of correspondence used by the Vehicular Network, so it makes tangle to send isolating data to its end of the line. It additionally extends the risk to the driver, on the off chance that it needs to depend upon the application's data. For example, in the event that malignant needs to make a colossal burden up on the roadway, it can make a disaster and use the Dos strike to keep admonish from arriving to the approaching vehicles. Creators in [7] discussed a response for Dos issue and saying that the current arrangements, for instance, bouncing don't absolutely handle the issue, the usage of distinctive radio handsets, working in disjoint recurrence groups, can be a conceivable approach yet even blueprint will oblige adding new and more contraptions to the vehicles, and this will oblige more supporters and more space in the vehicle.

b) Message Suppression Attack

An assailant specifically dropping packets from the system, these bundles may hold discriminating data for the beneficiary, the aggressor choke these parcels and can use them again as a part of other time.

The objective of such an assailant would be to keep enlistment and insurance powers from investigating accidents including his vehicle and/or to go without passing on accident reports to roadside access centers. Case in point, an aggressor may smother a blockage cautioning, and use it in an alternate time, so vehicles won't get the cautioning and compelled to hold up in the activity.

c) Fabrication Attack

An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personality.

d) Alteration Attack

This assault happens when aggressor modifies current information, it incorporates deferring the transmission of the data, replaying prior transmission, or changing the genuine section of the information transmitter. For example, an aggressor can modify a message telling different vehicles that the current street is clear while the street is congested.

e) Replay Attack

This assault happens when an aggressor replay the transmission of a prior data to exploit the circumstances of the message at time of sending.

f) Black hole Attack

When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node.

g) Grey hole Attack

This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcast.

h) Sybil Attack

In this attack, attacker makes different identities to re-enact diverse centers. Every hub send messages with various characters, accordingly distinctive hubs understand that there are numerous hubs in the system in the meantime. This assault is extremely unsafe on the grounds that a one hub can issue its different areas in the meantime and this making security risk. The Sybil attack in PC security is an assault where a reputation structure is subverted by delivering identities in distributed systems. In a Sybil attack the aggressor subverts the notoriety arrangement of a distributed system by making a considerable number of pseudonymous personalities, using them to get an unnecessarily tremendous effect. A notoriety framework's powerlessness to a Sybil attack depends on upon how reasonably identities can be made, the extent to which the notoriety structure acknowledges inputs from substances that don't have a chain of trust connecting them to a trusted component, and whether the notoriety framework treats all components indistinguishably. Affirmation shows considerable scale Sybil attack can be completed in an amazingly trashy and effective path in sensible frameworks like Bit Torrent Mainline DHT.

An entity on a peer to peer network is a bit of programming which has section to close-by resources. An element promotes itself on the shared system by showing a character. More than one character can identify with a lone component. At the end of the day, the mapping of characters to substances is various to one. Components in shared systems use diverse characters for purposes of repetition, resource offering, reliability and dependability. In shared systems, the personality is utilized as a deliberation so that a remote element can be mindful of characters without essentially knowing the correspondence of personalities to neighborhood substances. Of course, every unmistakable character is normally accepted to compare to a particular neighborhood element. Actually numerous characters may relate to the same nearby element.

A broken hub or a foe may exhibit numerous characters to a distributed system keeping in mind the end goal to show up and work as various unmistakable hubs. In the wake of getting to be a piece of the shared system, the foe might then catch interchanges or act noxiously. By disguising and displaying various characters, the enemy can control the system significantly.

2. PREVENTION OF SYBIL ATTACK

Validation techniques can be utilized to avoid Sybil assaults and reject disguising unfriendly elements. A nearby element may acknowledge a remote personality taking into account a focal power which guarantees a coordinated correspondence between a character and a substance and may even give a converse lookup. A personality may be accepted either straightforwardly or in a roundabout way. In immediate acceptance the neighborhood substance questions the focal power to accept the remote characters. In circuitous approval the nearby element depends on officially acknowledged characters which thus vouch for the legitimacy of the remote character being referred to.

Character based approval strategies by and large give responsibility to the detriment of namelessness, which can be an undesirable trade off especially in online gatherings that wish to permit restriction free information trade and open dialog of delicate subjects. An acceptance power can endeavor to safeguard client's obscurity by declining to perform reverse look ups, yet this methodology makes the approval power a prime focus for assault. Then again, the power can utilize some system other than learning of a client's genuine personality, for example, check of an unidentified individual's physical vicinity at a specific place and time.

2.1 GPSR

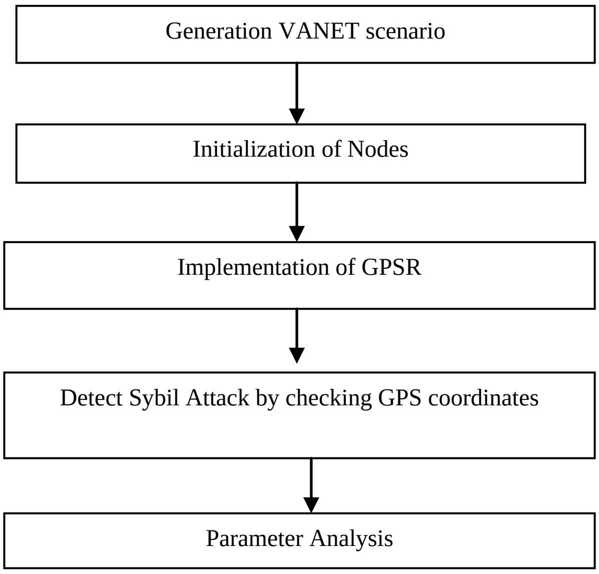
In wireless networks contained various versatile stations, the routing problem of finding ways from a traffic source to a traffic destination through a progression of intermediate forwarding nodes are particularly challenging. When nodes move, the topology of the network can change quickly. Such networks require a responsive routing algorithm that discovers valid routes rapidly as the topology changes and old routes break. Yet the constrained limit of the network channel requests efficient routing algorithms and protocols that do not drive the network into a congested state as they learn new routes. The pressure between these two objectives, responsiveness and bandwidth efficiency, is the embodiment of the mobile routing issue.

Greedy Perimeter Stateless Routing, GPSR, is a responsive and effective routing protocol for mobile, wireless networks. Unlike established routing algorithms before it, have which utilized graph-theoretic notions of most brief ways and transitive reach ability to discover routes, GPSR exploits the correspondence between geographic position and integration in a wireless network, by utilizing the positions of nodes to make packet forwarding decisions. GPSR utilizes greedy forwarding to forward packets to nodes that are dependably dynamically closer to the destination. In regions of the network where such an avaricious way does not exist (i.e., the main way requires that one move temporarily farther away from the destination), GPSR recovers by sending in perimeter mode, in which a packet navigates successively closer faces of a planar sub chart of the full radio network connectivity graph, until coming to a node closer to the destination, where greedy forwarding resumes.

3 METHODOLOGY

In previous work three routines were utilized to locate the physical estimation of message that was Time of Arrival (TOA), Angel of Arrival (AOA), and Received Signal Strength (RSSI). In previous research researcher judge the estimated physical measurement on the bases of three parameter but it may also be the case that message delay occur due to various another reasons like queue problem, congestion problem, accidental problem, so this approach is not accurate due to absence of GPS. According to this work GPSR protocol will be used through which physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If GPS coordinate matched then there is no attack. Firstly, scenario will be generated in which number of nodes will be initialized and then GPSR will be implemented on the bases of which GPS coordinates will be verified at any time. If some node is coming in the range of another node then its verification will be done on the bases of coordinates, in this way malicious nodes will be detected and verification will also be done by the RSU (Road Side Unit). In which RSU keep checking the identities of nodes and compare it with its node table, if two or more than two identities exist then attacker is identified.

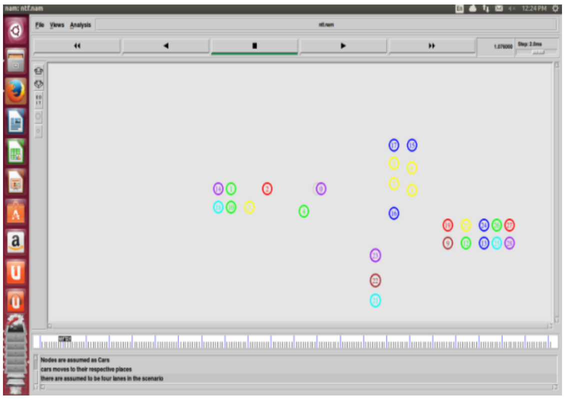
3.1 Flow of Work


Generation VANET scenario
Initialization of Nodes
Implementation of GPSR
Detect Sybil Attack by checking GPS coordinates
Parameter Analysis

3.2 Simulation Parameter Specification

Parameters	Values
Routing Protocol	DSR, GPSR
Number of Nodes	30
Simulation time	900 sec
Mac Protocol	Mac 802.11
Queue Length	50
Radio Propagation Model	Two Way Ground
Antenna	Omni Antenna
Simulation Area	1000*1000 m
Transmission Range	250 m

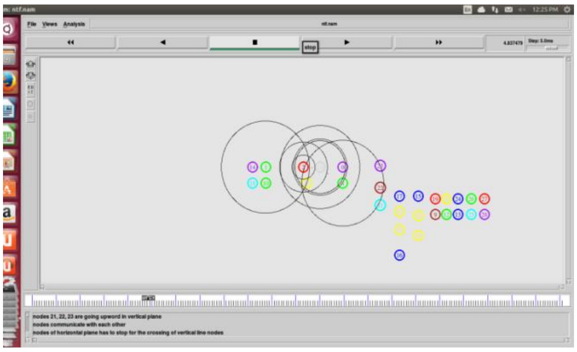
4 RESULTS



Nodes are assumed as Cars
cars moves to their respective places
there are assumed to be four lanes in the scenario

Fig 1. Represents Initialization of Nodes

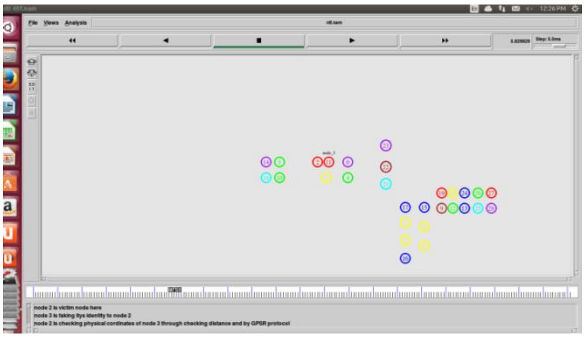
In above scenario cars are represented as nodes. There are four lanes in the scenario in which vehicles of right lane have to move (from right to left) in forward direction, vehicles on left lane have to move from left to right direction and vehicles of upward and downward road have to their respective places.



nodes 21, 22, 23 are going upword in vertical plane
nodes communicate with each other
nodes of horizontal plane has to stop for the crossing of vertical line nodes

Fig. 2 Represents Communication and Movement of Nodes

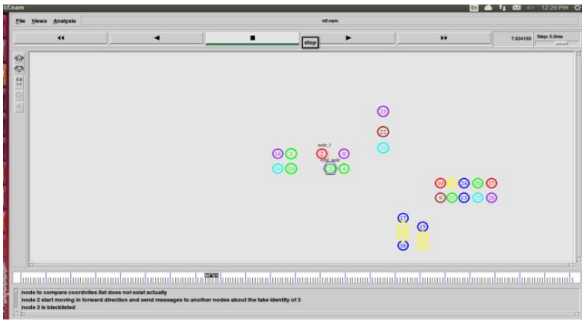
In above scenario it has been shown that nodes are communicating with each other and moving towards their respective destinations.



node 2 is victim node here
node 3 is faking ifys identity to node 2
node 2 is checking physical cordinates of node 3 through checking distance and by GPSR protocol

Fig. 3 Represents Sybil Attack

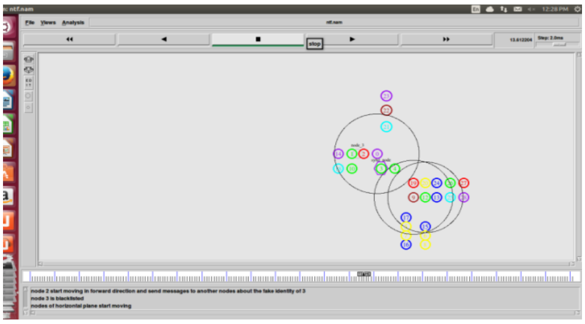
In above scenario node 2 acts as victim node and node 11 is act like a Sybil node, which is a fake identity of node 3. Here node 3 claims that it is present in front of node 2.



node to compare coordnites ttat does not exist actually
node 2 start moving in forward direction and send messages to another nodes about the fake identity of 3
node 3 is blacklisted

Fig. 4 Represents Avoidance of Sybil Attack

In above scenario has been shown that node 2 checked the GPS coordinate of node 3 and then calculated the actual physical position node of 3 through distance formula. In this way Sybil attack is avoided.



node 2 start moving in forward direction and send messages to another nodes about the fake identity of 3
node 3 is blacklisted
nodes of horizontal plane start moving

Fig. 5 Represents Successful Avoidance of Sybil Attack

In above Scenario it has been shown that after matching the coordinates Sybil nodes is declared as attacker and broadcast information to all other vehicles in the network.

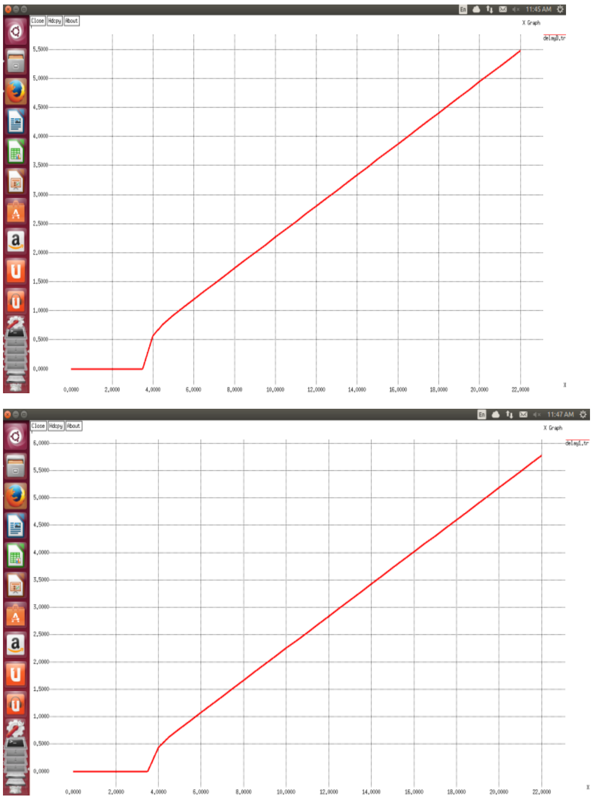


Fig. 6 Represents Delay

Above figure represent that delay for GPSR is little bit more than the delay for DSR protocol. Delay for DSR is 5.5 and delay for GPSR is 5.8

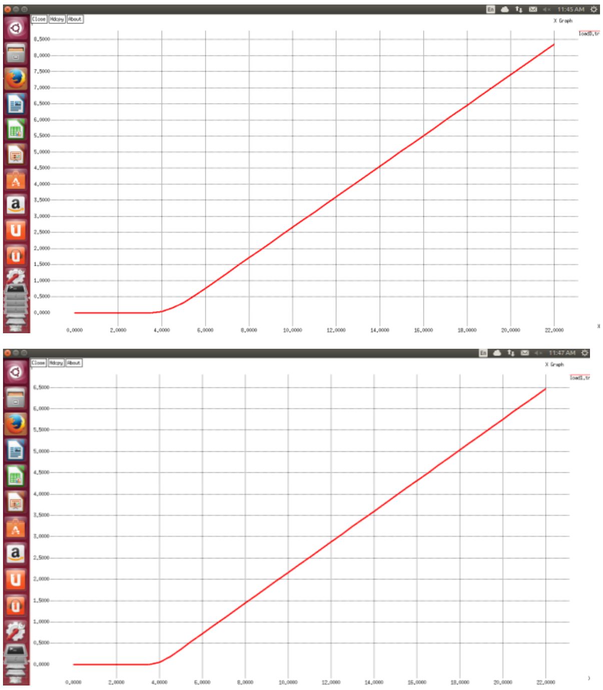


Fig. 7 Represents Load for DSR and GPSR

From this parameter we analyze that load for DSR protocol is 8.4 but for GPSR it is only 6.4. Which shows that GPSR is better than the DSR?

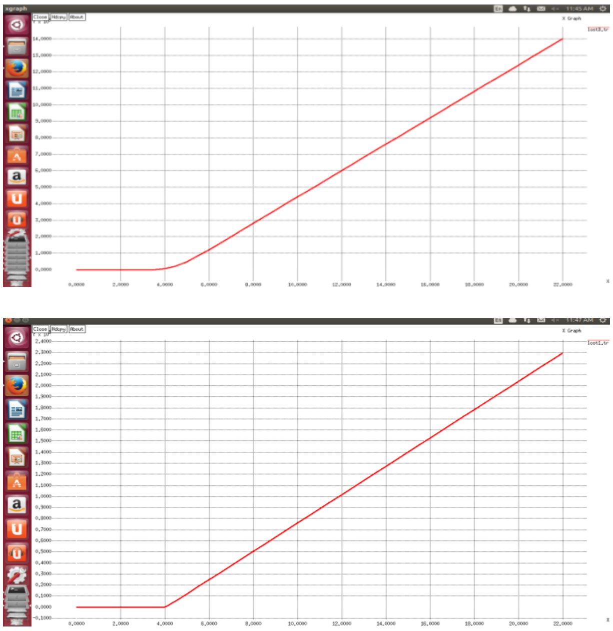


Fig. 8 Represents Loss for GPSR and DSR

Above figure shows that loss for DSR is more as compare to GPSR.

5 CONCLUSION

Security in VANETs is one of the major concerns in the safety of networks. But, because of security attack, VANTEs are facing so many serious issues which can degrade their performance. The attacks include Denial of Service attack, gray hole attack, black hole attack and fake message attack in the form of prank message. Hence, in this work GPS module is proposed which overcomes this issue in an efficient manner. The simulation results have been carried out showing that the attacks can be minimized when the nodes within VANETs get modeled with GPS module. The simulated results also reveal that the proposed scenario works in an efficient manner to diminish the prankster attack by selfish driver after the implementation of location aware nodes in VANETs. This research is concluded on the basis of some parameters (Network Load, Packet Delay and Packet Loss). These parameters are calculated for two protocols that is DSR and GPSR. It has been observed that one parameter gave better results with DSR (Packet Delay) on the other hand two parameters (Network Load and Packet Loss) gave better results with GPSR. In future this work can be tested for large number of nodes and this methodology can also be used to resolve another attacks.

6 REFERENCES

[1] Kumar, P.Vinoth, Maheshwari, M. “Prevention of Sybil attack and priority batch verification in VANETs” International Conference on Information Communication and Embedded Systems (ICICES), 2014, pp. 1 – 5.

[2] Dongxu Jin,JooSeok Song “A Traffic Flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad-hoc Networks” 13th International Conference on Computer and Information Science (ICIS), 2014, pp. 281 – 286.

[3] de Sales, T.M., Almeida, H.O., Perkusich, A., de Sales, L. “A privacy-preserving authentication and Sybil detection protocol for vehicular ad hoc networks” International Conference on Consumer Electronics (ICCE), 2014,pp. 426 – 427.

[4] Hussain, R.,Abbas, F., Junngab Son, Hasoo Eun “Privacy-aware route tracing and revocation games in VANET-based clouds” 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 730 – 735.

[5] Hussain, R., Junggab Son, Hasoo Eun, Sangjin Kim “Rethinking Vehicular Communications: Merging VANET with cloud computing” 4th International Conference on Cloud Computing Technology and Science (CloudCom), 2012, pp. 606 – 609.

[6] Janech, J., Lieskovsky, A., Krsak, E. “Comparation of Strategies for Data Replication in VANET Environment” 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2012, pp. 575 – 580.

[7] Ku, I, You Lu, Gerla, M., Ongaro, F. “Towards software-defined VANET: Architecture and services” 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), 2014, pp. 103 – 110.

[8] Azogu, I.K., Ferreira, M.T., Hong Liu “A security metric for VANET content delivery” Global Communications Conference (GLOBECOM), 2012, pp. 991 – 996.

[9] Wanting Zhu, Qing Zhang, Fong, A.C.M. “Performance Analysis of a Hierarchical Structured VANET” IEEE International Conference on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), 2013, pp. 1352 – 1356.

[10] Hao Jiang, Siyue Chen, Yang Yang, Zhizhong Jie "Estimation of Packet Loss Rate at Wireless Link of VANET—RPLE" 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 2010, pp. 1 – 5.

[11] Yibo Yang, Hongling Li, Qiong Huang "Mobility management in VANET" 22nd Wireless and Optical Communication Conference (WOCC), 2013, pp. 298 – 303.

[12] Hsin-Te Wu, Wei-Shuo Li, Tung-Shih Su, Wen-Shyong Hsieh "A Novel RSU-Based Message Authentication Scheme for VANET" Fifth International Conference on Systems and Networks Communications (ICSNC), 2010, pp. 111 – 116.

[13] Ebers, S., Hellbuck, H., Pfisterer, D., Fischer, S. "Short paper: Collaboration between VANET applications based on open standards" Vehicular Networking Conference (VNC), 2013, pp. 174 – 177.

[14] Jie Luo, Xinxing Gu, Tong Zhao, Wei Yan "MI-VANET: A New Mobile Infrastructure Based VANET Architecture for Urban Environment" 72nd Vehicular Technology Conference Fall (VTC 2010-Fall), 2010, pp. 1 – 5.

[15] Nafi, N.S., Khan, J.Y. "A VANET based Intelligent Road Traffic Signaling System" Australasian Telecommunication Networks and Applications Conference (ATNAC), 2012, pp. 1 – 6.

[16] Noori, H., Olyaei, B.B. "A novel study on beaconing for VANET-based vehicle to vehicle communication: Probability of beacon delivery in realistic large-scale urban area using 802.11p" International Conference on Smart Communications in Network Technologies (SaCoNeT), 2013, pp. 1 – 6.

[17] Kun-chan Lan, Chien-Ming Chou "Realistic mobility models for Vehicular Ad hoc Network (VANET) simulations" 8th International Conference on ITS Telecommunications, 2008, pp. 362 – 366.

[18] Garai, M., Boudriga, N. "A novel architecture for QoS provision on VANET" 10th International Conference on High Capacity Optical Networks and Enabling Technologies (HONET-CNS), 2013, pp. 25 – 31.

[19] El Mouna Zhioua, G, Jun Zhang, Labiod, H., Tabbane, N. "VOPP: A VANET offloading potential prediction model" Wireless Communications and Networking Conference (WCNC), 2014, pp. 2408 – 2413.

[20] Rana, H., Thulasiraman, P., Thulasiram, R.K. "MAZACORNET: Mobility aware zone based ant colony optimization routing for VANET" IEEE Congress on Evolutionary Computation (CEC), 2013, pp. 2948 – 2955.

[21] Nikumbh, D.M., Kharadkar, R.D., Bhoi, A.D., Deshmukh, A.Y. "Analysis of distance based routing protocol in VANET" International Conference on Computing for Sustainable Global Development (INDIACom), 2014 , pp. 829 – 834.

[22] Sivaraj, R., Gopalakrishna, A.K., Chandra, M.G., Balamuralidhar, P. "QoS-enabled group communication in integrated VANET-LTE heterogeneous wireless networks" 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2011, pp. 17 – 24.

[23] Wagan, A.A., Mughal, B.M., Hasbullah, H. "VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination" International Symposium in Information Technology (ITSim), 2010, pp. 607 – 611.

[24] Wagan, Asif Ali, Jung, Low Tang "Security framework for low latency vanet applications" International Conference on Computer and Information Sciences (ICCOINS), 2014, pp. 1 – 6.

[25] Cardote, A., Sargento, S., Steenkiste, P "On the connection availability between relay nodes in a VANET" GLOBECOM Workshops (GC Wkshps), 2010, pp. 181 – 185.

[26] Kafil, P., Fathy, M., Lighvan, M.Z. "Modeling Sybil attacker behavior in VANETs" 9th International ISC Conference on Information Security and Cryptology, 2012, pp. 162 – 168.

[27] Gongjun Yan, Bista, B.B., Rawat, D.B., Shaner, E.F. "General Active Position Detectors Protect VANET Security" International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011, pp. 11 – 17.