ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Detail Review on Sybil Attack and Various Routing Protocols in Vehicular Ad Hoc Network

Swati Saini[1], Jaspal Kumar[2]

M.Tech. Student, Department of ECE, B. S. Anangpuria Institute of Technology & Management, Alampur, Ballabgarh-Sohna Road, Faridabad, Haryana, India [1]

Head of Department, Department of ECE, B. S. Anangpuria Institute of Technology & Management, Alampur, Ballabgarh-Sohna Road, Faridabad, Haryana, India[2]

ABSTRACT: Vehicular Ad Hoc Networks (VANET) is a kind of Mobile ad hoc networks which offers a different technique for Intelligent Transport System (ITS). VANET generally enables vehicle-to-infrastructure (V2I), infrastructure-to-vehicle (I2V) and vehicle-to-vehicle (V2V) communications. This paper review of various VANET routing protocols is significant and essential for smart ITS. This paper talks about Sybil attack and the benefits / drawbacks and the applications of several routing protocols for vehicular ad hoc networks. It examines the inspiration behind the designed, and traces the emergence of these routing protocols. At last the paper concludes the several routing protocols for VANET.

KEYWORDS: MANET, VANET, QoS, routing protocols, V2I, V2V,

I. INTRODUCTION

Vehicular networks show a specifically new class of wireless ad hoc networks that makes capable vehicles to interact with each other and/or with roadside infrastructure. Earlier, drivers were utilizing their gestures, voice, horns, and observation of each other's trajectory to maintain their nature. When the drastic increase of vehicles built this not sufficient to maintain, in the second half of the 19th century, traffic police took charge of managing and controlling the traffic utilizing semaphores, hand signals and colored lights [2]. The 1930s viewed the traffic signals automation and in the 1940s car indicators were deployed broadly. Variable-message signs were proposed in the 1960s to give information to the drivers to follow according to the current situations. The information communicated through all of these means is, since, very less: road infrastructure generally offers the same information to all cars, and the information amount that the drivers can share directly with one another is limited [8]. Currently, drivers can interchange more information i.e. traffic directions and information, to each other through citizen band radio and car phones. Wireless communication provides support to more customized and whole information to be interchanged. VANET approaches all these problems regarded to communications between vehicles and on-going research with wireless communication. It also deals with the aspects of Wireless Access for the Vehicular Environment (WAVE) standards depending on the evolving IEEE 802.11p specification.. In this paper, we utilize the term V2I to refer to both V2I and I2V communication. Organizations in several countries presently are investing in VANET to benefit wireless networking support to enhance state-of-the-art in road transportation. The US Federal Communications Commission (FCC) has distributed 75 MHz of spectrum in the 5.9GHz band for Dedicated Short Range Communications, a set of standards and protocols for short to medium-range wireless communication for automotive utilization. Many latest vehicular networking attempts are the USDOT's Vehicle Infrastructure Integration (VII), which is a cooperative first step between automobile manufacturers and USDOT, stressing on deploying communications systems feasibility for efficiency and safety of road transportation systems [9]. The ERTICO partnership is a multi-sector partnership continuing deployment and development of Intelligent Transport Systems in Europe.

DOI: 10.15680/IJIRCCE.2016. 0406359

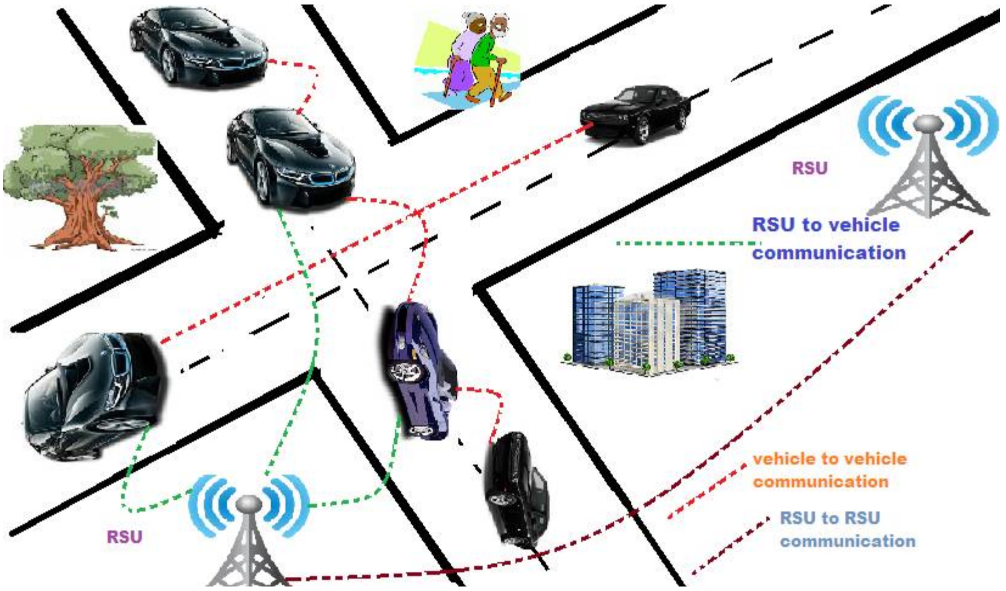
RSU
RSU to vehicle communication
vehicle to vehicle communication
RSU to RSU communication
RSU

Figure 1: Vehicular Ad Hoc Networks (VANET)

Apart from these attempts, numbers of VANET test-beds have been established in academia also for basic development and research of services. This paper introduces a serious and growing security problem in VANETs, namely discovering the existence of Sybil attacks. Sybil attacks are categorized as an attack on the faith of a peer-to-peer system by an attacker considering various pseudonymous identities. Employing these identities, the attacker can achieve a large effect on system services. In VANETs, the existence of a Sybil attack can have negative effects. For example, in an application i.e. road safety, assume a single harmful vehicle, *VM*, considering a large number of fraud identities wrongly reporting road situations. Other right vehicles will tend to trust such a message, since it seems to be coming from various vehicles, and may adjust their paths. In this case *VM* can potentially achieve exclusive access to the road, which it otherwise could not. Various other applications i.e. intelligent traffic signaling, content exchange and ramp metering can all be adjusted in the existence of Sybil attacks [12]. Unlike fix networks i.e. the Internet, vehicular nobilities build Sybil detection very complicated with the extra spatial-temporal constraints.

II. RELATED WORK

The problem of discovering Sybil attacks in VANETs has been studied previously. In [1] and [2], the suggested solution determines Sybil attacks when vehicles may only keep one reasonable pseudonym at a time. When a pseudonym requires to be reviewed, a novel pseudonym is achieved from a authorized Road-Side Unit (RSU). The benefit of this method is a possibly complicated pseudonym distribution method carried out by the road side unit network. Another mechanism supports directional antennas to determine the position/direction of message arrival [3]. A vehicle establishing a Sybil attack will likely be determined as several messages will reach from the position/direction. Since, in heavy networks, localization prone can cause to quick false positives. This method may be adjusted as a smart attacker may utilize directional antennas to misdirect its neighboring vehicles about its way. In [4], heavy-weight cryptographic mechanisms are employed for determining Sybil attacks in VANETs. Particularly, every vehicle is provided a list of pseudonyms to secure their privacy at the time of communication.

In [5], RSSI and GPS signal measurements are employed for determining Sybil nodes. The suggested method utilizes Vehicle-to-Vehicle (V2V) communications to ensure reported locations of vehicles by citing the RSSI measurements. To correct inaccuracies rising from RSSI measurement, lead by traffic patterns, vehicle mobility and support from roadside base stations are employed. Particularly, statistical algorithms are carried out to ensure the signal strength distribution of a mistrust vehicle over time to importantly decrease the detection rate.

III. SYBIL ATTACK AND ITS CLASSIFICATION

Because of the shared wireless channel, malicious nodes can collect identity information through passive monitoring and utilize this information to establish identity based spoofing attacks in vehicular Ad-hoc Network. A Sybil attack is a spoofing attack or an impersonation where an intruder node illegitimately fabricates numerous identities or spoofs the identity of another network node, thus generating an illusion of several nodes [11]. There are several forms of impersonation attacks i.e. invisible node attack, stolen identity attack and Sybil attack. In a Sybil attack, the node that spoofs or fabricates the other nodes identities is known as a malicious node/ Sybil attacker and the related extra identities are known as Sybil nodes. Every Sybil intruder tries to show a legitimate identity and one or more fake identities. A basic Sybil attack is presented in Fig 2. In this scenario, a Sybil intruder M generates an illusion of traffic congestion on the road. When an accident happens on a highway in VANET, the first vehicle that realizes the accident forwards a change route/deceleration alerting message to other vehicles moving towards the accident location. Recipients may send this message to alert following vehicles [17].

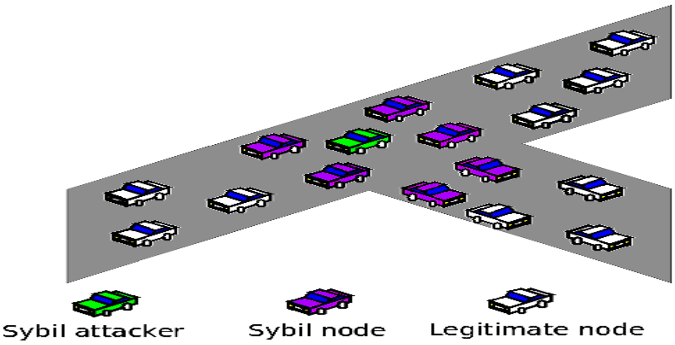

Figure 2: A typical Sybil attack.

This sending procedure can be interfered by Sybil nodes that select not to send the alerting messages, thus putting the passenger life in danger. VANET service can be interrupted by importantly increasing the no. of Sybil intruders and faked identities utilized by intruders. Sybil intruder generates a no. of Sybil nodes based on the storage, communication and computation resources of the intruder. There is no limitation on the resources procurement on VANET nodes, thus they are more susceptible towards the Sybil attack. A Sybil intruder can damage the VANET by performing one or more of the following operations

– Drop packets: An intruder may drop all alerting packets in the existence of an accident.

– Insert wrong information or modify available packets: An intruder may generate an illusion of a traffic jam before choosing an alternate route to its benefit.

– Replay packets: An intruder may dishonestly repeat or delay normal data transmission in VANET. A Sybil attack can be categorized into three classes depending on the following three orthogonal dimensions: the mode of achieving Sybil identity, communication type, and their participation in the network [6, 7] as illustrated in Fig 3. These categories are briefly explained below. In the

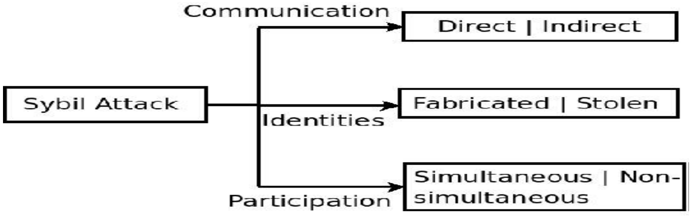

Figure 3: Sybil Attack Variants.

worst case, a Sybil intruder can generate an infinite no. of Sybil identities utilizing only one malicious device and playing role in the network utilizing all these Sybil identities at the same time.

– **Communication Category**: The communication mode between the Sybil identities generated by an intruder and legitimate nodes can be of two kinds–Direct and Indirect. In direct interaction, Sybil nodes generated by an intruder node interact directly with a legitimate node. This mechanism is viable in a scenario, where an intruder spoofs the physically available nodes identities. Often, Sybil nodes and legitimate nodes interact indirectly in cases where an intruder playing role in the network utilizing fabricated identities. In this case, an honest node forwards a safety message to the Sybil node and the Sybil intruder (that has generated Sybil nodes) hears to this message. Similarly, messages forwarded by Sybil nodes are actually forwarded by the Sybil intruder. This scenario shows an example of indirect communication where legitimate nodes arrive Sybil nodes through a malicious node [6].

IV. LAYERED VIEW OF VEHICULAR NETWORKS

Vehicular networks can be categorized based on five different aspects as indicated in table 1. Vehicular Networks has the diverse range of applications that changes safety applications to comfort applications. Safety Applications improves the driving conditions and decreases the possibility of accidents by offering enough time to the driver and using the brakes automatically. These can be further classifying into the following: -

- Cooperative collision warning
- Incident management
- Emergency video streaming

Intelligent transport applications aim at offering faster delivery of traffic information, and enhancing the accuracy and efficiency of traffic detection by permitting collaborative processing of information among vehicles. These applications concentrate on observing the traffic pattern and maintaining traffic accordingly. It can be further classified into the following: Traffic Management, Traffic Monitoring ,Notification services, Vehicle tracking, Platooning. Comfort applications are the VANET applications related to comfort level of the passenger travelling in the vehicle. It can be further classified into the following: Parking place management, Distributed games and/or talks.Accordingly, the Quality of Service (QoS) needed for the network changes from *non-real-time*, to *soft real-time* where a timing failure might compromise service quality, up to *hard real-time* where a timing failure might yield to a catastrophe [8, 9]. These applications can also be represented by their scope, such as whether they offer communication across a *wide area*, or are *local* only. Eventually, such applications can vary in their networking technique: *ad hoc*, where vehicles interact randomly, or *infrastructure-based*, where communication is controlled by static base stations. VANET has the communication type: Vehicle to Vehicle (*V2V)* and Vehicle to Infrastructure (*V2I).*

V. VANET CHARACTERISTICS, ISSUES AND REQUIREMENTS

Wireless communication, specifically real-time communication is highly unreliable. Additionally, VANET has particular unique issues that build it different from other wireless networks. Because no central coordination can be considered, a sole shared control channel is needed at the MAC layer (the so-known as one channel paradigm). Mobility movements of vehicular networks are also very particular, e.g. vehicles move along the roads, in pre-specified directions, and this needs new particular mobility models to be devised. Basic mobility models could not approach the VANET needs. Furthermore, now a day’s cars are having very high mobility rates and so change the configuration in an in-deterministic way that builds wireless transmission very challenging [8].

Moreover, the vehicle density has spatial-temporal variations: it might be very hardly (for example Highway), with no vehicle or only few, up to very dense (such as city area), with over 500 vehicles per kilometer. Both ends of the density spectrum are specifically challenging. The vehicular networks applications should also satisfy a no. of nonfunctional needs, i.e. powerfully very high reliability, but also security to assure that safety-critical applications cannot be flexible with. Vehicles range over very huge geographical regions (countries or cities), and thus need potentially large-scale networks, and particularly a very extensive deployment of resource if infrastructure-based networks are utilized. Some VANET applications have either delay restraints or other QoS needs. Effective broadcasting of safety messages for obtaining full coverage and low latency to offer reliability and QoS in VANET routing is still a challenging issue [8].

However, VANETs mobility cannot be achieved by normal mobility models. Traffic flow (both in space and time) requires be studying and combining in the design of flexible and high-performance mobility models.

DOI: 10.15680/IJIRCCE.2016. 0406359

VI. OVERVIEW OF ROUTING PROTOCOLS

In VANET, the routing protocols are categorized into five classes: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, and Geo cast routing protocol and Broadcast routing protocol. These protocols are featured based on area / application where they are most appropriate [1].

A. Topology Based Routing Protocols: These routing protocols utilize connections information that presents in the network to perform packet sending. They are further classified into Proactive and Reactive.

i) Proactive routing protocols

The proactive routing implies that the routing information, like next sending hop is managed in the background irrespective of communication requests. The benefits of proactive routing protocol is that there is no route discovery however the destination route is recorded in the background, but the drawback of this protocol is that it offers low latency for real time application [2]. A table is built and managed within a node. So that, every entry in the table shows the next hop node towards a particular destination. It also yields to the management of unutilized data paths, which causes the decrement in the existed bandwidth. Several kinds of proactive routing protocols are: FSR, LSR [1].

ii) Reactive/Ad hoc based routing

Reactive routing opens the route only when it is essential for a node to interact with each other. It manages only the routes that are currently in use, as a result it decreases the network burden. Reactive routing contains route discovery phase in which the query packets are broadcasted into the network for the path discovery and this phase finishes when route is discovered. Several kinds of reactive routing protocols are AODV, DSR, PGB and TORA [11].

B. Position Based Routing Protocols

Position based routing contains class of routing algorithm. They share the feature of utilizing geographic location information for selecting the sending hops [2]. The packet is forwarded without any map information to the one hop neighbor, which is nearest to destination node. Position based routing is advantageous however no global route from source node to destination node require to be generated and managed. Position based routing is widely clssified in two types: Position based greedy V2V protocols, Delay Tolerant Protocols [25].

1) Position Based Greedy V2V Protocols: In greedy approach and intermediary node in the route forward message to the farthest neighbor in the direction of the next destination. Greedy technique needs that intermediary node should possessed position of itself, neighbor position and destination position. The objective of these protocols is to transfer data packets to destination as soon as possible that is why these are also called min delay routing protocols. Several kinds of position based greedy V2V protocols are CAR, GPCR and DIR [25].

2) Greedy Perimeter Coordinator Routing (GPCR): GPCR depends upon the fact that city street make a natural planner graph. GPCR does not need external static street map for its operation. GPCR contains two components: A Restricted Greedy forwarding strategy, A repair strategy for routing algorithm. A GPCR adopts a destination based greedy forwarding approaches, it forwards messages to nodes at intersection. However, GPCR does not utilize any external static street map so nodes at intersection are hard to discover. GPCR utilizes heuristic technique for discovering nodes positioned at intersections and considers those nodes as coordinators. Coordinator has the duty of making routing decisions. There are two mechanisms utilized for coordinator determination they are (a) Neighbor Table technique: The nodes periodically transfer beacon messages which has their position information and last known position information of all neighboring nodes, by hearing to beacon messages a node as information about its own position, neighbor position and neighbor's neighbor. Utilizing this information node X assume itself to be within the intersection. (b) Correlation coefficient technique: In this case node utilizes its position information and the position information of its immediate neighbor to determine the correlation coefficient, $p_{xy.}$ This technique performs better as compared to neighbor table technique. By utilizing this technique the algorithm can neglect dependencies on external street map [24, 25].

3) Connectivity Aware Routing Protocols (CAR): CAR protocols discover a route to a destination node; it has unique features that it manages the cache of successful route among several source and destination pairs. It also assumes the position of destination vehicle repairs route as the position changes. Nodes utilizing CAR protocols forward periodic Hello beacons that have their velocity vector information. On obtaining Hello beacons a node will record sender in its neighbor table and compute its own velocity vector and neighbor velocity vector. Beacons can also be piggybacked on sent data packets to decrease bandwidth and congestion wastage. Entries expire from the neighboring table when the distance among nodes exceeds the threshold value. The CAR protocols sets up the guard notation which is a geographic marker message, it is stored and passed from one vehicle to another to propagate the information. A guard is a local message that has an ID, a radius, a TTL (Time to live) counts and some state information. CAR offers two forms of guards. The Traveling guard and The Standing guard. Routing errors may takes place because of communication gap among anchor points or because of guards. So CAR protocol has two recovery approaches to cope with the issue. The first approach is Time out algorithm with active waiting cycle. The second approach is walk around error recovery. The CAR protocol has the capability to create virtual information in the form of guards, which is a different benefit over other protocols [25].

4) Diagonal-Intersection-Based Routing Protocol (DIR): DIR protocol builds a series of diagonal intersections between the source and target vehicle. The DIR protocol depends upon the geographic routing protocol in which source vehicle geographically sends the data packets towards the first diagonal intersection, second diagonal intersection and so on until the last diagonal intersection and eventually geographically arrives to destination vehicle. DIR vehicle is auto adjustable, Auto adjustability implies that one sub path with low data packet delay between two neighboring diagonal intersections, which is dynamically chosen to send data packets. To decrease the data packet delay the route is automatically chosen with lowest sub path delay. DIR protocol can automatically set routing path for keeping the lower packet delay [25].

5) Delay Tolerant Protocols: In urban scenario where vehicle are densely packed positioning a node to carry a message is not a issue but in rural highway situation or in cities at night fewer vehicles are running and setting up end to end route is complex. So in such cases particular consideration requires to be provided in sparse networks. The various kinds of Delay Tolerant Protocols are VADD, MOVE and SADV.

6) Motion Vector Routing Algorithm (MOVE): The MOVE algorithm is an algorithm for sparse VANET scenario. In these scenarios vehicle behave as mobile router that have intermittent link with other vehicles. Link opportunities must be scrutinized carefully however they happen infrequently and global configuration is also frequently changes. The algorithm must predict whether sending message will offer progress toward targeted destination. MOVE algorithm considers that every node has information of its own position, heading and destination. From this knowledge the current vehicle node can compute the nearest distance between the vehicle and message destination. MOVE algorithm utilizes less buffer space. MOVE algorithm is particularly planned for sparse networks and for vehicles that transmit data from sensor networks to BS [25, 27].

7) Vehicle Assisted Data Delivery (VADD): VADD utilizes a carry and forward technique to permit packets to be carried by vehicle in sparse networks for sending when the node enters the broadcast range, thus permitting a packet to be sent by relay in case of sparse networks. VADD need every vehicle to know its own position and also need an external static street map. Every packet has three modes: Intersection, Straight Way and Destination, where every mode depends on the node location carrying the packet. Intersection mode is utilized when the packet has arrived an intersection at which routing decisions can be built for the packet to be sent to a vehicle along any of the existed intersection directions. In Straight Way mode the current node is on a road where there are only two possible directions for the packet to propagate, in the current node direction or in the opposite direction. Destination mode is when the packet is near to its final destination [25, 26].

8) Static Node Assisted Adaptive Routing Protocol (SADV): SADV objectives at decreasing message delivery delay in sparse networks. SADV also dynamically follows to varying traffic density by permitting every node to evaluate the time amount for message delivery. SADV considers that every vehicle knows its position via GPS and every vehicle has accessed to external static street map. SADV has three modules; Static Node Assisted Routing (SNAR), Link Delay Update (LDU) and Multipath Data Dissemination (MPDD). SADV works in two modes: “In Road Mode” and “Intersection Mode”. SNAR make usage of optimum paths, which are determined based on the graph abstracted from road map. LDU manages the delay matrix dynamically by evaluating the delay of message delivery among fixed nodes. MPDD supports in multipath routing [26].

C. Cluster Based Routing: Cluster based routing is suitable in clusters. A set of nodes identifies themselves to be a part of cluster and a node is targeted as cluster head will flood the packet to cluster. Good scalability can be offered for large networks but network overhead and delays are incurred when building clusters in highly mobile VANET. In cluster based routing virtual network infrastructure must be generated through the nodes clustering for providing scalability. The several Clusters based routing protocols are COIN and LORA_CBF

D. Broadcast Routing: Broadcast routing is generally utilized in VANET for sharing, weather, traffic and emergency, road situations among vehicles and providing advertisements and announcements. Several Broadcast routing protocols are UMB, BROADCOMM, V-TRADE, and DV-CAST [26].

DOI: 10.15680/IJIRCCE.2016. 0406359

E. Geo Cast Routing: Geo cast routing is generally a location based multicast routing. Its aim is to deliver the packet from source node to all other nodes within a mentioned geographical region (Zone of Relevance ZOR). In Geo cast routing vehicles outside the ZOR are not alerted to neglect unessential hasty reaction. Geo cast is assumed as a multicast service within a particular geographic area. It basically defines a sending zone where it directs the broadcasting of packets for reducing message overhead and network congestion caused by simply broadcasting packets everywhere. In the destination zone, unicast routing can be utilized to send the packet. One pitfall of Geo cast is network partitioning and also unfavorable neighbors, which may hinder the appropriate sending of messages. Several Geo cast routing protocols are IVG, DRG and DG-CASTOR [26].

VII. CONCLUSION

In this section we have surveyed available routing protocols. Previous forwarding mechanism defines the first protocol routing decision when there are packets to be sent. In case of Delay Bounded protocols the prior forwarding mechanism is utilized, while in all other routing protocols wireless multi hop mechanism of sending is utilized. Digital map offers street level map and traffic statistics i.e. traffic density and vehicle speed on road at various times. Digital map is necessary in case of Some of Cluster Based Routing Protocols. Virtual Infrastructure is generated through nodes clustering for providing scalability. Every cluster can have a cluster head, which is responsible for protected interaction between intra-cluster and inter cluster coordination in the network. Recovery technique is utilized to recover from unfavorable situations. Recovery approach is the criteria, which is utilized to judge the protocol performance.

REFERENCES

[1] Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," *Communications Surveys & Tutorials, IEEE* , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[2] Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," *Wireless communication, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1,4, 12-14 Oct. 2008.

[3] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen,Angela Irwin, Aamir Hassan,“ *Vehicular Ad hoc Networks(VANET):Status, Results, Challenges*”. Springer Science, Business Media.2010

[4] Samara, Wafaa A.H. Al-Salihy, R.sures, “Ghassan *Security Analysis of Vehicular Ad hoc Networks”2010 International Conference on Network Applications,Protocols and Services.*

[5] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[6] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, *Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a* , vol., no., pp.1,6, 25-28 June 2012

[7] Jie Li, Huang Lu, “ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs” , IEEE Transactions on Parallel and Distributed Systems, 2012

[8] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," *Computers, IEEE* Transactions *on* , vol.63, no.2, pp.510,524, Feb. 2014[9] Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on* , vol., no., pp.611,615, 8-10 Aug. 2012

[10] Dalbir Singh and Manjot Kaur, “Mitigation of Sybil Attack Using Location Aware Nodes in VANET”, International Journal of Science and Research (IJSR), Volume 4 Issue 11, November 2015

[11]Jaydip Kamani and Dhaval Parikh, “A Review on Sybil Attack Detection Techniques”, Journal for Research, Volume 01, Issue 01, March 2015

[12] Kewei Sha, Shinan Wang and Weisong Shi, “RD4: Role-Differentiated Cooperative Deceptive Data Detection and Filtering in VANETs”, International Journal of Network Security & its Applications(IJNSA), Vol 3, No.6, 2010.

[13] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[14] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *Communications Letters, IEEE* , vol.18, no.1, pp.110,113, January 2014

[15] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on* , vol., no., pp.26,27, 24-26 Sept. 2014

[16] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[17] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on* , vol.3, no., pp.261,265, 25-27 May 2012

[18] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on* , vol., no., pp.152,157, 10-12 Feb. 2014

[19] Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," *ELEKTRO, 2014* , vol., no., pp.424,429, 19-20 May 2014

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian* , vol., no., pp.135,140, 26-28 Nov. 2014

[21] Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on* , vol., no., pp.792,797, 5-7 March 2014

[22] Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," *Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on* , vol., no., pp.78,79, 16-18 Dec. 2013

[23] Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," *Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian* , vol., no., pp.1,6, 7-9 Nov. 2012

[24]Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[25] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," *Vehicular Technology Conference, 2011 IEEE 73rd* , vol., no., pp.1,5, 15-18 May 2011

[26] Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," *Communications and Signal Processing (ICCSP), 2013 International Conference on* , vol., no., pp.1170,1174, 3-5 April 2013

[27] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1,5, 26-28 July 2013