Review of Internal Security Attacks in Vehicular Adhoc Networks (VANETs)

Vikash Porwal
Dept. of Computer Engineering
&Application
NITTTR, Bhopal

Rajeev Patel
Dept. of Computer Engineering
&Application
NITTTR, Bhopal

Dr. R. K. Kapoor
Dept. of Computer Engineering
&Application
NITTTR, Bhopal

***Abstract*— Vehicular ad hoc networks (VANETs) have becoming a fundamental component of many intelligent transportation systems. They are being increasingly advocated for on road travel management, accident prevention, and managing of parking lots and open areas. Safety and solitude are two key concerns in VANETs. The growth of wireless messages in VANET implies to take into account the need of data security. Compromising with security and threats in VANET may lead to disasters hence may spoil the purpose of VANET. Therefore key objective of VANET designers is to make VANETs communication secure. This research paper presents various types of possible security threats and some general security requirements that must be taken into consideration in order to mitigate vulnerabilities and attacks against VANETs in inter-vehicular communication. The paper also proposed an approach to identify and isolate attacker in order to make communication more secure in VANET.**

Keywords- VANET; Dos Attack; VANET Security;

I. INTRODUCTION

A vehicular ad-hoc network (VANET) is a set of vehicles that communicate with each other via unfettered, thoughtless wireless technology such as Wi-Fi or DSRC [1]. The use of VANETs has allowed the creation of systems for information dissemination, many of which related to dissemination of real-time traffic data [2]. Due to limited transmission radius and bandwidth, the quantity of disseminated information that can be disseminated using a VANET is constrained. Although individual pieces of information may be small in size, in combination, they could easily exceed the bandwidth capacity of a VANET. The development and wide utilization of wireless communication technologies have transformed human lives by providing the most convenience and flexibility ever in accessing Internet services and various applications. Lately, researchers conceptualized the idea of communicating vehicles, giving rise to vehicular ad hoc networks (VANETs), which are the main focus of engineers who desire to turn cars into intelligent machines that communicate for safety and comfort purposes. A VANET is composed of vehicles that are equipped with wireless communication strategy, arrangement systems, and digital drawings. VANETs permit vehicles to tie to roadside units (RSUs), which may be interconnected with each other through a high-capacity mesh network [3].

Vehicular ad hoc networks (VANETs) have some very specific characteristics and solutions to security issues are still in a very early stage of development. Especially the issue of trust between communicating vehicles (referred to as nodes) is an open question: How can one node trust a message it received from another node? Thus, trust establishment is a major challenge in vehicular ad hoc networks as the outcome of the trust establishment process is a trusted relation between nodes. Especially in critical applications like hazard warning a receiving node needs to ensure authenticity and trust ability of received messages before reacting to them [4].

II. VANET NETWORK STRUCTURAL DESIGN

The network architecture [5] of VANETs mainly falls at interval 3 categories: pure cellular/WLAN, pure ad hoc, and hybrid. They are mentioned as follows:

A. *WLAN and cellular*

In this type of network architecture, a hard and fast cellular gateways and WLAN/WiMAX access points at traffic intersections are employed in order to attach to the web, gather traffic info, or for routing functions. The spec beneath this situation may be a pure cellular or LAN structure as shown in Fig.1. VANET can combine both cellular network and WLAN to form the network so that a WLAN is used where an access point is available or a 3G connection otherwise.

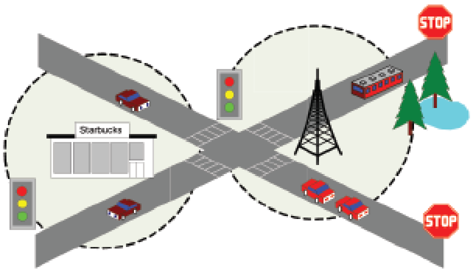

Fig.1 Cellular/WLAN Network Architecture

B. Ad Hoc Network

The cellular/WLAN network architecture is costlier since it include a fixed gateways and other hardware devices hence to overcome this problem vehicles and all the roadside wireless devices can form a pure adhoc network among themselves. The adhoc network architecture is as shown in Fig. 2. It helps in vehicle to vehicle communications and achieves confident goals, such as unsighted crossing.

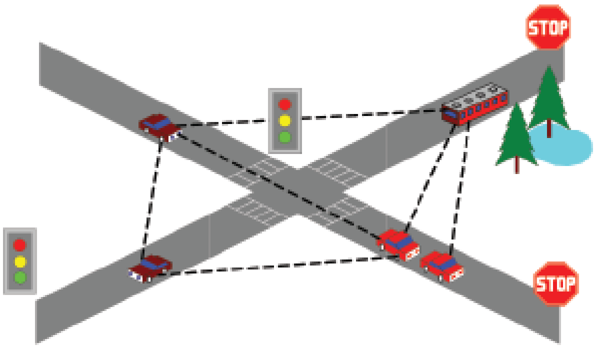

Fig. 2 Ad Hoc Network Architecture

C. Hybrid Network

Hybrid architecture in Fig. 3 is a combination of infrastructure network and ad hoc network. This is also a possible solution for VANET. The hybrid architecture though can provide better coverage, arises a new problem such as the seamless transition of the communication among different wireless systems.

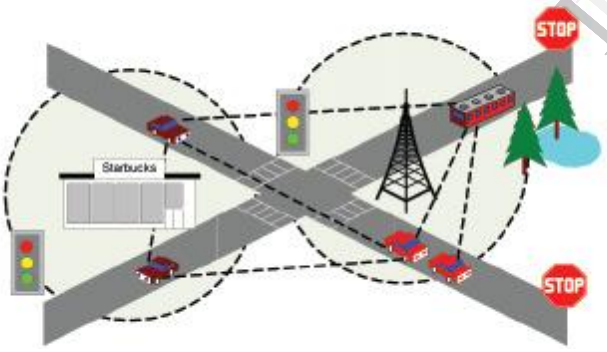

Fig. 3 Hybrid Network Architecture

III. VANET STEERING PROTOCOLS

Steering protocols [5][6][7] are the basic building block for efficient communication in any type of network. The goal of routing protocols is to select best path with least time and least expensive route. The routing operation involves finding the best route from source to destination and destination to source. There is two basic platforms are works, source routing or hop by hop routing. It is a challenge to the researchers to develop routing protocols for highly dynamic topology like VANET. The routing protocols for VANET are classified into different categories which are discussed as follows.

A. Topology Based Mostly Routing

This routing protocol uses link data that exists within the network to perform packet forwarding. They're any divided into Proactive and Reactive routing protocols.

B. Active routing protocols

Active routing means the routing data, like next forwarding hop is maintained within the background no matter contact requirements. The advantage of proactive routing protocol is that there's no route discovery since the destination route is hold on within the background. The drawback encountered with this protocol is that it provides stumpy latency for actual moment application. The varied varieties of proactive routing protocols are: DSDV, OLSR, WRP, CGSR and TBRPF, FSR.

C. Imprudent routing Protocols

Imprudent routing opens the route only it's necessary for a node to speak with one another. Reactive routing consists of route discovery introduce that the question packets area unit flooded into the network for the trail search and this section completes once route is found. The varied varieties of reactive routing protocols area unit AODV, PGB, DSR, TORA, and JARR.

D. Location Based Mostly Routing

Location based routing may be a routing technique during which every node is aware of its own neighbor node geographic location by location critical services similar to GPS. It doesn't maintain any routing table or replace any link state data with neighbor nodes. Data from GPS device is engaged for routing call.

E. Cluster-Based Routing

In cluster-based routing a virtual grouping is formed among the vehicles called clusters. Each cluster has a cluster head which is responsible for intra and inters cluster communication. Nodes in a cluster communicate via direct links.

F. Broadcast Routing

In broadcast routing, flooding mechanism is used where each node rebroadcasts messages to all of its neighbors except the one it got this message from. Flooding mechanism guarantees that the message will reach to each node in the network congestion. Broadcast may be a of period used routing method in VANETs like sharing traffic, weather, urgent situation, road situation among vehicles, and for delivering advertisements and announcements.

G. Geocast Routing

Geocast routing may be a location-based multicast routing. The target of a geocast routing is to deliver the packet from a supply node to any or all different nodes at intervals in such geographic area. Geocast are often enforced with a multicast service by merely shaping the multicast cluster over a definite geographic area. The various geocast primarily based routing protocols are IVG, DG-CASTOR and DRG.

IV. VANET'S SECURITY REQUIREMENTS

In order to have a secure and dependable vehicular network, a number of security requirements must be considered. Some of these security requirements are the same for all networks but some are valid and specific to vehicular networks only. With respect to the mentioned attacks and vulnerabilities securing vehicular communications in all aspects is a must. Here we provide a list of some general security requirements that must be taken into consideration in order to mitigate vulnerabilities and attacks against VANETs. As far as security requirements are concerned the applications of VANET are focused on safety messaging, cooperative driving, toll application etc. Therefore the integrity, liability of message, liability of the user has to be ensured and at the same time privacy has to be looked upon. A secure VANET system should satisfy following requirements [14]:

A. Validation

Despite the lack of need for confidentiality, network nodes must be validated in order to be able to send messages through the network. Before reacting to messages and events a vehicle must verify the legitimacy of the message and its sender, therefore there is a need for validation. Without validation, criminal and malicious users can inject false messages into the network and confuse other vehicles by distributing false information. With authentication, vehicles can simply drop messages from unauthenticated users.

B. Authorization

Authorization is on a higher level implemented by access control which itself is defined by network policies. Authorization defines the role of a node in the network which includes the types of messages a node can read or write on the network, actions it is allowed to take and generally the protocols that it can execute.

C. Data stability

In addition to authenticating the sender, the consistency of messages with similar ones regarding time and location must also be considered, because false messages from legitimate senders are not impossible. It is extremely important for warning messages to meet the time and location constraints. A warning message must be shown to the driver before it is too late to react and also before passing the corresponding geographic location of the warning.

D. Confidentiality

Since security in vehicular networks is related to safety, all network users should normally have full access to network information, i.e. traffic data, road circumstances, etc. in order to make informed decisions. Since messages in VANETs don't contain any sensitive information and are not confidential, there is no need for encryption and confidentiality is not an important issue. Therefore, vehicular networks do not have to be protected against eavesdropping. However, network data should be sent from authenticated sources and this can be done by source authentication.

E. Integrity

All messages which are sent and received on the network should be protected against alteration attacks. A secure vehicular network should provide protection against message alteration. A message can be altered in several ways during its transit from source to destinations and all possible attacks must be considered. When it comes to integrity there are three main threats directly related to message contents. System threats regarding integrity include (1) wrong or forged messages, (2) messages which are modified during transmission and (3) replayed messages.

F. Availability

Since vehicular networks require real-time responses, they are vulnerable to DoS attacks. In order to remain operational, protocols and services must be resilient against denial of service attacks. The communication channel must be available at all times, it must also be reliable otherwise attackers can launch DoS attacks. Such attacks can disrupt the entire network which will lead to failure in delivering network messages to other vehicles in range. Therefore they must be securely designed and be fault-tolerant in order to work under faulty conditions. There are a couple of security measures such as channel monitoring which is a means to increase channel accessibility.

G. Non Repudiation

When a node sends out a message, it shouldn't be able to later deny sending that message. In case of accidents or analysis, difficulty-causing drivers should be dependably identified, to correctly address the sequence and contents of exchanged messages. This can be done by signing outgoing messages with an anonymous key exclusively related to the sender and also a time- stamp associated to the message preventing the user to claim that a particular message has been replayed. In case of using digital signatures, each message is signed with its private but anonymous key. Therefore the vehicle owner cannot claim that he hasn't sent the message.

H. Privacy

Driver privacy is an important issue in vehicular communications. Drivers don't want their personal and private information to be accessible by others. Since the vehicle information such as location, speed, time and other car data are transmitted via wireless connection, there should not be achievable to conclude the driver's identity from this information. Among this information, driver's location and tracing vehicle movements are more sensitive and must be taken into consideration carefully. Regarding this issue we come to another requirement called "anonymity" which is discussed below.

I. Anonymity

Anonymity defines the requirement that network nodes must not be able to infer if a node performed or will perform some specific action in future. In order to prevent such inferences, there must be an equal probability of doing a specific action by all nodes, or have strong probabilistic anonymity, with the probabilities being equal for all nodes. It not requires a vehicle to authenticate with its exact identity to other vehicles to which it sends information.

J. Real-time Constraints

In order to have vehicular networks secured, specific measures and techniques have been suggested. Although these techniques seem applicable and useful, there is one important issue that must be taken into account, real-time constraints. Out-dated messages, e.g. out-dated traffic or road/weather conditions, must be eliminated in order to let the newly generated messages get to their destinations on time.

V. VANET ATTACKS

Many sorts of attacks are known and classified on the premise of layers employed by the assailant. At the physical and link layer, AN assailant will disturb the network system by overloading the line with useless messages. AN assailant will inject false messages or air a recent message additionally. Some at network layer, AN attacker will insert false routing messages or overload the system with routing data. Privacy of drivers may be disclosed by revealing and following the position of drivers. Following figure shows the different VANET attacks [15][16]:

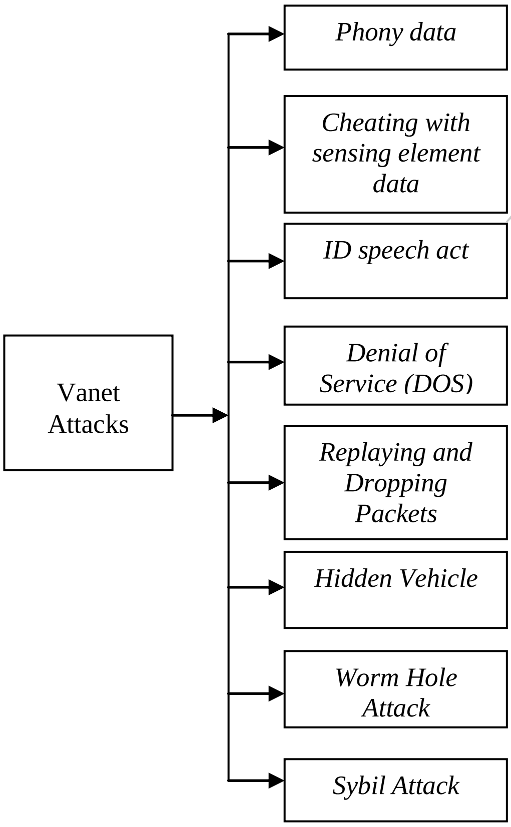

Fig. 4 Attacks in VANET

A. Phony data

In this case, attackers square measure insiders, rational, and active. They will send wrong data within the network so it can have an effect on the behavior of different drivers.

B. Cheating with sensing element data

This attack is launched by AN assailant UN agency is corporate executive, rational, and active. He uses this attack to change the perceived position, speed, and direction of different nodes so as to flee liability just in case of any mishap.

C. ID speech act

An assailant is corporate executive, passive, and malicious. It will monitor trajectories of a target vehicle and may use this data for deciding the ID of a vehicle.

D. Denial of Service (DOS)

Attacker is malicious, active, and native during this case. Assailant might want to bring down the network by causing needless messages on the guide. Example of this attack includes direct electronic countermeasures and injection of dummy messages.

E. Replaying and Dropping Packets

An assailant might drop legitimate packets. As an example, AN assailant will drop all the alert messages meant for warning vehicles continuing toward the accident location. Similarly, AN assailant will replay the packets at the moment event has been occurred to make the illusion of accident.

F. Hidden Vehicle

This type of attack is feasible in a very situation wherever vehicles neatly attempt to cut back the congestion on the wireless channel. As an example, a vehicle has sent a warning message to its neighbor and it's awaiting a response. Once receiving a response, the vehicle realizes that its neighbor is in a very higher position to forward the warning message and stops causing this message to different nodes.

G. Worm Hole Attack

It is difficult to discover and forestall this attack. A malicious node will record packets at one location within the network and tunnel them to different location through a personal network shared with malicious nodes. Severity of the attack will increase if the malicious node sends solely management messages through the tunnel and not information packets.

H. Sybil Attack

In this attack, a vehicle forges the identities of multiple vehicles. These identities may be wont to play any variety of attack within the system. These false identities additionally produce AN illusion that there square measure extra vehicles on the road. Consequence of this attack is that each variety of attack may be competing once spoofing the positions or identities of different nodes within the network.

VI. RELATED WORK

Xu et al. [9] propose two methods to respond at jamming attacks: channel surfing and spatial retreats. The first technique has been motivated in some way from the rate of recurrence hopping method. Unlike rate of recurrence hopping that takes location at the PHY layer, channel surfing takes place at the MAC layer. When a node detects that it is blocked it can change its channel and send a beacon communication on the new channel rate band. Its non-jammed neighbors will detect the nonappearance of this node and modify its channel to get the beacons broadcasted in new channel. If no beacon is detected then they suppose that the node just moved away. In the further side, if they intelligence a beacon they will inform the rest of the network at the primary channel to change the channel. There are two possible approaches. At the first approach the whole network will finally change channel while in the second approach only the boundary nodes of the jam region will modify their channel and they will be used as relays for the rest of the network and the blocked area. In spatial retreats method, when a node detects that it is being jammed, it firstly escape from the jammed area and then tries to stay connected within the rest of the network in order to avoid the separation of the network reconstruction phase. More specifically, when a node senses that it is being jammed, it starts moving out of the jammed region and concurrently runs the detection algorithm. When it detects that it has moved away the jamming area, it tries to stay connected with its previous neighbors. In order to stay linked it keeps rousing at the boundary of the uncreative region. If the node does not distinguish that it is out of the blocked area and it continuous to go away, it could be out of the network divider that makes it not possible to stay joined.

Usha et al [10] proposed that the vehicle that wants to go into the network sends a request to the Road side radio tranductor that contains the record of the vehicles validation and hop counts. If the hop count in the request and in the roadside unit doesn't equivalent, it means that it is a malicious node. Else the vehicle is added in the network. The request and response tables that are maintained by the road side transduction unit. The request table store the Vehicles identity and No of hops. The response table consists of Request, Validations, Next Hop, Hop count, Response, Updated counter. In this proposed model she introduces a unique packet called decision packet. After the pre validation algorithm, a route has been recognized in the network between the vehicles. Now during the legalization time there may be chances of vehicles falsifying their identity to go into in the network as a result it apply hash tables called request table and response table to further decrease the DOS attacks that results due to flooding.

Each vehicle in the network sends the decision packet to the target vehicle through the path recognized during the revalidation. All the vehicles between the source and the destination promote this packet and update the hop count by incrementing it. This gives the information about the neighboring vehicles and also the space between them. At the destination a response table is used which evaluates the packets with the help of the hop count and updates the counter. We have reduced the delay in the packets and the rebroadcasting of the requests by limiting the capacity of the oppose and updating it frequently, also Requests that are sent by the vehicles more than once within a exacting span of time are discarded thus giving priority to all the requests. We think that all the nodes as unicast whereas the malicious node is multicast. Therefore a node requests only once, if it is requesting for the similar service more than a few times it is considered to be attacked. The Tables for requests and response are helpful in fading such nodes, thus preventing from DOS attack. The maximum capability is fixed which depends on the communication range of radar at the road side and fixing the counter to a pre-determined value. This reduces the effect of flooding.

Bayrem et al. [11] proposed that the attacker could do more than a few forms of Sybil attacks, either when it is below the exposure of an RSU or not. The first form of a Sybil attack consists in use a certificate linked to any more zones. The neighboring vehicles will get a broadcast message from the attacker which can be authentic using a certificate related to any more zones. Accordingly, they detect a potential incidence of a Sybil attack due to a hesitant of using another identity. A report containing the sequential identity of the Sybil attacker extracted from vehicle certificate, mutually with the timestamp of the event incidence, will be generated and sent to the RSUs. The report is generated each time that a Sybil attack occurs and is forwarded to the near RSU by the vehicles that detected the incident. The number of linked reports sent to the RSU is equivalent to the number of detected attackers. Although the Sybil attack occurs when the vehicle uses more than a few identities in the similar time, this events could be detected since each vehicle has a certificate. However, since the vehicle could obtain more than a few certificates during navigation, two situations should be distinguished: either a) the vehicle is conducting a Sybil attack by means of a certificate previously generated in the present zone mutually with the certificate generated in one more zone; b) the vehicle has not obtained a new certificate, yet, due to the personality of the network (the vehicle went through an revealed area); c) the vehicle has not detected the first RSU of the new region; or d) some communication problems in analysis its tag have occurred.

To avoid fake positives, the RSU frontwards the aware to the RSC, to verify whether the vehicle has already obtained another certificate in the recent region. If yes, it checks with neighboring RSU whether the vehicle has acknowledged this new certificate. If yes, the RSU confirms the incidence of the Sybil attack and generates an alert to be broadcast through the attached RSC to all RSUs of the network. The detection of this attack would be immediate and easier if the attacker executes this attack below the coverage of an RSU. Ning *et al.* [12] presented a proficient method called message precise puzzle to diminish such DoS attacks. The mechanism added a fragile authenticator in all broadcast packet, which can be confirmed rapidly by a standard sensor node but takes an attacker a large amount of time to fake.

VII.PROPERTIES OF ATTACKERS

Attackers produce drawback within the network by obtaining full access of communication medium DSRC. Here we tend to discuss some properties and capability of the attackers that has been mentioned in studies [13].

A. Internal

This type of attackers WHO is AN authentic user of the network and have detail data of network, corporate executive assaulter might need access to corporate executive data and this information are going to be used for understanding the planning and configuration of network. After they have all info regarding the configuration then it's straightforward for them to launch attacks and make a lot of drawback as compare to outsider assaulter. It will produce drawback within the network by ever-changing the certificate keys. We will merely say that corporate executive assaulter is that the right man doing the incorrect job within the network.

B. External

The outsider assaulter is taken into account as AN authentic user of the network. It's a sort of entrant that aims to misuse the protocols of the network and therefore vary of such attacks are restricted. Outsider assaulter conjointly incorporates a restricted diversity for launching totally different quite attacks as compare to corporate executive assaulter.

C. Coverage space

Coverage space is that the main property of assaulter after they launch any quite attacks. Assaulter may cowl the most space of road, and it depends on the character of the attacks. Basic level assaulter has controlled one DSRC channels {and cowl and canopy}s the vary of at the most a thousand meters however the extended level attackers are a lot of organized and cover a lot of space mistreatment of hundred DSRC channels.

D. Technical Experience

Technical experience of the assaulter makes them stronger for making attacks within the network. It's tough for assaulter to mount attacks on science algorithms. Probability is low for assaulter to compromise the infrastructure network and information capture from restricted space of network. Assaulter having ability to extracts the program code and secret keys of the computing platform of OBU and RSU by launching physical attacks.

E. Resources

Budget, hands and tools are the 3 main key resources and attackers depend upon it to attain their goals. Would like budget to borrow technical knowledgeable and pay time to know the configuration of specific network and so disturb network with launching of various quite attacks. Assaulter will use totally different quite tools for launching attacks. These software package tools will develop by own self or get from the market. Several business parties build setup their business nears the road and supply non safety application services (Internet, diversion services). One business party are often used their own most resources to form issues for different parties and destroy their business with totally different quite attacks, and implementation of security requirements for transport communications.

VIII. PROPOSED FUTURE WORK

In future work we will attempt to develop such a system to Detect and prevent DOS attack in VANET. In this proposed approach node are clustered based on connectivity, battery power, memory and distance. The above process creates a cluster head. This cluster head sends an ACK message to infrastructure server of every vehicle in his group that includes node id max flooding and max PDR (packet dropping) to the server. So that server can locate the attacker on the basis of max flooding and max packet dropping and send the response to road side unit (RSU). The RSU broadcast this node id in the group. Every vehicle will remove this node id with the help of AODV protocol. With the help of this methodology we will be able to detect the DOS attack and prevent the VANET so as to increase the network performance.

IX. CONCLUSION

In this paper numerous attacks in VANET are classified. It has been discovered that the classification helps to handle differing kinds of attack on VANET. Correct security mechanisms should be developed in parallel to scale back the danger of malicious and unauthorized behavior within the transport network domain. Users need safety on road in future transport network and it may well be attainable by implementing VANET applications. Lastly we have proposed an approach to identify and isolate attacker which we are going to develop and test.

REFERENCES

[1] DSRC. 2003. DSRC ITS Standards Advisory. http: //www:standards:its:dot:gov/Documents/advisories/dsrcadvisory:htm : Accessed on Nov.15, 2009.

[2] Caliskan, M., Graupner, D., and Mauve, M. 2006. Decentralized discovery of free parking spaces. In Proceedings of the 3rd international Workshop on Vehicular Ad Hoc Networks (Los Angeles, CA, USA, September 29, 2006). VANET '06. ACM, New York, NY, 30-39.

[3] C. Laurendeau and M. Barbeau, "Threats to security in DSRC/WAVE," in Proc. ADHOC-NOW, 2006, vol. 4104, pp. 266–279.

[4] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security issues in a future vehicular network," in Proceedings of European Wireless 2002, 2002.

[5] Watfa, Mohamed. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. Information Science Reference, 2010.

[6] Paul, Bijan, Md Ibrahim, Md Bikas, and Abu Naser. "VANET Routing Protocols: Pros and Cons." arXiv preprint arXiv:1204.1201 (2012)

[7] Kumar, Rakesh, and Mayank Dave. "A Comparative Study of Various Routing Protocols in VANET." arXiv preprint arXiv:1108.2094 (2011).

[8] J.T. Isaac S. Zeadally J.S. Ca´mara "Security attacks and solutions for vehicular ad hoc networks" IET Communications 2009.

[9] W. Xu, T. Wood, W.Trappe, and Y. Zhang." Channel Surfing an Spatial Retreats: Defenses against Wireless Denial of Service" In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2004.

[10] Usha devi gandhi R.V.S.M. Keerthana"Request response detection algorithm for DOS attack in VANET" 2014 International Conference on Reliability, Optimization and Information Technology -ICROIT 2014, MRIU, India, Feb 6-8 2014.

[11] the Bayrem TRIKI, Slim REKHIS, Mhamed CHAMMEM, and Noureddine BOUDRIGA" A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Networks" 978-1-4673-5616-9/13/$31.0 ©2013 IEEE.

[12] Jan. P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks againstbroadcast authentication in wireless sensor networks," ACM Transactions on Sensor Networks, vol. 4, no 2008

[13] "VANET Wikipedia Article http://en.wikipedia.org/wiki/VANET

[14] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences EPFL,Switzerland SASN'05, Nov 7 2005.

[15] Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim "A Literature Survey on Security Challenges in VANETs" International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012.

[16] Ayonija Pathre1,Chetan Agrawal2, Anurag Jain" Identification of malicious Vehicle in VANET environment from ddos attack" Journal of Global Research in Computer Science, Volume 4 No 6, 30-34.