Journal of the Maharaja Sayajirao University of Baroda
ISSN : 0025-0422

Attacks in Vehicular Adhoc Networks (VANETs) – Perspectives, Issues & its Illustrations in Network Layer Attacks

Ms. B. Manimekala, Ms. KS. Divya, Ms. K. Soumya, Ms. Sreeparna Chakrabarti
Assistant Professor, Department of Computer Science (UG)
Kristu Jayanti College (Autonomous), Bengaluru

Abstract:
VANET has turned into an effective area of research, standardization and advancement, because it has impressive potential to raise vehicle and road safety, welfare, as well as convenience to both drivers and passengers and traffic adaptability. A lot of VANET Research work has been centered on particular areas including broadcasting, routing, surveillance and quality of service. The security benchmarks of vehicular Ad hoc network are examined here. Due to the unguarded nature of the VANET system routing protocols, such networks are also unsafe from the malicious mobile nodes in the structure itself. Hence the fundamental objective of vehicular ad hoc networks (VANETs), i.e., safe transmission of the time critical data, is possible only if a sturdy framework provides this insurance at all times. In this paper, various security protocols for vehicular ad hoc networks and achievement of mechanisms are discussed to give security. In this paper various types of security complications and objections of VANET have been figured out and examined.

Keywords: VANET, MANET, Security, Broadcasting, Routing

1. INTRODUCTION

Nowadays, growth in the wireless communication system and association of Internet as an important part of our lives. In latest years, driving is one of the most incident aspects of traffic safety. A new concern of Wi-Fi surroundings like a Wi –Fi city with WI –Fi road situation is appearing quickly [1]. For this cause an advanced kind of data technology called VANET is being developed. VANET are the subclass of MANET (Mobile Ad-hoc Network) in which transmission nodes are mainly vehicles. VANET is a mechanization that uses moving vehicles as modules in a system to create a mobile network. VANET network is elaborated further as shown in figure 1. The VANET communication has been characterized into two types of connections:

Vehicle to vehicle (V2V): A vehicle communicates to another vehicle in the network to change the data related traffic jams, accidents on roads etc.

Vehicle to infrastructure (V2I): A vehicle makes a communication with locked equipment unit assigned as the Road Side Unit (RSU). The RSU connect each other through wireless medium or wired transmission.

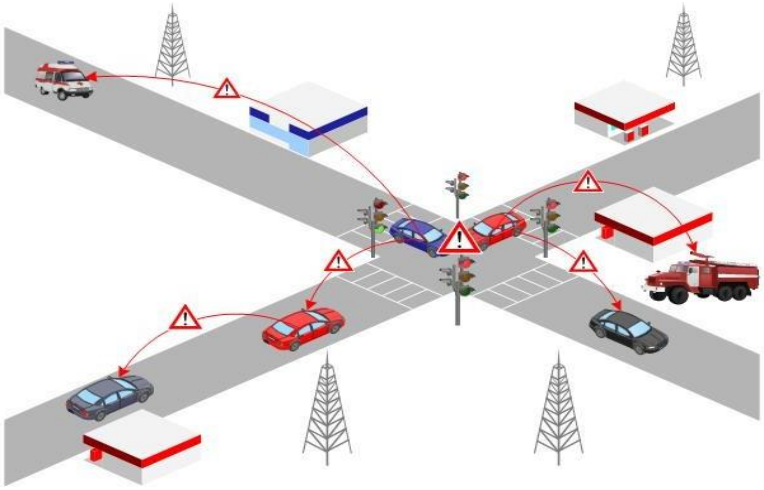

Fig 1: Vehicular Adhoc Network (VANET)

2. SUSCEPTIBILITIES OF THE VEHICULAR ADHOC NETWORKS

Because Vehicle ad hoc systems have far more susceptibility than the classic wired systems, security is much more difficult to maintain in the Vehicle ad hoc network than in the wired system. In this part, the diverse vulnerabilities are explained that lie in the mobile ad hoc structure [2].

Lack of Secure Boundaries The meaning of this vulnerability is understandable: there is not such a clear protected *barrier* in the mobile ad hoc network, which can be related with the fair line of defense in the common wired network. This vulnerability initiates from the quality of the mobile ad hoc system: flexibility to join, leave and action inside the structure. In the wired system, competitors must get physical approach to the network the description of the mobile ad hoc system: independent to join, permitted and movement inside the structure. In the wired network, competitor must get real approach to the network intermediate, or even pass through many lines of aegis such as firewall and gateway before they can implement malicious behavior to the goals. However, in the vehicular ad hoc system, there is no requirement for a competitor to benefit the physical access to visit the network: once the attacker is in the radio area of any other nodes in the vehicular ad hoc structure, it can connect with those nodes in its radio area and thus unite the network automatically. As a result, the VANET does not provide the so-called secure border to conserve the system from some potentially unsafe network accesses.

Threats from Compromised Nodes Inside the Network in the previous subsection, the susceptibility that there are no fair secure borders in the vehicular ad hoc network, which may cause the happing of various link attacks. These link attacks place their force on the links between the nodes, and try to perform some malicious behaviors to make elimination to the links. However, there are some other attacks that aim to gain the supervision over the nodes themselves by some illegitimate means and then use the negotiate nodes to assassinate further malicious actions. This accountability can be viewed as the threats that come from the negotiate nodes inside the network. Since vehicles are self-governing units that can join or leave the network with flexibility, it is tough for the nodes themselves to work out some impressive arrangements to prevent the possible malicious action from all the nodes it broadcast with because of the detachable assortment of distinct nodes.

Lack of Centralized Management Facility Adhoc organizations do not have a centralized portion of executive machinery such as a name server, which point to some vulnerable complication. Now let us discuss this complication in a more accurate manner. First of all, the nonappearance of centralized executive equipment makes the apprehension of attacks a very challenging problem because it is not easy to supervisor the vehicles in a deeply changing and large range ad hoc network [3]. It is rather frequent in the ad hoc network that favorable collapse, such as direction damage, communication impairments and packet drooping, happen periodically.

Restricted Power Supply, due to the portability of nodes in the ad hoc network, it is common that the nodes in the ad hoc system will await on battery as their capability stockpile process. While nodes in the wired network do not need to acknowledge the power supply controversy because they can get electric power supply from the channel, which commonly mean that their power supply should be roughly infinite; the nodes in the mobile ad hoc network need to consider the blocked battery power, which will cause several complications. The first problem that may be generated by the restricted power supply is denial-of-service attacks.

Scalability, address the scalability problem when discuss the vulnerabilities in the vehicular ad hoc network [4]. Unlike the common wired structure in that its extend is generally predefined when it is formed and will not alter much during the usage, the scope of the ad hoc system keeps altering all the moment: because of the flexibility of the nodes in the vehicular ad hoc structure, forecast how many nodes there will be in the network ultimately.

3. SECURITY DIMENSIONS

There are a few important conditions to achieve security in VANETs, which are discussed as follows. Authentication: Vehicles should acknowledge only to the messages transmitted by appropriate members of the network. Thus, it is very necessary to authenticate the operator of a message.

- Data Verification: Once the sender vehicle is authenticated the acquiring vehicle complete data authentication to check whether the message consist of the correct or depraved data.
- Availability: The network should be available even if it is under an attack using substitute mechanisms without affecting its execution.
- Data Integrity: It ensures that data or messages are not modified by attackers. Otherwise, users are precisely affected by the modified emergency data. For example, if a vehicle B sends a message to a malicious vehicle C and C this message to appropriate vehicle D, it (D) will be affected by this message since D will change the road and be in problem later on.
- Non-repudiation: A sender must not oppose a message transmission whenever an analysis or identity of a vehicle is required.

In VANETs, nasty vehicles launch attacks on appropriate vehicles in different ways. Thus, malicious or attacker vehicles are classified as follows.

- Insiders Vs Outsiders, in a system, a representative node that can connect with other members of the structure is known as an Insider and can attack in several ways. Outsiders who cannot connect directly with the representatives of the network have a defined scope to attack (i.e., have lesser diversity of attacks).
- Malicious Vs Rational, a wicked attacker uses different methods to ruin the representative nodes and the system without looking for its individual gain. On the adverse, a realistic attacker predicts personal assistance from the invasion. Thus, these attacks are more certain and follow some arrangements [2].
- Active vs Passive, an active attacker can achieve new packets to corrupt the system whereas a passive attackers active only eavesdrop the wireless carrier but cannot make new packets (i.e., lesser harmful).

4. ATTACK TYPES IN VEHICULAR ADHOC NETWORKS

There are plentiful kinds of attacks in the vehicular ad hoc system, almost all of which can be characterized as the following two categories [2]:

- External attacks, in which the attacker targets to cause congestion, reproduce bogus routing information or disrupt nodes from providing duties.
- Internal attacks, in which the attacker wants to hike the routine access to the system and cooperate in the network activities, either by some malicious imitation to get the approach to the network as a new module, or by directly compromising a present node and using it as a support to handle its malicious nature.

Passive Attacks, are those where the attacker does not interrupt the operation of the routing protocol but try to seek some beneficial information through traffic analysis. This in turn can point to the acknowledgement of critical information about the network or nodes such as the network topology, the location of nodes or the identity of important nodes.

Active Attacks, intruders launch invasive movements such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various interruption to the network. Some of these attacks are caused by a single exercise of an intruder and others can be caused by an array of activities by connive intruders [9].

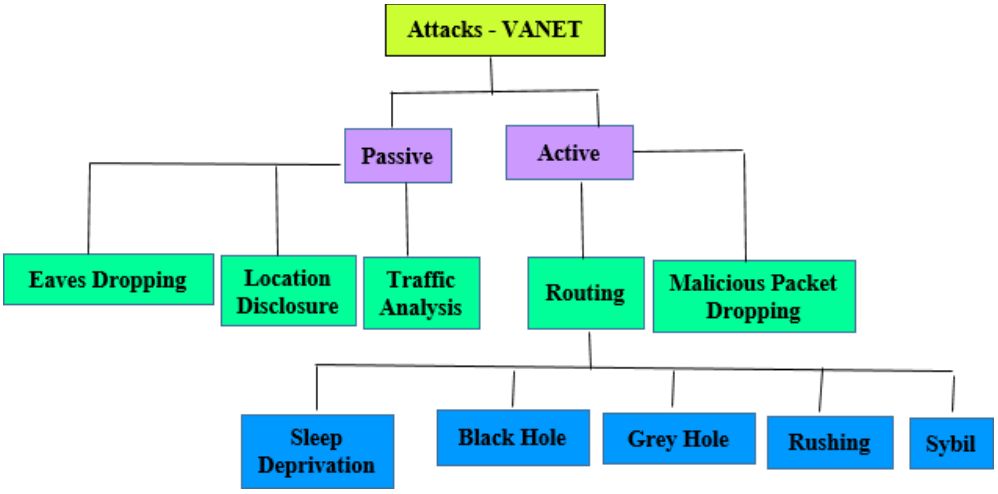

Fig 2: Types of Attacks - VANET

Active attacks (as compared to passive attacks) interrupt the operations of the network and can be so serious that they can bring down the full network or degrade the network performance significantly, as in the case of denial of service attacks.

Name of the Attack	Attacker type	Security attributes and requirements	Requires Physical Access?	Communication types
Bogus Information	Insider	Data Integrity/ Authentication	No	V2V
Denial of Service (DoS)	Malicious, active, insider, network attack	Availability	Yes/No	V2V/V2I
Masquerading	Active, insider	Authentication	Yes/No	V2V
Black Hole (BH)	Passive, outsider	Availability	Yes/No	V2V
Malware	Malicious, insider	Availability	No	V2V/V2I
Spamming	Malicious, insider	Availability	Yes	V2V
Timing Attack	Malicious, insider	Data Integrity	No	V2V/V2I
GPS Spoofing	Outsider	Authentication	No	V2V
Man-in-the-middle	Insider, monitoring attack	Data integrity, confidentiality, privacy	Yes	V2V
Sybil	Insider, network attack	Authentication, privacy	Yes	V2V
Wormhole / Tunneling	Outsider, malicious, monitoring attack	Authentication, confidentiality	Yes/No	V2V
Illusion attack	Insider, Outsider	Authenticity, data integrity	Yes	V2V/V2I
Impersonation attack	Insider	Privacy, confidentiality	Yes	V2V

Table 1: Different types of security attacks in VANET with attacker types and respective security Attributes.

- Impersonating another node to spoof route message.
- Advertising a fake route metric to confuse the topology.

- Sending a route message with false sequence number to suppress other consistent route messages.
- Flooding Route Discover unreasonably as a DoS attack.
- Modifying a Route Reply message to implant a false route.
- Generating bogus Route Error to disturb a working route.
- Suppressing Route Error to misrepresent others.

5. ILLUSTRATION OF NETWORK LAYER ATTACKS

In this subsection we illustrate the operation of some of the major network layer attacks that were introduced in above section.

Sleep Deprivation Attack

The sleep deprivation attack defined using AODV as the routing protocol as an example to illustrate in detail the ways this attack can be introduced in the network [10]. When a node needs a route towards a destination, it initiates a route discovery process by broadcasting a RREQ with its current destination sequence number. If an intermediate node that receives the RREQ knows the route, it unicasts a RREP back to the source node, otherwise it rebroadcasts the RREQ packet. To control the dissemination of RREQs, AODV uses an expanding ring search technique, where the source node first sends a RREQ with its Time to Live (TTL) field set to some initial value, TTL_start. The source then waits for the ring_traversal_time.[14] If this time expires without receiving a RREP the source node may send a RREQ again with increased TTL value. This process can be repeated until the TTL value reaches some value TTL_threshold, where TTL_threshold >TTL_start.

- The node v6 generates a RREQ with a destination IP address for some non-existent node v25, (i.e. the IP address is within the network's address range but the node does not exist). Intruder v6 broadcasts this RREQ (we assume here that the TTL value is sufficiently large to allow the RREQ to propagate across the network).
- Nodes v2, v1, v5 and v9, which are within the radio range of v6, will receive the RREQ (the solid arrows show the RREQ flow), and check their routing table entries for routes to the destination node v25.
- Because nodes v2, v1, v5 and v9 do not have the route for node v25, they will rebroadcast the RREQ initiated by the intruder.
- Nodes that receive RREQs from v2, v1, v5 or v9 will first check whether they have processed earlier copies of these requests; if not, then they will also have advertised this malicious RREQ further.

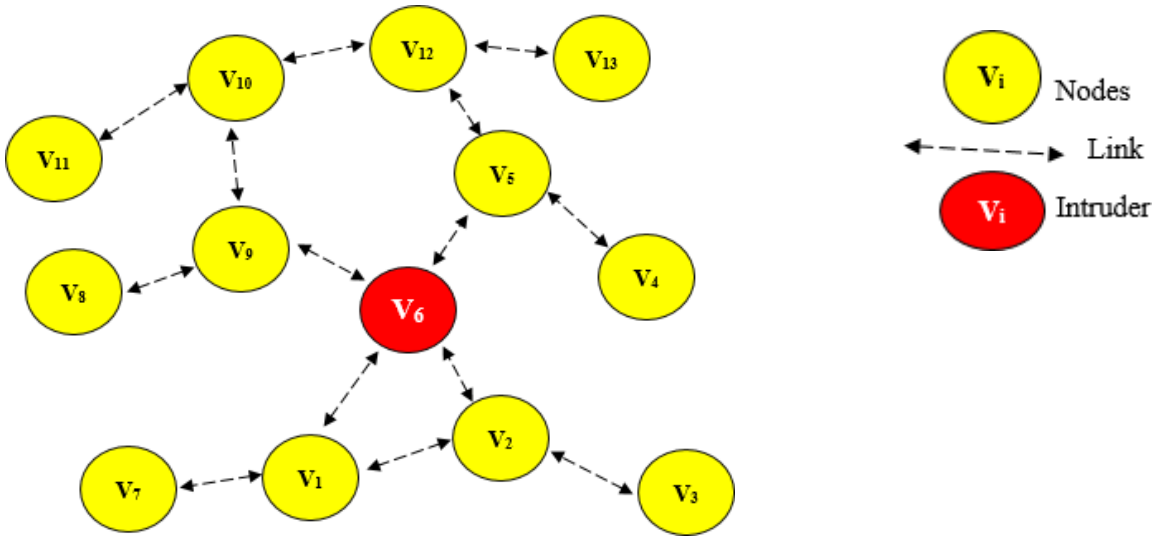

Fig 3 shows the network after this initial broadcast.

Since no nodes know the route for this destination node, this process continues across the network.

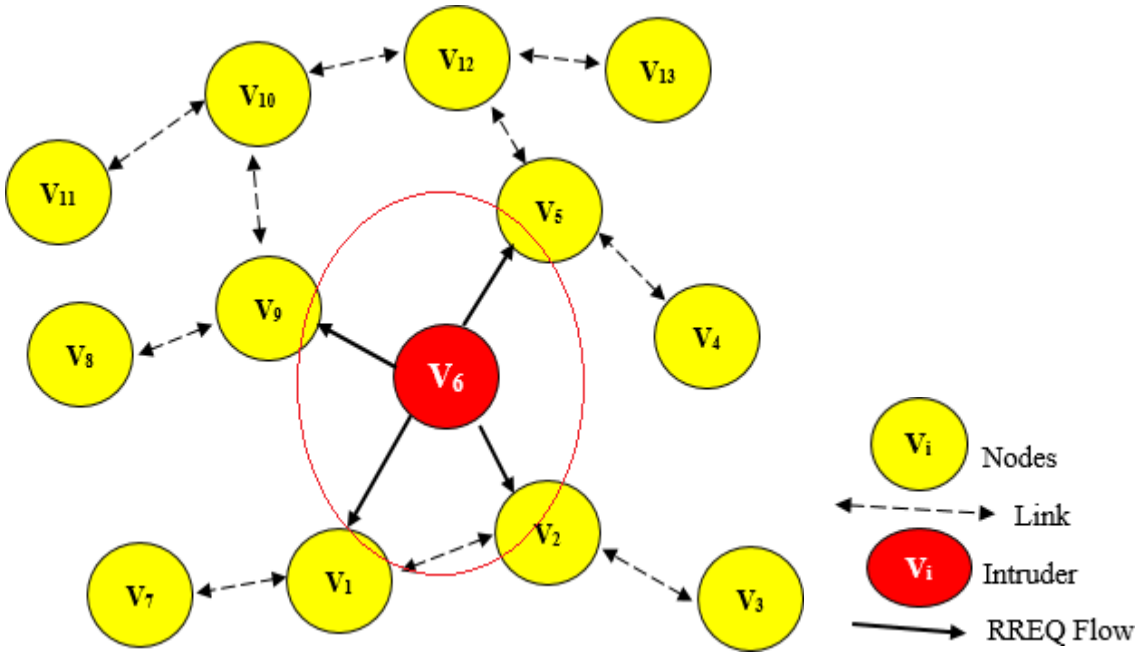

Fig 4 shows the state of the network after the RREQ has been advertised for three hops.

The part of the network shown in the figure is flooded with malicious RREQs, and ultimately the entire network will be flooded with these RREQs. Nodes alter these unnecessary packets drain their batteries and, hence, may no longer be able to provide services in the network [14].

6. RESEARCH RESULTS

VANET is becoming an increasingly popular and promising application of the mobile *ad hoc* networks (MANET) technology. VANET has attracted significant attention from leading car manufacturers and wireless communication research community alike [2]. Despite at suffers from a range of security and privacy issues that have dramatically restricted their applications as yet. This research has evaluated the potential threats to the V2V/V2I communications system, an assessment of the severity of such attacks, and an analysis of the level of risk resulting from the threat. The research confirms that whereas VANET has emerged as an active area of research, standardization, and development due to its tremendous potential to improve vehicle and road safety, improve traffic efficiency and enhance driving comfort, a strong emphasis needs to be laid on designing novel VANET architectures and implementations. VANET suffers from considerable threats to security of the users, and therefore research needs to be focused on specific areas including routing, broadcasting, QoS and security [9]. Wireless access standards have escalated from research and prototype to actual implementation domain. The outlined challenges that still need to be addressed in order to enable the ubiquitous deployment and widespread adoption of scalable, robust, reliable VANET architectures, protocols, technologies, and services are to enhance the security measures adopted in VANET [4]. There are a number of high risk attacks on the users and there appears to be a significant risk to safety in the event of a successful attack. This is partly due to the short-range nature of the communications and thus the geographical feasibilities of such attacks [4] [13].

7. CONCLUSION

Regardless of the encryption and secure routing protocols, the VANET architecture continues to remain potentially insecure as the attacker can listen in even without gaining traceable physical access. Thus, the protocol designs prove to be security-naive. Various mechanisms have studied and pointed out and tools used by the attackers posing as innocent vehicles in the network, to implement attacks by exploiting the weaknesses in the protocol designs. The integration of RSUs and comfort

applications in VANET has also led to increased network vulnerabilities. The study also analyzed a few practices and theoretical constructs employed to mitigate the insecurities in VANET their drawbacks were studied. Major security flaws in VANET and their adversaries are also presented in the paper. Arrive at a conclusion that amidst the evolving network environment, VANET needs to be supported with more secure architecture, with privacy of the users being acknowledged as the foremost exponent of VANET requirements.

Due to the lack of a cognitive framework to detect vulnerabilities and to prevent exploitation of the network, VANET provides a fertile turf for attackers to carry out malicious activities, and VANET is loaded with an incredible amount of spam. Though barriers exist on vehicles today that make launching a successful attack slightly difficult and the technological complexity of vehicles offers a degree of tamper-resistance, it is inevitable that an attacker quite well familiar with the vehicular architecture would be able to compromise a key, sensor, or GPS receiver.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book *Ad Hoc Networks Technologies and Protocols (Chapter 9),* Springer, 2005.

[3] Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 31),* CRC Press LLC, 2003.

[4] Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book *The Handbook of Ad Hoc Wireless Networks (Chapter 30),* CRC Press LLC, 2003.

[5] J. Kong, X. Hong and M. Gerla, "A new set of passive routing attack in Mobile ad hoc networks", Proc. IEEE Military Communication Conference MILCOM, October 2003.

[6] M. Pirrete and R. Brooks, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence", International Journal of Distributed Sensor Networks, Vol.2, No.3, pp 267-287, 2006.

[7] S. Kurosawa and A. Jamalipour, "Detecting Blackhole Attack on AODVbased Mobile Ad Hoc Networks by Dynamic Learning method", International Journal of Network Security, Vol.5, No.3, pp 338-345, November 2007.

[8] Soyoung Park, B. Aslam, D. Turgut and C.C. "Defense Against Sybil attack in vehicular ad hoc network" *Military Communications Conference, MILCOM,IEEE, 2009*, pp. 1-7

[9] Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM Mobi Com Workshop - WiSe'03,2003.

[10] P.Yi, Z.Dai, Y. Zhong and S.Zhang, "Resisting Flooding Attack in Ad Hoc Networks", Proc. IEEE International Conference on Information Technology Coding & Computing ITCC, April 2005.

[11] Yi Qian; Moayeri, N. 2008. Design of Secure and Application-Oriented VANETs. Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, vol., no., pp.2794-2799, 11-14 May 2008.

[12] Ching-Hung Yeh, Yueh-Min Huang, Tzone-I Wang, Hsiao- Hwa Chen. 2009. DESCV - A Secure Wireless Communication Scheme for Vehicle Adhoc Networking. MONET. *Published in Journal Mobile Networks and Applications*, Volume 14, Issue 5, pp.611-624, October 2009.

[13] Gosman, C.; Dobre, C.; Cristea, V. 2010. A Security Protocol for Vehicular Distributed Systems. *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2010 12th International Symposium on*, vol., no., pp.321- 327, 23-26 Sept. 2010.

[14] Rawat, D.B.; Bista, B.B.; Yan, G.; Weigle, M.C. 2011. Securing Vehicular Ad-hoc Networks Against Malicious Drivers: A Probabilistic Approach. *Complex, Intelligent and Software Intensive Systems (CISIS), 2011 International Conference on*, vol., no., pp.146-151, June 30 2011-July 2 2011.

[15] P. Papadimitratos *et al*., "Secure vehicular communication systems: design and architecture, *IEEE Communications Magazine*, vol. 46, no. 11, pp.:100–109, Nov. 2008.

[16] P. Yi *etal*., "Resisting Flooding Attack in Ad Hoc Networks", *Proc. IEEE Int. Conf. on Information Tech. Coding & Computing* (*ITCC*), April 2005.

[17] Q, Wu *etal*., "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications", *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp.559-573, 2010.

[18] R. Mehmood and M. Nekovee, "Vehicular Ad hoc and Grid Networks: Discussion, Design and Evaluation", *Proc. 14th World Congress on Intelligent Transport Sys.*, pp. 8-21, 2007.

[19]. Parul Tyagi, Deepak Dembla, "A Taxonomy of Security Attacks and Issues in Vehicular Adhoc Networks (VANETs), *International Journal of Computer Applications* (0975 – 8887) Volume 91 – No.7, April 2014.