SECURITY ISSUES IN VANET TECHNOLOGY

[1]Fathima Sambreen, [2]Alima Thamanna Valiyakath, [3]Khadeeja Raeesa, [4] Mustafa Basthikodi
[1,2,3]Student, [4]Professor, Dept. of CSE,
Bearys Institute of Technology Mangalore.

ABSTRACT

Vehicular Ad-hoc Network (VANET) is basically the solution of several problems associated while vehicles are plying on the road. It is the sub category of MANET (Mobile Ad-hoc Network). The development of inter-vehicle communication technology leads to improved safety and efficiency of traffic. Vehicular Ad-hoc Network (VANET) serves users with applications for safety and non-safety, but needs security to implement the wireless environment.
In VANET vehicles, due to the reasons that vehicles are nodes with mobility, there is no fixed infrastructure. It serves safe and non-safe wireless applications because VANET is most concerned about security.
Each node in VANET acts as a vehicle or roadside unit that can move freely and stay connected within the network range.
The communication between the nodes is in a single hop or multiple hop.
VANETs, however, are themselves vulnerable to attacks that can lead directly to network corruption and possibly result in large losses of time, money, and even lives. This paper provides Overview of VANET and discussing about various threats facing by the VANET and going to discuss some of the issues with details and solutions for the same and some with the overlook knowledge in various threats in VANETs.

1. INTRODUCTION

In the last few years, accompanying the massive deployment of wireless technologies and the growing number of wireless products on motorized vehicles including remote keyless entry devices, personal digital assistants (PDAs), laptops, and mobile telephones, automotive industries have opened a wide variety of possibilities for both drivers and their passengers.Vehicle ad hoc networks (VANETs) have attracted a great deal of attention in the research community due to their varied value-added services, namely vehicle safety, automated toll payments, traffic management, enhanced navigation, location-based service to find the nearest fuel station, travel lodge or restaurant and easy access to the Internet.

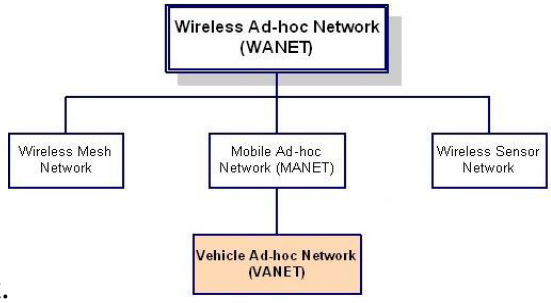

Fig. 1. Hierarchy of wireless ad hoc networks

However, many forms of attacks against VANETs have emerged recently and alarmed the unsettling situation of these networks' security. Being an implementation of Mobile Ad hoc Networks (MANETs) (Fig. 1), VANETs inherit all the discovered and undiscovered security and privacy vulnerabilities related to MANETs. Furthermore, VANETs have a number of distinctive properties that could be also vulnerabilities for attackers to exploit. Those properties include the particular nature of communication in VANETs. Connections are based on node-to-node communications in particular in a VANET and in any wireless ad hoc network in general: Each node can act as either a data requesting host or a data forwarding router. Two types of nodes exist:
(i)Roadside Units (RSUs) standing for fixed route nodes and (ii) Onboard Unit (OBU) referring to mobile nodes (i.e. vehicles) equipped with some kind of radio interface that allows wireless connection to other nodes. Fig. 2 depicts a general view of VANETs structure. It is worth mentioning that the speed of mobile nodes- vehicles in VANETs may be much higher than in MANETs. This reason makes VANETs very dynamic in nature. A number of nodes can communicate once as a group but can then rapidly change their own structure caused by leaving of a member or joining of another node. Therefore, it is expected that nodes are continuously "keeping in touch" with other nodes in the group to maintain the survival of the network. This aspect of VANETs seems to be very

vulnerable and attacks can be unconsciously or intentionally performed to damage a part of or the total network. As mentioned above, VANETs provide many added applications that are safety, entertainment, or infotainment oriented. Attacks to VANETs may lead to catastrophic consequences such as the losses of lives in the case of traffic accident, losses of time (e.g., tampering traffic jam made by attacks) or financial losses (i.e., in payment services).

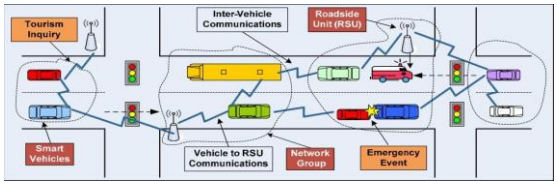

Fig. 2. A basic structure of VANETs

The researches on VANETs security were triggered in the middle of 2000s and genuinely bloomed since 2007. In order to provide a thorough survey covering a big number of publications related to VANETs attacks, we searched for and collected papers approaching this topic from 2007 to 2013 that had made a significant contribution to the improvement of VANETs security. Fig. 3 indicated the numbers of publications each year that we found by searching on five main technical publishers, including IEEE explore, ACM Portal, Springer Online Library, Wiley Inter Science, and Elsevier Online Library, with either "VANETs security" "VANETs attacks" "VANETs vulnerabilities" keywords in title or abstract.

There has been many research works on the VANETs security in general and VANETs attacks in particular, especially the last three years from 2011 to 2013. However, there is a few survey works in the literature on VANETs attacks. In the existing surveys, some of attacks were not enough illustrated in detail and some were missed. Our paper aims to introduce more concisely the possible attacks, their mechanisms and influences as well as their corresponding solutions to thwart those attacks. We characterize the attacks (e.g., type of attacker, security aspects that are damaged) for a further classification. For each attack, we try to perform a concise scenario to better identify this attack. We equally point out the properties that can be collected to detect the attacks. These properties could be the input for an intrusion detector that we consider as future work of our research. Our purpose in this study is to not only depict a detailed list containing up-to-date attacks but also a global view of security threats in VANETs, in order to provide a useful starting point for researchers interested in the subject and to help VANETs designers to develop and deploy secure VANETs infrastructures.

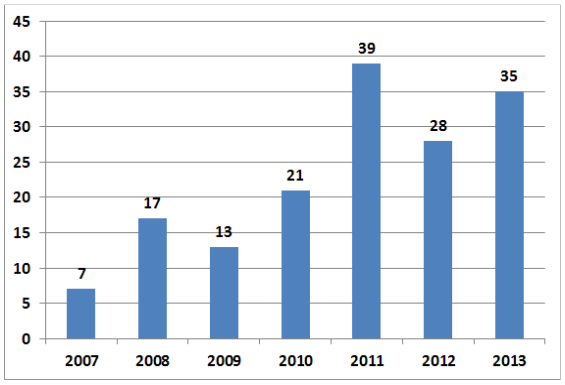

Fig. 3. VANETs security publications from 2007 to 2013

The rest of this paper is organized as follows: Section 2 presents some similar works to our study. Section 3 is devoted to the VANETs security requirements. Section 4 contains the VANETs attacks and their corresponding solutions as well as examples. Section 5 summarizes the attacks that were mentioned in previous section, characterizes, and classifies them. Finally, we discuss about our study, conclude, and propose the future work in section 6.

2. TYPES OF ATTACKERS IN VANET

Insider vs. Outsider

If the attacker is a member node capable of communicating with other network members, they will be known as an insider and will be able to attack in different ways.Whereas, an *outsider*, who is not authenticated to directly communicate with other members of the network, have a limited capacity to perform an attack (i.e., have less variety of attacks).

Malicious vs. Rational

A malicious attacker uses different methods to damage the member nodes and the network without seeking their personal advantage. On the contrary, the attacks expect a rational attacker to take advantage of their own. These attacks are therefore more predictable and some patterns follow.

Active vs. Passive

An active attacker can generate new packets to da mage the network while a passive attacker only e avesdrops the wireless channel but is unable to ge nerate new (i.e. less harmful) packets.In fact, there is another attribute to characterize an attacker, which is presented in [8]:

Local vs. Extended

An attacker is considered to be local if its scope is limited, even if it has multiple entities (e.g. vehic les or base stations). Otherwise, by controlling se veral entities that are scattered across the network , an extended attacker extends its scope.This distinction is especially important in wormhole attacks that we will describe later.

Table 1: Proposed classification of attacks in VANET

Monitoring Attacks
Social Attacks
Timing Attacks
Application Attacks
Network Attacks

Attackers can directly affect other vehiclesand inf rastructure in first-
class Network Attacks. These attacks are at a high risk level as they affect the entire network.While the targets of attackers are applications in the App lication Attacks class that provide added service i n VANETs.
The attacker is mainly interested in changing appl ications content and abussing it for their own ben efit.
The third class — Timing Attacks — is a type of attacks in which the main goal of the attackers is t o add some time slot in the original message, for example, to create delays to block this message fr om coming to the receiver before its lifetime expi res. All immoral messages that trigger other drive rs ' bad emotions are classified into the Social Att acks class.Finally, in the Monitoring Attacks clas s, there are attacks in which monitoring and tracki ng activities are performed.
The related works above alert an alarming situation of VANETs security. In the next sections, we aim to emphasize security requirements in VANETs, then introduce more concisely the possible attacks, their corresponding countermeasures and propose another classification of these attacks.

3. VANETS SECURITY REQUIREMENTS

In this section, we present the main security requirements for VANETs. Three properties regarding security that cannot be ignored are confidentiality, integrity, and availability. In terms of VANETs security, these three properties stand for some more specific meaning.

Confidentiality

The confidentiality definition in VANETs refers t o **"confidential communication".**
In a group, none other than group members can decry pt the messages broadcast to each group member ; and none (including other members) except a dedicated re ceiver member can decrypt the message dedicated to it .

Integrity

It ensures that attackers do not alter the data or m essages delivered between nodes.
This concept in VANETs often combines with the concept of "authentication" to ensure that: a node should be able to verify that another node actuall y sends and signs a message without anybody mo difying it. In order to gain this property, Data Verification is also required: Once the sender vehicle is authenticated, the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.

Availability

The network should be available even if it is under an attack without affecting its performance. This concept of VANETs is not different from itself in other kinds of networks but not easy to ensure because of the mobility in high speed of vehicles.
Besides three main security requirements above, the following security aspects should be also satisfied in VANETs:

Privacy

It is necessary to maintain the profile or personal i nformation of a driver against unauthorized acces s. We consider the following two cases:
-
Communications between vehicles and RSUs: Pri vacy means that it is impossible for an eavesdrop

per to decide if two different messages come fro m the same vehicle.

-

Communications between vehicles: Privacy mean s determining whether two different valid messag es from the same vehicle are heavily burdensome for all but a legitimate component.

Identity privacy preserving is similar to the concept of **"Anonymity"**. That means identifying the physical identity of a message's originator should be computationally expensive.

Traceability and revocability

Although a real vehicle identity should be hidden from other vehicles, there should still be a compo nent (e.g. Trace Manager) capable of acquiring th e real identities of vehicles and revoking them fro m future use.

Non-repudiation

In the event of an accident, drivers must be reliabl y identified. A sender should be responsible for tr ansmitting the investigation messages that will de termine the correct sequence and content of pre-accident exchanged messages.

Real-time constraints

Because vehicles can move in randomly and mov e quickly to a VANET group for a short period of time, real-time constraints should be maintained.

Low Overhead

All VANET messages are time-consuming. Therefore, to retain the usefulness an d validity of messages, "low overhead" is essentia l.

4. ATTACKS AND COUNTERMESURES IN VANETS

In this paper, only the attacks perpetrated against VANETs communication are taken into consideration. Physical problems (e.g., hardware tampering) are out of the scope of our research.

4.1. Timing Attack

Safety applications are one of the most important and promising advantages of VANETs. However, they are time critical applications and require data transmissions from one vehicle to another vehicle at the right time. In timing attacks, when malicious vehicles receive a message, they do not forward it as normal but add some timeslots to the original message to create delay. Thus, neighbouring vehicles of the attackers receive the message after they actually require or after the moment when they should receive that message.

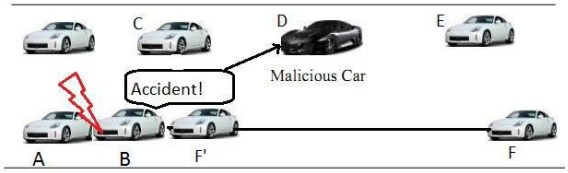

Fig. 4. Timing attack

In Fig. 8, there was an accident between two cars A and B. Malicious car D was announced about this accident but it delayed to transmit the message to the others by adding some timeslots to the Original message. F should receive this message soon to change the lane but because of the delay, it only received the message about accident when it has already reached the accident position (F'). There are also some other scenarios that are presented in including both attacks to V2V communications and V2I communications.

4.1.1: Solution to timing attack

In order to avoid timing attacks, data integrity verification is required to eliminate any timeslots that can be added to packets. TPM (*Trusted Platform Module*) is one of the major security approaches to maintain the integrity of message by using the strong cryptographic functioning modules. Together with two protocols, namely Privacy Certification Authority (PCA) and Direct Anonymous Attestation (DAA), TPM has proved its two main advantages: (1) -Secure piece of hardware with cryptographic capabilities and (2) - Abilities to protect and store data in shielded location. TPM plays the role as a powerful solution for evenly other attacks that violate data integrity. However, like any other cryptographic solution, TPM can negatively affect to the performance of network.

4.2 : Denial of Service (DoS)

In wireless environment, typically the attacker attacks the communication medium to cause the channel jam or to create some problems for the nodes from accessing the network. The basic purpose is to prevent the authentic nodes from

accessing the network services and from using the network resources. The attack may result in devastation and overtiredness of the nodes' and network's resources. Ultimately, the networks are no longer available to legitimate users. In VANET, DOS shall not be allowed to happen, where seamless life critical information must reach its intended destination securely and timely. In summary, there are three ways the attackers may achieve DOS attacks, namely communication channel jamming, network overloading, and packets dropping. There are three levels of DOS attacks as described below.

1) Basic Level: Overwhelm the Node Resources

In this DOS basic level attack, the goal of the attacker is o overwhelm the node resources such that the nodes cannot reform other important and necessary tasks. The node becomes continuously busy and utilizes all the resources to verify the messages.

a) Case 01: DOS Attack in V2V Communications

As shown in Figure 1, an attacker sends a warning message *Accident at location Y*". A victim node behind the attacker ode receives this message. However, the sending of the same message is repeated continuously, thus keeps the victim node use and thus completely denied for accessing the network.

Fig. 5 DOS attack in vehicle-to-vehicle communications

b) Case 02: Launch DOS Attack in V2I Communications In this case, the attacker launches attack to Road Side Unit RSU) as depicted in Figure 2. When RSU is continuously Busy to verify the messages, any other nodes want to Communicate with the RSU will not be able to get any response from it, thus the service is unavailable. Hence, sending critical life information in this situation is full of risk.

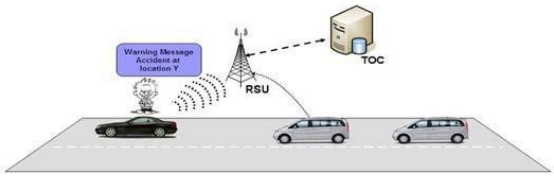

Fig. 2. DOS attack in vehicle-to-infrastructure communications

2) Extended Level: Jamming the Channel

This is a high level of DOS attack in which attacker jams the channel, thus not allowing other users to access the network. The following are two possible cases.

• *Case 01:* Attacker sends high frequency channel and jams the communication between any nodes in a domain, as depicted in Figure 3. These nodes cannot send or receive messages in that domain, i.e. services are not available in that domain due to this attack. When a node leaves the domain of attack, only then it can send and/or receive messages.

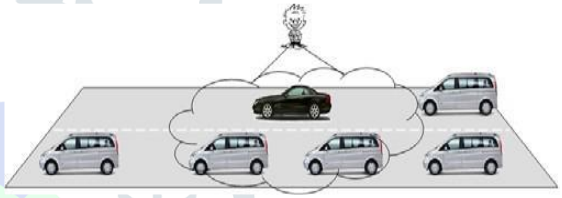

Fig. 6. A domain of jammed channel for vehicle-to-vehicle communications

• *Case 02:* The next stage of attack is to jam the communication channel between the nodes and the infrastructure. Figure 4 showed the situation where the attacker launches an attack near the infrastructure to jam out the channel, leading to network breakdown. In this way, sending and/or receiving messages to/from other nodes is not possible and would fail due to network unavailability.

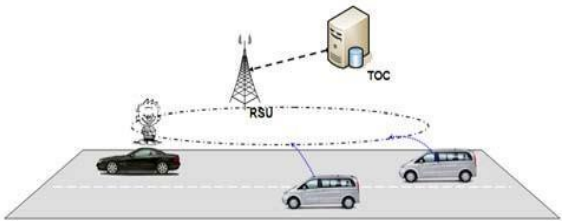

Fig. 7. Jam the channel between vehicle-to-infrastructure

4.2.1: Solution to denial of service (DoS) attack

One of DoS attack solutions is based on the support of OBU (Onboard Unit) that is equipped in vehicles. There is a processing unit that has the role to suggest to the OBU to switch channel, technology, or to use frequency hopping technique or multiple transceiver in the case of DoS attack. The work in present a distributed and robust defense against DoS attacks where a malicious node forges a large number of fake identities, i.e., Internet Protocol (IP) addresses in order to disrupt the proper functioning of fair data transfer between two fast-moving vehicles. In the proposed approach, these fake identities are analyzed through the medium of the consistent existing IP address information. All the vehicles exchange frequently beacon packets to claim their presence and be aware of the neighbors. Each node periodically keeps and updates a record of its database by exchanging the information with the community. If a node detects in its record that there are some similar IP addresses, these identic IP addresses are likely evidences of a DoS attack. The authors developed a model for DoS prevention called *IP-CHOCK* that prove the significant strength in locating malicious nodes without the requirement of any secret information Exchange or special hardware support. Simulation results depict an encouraging detection rate that will be even enhanced whenever optimal numbers of nodes are forged by the attackers.

4.3: Distributed Denial of Services (DDoS)

The Distributed DoS (DDoS) is more severe than the DoS where a number of malicious cars attack on a legitimate car in a distributed manner from different locations and timeslots. Fig. 8 demonstrates that three malicious black cars attack on the car A from different locations and time so that A cannot communicate with the other vehicles.

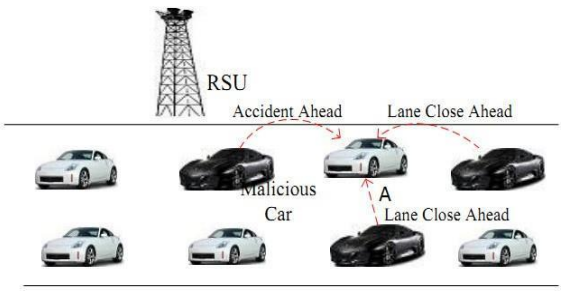

Fig. 8. Distributed Denial of Service (DDoS) Attack

4.3.1: Solution to Distributed denial of Service (DDoS) attack

The proposed model of solution to the DOS attack was used on previous works by. The model is relying on the use of On-Board-Unit (OBU) that is fitted on each vehicle node, to make decision as to deter a DOS attack. n the case of DOS attack, the Processing Unit will suggest to e OBU to switch channel, technology, or to use frequency hopping technique. Four options are available for the OBU to take decision based on the received attack message. After necessary processing and decision, the information is sent to next OBU in the network. Each switching option is explained

A. Technology Switching

There are a number of communication technologies that work with VANET, such as UMTS's Terrestrial Radio Access-Time Division Duplex (UTRA-TDD), Wi-MAX, Wi-Fi, and Zig-Bee. Whenever attacker launches attack, accessing to the network is switched between these technologies, making the attack terminated at a network type. Hence, the services of the overall network remain unaffected. Table I explained the detailed features of these technologies and also did comparison of different parameter (standard, frequency band, data rate, range and primary uses). The features of these technologies provide help to system to switch between technologies. If the intensity of the attack is low then we select low range technology and when the level of attacker/range of the DOS attack is large then we use cellular technology

B. Frequency Hopping Spread Spectrum (FHSS)

Spread spectrum is a famous technology used in GSM, Bluetooth, 3G, and 4G. The purpose of spread spectrum is to expand the bandwidth of a signal by adding some keys/codes so that data packets can be transmitted over a set of different frequency range. Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) are two basic techniques used in spread spectrum communication. FHSS changes the communication channel using some regular interval and follow some pseudo-random sequences.

4.4: Sybil Attack

The attack on Sybil is a well-
known hurtful attack that Douceur first described and formalized in peer-to-peer networks context. A vehicle declares to be several vehicles either si multaneously or in succession to carry out this ty pe of attack. This attack is very dangerous as a ve hicle can claim to be simultaneously in different p ositions, creating chaos and enormous security ris ks in the network.
The attack on Sybil damages network topologies and connections as well as consumption of netwo rk bandwidth.
In the Fig. 9, Attacker A sends multiple messages to other vehicles with different identities. Other v ehicles therefore realize that there is a heavy traffi c at the moment.

Fig. 9. Sybil attack

4.5: Node Impersonation attack

In VANET each vehicle has a unique id and with the help of these ids each vehicle is identified in the VANET network. It becomes most important when an accident happens. In node impersonation attack an attacker can changes his/her identity and acts like a real originator of the message. An attacker receives the message from the originator of the message and changes the contents of the message for his/her benefits. After that an attacker sends this message to the other vehicles.

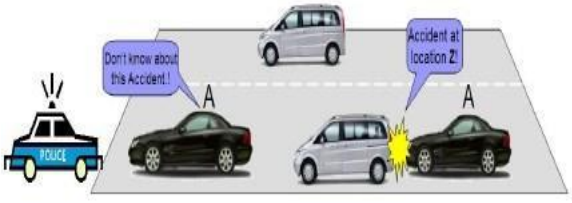

Fig. 10. Node impersonation attack

4.6: Social attack

The basic idea of the attack is to confuse and bedazzle the victim by sending unethical and unmoral message so that driver gets disturb. The legitimate user reacts in annoyed manner after getting such kind of messages which is the main objective of the attacker, It effects the driving of the vehicle which indirectly creates the problem in the network.

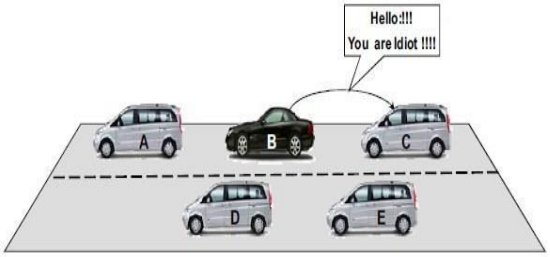

Fig. 11. Social attack

4.7: Application Attack

The main motive of attacker in this kind of attacker in this kind of attack is to content that are related to safety and non-safety related applications. Safety applications play very important role as they provide warning messages to other users. In this attack the attackers alter the contents of the actual message and send wrong messages to other users."

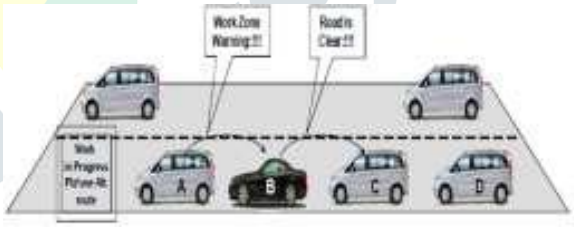

Fig. 12. Social attack

5: CONCLUSION

Risks caused by security attacks are one of the V ANETs ' major security issues that restrict the veh icle ad hoc networks ' deployment. In this paper, we presented an up- to-date collection of attacks damaging VANETs, sampled the practical scenarios, discussed the existing solutions to deal with attacks, and characterized each attack to have a thorough look over it. Our study is useful for VANETs researchers as a study on the state of the art and for designers in building the architecture or framework parameters of VANETs security. From this paper, we want to clear that: For the strong security of VANETs communication, we not only

need the secured communication frameworks but also we need powerful routing algorithms those can facilitate the detection of malicious vehicles in networks and mitigate them.

REFERENCES

[1] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah Computer and Information Sciences Department Universiti Teknologi PETRONAS-2013 on "**Classes of Attacks in VANET"**

[2]Vinh Hoa LA, Ana CAVALLI Telecom South Paris Department of Software and Networks, 9 ru e Charles Fourier 91011 EVRY, France-2014 on'' **SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY**''

[3] Ujwal Parmar, Sharanjit Singh- Astt.Prof. M.tech (CSE) Student - M.tech (CSE) Guru Nanak Dev University RC Gurdaspur, India-2015 on "**Overview of Various Attacks in VANET**"

[4] Kadam Megha V, "Security Analysis in VANETs: A Survey", in International Journal of Engineering Research and Technology (IJERT), Vol. 1 Issue 8, October - 2012.

[5]It's J.T. S. Zeadally, Isaac, and J.S. Cmara, "V ehicle ad hoc security attacks and solutions," in I ET Communications, pp. 894-903, 2009.

[6]In Journal of Computer Security, vol. 15, Janu ary 2007, pp. 39-
68, M. Raya, J. Pierre Hubaux, "Securing vehicul ar ad hoc networks."

[7] I.Ahmed Soomro, H.B.Hasbullah, J.lb.Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET", in WASET, issue 65, 2010 ISSN 2070-3724.

[8]In the Distributed Computing Systems Worksh op, I.Chen Chen, Xin Wang, Weili Han, and Biny u Zang, ' Robust Detection of Sybil Attack in Urb an VANETs, ' ICDCS Workshops ' 09. 29th Inter national Conference of IEEE, 2009, pp. 270-
276, 2009.

[9]GMT Abdalla, SM Senouci, "Current Trends i n Ad Hoc Vehicle Networks," in UBIROADS W orkshop Proceedings, 2007.

[10] Vern Paxson, "Bro: A System for Detecting Network Intruders in Real- Time", in Proceedings of the 7th USENIX Security Symthosium, San Antonio, Texas, 1998.

[11] Bachar Wehbi, Edgardo Montes de Oca, Michel Bourdelles, "Events- Based Security Monitoring Using MMT Tool ", in Software Testing, Verification, and Validation, 2008 International Conference.