Security Attacks with an Effective Solution for DOS Attacks in VANET

Adil Mudasir Malla
Department of CSE
Lovely Professional University
Jalandhar, India

Ravi Kant Sahu
Department of CSE
Lovely Professional University
Jalandhar, India

ABSTRACT

Vehicular Ad hoc Networks is a special kind of mobile ad hoc network to provide communication among nearby vehicles and between vehicles and nearby fixed equipments. VANETs are mainly used for improving efficiency and safety of (future) transportation. There are chances of a number of possible attacks in VANET due to open nature of wireless medium. In this paper, we have classified these security attacks and logically organized/represented in a more lucid manner based on the level of effect of a particular security attack on intelligent vehicular traffic. Also, an effective solution is proposed for DOS based attacks which use the redundancy elimination mechanism consists of rate decreasing algorithm and state transition mechanism as its components. This solution basically adds a level of security to its already existing solutions of using various alternative options like channel-switching, frequency-hopping, communication technology switching and multiple-radio transceivers to counter affect the DOS attacks. Proposed scheme enhances the security in VANETs without using any cryptographic scheme.

General Terms

Denial of Service Attacks, On-Board Units, Security Attacks, Vehicular Ad hoc Networks.

Keywords

Security attack pyramid, Redundancy elimination mechanism

1. INTRODUCTION

The Vehicular Ad hoc Network is a technology having the art of integrating ad hoc network, wireless LAN and cellular technology to achieve intelligent Inter-Vehicle Communications (IVC) also known as Vehicle-to-Vehicle (V2V) Communications and Roadside-to-Vehicle Communications (RVC or R2V).VANETs provide us the valuable concept for improving efficiency and safety of future transportation[1].Rapid development in wireless communication networks has made Inter-Vehicular Communications (IVC) and Road-Vehicle Communications (RVC) possible in Mobile Ad Hoc Networks (MANETs) which led to the development of a new type of MANET known as the Vehicular Ad Hoc Network (VANET),aiming to enable road safety, efficient driving, and infotainment. It has been observed that traffic accidents have been taking thousands of lives each year which is more in number than caused by any deadly diseases or natural disaster. The studies [2] show that about 60% roadway collisions could be avoided if the operator of the vehicle was provided warning at least one-half second prior to a collision. So, based on these statistic figures, scientists switch to computerize and automate the vehicular transportation system to reduce the road accidents which in estimation takes lives of about 1.2 million people per year worldwide according to a report published in 2004 by an organization [3], and injures about forty times of this number, without forgetting that traffic congestion that makes a huge wastage of time and fuel based . Figure 1 shows the general structure of VANET.

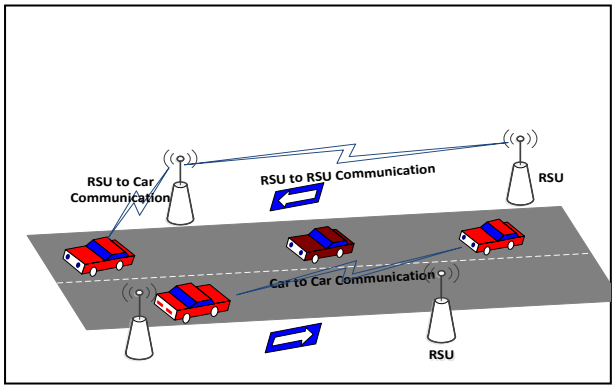

Figure 1: VANET Structure

Dedicated Short Range Communication (DSRC) is used as communication medium and it operates on 5.9GHz frequency band and is also based on IEEE802.11p for special vehicular communication [4]. Seven channels are provided for safety and non safety applications with 10 MHz bandwidth. The DSRC provides 6 to 27 Mbps data rate over 1000m communication range [5]. Safety and non safety messages are forwarded between the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) on this communication medium. Cooperation between the vehicles is essential to communicate with each other because of the short range of wireless communication medium[6].The attacker generates problems in the network by getting full access of communication medium DSRC due to open nature of the medium. Attacker may be authentic user/users (insiders) of the network that possess detail knowledge of network which they will be use for understanding the design and configuration of network. Therefore, it is easy for them to launch attacks and create more problem as compare to outsider attacker which is a kind of intruder which aims to misuse the protocols of the network.

2. LITERATURE REVIEW

Due to the nature of open wireless medium used in VANETs, there are chances of a number of possible attacks by which the network is exposed to. So, there are fairly high chances of possible attacks. The main goal of the attackers is to create problem for legitimate (genuine) users, and as a result services are not accessible which concludes in denial of

service. Researchers have described different types of attacks in their studies [7, 8 and 9] .These Security attacks are divided into five classes as proposed, by *Irshad et al.[10]* which includes almost all possible attacks. These five classes are as:

2.1 Network Attacks

It includes all those attacks which directly affect the communication medium of the network which consists of infrastructure and other vehicles. Some of network attacks are:

2.1.1 *Denial of service (DOS) Attack*

In this type of attack, 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 main purpose of the attacker is to prevent authentic nodes from accessing the network services and from using the network resources. The attacker may attack either vehicular nodes or network infrastructure i.e. RSU (access points) and sometimes both. In Fig.2, attacker A launches DOS attack both on vehicular nodes and infrastructure.

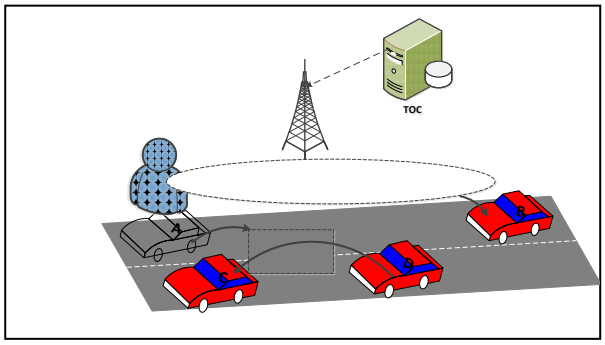

Figure 2: DOS Attack on Vehicular Nodes & Infrastructure

2.1.2 *Distributed Denial of service Attack:*

In this case attacker launches DOS attacks from different locations. The attackers may use different time slots/slices for sending the messages and the nature of the messages and time slot may be varied from vehicle to vehicle of the attackers. The aim of the attacks is to down the network as that of in DOS attack. In this case also, attacker may attack both vehicular nodes and infrastructure.Fig.3 explains DDOS attack in which attacker B and C from different locations attacks node A.

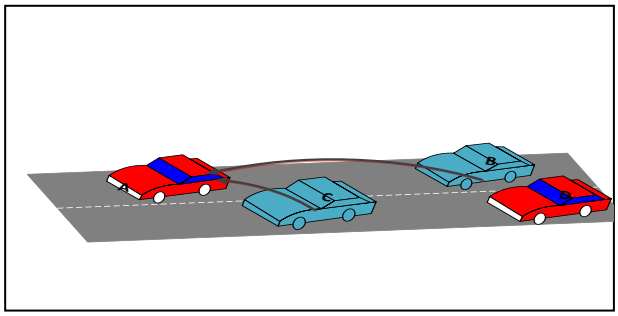

Figure 3: DDOS Attack on vehicular nodes

2.1.3 *Sybil Attack*

In this case attacker creates multiple vehicles on the road with same identity. The main motive is to enforce other vehicles on the road to leave the road for the benefits of the attacker. Scenario in fig.4 explains Sybil attack where attacker C creates its multiple duplicate copies.

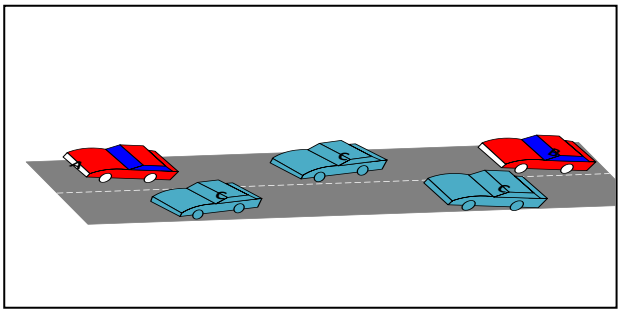

Figure 4: Sybil Attack

2.1.4 *Node Impersonation*

In this type of attack, the attacker changes his identity in order prevent from being detected. For instance if a vehicle is responsible for a specific accident then that vehicle acts as an attacker if it changes its identity before being detected.

2.2 Second class: Application Attack

In this class of attacks the main motive of the attacker is to alter the content of the applications (safety or non safety related) and use it for their own benefits. The safety related applications has more importance as they provide warning messages to other users. The attackers alter the content of the actual message and send wrong or fake messages to other vehicle which causes accident. Scenario shown in fig.5 explains safety application attack where attacker C modifies the warning message and then forwards it to node E.

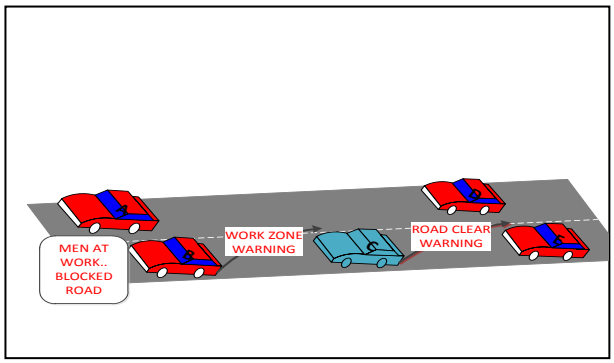

Figure 5: Safety Application Attack

Similar is the case with non-safety application attacks but the only difference is that safety-application attacks may lead to huge losses like death of a person while as this is not the case with non-safety application attacks.

2.3 Third class: Timing Attack

This is type of attack in which attacker's main objective is to insert delay in original message by adding some delay slot to it. Attackers do not disturb the other content of message but they only create delay in the message and these messages are received after their expiration time. The safety applications are time critical as if delay occurred in these applications then main objective of the application are finished.

2.4 Fourth class: Social Attack

It is kind of emotional and social attack. The sole purpose of this attack is to indirectly create problem in the network by sending unmoral messages and thus legitimate users show angry behavior when they receive such kind of messages. This is what attacker wants by launching such attacks.

2.5 Fifth class: Monitoring Attack

In this attack, the attackers monitor and listens the communication between V2I and V2V. So, whenever they find any related information then pass this information to concerned person.

Ajay Rawat et al [11] have divided security attacks on the basis of security threats to basic security requirements i.e. confidentiality, availability, authentication or integrity. These threats along with their examples are as:

Threat to availability— DOS, DDOS, Black Whole, spamming, Malware etc.

Threat to confidentiality— Timing attack, Home attack, Man-in-the-Middle attack,Traffic Analysis, Brute force attack, Bogus information, ID disclosure.

Threat to Authentication or Integrity— Sybil attack, Node impersonation, Message suppression, Replay attack, GPS spoofing, Tunneling.

All these attacks are described in [11] in detail. But the main limitation found in both [10] and [11] is that they do not depict or represent graphically effect of these attacks on network performance so that it will be easy for a common layman to handle a specific attack among many security attacks once they are detected.

3. PROPOSED SOLUTION

We organize the security attack classification of irshad et al [10] in a more lucid manner based on their effect on VANET nodes and infrastructure as shown in fig.6, known by the name *Security Attack Pyramid in VANET*.

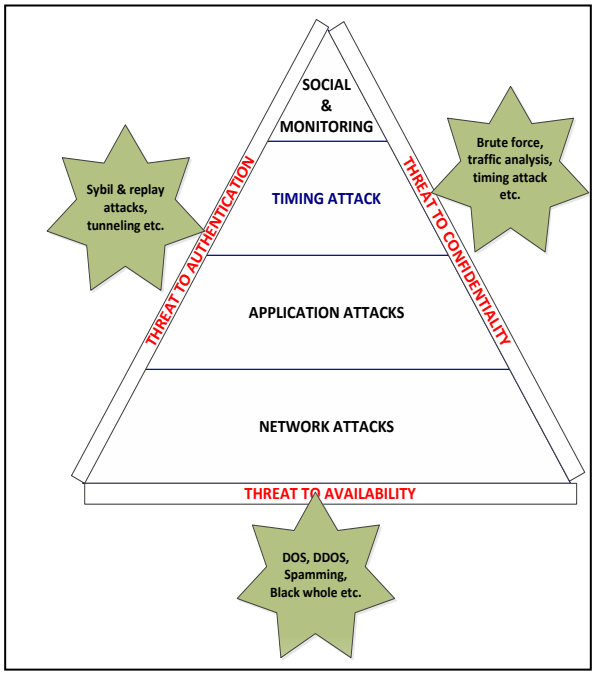

Figure 6: Security Attack Pyramid in VANETs

More the area covered by certain security attack class more will be its power of degrading communication network, so higher will be its priority in tackling it first once detected.

The classes of attacks are already explained above along with examples This organized classification will use the concept of priority to be implemented in On-Board Units (OBUs) in Vehicles and in Road Side Units (RSUs) present on road sides for these different classes of attacks so as to handle them on priority basis once these attacks are detected.

In order to identify a particular attack there should be enough information in the database of the VANET nodes and other related infrastructure as shown in the model [10] which is used for identification of different attacks but we can also implement honey pot concept in VANET in order to discover and reveal the unknown attacks (i.e. no information about these attacks are present in the database of VANET nodes).After proper analysis and audit of the honey pot sites, one can identify these unknown attacks and put them into one of classes as proposed and put the related information in the database of VANET nodes and related infrastructure for their future detection..

This means that the representation of classification as shown in fig.6 will theoretically define as to which security attack should be tackled first if more than one attacks occur simultaneously occur on a vehicle or a RSU.

3.1 Given approach to solution of DOS Attack

Following are different defense lines as a *security mechanism* to maintain reliability and availability of VANET message communication, so as to counter effect the DOS attacks .The model is relying on the use of On-Board-Unit (OBU) that is fitted on each vehicle node for make decision as to deter a DOS attack. For handling this attack, the Processing Unit will suggest to the OBU to switch technology, channel or to use frequency hopping technique. Four options are available for the OBU to make decision based on the received attack message. The information is sent to next OBU in the network after necessary processing and decision,. Each switching option is explained in the following:

1) Channel Switching: DSRC spectrum is divided into seven channels and each channel is 10MHz, as depicted in Figure 7.

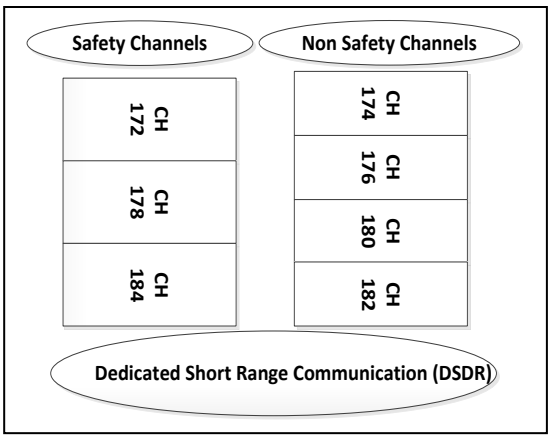

Figure 7: DSRC with its safety and non safety Channels

2) Technology Switching : As 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. Switching between these technologies for accessing the network as and when attacker launches attack paves less chance for making DOS attacks successful.

3) *Frequency Hopping Spread Spectrum (FHSS):* FHSS changes the communication channel using some regular interval in frequency range and by following some pseudo-random sequences. Whenever the attacker launches the DOS attack, the system has options to hop into different frequency channels to achieve secure transmission which results in network availability to VANET users.

4) Multiple Radio Transceivers: By applying the Multiple Input Multiple Output design principle It is also possible for the OBU to have multiple transceivers for sending and receiving messages, so that the system will have the option to move from one transceiver to another when there is any sort of DOS attacks which in turn results in elimination of the total network collapse.

3.2 Proposed approach (methodology)

The proposed approach as solution to DOS attack is based on above given solution but this approach adds one more defense base line as security to counter effect the DOS and DDOS attack not only that it also increases the general efficiency and performance of VANET in emergency warning message dissemination .

The principle which is added to the given approach is referred *as* ***redundancy elimination mechanism*** as it counter effects both *broadcast storm* in normal traffic environment and DOS and DDOS attack in case of abnormal environment in VANET. This mechanism is implemented in OBUs and RSUs. It consists of two basic modules, which are described as under:

1) Rate decreasing Algorithm: As there are higher chances of packet loss and connection loss due to mobility factor in VANET. Due to this reason, emergency warning messages (EWM) or (DOS attacker messages) are retransmitted at certain rate but it may lead to broadcast storm which is similar to some extend to DOS attack, so retransmission rate is decreased to half after every certain threshold time by each source node according to the equation given below. and if it is detected that source node does not decrease this rate by the immediate neighboring node and is retransmitting continuously with same speed, then the effected node(attacked or pray node) or intermediate node will communicate with neighboring nodes whether to block the source node (may be the attacker) based on majority voting scheme. The equation for rate decreasing as described in [12] is:

$$f(\lambda_o, k) = \max\left(\lambda_{min}, \frac{\lambda o}{a^{\,k/L}}\right) \qquad (1)$$

Where f(λ_o,*k)* = EWM transmission rate of an AV after the k_{th} transmitted EWM, λ_o is the highest transmission rate possible, λ_{min} is the minimum transmission rate possible. The equation (1) depicts that the EWM transmission rate is decreased by a factor of *a* after every *L* transmitted EWMs. The results as observed by *Xue Yang et al* [12] shows that value of *a=2* is adequate in achieving low EWM delivery delay for a wide range of co-existing AVs. Not only that, this scheme along with voting sub scheme could mitigate with DOS and DDOS attacks.

2) State Transition: As shown in figure 8, in order to implement rate decreasing algorithm as an effective tool for tackling broadcast storm and DOS attack, all nodes have to go through from *initial abnormal state,* starting transmitting emergency warning messages following rate decreasing algorithm to a *non-flagger state (retransmission rate=0)* after certain *threshold time (*based on network range) and if required, based on acknowledgement to a final *flagger state (minimum possible retransmission rate).*

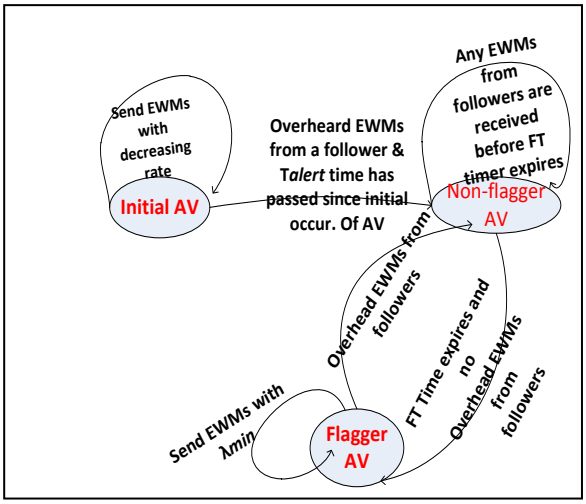

Fig. 8 State Transition Diagram

So, the overall proposed solution to DOS attack is shown in fig.9.

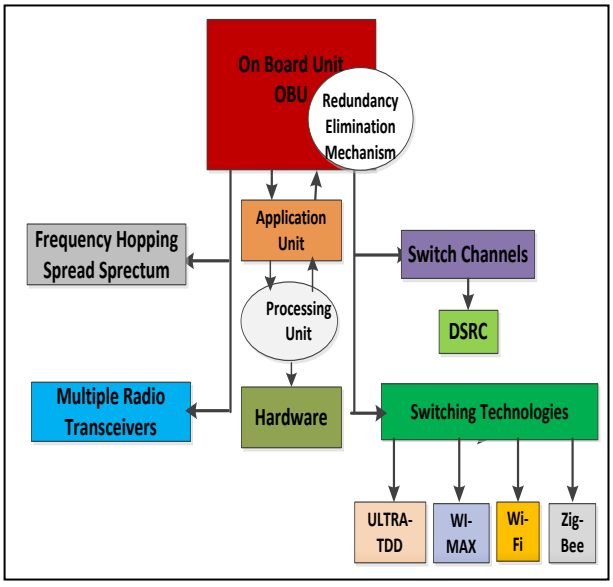

Figure 9: The proposed model of solution to DOS attacks

Advantages of proposed solution for DOS attacks:

1. Reduces or eliminates DOS attack by reducing redundancy of messages generated by the attacker.
2. Controls congestion of traffic generated by the vehicular nodes even when there are no DOS attacks.
3. Avoids broadcast storm and collision of messages.
4. Controls delay while transmitting messages among nodes by limiting or decreasing retransmission rate.
5. Efficient utilization of network bandwidth by avoiding unnecessary retransmissions.

This means that the proposed solution for DOS attacks not only handles and eliminates these attacks but it also improves the efficiency of transmitting the emergency/alert warning messages among vehicular nodes which leads to avoidance of traffic accidents.

4. RESULTS

In order to evaluate the performance of the proposed rate decreasing algorithm for avoiding the DOS attacks, we have chosen two parameters, number of collisions and delay (time) which in turn depicts how much redundancy of messages is controlled even in case of DOS attacks in VANETs. The observed values for collision and delay for different schemes as calculated by different researchers also while transmitting messages among nodes is shown in Fig 10 and Fig 11 respectively.

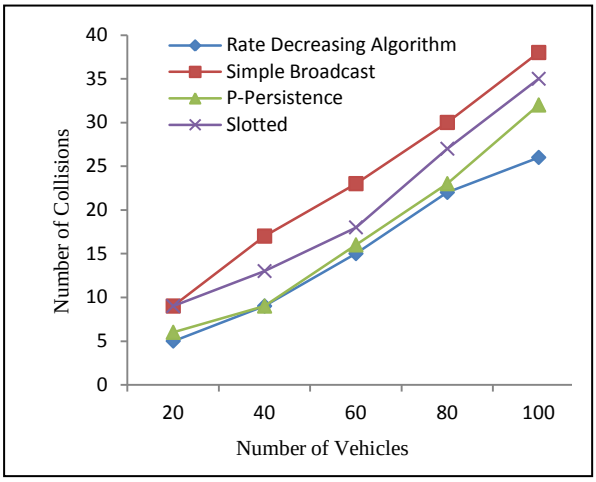

Fig 10: Number of Collisions Vs Number of Vehicles

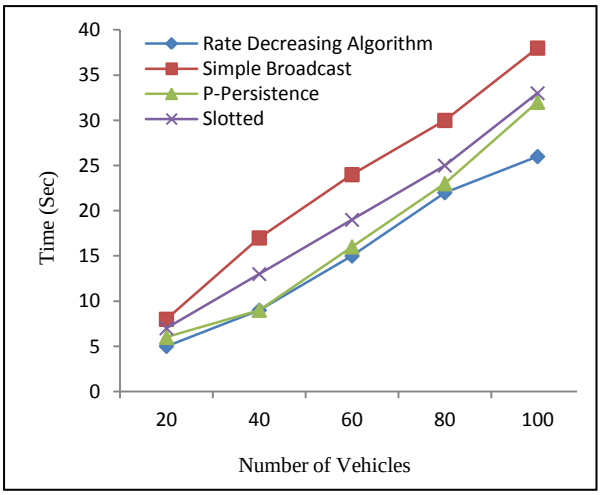

Fig 11: Delay Vs Number of Vehicles

5. FUTURE SCOPE

With the advancement in technology i.e. with the new processors having high processing capacity and with decreasing hardware cost in the market, the proposed solution will be able to increase its efficiency not in terms of handling the DOS attacks and but also in handling the normal network traffic in VANETs.

6. CONCLUSION

The proposed solution to DOS attacks use more than one lines of defense as to counter attack its (DOS) effect. Due to various defense lines along with the decreasing message retransmission rate mechanism, the solution is good enough in handling any type of DOS attack. Apart from this it also controls network traffic congestion, broadcast storm and delay while propagating emergency warning messages among vehicular nodes even in absence of DOS attacks. In short, it efficiently handles both DOS attacks and network transmissions.

7. ACKNOWLEDGMENTS

I would like to thanks my parents ,grandparents and my friend Kalimullah Lone who always urged me to go for higher studies especially to join the research arena.

8. REFERENCES

[1] Yuen Liu, Jun Bi, Ju Yang, “Research on Vehicular Ad hoc Networks”, 2009 Chinese Control and Decision Conference (CCDC 2009),978-1-4244-2723-9/09/2009 IEEE.

[2] C. David Wang and James P. Thompson, “Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network”,1997, US. Patent No. 5,613,039. Or S.Yousefi, M.S.Mousavi, M.Fathy.”Vehicular ad hoc networks (VANETs) challenges and perspectives”, in proc. of 6th IEEE international conference on ITS.

[3] http://www.who.int/en/

[4] D.Jiang, V.Taliwal, A. Meier, W.Holfelder and R.Herrtwich, "Design of 5.9GHz DSRC based vehicular safety communication", IEEE Wireless Communication Magazine, Vol.13, No.05, Nov 2006, pp:36-43.

[5] SU. Rahman, H.Falaki, ”Security & Privacy for DSRC-based automotive Collision Reporting” , www.cs.ucla.edu/falaki/courses/security project.pdf.

[6] G. Guette, B.Ducourthial,"On the sybil attack detection in VANET", Laboratoire Heudiasyc UMR CNRS 6599, France.

[7] M. Raya, J. Pierre, Hubaux,”Securing vehicular ad hoc Networks” Journal of Computer Security,vol.15, january 2007, pp: 39-68.

[8] B. Parno and A. Perrig, “Challenges in Securing Vehicular Networks,”, Hot Topics in Networks (HotNets-IV), 2005.

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

[10] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan,“Classes of Attacks in VANET“, Saudi International Electronics, Communications and Photonics Conference - SIECPC , 2011.

[11] Ajay Rawat, Santosh Sharma, Ramasushil, “VANET: Security Attacks and Its Possible Solution”, Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012.

[12] Xue Yang, Jie Liu, Feng Zhao and Nitin H. Vaidya,”A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning”,in proceeding of 1st Annual International Conference on Mobile and Ubiquitous Systems (MobiQuitous 2004), Networking and Services, 22-25 August 2004, Cambridge, MA, USA.