A Mechanism for Detecting and Identifying DoS attack in VANET

Kayvan Khajavi
Islamic Azad University
E-Campus
Faculty of Engineering and
IT

Navid Hajhasan
Islamic Azad University
E-Campus
Faculty of Engineering and
IT

Abstract
VANET (Vehicular Ad-hoc Network) which is a hybrid network (combination of infrastructure and infrastructure-less networks) is an emergent technology with promising future as well as great challenges especially in security. By the other hand this type of network is very sensible to safety problem. This paper focuses on a new mechanism for DoS (denial of service) attacks on the physical and MAC layers in IEEE standard 802.11p. In this proposed solution, DoS attack is detected and identified by using the values of packet delivery ratio (PDR) metric. Simulation results show the acceptable performance.

Keywords:
Security, VANET, attacks, DoS, detection.

1) Introduction
VANET is a special class of MANET (mobile ad-hoc network) with pre-defined routes (roads). It relies on specific authorities for registration and management, Roadside units (RSUs) and On-Board units (OBUs). RSUs are widespread on the road edges to fulfill specific services and OBUs are installed in the vehicles navigating in VANET. All vehicles are moving freely on road network and communicating with each other or with RSUs and specific authorities.
Using DSRC (Dedicated Short Range Communication) in a single or multi-hop, the communication mode is either V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) or hybrid. Fig.1 elaborates VANET architecture.

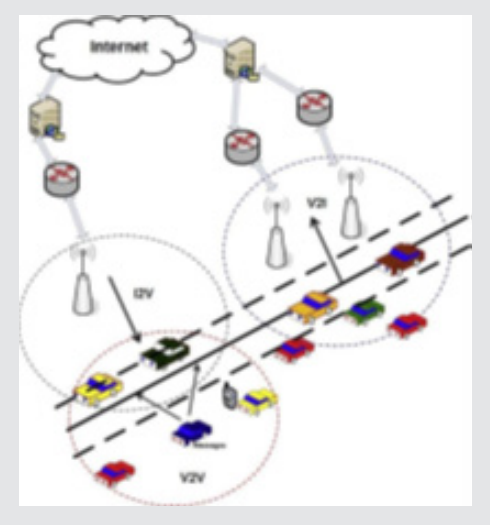

Fig.1. VANET Architecture system

In the coming days, most of the vehicles in VANET as shown in Fig.2 will be equipped with on board wireless device (OBU) including:
- GPS (Global Positioning System)
- EDR (Event Data Recorder) this is a device inspired by the black box in aircraft. It records all the information throughout the trip and can also help in the reconstruction of past events an accident.
- Sensors (radar and ladar)
- A wireless communication interface takes into account the DSRC signals and are dedicated to specialized rapid communications for VANET
- A unique electronic identifier of the same type as the license plate.

These equipment are used to sense traffic congestions and status. Then automatically take appropriate actions in vehicle and relay this information throughV2V or V2I within the vehicular network.

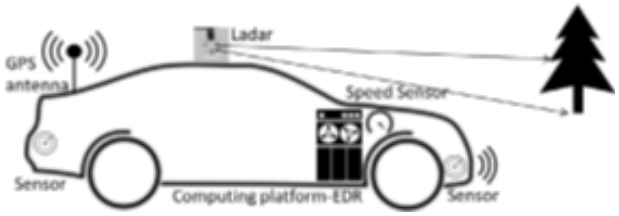

Fig.2. Future vehicle design in VANET.

Given the openness of the VANET environment, and the importance of the information exchanged, an attacker can send message whose content is adulterated, or prevent the delivery of legitimate messages to cause accidents. In order to ensure security at the user level of VANETs, we develop a method against DoS attack. Denial of services designed to make the network unavailable for a certain period. The general principle of DoS attacks is to send data or packets whose size or content is unusual, this has the effect of causing unexpected reactions of the network, up to the interruption of service. A number of network parameter suggests that there could be a DoS attack against the network led by the Attacker. In this paper, we focus on DoS attacks. In fact, the mobile hosts in mobile ad hoc networks share a wireless medium as well a radio signal can be affected, causing the service to be corrupted. There are a lot of different attack strategies that an attacker can carry out in order to interfere. This work proposes a method to detect and to identify attackers who send the same messages many times or when the majority of packets send are lost. Our mechanism can be used to improve the above contributions. The different sections of this article are structured as follow:

2) Standards of communication in VANET.
3) Network model
4) Attacker model
5) Focusing on DoS attack in VANET networks
6) Detection and Identification Mechanism
7) Simulation Results
8) Conclusion

2) Standards of Communication in VANET

A. DSRC: Dedicated Short Range Communications

DSRC is intended to be an adjunct to the cellular communications by providing very high data transmission rates under circumstances where minimizing latency in the communication link and of relatively small communication areas isolation are important. DSRC is known as WAVE (Wireless Access in Vehicular without Environments). The main reason for the MAC and physical (PHY) layers are developed under 802.11 is to ensure that the standard is stable over time.

B. WAVE: Wireless Access Vehicular Environment

The WAVE standards establish architecture and standardized complementary set of services and interfaces that allow the security V2V and vehicle-to-Infrastructure (V2I) wireless communication collectively. Together, these norms provide the basis for a variety of applications in the transport environment, including vehicle safety, automatic toll, improved navigation, traffic management and many others. The figure shows the WAVE architecture which is an association of the amendment IEEE 802.11p and four IEEE1609.1 standard, 1609.2, 1609.3, and 1609.4 defined by the IEEE 1609 working group to describe specifications of higher layers for communications WAVE.

-IEEE 1609:1: Resource Manager designed to allow remote applications to communicate with the OBU (On Board Unit) via the RSU (Road Side Unit). It defines command message formats and the appropriate responses to those messages, data storage formats that must be used by applications to communicate between architecture components, and status and request message formats.

-IEEE 1609:2: Security Services for Applications and Management Messages: This standard defines the format of packets and the security, encryption and authentication, for the three types of messages, security, and data management.

-IEEE 1609:3: Networking Services defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange.

-IEEE 1609:4: Multi-Channel Operations being based on the DSRC, WAVE devices must provide a multi-channel access and enable communications on the control channel and service channels. It is the role of the 1609:4 standard that defines all necessary mechanisms for access to priority channels, coordination and routing of data to the channels and data transmission.

This range of norms should be utilized for transportation, automotive engineers and traffic engaged in the design, specification, implementation and control of WAVE systems. Network engineers, hardware engineers, and designers IntelliDrive support applications will use these standards as they define the communication architecture for DSRC-based V2V and V2I interactions, and as a basis for designing low latency on-board and Roadside device.

C. IEEE Standard 802.11p

The IEEE 802.11p, also known as DSRC for the VANET. It is currently the sole standard with support V2V com-

munication directly from vehicle to vehicle. DSRC original standards are more specific standards for application contain the total protocol stack with a PHY, a MAC and application layer. They are designed for communication hotspots such as electronic toll collection systems. The PHY 802.11p and capabilities were processed in several papers. PHY primarily affects the reliability of the system; however, if we do not receive access to channel the advantages of the PHY may not be exploited. VANET use CSMA (Carrier Sense Multiple Access) as MAC method in spite of its failure to support realtime deadlines. A VANET is not a limited geographical area, it cannot be predictable by a central controller because of its characteristics and requirements on small very dynamic period. Traffic shaping just reduces the average time and the main problem with unbounded worst event of delay remains.

3) Network model

One of the network models is the case of cells based on the geographical location that we consider this model in this paper. Thus the set of neighbors will all vehicles present within the diameter of the cell and with which communication is established. Any node that attempts to communicate with the network nodes must send a message of the same type as that of Table I proposed by Jyoti Grover et al.

ID	Position	Speed	Time	Direction	Acceleration	Message

Table 1. Structure of a Packet type VANET

4) Attacker model

The deployment of a security system for VANET is challenging. In fact, the highly dynamic nature with frequent disconnection, instantaneous arrivals and departures of vehicles, the usage of wireless channels to exchange emergency and safety messages, expose VANET to various threats and attacks. In this section, we will classify the attacks, the attackers and analyze which VANET communication mode they affect.

4-1) Attacks

Attacks can be categorized into four main groups: (1) those that pose a risk to wireless interface, (2) those that pose a threat to hardware and software, (3) those that pose a hazard to sensors in-put in vehicle and (4) those that pose a danger behind wireless access, which means in the infrastructure (CAs or vehicle manufacturer). The following sub-sections present the threats posed to each of the areas mentioned above.

1) Threats to Wireless Interface

- Identity and geographical position revealing (Location Tracking): an attacker tries to get info of the driver and trace him. This exposes a certain node at risk. For example, a car rental company that wants to follow in an illegitimate manner its own vehicles. Users will be tracked and no privacy preserving.

- DoS: an attacker tries to make the resources and the services unavailable to the users in the network. It is either by jamming the physical channel or by “Sleep Deprivation”.

- DDoS (Distributed Denial of Service): it is a DoS from different locations.

- Sybil Attack: an attacker creates multiple vehicles on the road with same identity. It provides illusion to other vehicles by sending some wrong messages for the benefits of this attacker.

- Malware: an attacker sends spam messages in the network to consume the network bandwidth and increase the trans-mission latency. It is difficult to control this kind of at-tack, due to lack of necessary infrastructure and centralized administration. Attacker disseminates spam messages to a group of users. Those messages are of no concern to the users just like advertisement messages.

- Spam: an insider node transmits spam messages to increase transmission, latency and bandwidth consumption.

- Man in the Middle Attack (MiM): a malicious node listens to the communication established between two other vehicles. It pretends to be each one of them to reply to the other. It injects false information between them.

- Brute force Attack: is a trial-and-error method an attacker uses to obtain information such as a user password or personal identification number or to crack encrypted data, or to test network security.

- Black Hole Attack: a malicious node declares having the shortest path to get the data and then routes and redirects them. The malicious node is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packet to wherever he wants.

2) Threats to Hardware and Software:

- Injection of erroneous messages (bogus info): an attacker injects intentionally falsified info within the

network. It directly affects the users' behavior on the road. It causes accidents or traffic redirection on the used route.

- Message Suppression or alteration: attacker drops packet from the network or changes message content. In addition to Fabrication Attack where new message is generated. Or Replay Attack by replaying old messages or Spoofing and Forgery attacks that consist of injection of high volume of false emergency warning messages for vehicles. Or Broadcast tampering: in which attacker injects false safety messages into the network to cause serious problems.

- **Usurpation of the identity of a node (Spoofing or Impersonation or Masquerade):** an attacker tries to impersonate an-other node. To receive his messages or to get privileges not granted to him. Doing malicious issues then declaring that the good one is the doer.

- **Tampering Hardware:** during yearly maintenance, in the vehicle manufacturer, some malicious employees try to tamper the hardware. Either to get or put special data.

- Routing Attack: an attacker exploits the vulnerability of the network layer, either by dropping the packet or disturbing the routing. It includes in addition to the Black Hole Attack:

- **Wormhole attack:** Overhearing data; an attacker receives packets at a point targeted via a tunnel to another point. He replays it from there.
- **Greyhole attack:** a malicious node misleads the network by agreeing to forward the packets. But sometimes, he drops them for a while and then switches to his normal behavior.

- Cheating with position info (GPS spoofing) and tunneling attack: hidden vehicles generate false positions that cause accidents. GPS doesn't work.

- Timing attack: Malicious vehicles add some timeslots to the received message, to create delay before forwarding it. Thus, neighboring vehicles receive it after they actually require, or after the moment when they should receive it.

- Replay attack: malicious or unauthorized users try to impersonate a legitimate user/RSU by using previously generated frames in new connections.

3) Threats to Sensors input in vehicle

- Illusion attack: the adversary deceives purposefully the sensors on his car to produce wrong sensor readings. Therefore, incorrect traffic warning messages are broadcasted to neighbors.

- Jamming attack: the attacker interferes with the radio frequencies used by VANET nodes.

4) Threats to Infrastructure

- Unauthorized access: malicious entities try to access the net-work services without having the rights or privileges. This causes accidents, damage or spy confidential data.

- Session Hijacking: authentication is done at the beginning. After that, the hackers take control of the session between nodes.

- Repudiation (Loss of event traceability): denial of a node in a communication.

4-2) Attackers

VANET attackers are one of the basic interests of the researchers. They got many canonical names listed below based on their actions and targets:

- Selfish driver: he can redirect the traffic.

- Malicious attacker: he has specific targets. He causes damages and harms via applications in VANET.

- Pranksters: attacker does things for his own fun; such as DoS or message alteration (hazard warning) to cause road traffic for example.

- Greedy drivers: they try to attack for their own benefit. For example: sending accident message may cause congestion on road. Or sending false messages for freeing up the road.

- Snoops/eavesdropper: attacker tries to collect information about other resources.

- Industrial insiders: while firmware update or key distribution, malicious employees do hardware tampering.

The attackers are classified into:

- Insider vs. outsider: insider represents authenticated user on the network vs. outsider one with limited capacity to attack.

- Malicious vs. rational: malicious presents any personal benefit vs. rational which has personal and predictable profit.

- Active vs. passive: active attacker generates signals or packets vs. passive one who only senses the network.

- Local vs. extended: local attacker works with limited scope even on several vehicles or base stations vs. extended attacker which broadens his scope by controlling several entities scattered across the network.

5) Focusing on DoS attacks in VANET networks

Denial of Service consists in making different resources and services for users in the network unavailable; it is usually caused by other attacks on bandwidth or energy resources of other nodes. The most naive technique to cause a denial of service in a wireless network is to cause interference channel "Jamming"; another attack called "sleep deprivation" of requesting a service that the offer repeatedly referred node to squander his resources and systems to prevent "rest". The goal of this attack is to prevent the receipt of a message related to security, so it aims to cancel the security services offered by these networks.

5-1) Detection of DoS attack

It is necessary to provide means of supervision and alert in order to detect an incident. Our supervision means to base using the delivered package rates PDR (Packet Delivery Ratio). DoS attacks can lead to abnormal conditions, preventing, intercepting or blocking communication between vehicles in a VANET network. The PDR is the ratio between the number of packets that are successfully delivered to a destination on the number of packets that were sent by the sender.

$$PDR = \frac{r_i}{s_i}$$

where is the data packets successfully received and is the data packets sent. Then, the average PDR is given by:

$$PDR_{\mu} = \frac{\sum r}{\sum s}$$

A transmitter node confirms the issuance of a packet only when it receives an ACK packet from the receiving node. If the mechanism (RTS / CTS / DATA / ACK) is used, the PDR can be calculated by comparing the number of packets sent (RTS and DATA) to the number of received packets (CTS and ACK). This method can be applied to the transmitter.

Calculation of the PDR's threshold: We use a statistical method to determine normal and abnormal network conditions. This method includes a simple approach in which a lower limit (LCL: Lower Control Limit) and an upper limit (UCL: Upper Control Limit) can be calculated using the mean value μ and standard deviation of the normal distribution. Values outside of the range [LCL, UCL] are designated as abnormal values. The threshold for the PDR is calculated according to the following equation:

$$PDR_{th} = PDR_{\mu} - \sigma$$

The values of PDR which are less than PDRth will be considered abnormal values, because these values mean that the number of packets successfully received is low and therefore there is a problem with the communication medium.

5-2) Reactions against the attack

- The failed component. Is it a saturation of network links, an overload at a server or more?
- The sources of the attack: Is the packets from an internal network to the entity, or from outside? Is the attack generated by a small number of sources?
- Protocols used: We have to consider if the protocol allows identifying sources of attack (spoofing possibility of the source IP address).

Once the characteristics of the attack identified several actions may be taken depending on the nature of it (e.g. blocking source IP addresses identified as the source of the attack). In our work, we built a blacklist which puts source IP addresses of attackers.

5-3) Declaration of attack

In this work, in order to report the attack to the base station, the blacklist is encrypted at the vehicle processing platform to send to the RSU using equipment communication.

6) Detection and Identification Mechanism

In this section, we describe our model to detect the DoS attack in ad hoc networks; this solution is based on the values of PDR. In standard environment situation, all packets sent by the transmitter must be received accurately by the receiver, in such case when there is no obstacle in the communication channel or medium. But when a vehicle is moving on the road, it is considered under attack, when

the PDR values are decreased according time, and also falls below a fixed threshold. Figure 3 shows an example of the network where we will evaluate our algorithm. It presents a node that belongs to the network, represented by a vehicle, which is characterized by its coverage area that changes depending on the nature of the node and other criteria related to mobility.

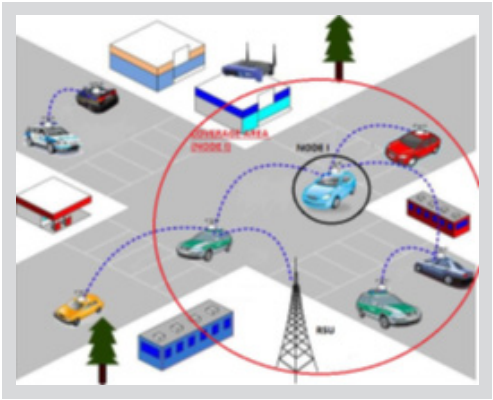

Fig. 3. Example of VANET

– For each communication between two nodes, the vehicle position is determined. If the receiving node J is located in the coverage area of the transmitter I node, it is checked that the node I has not sent a packet number that exceeds the threshold (Sent the same packet several times and to the same destination prevents receiver using the service and makes it unavailable)
– For each node i, the value of the PDR is calculated in different time instant.
– In the case where the packet rate successfully delivered decreases. If its value is below a certain threshold, and attacked node receives the same packet multiple times a DoS attack is detected.
– At the receiver, PDR value is measured at the MAC layer; by ratio of packets number passing the CRC check to the packets number received. Packets passing the CRC check are sent by the sender. The received packets are packets sent by the attacker or sender.
– If the node I is identified as a forward, we modify its fidelity level to add nodes with a level equal to 1 in the blacklist.
– We construct a black list where we put the IP addresses of attackers, then working on the encryption of this list in order to send to RSU so they can send it to other nodes to prevent packets sent from the attacker.

Algorithm 1 Detection and identification of attacks in VANET

INPUTS : Status_ATT=false,
Nodes, Nodes_ID, Nodes_Pos(x,y), Dmax,
Nb_packet_send, Nb_packet_th,
Level_of_Fidelity=0,Black_List=∅
OUTPUTS : Status_ATT,Black_List
for all $i \in Nodes$ **do**
  for all $j \in Nodes$ **do**
    $D_{ij} = Node\_Pos(j) - Node\_Pos(i)$
    if $D_{ij} \prec D_{max}$ **then**
      if $Nb\_packet\_send_{ij} \geq Nb\_packet\_th$ **then**
        $PDR_i = procedure\_of\_calcul\_PDR$
        if $PDR_i \prec PDR_{th}$ **then**
          $Status\_ATT = true$
          Level_of_Fidelity(i)=1
        else
          $Status\_ATT = false$
        end if
      end if
    end if
  end for
  if $Level\_of\_Fidelity(i) = 1$ **then**
    $Black\_List.add(Nodes\_ID(i))$
  end if
end for

7) Simulation Results

Parameters	Values
Simulation tool	NS-2 version 2.35
MAC Protocol	IEEE 802.11P
Numbers of vehicles	10
Simulation Time	30s
VANET region	1600m x 1600m
Channel type	Wireless

Table 2: Parameters used in the network

We use the MATLAB and NS-2 to implement and validate the proposed solution. We can compare performance of the communication between vehicles in the case where there is no DoS attacks and where there is DoS attacks. The simulation was executed with 10 nodes.

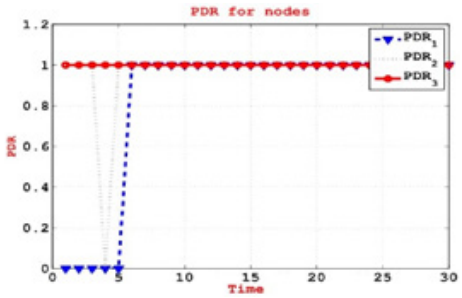

Fig.4. Packets delivered between nodes 1, 2 and 3.

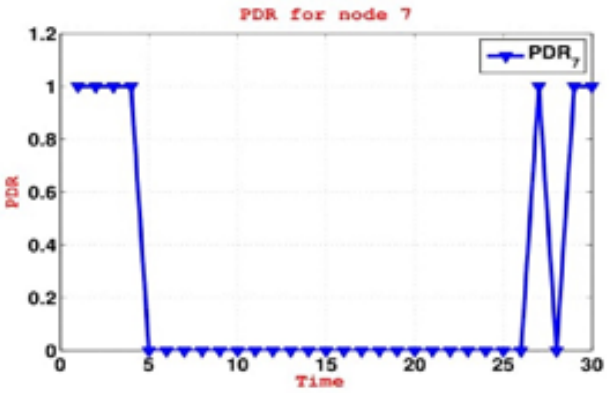

Fig.5. Packets delivered for node 7.

Simulations occur during 60s. In the simulations, the performance metric which was discussed is the packets delivery ratio (PDR) according to the communication between the nodes. We see that the majority of packets sent to the node 7 (figure 5) are not delivered successfully, unlike other network nodes (figure 4). Figure 6 shows the average value of the packet rate issued for each node. In compare with the threshold it can be inferred that there is a DoS attack, and node 7 are under attack.

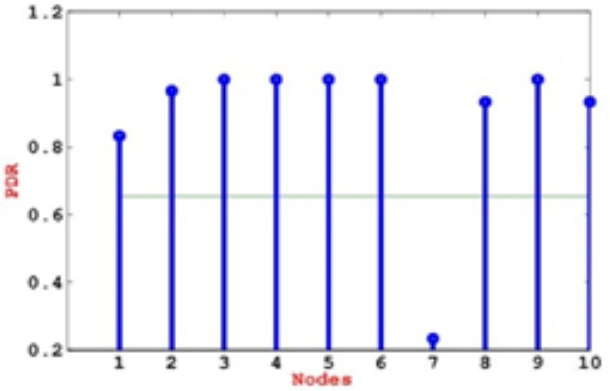

Fig.6. Average value of PDR.

After the detection of the presence of a DoS attack. The IP address of the packet transmitter allows you to specify the attacker.

Attacker's IP address is added to or all attackers (if it is a DDoS (Distributed Denial-of-Service) attack) in a blacklist. So we can conclude from the black list that nodes 2 and 4 are the attackers, and it is a DDoS attack (node 7 is attacked by the nodes 2 and 4) our method has allowed us to detect the attack and to identify the attackers using the transmitter ID.

LF -

0 1 0 1 0 0 0 0 0 0

BL -

2 4

Fig.5. Level of fidelity (LF) for each node and the blacklist (BL).

8) Conclusion

Users want safety and security much more on the road as many people life end there, due to misbehaving and maliciously of others. Overcoming these problems requires more efforts in the future to reach a secure VANET environment. This paper presented an overview of the most of VANET security challenges and their causes as well as introducing a mechanism for detecting and identifying DoS attack in VANET. In this study, we proposed one solution based on the change of packets delivery ratio. It can detect the presence of DoS attacks as soon as their attacks are effective. As a new study in the future the black list would be encrypted to be sent to the RSU to be disseminating it to users of the network to prevent packets sent by attackers.

References

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Ve-hicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Commun. Surv. Tutor. 13 (4) (July 2011) 584–616.

[2] R.S. Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for VANET, Int. J. Netw. Secur. Appl. 5 (5) (September 2013).

[3] Gh. Samara, W.A.H. Al-Salihy, R. Sures, Security analysis of vehicular ad hoc networks (VANET), in: Second International Conference on Network Applica-tions Protocols and Services (NETAPPS), IEEE, 2010, pp. 55–60.

[4] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. 1 (2014) 53–66, contents available at ScienceDirect, www.elsevier.com/locate/vehcom.

[5] N.K. Chauley, Security analysis of vehicular ad hoc networks (VANETs): a com-prehensive study, Int. J. Netw. Secur. Appl. 10 (5) (2016) 261–274.

[6] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, Alex. Eng. J. 54 (2015) 115–1126, available at www.elsevier.com/locate/aej.

[7] K. Lim, D. Manivannan, An efficient protocol for authenticated and secure mes-sage delivery in vehicular ad hoc networks, Veh. Commun. 4 (2016) 30–37.

[8] R. van der Heijden, Security architectures in V2V and V2I communication, in: 13th Twenty Student Conference on IT June 21st, Enschede, The Netherlands, 2010.

[9] V. La Hoa, A. Cavalli, Security attacks and solutions in vehicular ad hoc net-works: a survey, Int. J. Netw. Syst. 4 (2) (April 2014).

[10] A.Y. Dak, S. Yahya, M. Kassim, A literature survey on security challenges in VANETs, Int. J. Comput. Theory Eng. 4 (6) (December 2012).

[11] M. Raya, A. Aziz, J.P. Hubaux, Efficient secure aggregation in VANET, in: Pro-ceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks,VANET '06, 2006, pp.67–75.

[12] M. Raya, J.P. Hubaux, The security of vehicular ad hoc networks, in: Proceed-ings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'05, November 7, Alexandria, Virginia, USA, 2005, pp. 11–21

[13] Haixia Peng , Dazhou Li , Khadige Abboud , Haibo Zhou ,Weihua Zhuang , Xuemin (Sherman) Shen , Hai Zhao. "Performance Analysis of IEEE 802.11p DCF for Inter-platoon Communications with Autonomous Vehicles". IEEE Transactions on Vehicular Technology, 23 mai 2016

[14] J. P. Hubaux, S. Capkun, and L. Jun. "The security and privacy of smart vehicles". Security and Privacy, IEEE, vol. 2, pp. 49-55, 2004.

[15] G. Jyoti, G. M, and L. V. "Sybil Attack in VANETs". In Security of Self-Organizing Networks, ed: Auerbach Publications, pp. 269-294, 2010

[16] M. Burmester, E. Magkos, and V. Chrissikopoulos. "Strengthening Privacy Protection in VANETs". In IEEE International Conference on Wireless and Mobile Computing, Networking and Communications(WIMOB),Avignon, 2008.

[17] Hasbullah Halabi, Soomro Irshad Ahmed, Ab Manan Jamalul-lail."Denial of Service (DoS) Attack and Its Possible Solution in VANET".World Academy of Science, Engineering & Technology 2010.

[18] A. Burg. "Ad hoc network specific attacks". In Seminar Ad hoc networking: concepts, applications, and security, Technische Universitt Mnchen, 2003.

[19] Abdelfettah Mabrouk , Abdellatif Kobbane , Essaid Sabir , Jalel Ben-Othman , Mohammed EL Koutbi. "A Signaling Game-based Mechanism to Meet Always Best Connected Service in VANETs". In IEEE Global Communications Conference (GLOBECOM),San Diego, CA, USA, 2015

[20] Khaoula Jeffane and Khalil Ibrahimi, Detection and Identification of Attacks in Vehicular Ad-Hoc Network, 978-1-5090-3837- 4/16/2016 IEEE (http://ieeexplore.ieee.org/document/7777191)

[21] HamssaHasrouny, Abed EllatifSamhat, CaroleBassil, AnisLaouiti, "VANET security challenges and solutions: A survey" veh. Commun (2017), http://dx.doi.org/10.1016/j.vehcom.2017.01.002