Classification of Security Attacks in VANET: A Review of Requirements and Perspectives

Mohammed Ali Hezam Al Junaid[1], Syed A. A[1], Mohd Nazri Mohd Warip[1], Ku Nurul Fazira Ku Azir[1], Nurul Hidayah Romli[1]

[1] School of Computer and Communication Engineering University Malaysia Perlis, Malaysia.

Abstract. Vehicular Ad Hoc Network (VANET) is a pillar of the envisioned Intelligent Transport System (ITS) and a subset of Mobile Ad Hoc Network that grants the communication in between the vehicles alongside with the absence of established communication infrastructure. Exposure to vulnerabilities of Vehicular Ad-Hoc Network (VANET) has been shown to be related to its nature of the environmental. For this reason, VANET security becomes a critical challenge that need to be resolved. In this paper, we assess the VANET security issues and discuss the challenges in VANET. Equally important, we comparatively review the security requirements, the type of attacks and capabilities of attackers present in VANET.

1 Introduction

Recently, Vehicular Ad Hoc Network (VANET) is fast becoming a key catalyst in the Internet of Things (IoT) area. In general, Vehicular Ad Hoc Network (VANET) is a portion of Mobile Ad Hoc Network (MANET) which receiving numerous attention from researchers and automotive industry [1]. In addition, VANET is capable in improving road safety by allowing each of vehicles on the road communicates to each other with inadequate fixed infrastructures [2]. VANET applications are graded into safety applications and non-safety applications [3]. The former relates to the safety-comfort application in which linked to the safety of users. It aids in providing an alert and warning information to the users regarding to any incidents occurs on the road such as accidents. The latter consists of the non-safety applications responsible in providing comfort to the users and acts as traffic-enhancer. Additionally, VANET provides legitimate information to the users on the road in order to increase the road and users safety. However, it is not guaranteed that vehicular network environment is get off from any jeopardized since VANET is exposed to the vulnerabilities.

It One of the key challenges in the implementation of VANET in relation to security is providing secure vehicular communication. The authors in [4] examined that there are lots of attacks and threat that can compromise the network and communication. The most potential attacks that VANET faces are classified into data threat and VANET system threat. Denial of service attacks is one of the malicious attacks that can deny the On-board units (OBU) or Road Side Units (RSU) from entering the network as well as interruption to the radio channels.

This paper is organized as follows; In Section 2, we discuss the architecture of VANET. Section 3 presents the characteristics of VANET. Section 4 reviews the taxonomy of security concept in VANET and divided into three subsections. The first sub-section reviews the type of the attackers, the second sub-section discuss the capabilities of the attackers while the last sub-section presents the series of attacks that compromised in VANET. In Section 5, we present the network challenges in VANET. Section 6 explains the security requirements in VANET. Conclusion is provided in Section 7.

2 The VANET Architecture

VANET can be categorized into three which are (1) Pure IV. TAXONOMY OF SECURITY CONCEPT IN VANET Cellular/WLAN architecture, (2) Pure ad hoc architecture and (3) Hybrid architecture. Figure 1 exhibits the network In VANET, vulnerabilities are presented due to the architecture in VANET· wireless medium used. As a result, VANET are exposed to various kinds of attacks that could disrupt the communication operations between vehicles. Thus, the security concept in VANET as shown in Figure 2 can be classified into three which are (1) Attackers, (2) Attackers Capabilities and (3) Type of the Attacks. In sub-section 4.1, six types of the attackers are discussed. Sub-section 4.2 reviews four potentials that can.

* Corresponding author: aljunaid200@gmail.com

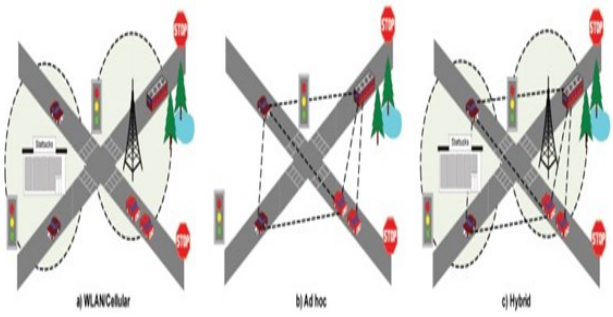

Fig. 1. The Network Architecture of VANET [3].

Generally, the communication and information exchanged in VANET independents from any fixed infrastructure. This possibly because of VANET environment is highly dynamic. According to authors in [3] proposed, the architecture of Fig. 1. The Network Architecture of VANET [3]
The communications patterns in VANET can be classified into.

- Vehicle-to-Vehicle (V2V) communications
- Vehicle-to-Infrastructure (V21) communications
- Infrastructure-to-Infrastructure (I2I) communications

3 VANET Characteristics

VANET is well-known as the subspace of MANET. However there are few characteristics of VANET that makes different from MANET, whereas VANET exhibited complexity in designing it as well as more challenges compared to MANET [3].

3.1. Frequent Disconnected Network

Vehicles are moving while exchanging information. Due to the rapid topology changes, the connections between two vehicles are easily disconnected. Usually the disconnections occur in infrequent networks.

3.2. Rapid Topology Changes

Due to the fast moving of vehicles, VANET topology changes quickly.

3.3. Battery Power and Storage Capacity

The communications in MANET consumes battery power conversely in VANET, the power and storage is boundless.

3.4. Communication Environment.

Obstacles in VANET are presented in dense network as well as sparse network. Trees, buildings, and other objects could obstruct the communications in VANET especially in dense network. For this reason, routing protocol for sparse and dense networks should be considered.

3.5. Mobility Modelling

The pattern of mobility in VANET is dependent on the traffic environment, vehicle's speed and driving behaviour. facilitate the attackers to launch the attacks. Sub-section 4.3 defines the type of attacks based on (1) Attacks on Confidentiality, (2) Attacks on Integrity, (3) Attacks on Availability, (4) Attacks on Authentication/Identification, and (5) Attacks on Privacy.

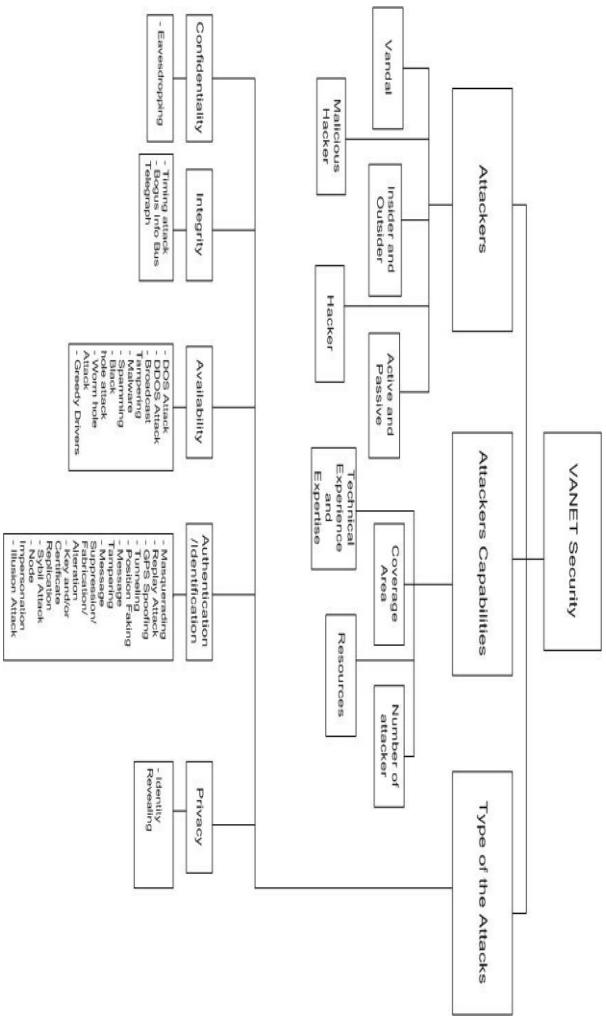

Fig. 2. Taxonomy of Security Concept in VANET

3.5.1. Type of the Attackers

According to the [4], attackers can be categorized based on the following category:

- Vandal: This kind of attacker is ill-motivated. The just want to show their abilities to attacks.
- Hacker: The hacker is motivated by the enthusiasm and interest without getting back any benefit from the attacking.
- Malicious hacker: The malicious hacker is driven by the monetary purposes of organizational or for personal/political gain.
- Insider vs. Outsider: The former relates to the attacker that is authenticated in the network and

known best about the network. The latter uses the attacker from the outside having a limited knowledge about the network that they want to penetrate.

3.5.2. Capabilities of Attackers

- Technical: Experience and Expertise With adequate experiences and skills, attackers are able to generate attacks against the network for example like extracting the program code and secret keys in order to launch the attacks.
- Resources: Attackers are dependent on three main key resources like tools, budget and manpower. Without these key resources, it is hard for the attackers to achieve their goals.
- Coverage Area: The coverage area of the attackers is depending on the attackers 'capabilities and nature of attacks. The rookie attackers could be controlled one of the Dedicated Short-Range Communication (DSCR) channel within the range of 1000 meters whilst the expertise could covered more area and DSCR channels compared to the rookie attackers.

3.5.3. Type of Attacks

The communication medium used in VANET is through the open air which make possible for attackers to penetrate and invade the networks. The real intentions of the attackers are to create problems with the legitimate vehicles in the network [5]. The attacks are classified as the following:

- Attacks on Confidentiality: Eavesdropping in VANET is targeting against the confidentiality and occurs in network layer. It operates by sniffing the conversation in between two nodes. As a result, this attack enables the attacker to intercept the communication, steal the password and important data. The attacker can masquerade itself as one of the node, or located itself as false RSU with the aim to catch up valuable information [6][7].
- Attacks on Integrity: Timing Attack, without altering any contents in the message, the attacker carries on this attack by adding delay which causes the user to receive the message behind the time. Consequently, user may face traffic congestion or even worse, accidents. It is important to realize that the information and messages deliveries in VANET should be received by the users at the appropriate time [3][8]. In addition, timing attack is divided into two levels which are (1) Basic Level and (2) Extended Level. Both levels are targeting users in the vehicular network, where the basic level only pointed to the user in peer-to-peer (P2P) communication while extended level is rigorous compared to basic level since it focuses on group of users [9]. Figure 1 and 2 shows the basic level of timing attack occurs in VANET.

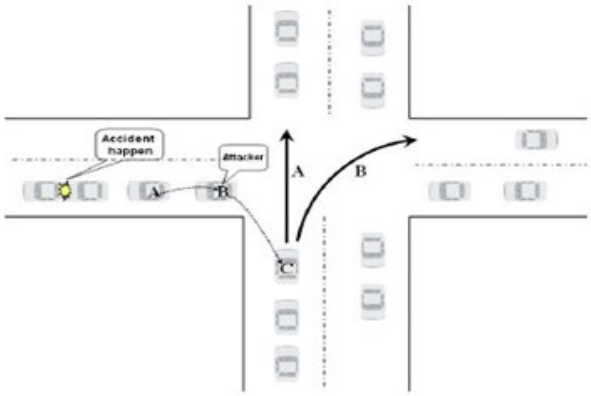

Fig. 3. Before Basic Level Timing Attack Occurs [9]

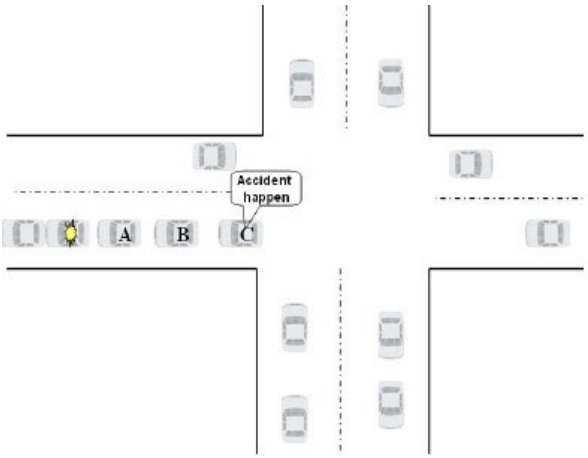

Fig.4. After Basic Level Timing Attack Occurs [9]

In Figure 3 presents the extended level of timing attack occurs in
VANET.

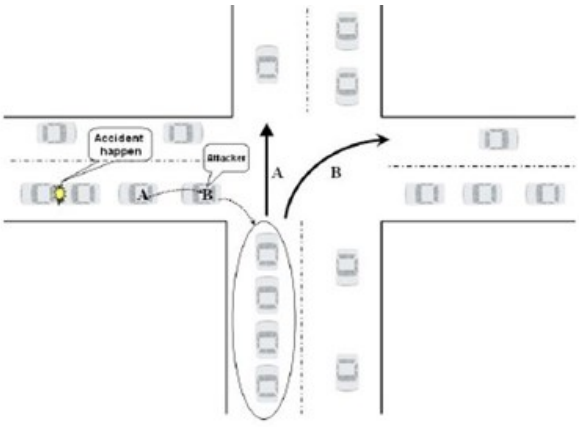

Fig. 5. Extended Level of Timing Attack [9]

Bogus Information and Bush Telegraph Bogus information attacks involving forwarding the counterfeit or false information throughout the network, intended to ignite disarray. In return, the attacker will gain the benefit from it [10].

- Attacks on Availability: Denial of Service Attack (DOS) Denial of Service attack is the most common intrusive attack against the availability. In fact, it can take place in each layer across the network. The purposes of the attacker could be denying the legal vehicles from accessing the network, control the vehicle resources and jamming the communication channels [11]. DOS can be classified into three levels of attacks which are (1) Basic Level, (2) Extended Level and (3) Distributed Denial of Service (DDOS) Attack [5].
- Distributed Denial of Service Attack This kind of attack is dangerous because it is launched from different locations. Consequently, the impact of this attack is dispersed in the network.
- Broadcast Tampering Through broadcast tampering attack, attacker practically injecting erroneous messages which lead to disturbance to the network. Likewise, this attack is akin to bogus information attacks. But in contrary, broadcast tampering only involving internal attackers [12] [8].
- Malware Malware is abbreviation of malicious software which created in order to contaminate the nodes or the network system in VANET. Malware such like worms or virus could take an action during software exchange or software update likely initiated by the insider [12]
- Spamming This attack is very hard to control due to the missing of fixed infrastructure and centralised administration in VANET. Spam messages could increase the latency in communication; thus, will causing the nodes not to receive the messages on time.
- Black Hole Attack In this type of attack, the malicious node will attracts the victims by advertising itself with a fresh route altogether with low hop count. The attacker is free to reply Route Reply (RREP) packet to victim without concerning its routing table. A false route will be created and sent to the victim during the flooding of Route Request (RREQ) packet in flooding-based routing protocol [13].
- Worm Hole Attack Entangle two attackers; a band wormhole is created when these two attackers are next to each other and advertising themselves to the other nodes that they have the shortest path to the destination. Both of the attackers will placed themselves in the most vital position in the network and forming an overlay tunnel over the wireless medium in order to intercept the communications throughout the network. This is the most preferable attack by the attackers because they can strengthens themselves when throughout the establishment at strong strategic location in VANET [14].
- Greedy Drivers The purpose of greedy drivers is to conquer all the network resources for its own used. They can create havoc by set up forged traffic jammed information so that other nodes will deviated from the attacker path. The attacker wisely will be modified the MAC layer parameters in order to expedite this attack [15].

3.5.4. Attacks on Authentication / Identification

Masquerading To perform masquerading attack, an attacker needed to enter the network and has functioning onboard unit. Attacker can disguised itself as legitimate node and carry out any of attacks. The easiest attack to be launched in a network is masquerading attack [12].

- Replay Attack: By injecting back the received packet into the network, the location table of the node is being poisoned by replaying beacons. This kind of attack is called as replay attack. On the other hand, in order to continuously defended from replay attack, VANET must maintained accurate source of time that used to keep cache of the received messages [12].
- Position Faking It is easier for an attacker to alter its position in a network with unsecured communications. Under that circumstance, accurate authentication and frequent reporting of node positions are required. Through location reporting, masquerading or impersonation is futile. Possibly through position faking in unsecured communication will lead the attacker to falsify their own position, creating additional vehicle identifiers which known as Sybil attack or blocking other nodes from receiving important messages [12].
- GPS Spoofing By making nodes thinking that they are in the different location, nodes are easily fooled by the attackers. This kind of attack can be carried out by producing false reading in the GPS devices. GPS spoofing permits the attackers to generate stronger signal than signal that generated by genuine satellite by using GPS satellite simulator [12]
- Message Tampering In this attack, attackers could modify the messages that being exchanged in the V2V and V2I communications. Message tampering attacks are arising from the vulnerabilities in authentications [12].
- Message Suppression/Fabrication/Alteration There are two ways those attackers can disable itself from responding to any beacons; either physically disabling the inter-vehicle communication or altering the application [12].
- Key and/or Certificate Replication In this case, attackers could erode the system by making several nodes with the same identity. This attack can be carried out by replicating key management and/or certificate. The purpose of the attacker is to bemuse the authorities and forbid the identification of attacker [12].
- Sybil Attack The attack is launched by sending wrong numerous messages to the other node but with different forgery identity of the sender. As a result, for example, other nodes will leave the road in order to ease the attacker to pass through the road freely. In this case, the real identities of the sender are hidden and the attackers created a delusion to the other nodes.
- Node Impersonation During the communication between the sender and receiver, the attacker may modified the message from the originator and send it to the receiver. Therefore, the malicious message may seems like originated from the sender. This problem could be curbing by assigning the unique identifier to each vehicle nodes. Henceforth, the real identity of the message originator could be detected.

3.5.5. Privacy

Identity Revealing The identity and the location of the target nodes are divulging in this attack. The attack is carried by monitoring the target node and sends "virus" to the nearby vehicle node. When the nearby vehicles are overwhelmed with virus will take the ID and the location of the target node.

4. Network Challenges in VANET

The key fundamental challenges in deploying vehicular system in real-life are not an easy task as it needs to address many issues and identified the required solutions. According to [16], the main challenges that encountered by VANET are as following aspects;

4.1. Wireless Access Technology

There are limited technologies available to be used as core base in VANET. Those technologies are included cellular technology; IEEE 802.11p based technology and combined wireless access.

4.2. Spectrum Issues

The FCC in US has allocated 75MHz of spectrum at 5.9GHz for car-to-car and car-to-infrastructure communications. Unfortunately, a continuous spectrum is not available in Europe. After that Car2Car CC has proposed allocations of 2x10 MHz for primary use which is for the safety applications at 5.9 GHz range. Conversely, this band is utilized as control channel in US and it allocation in Europe would grants as world-wide harmonization.

4.3. C. Routing Issues

Three main routing algorithms that available in VANET can be combined with concept 'carry and forward'. Those algorithms are (1) opportunistic forwarding, (2) trajectory based forwarding and (3) geographic forwarding. Furthermore, mixing two or multiple approaches also could be done as hybrid solutions.

4.4. D. Security and Privacy

Security and privacy are two issues that need to be concentrated in developing the solutions. This is because several threats are available that potentially could disrupted the traffic as well as compromising the private information like driver's information.

However, authors in [7] classified the challenges in VANET which sub-divided to (1) Technical Challenges and (2) Social and Economic Challenges. The first aspect is with regard to the technical challenges; there are five key issues that have been discussed as follows;

Article I. A. Network Management

Since one of characteristic of VANET is high mobility, the network topology and channel face rapid changes. Because of that, structures that able to maintain while rapid topology changes occur, should be deployed.

Article II. B. Congestion and Collision Control

The limitless network creates congestion and collision during peak hours since the traffic load is high.

4.5. C. Environmental Impact

In VANET, electromagnetic waves are used in communication. Unfortunately, electromagnetic waves can affect the environment. Thus, the environment should be taken into account before deploying it.

4.6. D. MAC Design

Since VANET are using the shared medium, MAC design become big challenges in VANET.
Article III. E. Security

Security of VANET must be fulfilled since VANET provides road safety applications.

Equally important, the social and economic challenges are being discussed based on the issues on how to convince the manufacturers to build up an application that can reveal the traffic violation. This application additionally will help the user to get information on the road such as police trap. While in [17] and [18], VANET challenges are listed out into (1) Mobility, (2) Volatility, (3) Network Scale and (4) Bootstrap. In addition, authors in [8] added up (5) Privacy vs. Authentication and (6) Privacy vs. Liability as additional challenges. The challenges issued are explained as follow;

A. Mobility

VANET has high mobility due to rapid changes of the topology.

B. Volatility

The connection between vehicles will not last long due to fast movements and changes in the directions of vehicles.

C. Network scale

Since the number of vehicles around the world increasing around to 800 millions, hence, network scalability becomes difficult. Throughout the time, another issue arises due to the absence of global authority that used to manage the standard for the network.

D. Bootstrap

Up until now, only few vehicles are equipped with DSCR. Thus, the communications only limited to a few vehicles and developers must take into account about this issue.

5. Security Challenges in VANET

Security issues in VANET are critical due to vulnerabilities exist during information transmission which causing VANET exposed to the attacks. In order to maintain a secure vehicular communication and networks, VANET security system should satisfy with the requirements. Some of the requirements are essential for all networks, but some are definite for VANET only [17]. Those requirements are;

A. Authentication

In order to allow the communication between vehicles which sending and receiving information, VANET should authenticate each of them. This process may comprise the identification of the sender identity and the legitimacy of the sender to use the network.

B. Availability

Availability is defined as the degree of the VANET system that must be operable and available when needed. A fast response time also must applicable for some applications.

C. Privacy

Privacy is one of the most important requirements in VANET. Privacy must ensure that the identity of the drivers and the location of the vehicles are not being exposed.

D. Integrity

The information exchange in between the sender and the receiver should be free from the alteration attacks. Thus, information can be trusted.

E. Non-repudiation

It ensures that the origin of the information cannot be denying that it has sending the information.

6 Conclusion

In summary, safety is the main attention for the road users. VANET has an ability to provide safety requirements by providing the information on the roads to the users. However, VANET is not immune from any vulnerabilities and threats. Because of that, secure solutions in order to enhance the security of the information in VANET must be deployed. Therefore, it is important to maintain the network availability and develop trust to the information in VANET.

References

[1] A. Agrawal, A. Garg, N. Chaudhiri, S. Gupta, D. Pandey, and T.
Roy, “Security on Vehicular Ad Hoc Networks (VANET) : A Review Paper,” vol. 3, no. 1, 2013.

[2] C. Kruegel and T. Toth, “A survey on intrusion detection systems,” TU Vienna, Austria, vol. 109, no. 1, pp. 6–15, 2000.

[3] O. Pattnaik and B. K. Pattanayak, “SECURITY IN VEHICULAR AD HOC NETWORK,” vol. 11, no. 2, pp. 337–346, 2014.

[4] C. Y. Shim, “A taxonomy for DOS attacks in VANET,” 2014 14th Int. Symp. Commun. Inf. Technol., pp. 26–27, 2014.

[5] H. Hasbullah, I. A. Soomro, and J. A. Manan, “Denial of Service (
DOS) Attack and Its Possible Solutions in VANET,” World Acad. Sci. Eng. Technol., vol. 4, no. 5, pp. 411–415, 2010.

[6] J. M. De Fuentes and A. I. González-tablas, “Overview of security issues in Vehicular Ad-hoc Networks,” Science (80-.)., 2010.

[7] R. S. Raw, M. Kumar, and N. Singh, “Security Challenges, Issues and Their Solutions for VANET,” Int. J. Netw. Secur. Its Appl., vol. 5, no. 5, pp. 95–105, 2013.

[8] M. Bharat, K. S. Sree, and T. M. Kumar, “Authentication Solution for Security Attacks in VANETs,” vol. 3, no. 8, pp. 7661–7664, 2014.

[9] I. A. Sumra, J. A. B. Manan, H. Hasbullah, and B. S. Iskandar,
“Timing Attack in Vehicular Network 2 VANET Applications and Time,” pp. 151–155.

[10] J. T. Isaac, S. Zeadally, and J. S. Cámara, “Security attacks and solutions for vehicular ad hoc networks,” IET Commun., vol. 4, no. 7, p. 894, 2010.

[11] K. M. A. Alheeti, A. Gruebler, and K. D. Mcdonald-maier, “An Intrusion Detection System Against Malicious Attacks on the
Communication Network of Driverless Cars,” IEEE Consum. Commun. Netw. Conf., no. 12, pp. 916–921, 2015.

[12] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan,
“Vehicular ad hoc networks (VANETS): status, results, and challenges,” Telecommun. Syst., vol. 50, no. 4, pp. 217–241, 2012.

[13] V. Bibhu, “Performance Analysis of Black Hole Attack in Vanet,” no. October, pp. 47–54, 2012.

[14] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, “A novel approach for avoiding wormhole attacks in VANET,” 2nd Int. Work. Comput. Sci. Eng. WCSE 2009, vol. 2, pp. 160–165, 2009.

[15] M. N. Mejri and J. Ben-Othman, “Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks,”

Glob. Commun. Conf. (GLOBECOM), 2014 IEEE, no. ii, pp. 5032–5037, 2014.

[16] J. Jakubiak and Y. Koucheryavy, "State of the Art and Research Challenges for VANETs," 2008 5th IEEE Consum. Commun. Netw. Conf., pp. 912–916, 2008.

[17] S. S. Shinde and S. P. Patil, "Various Issues in Vehicular Ad hoc Networks : A Survey," vol. 1, no. 2, pp. 399–403, 2010.

[18] G. Samara, W. a. H. Al-Salihy, and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," Netw. Appl. Protoc. Serv. (NETAPPS), 2010 Second Int. Conf., pp. 55–60, 2010.