International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Security Issues of Vehicular Ad Hoc Networks in OSI layers

Abdul Quyoom
Department of Computer Science, Baba Ghulam Shah Badshah University, Rajouri, India

ABSTRACT

A vehicular ad hoc network (VANET) is a mobile ad hoc network, where in place of mobile or network node we make use of vehicles. It is a special case of ad hoc networks that, besides lacking infrastructure, communicating entities move with various accelerations. VANET is intended to get better driver safety, avoid collisions, and offer traffic optimization, it present a unique range of different challenges and opportunities to get the availability of ubiquitous connectivity, reputation management systems and secure communications of routing protocols because of semi-organized nature of vehicular movements subject to the constraints of road geometry and rules. In this paper, we discuss challenges, security related features, and possible VANET attacks on OSI model layers.

Keywords: VANET, network protocols, Attacks, OSI Layers, Security.

I. INTRODUCTION

VANETs are a kind of MANETs (Mobile Ad Hoc Networks) where we use vehicles as communicating entities instead of mobile nodes. Interference is a biggest obstacle in ad hoc networks which appear in VANETs communications [1][5]. It affect in direct connection, in order to overcome this problem, multi-hop connection is used with some technologies such as frequency hopping and Bluetooth. Still in multi-hop transmission in VANETs, there exist routing problems [6]. VANETs have different applications that can be applied by Peer-to-Peer (P2P) communication or via multi-hop communication [5]. VANETs applications are like broadcasting information, traffic monitoring, route finding, weather forecasting and collision prevention. Such a wide variety of applications makes these networks Intelligent Transportation System (ITS) [3]. ITS is the term used to describe the application to road transportation of advanced technologies including communications, sensors, controls and coordination as well as computing. These systems are intended to improve the safety, efficiency and capacity of the highway system [3]. Goal of ITS is to enhance vehicle safety for elderly and less able travellers is examined. Vehicles have specific units that make them to communicate with other vehicles. These units are called On Board Units (OBUs). Vehicles exchange data with base stations also know by Road-Side Units (RSUs) [2]. Due to the self-organized nature of VANET, some security parameters are requirements such as Availability, Access Control, Data Confidentiality, Data Authentication and Integrity, Vehicle Privacy and Anonymity, Data Non-Repudiation, Vehicle ID Traceability, Scalability, Efficiency and Robustness, Resistance against In-Transit Traffic and On-Board Tampering, Impersonation, Anti-Jamming, and message Forgery etc [4][7][9][13]. Availability is the assurance of communication between vehicles and remote nodes. Even thought if some attack happens, still the services are provided. Vehicles should have the capability of accessing available services offered by remote nodes and this service is known as access control. Data Confidentiality provide the assurance of secret data transmission between vehicles and remote stations [9][12]. Data Authentication deals with the verification of transferred data through their identification parameters. The transferred messages have to be accessed by authorized vehicles and remote nodes, and not to be exposure by misbehaved vehicles [10]. Integrity assure that the message sent by a vehicle or a remote node have to be delivered to correct destinations and they are not even altered over the channel. In forgery, vehicles transmit false messages or warnings, which can lead to wrong reactions in the network [2]. Anti-jamming is caused of malicious vehicles send interfering messages to drop communication between legitimate vehicles [10]. Transit traffic tampering is that a malicious vehicle can corrupt or capture data of other vehicles when it is an intermediate node [9]. Some vehicles masquerade as emergency entities to attract other vehicles to communicate with and change their behaviour.

II. VANETs challenges and security impact

The characteristics and features of VANETs make some challenges which can affect applying security approaches to establish secure communications in V2V and V2R [3]. In the following section. (1) Heterogeneity: VANETs support different types of applications, to perform any function by using equipments [3]. Firstly, they are authenticated to preserve security issues, such as vehicle's velocity and location is defined by using GPS and corespondinglily effect of scalability and efficiency is monitored. (2) Network Volatility: Communication between vehicles take place when they are in range and it happens for a short interval of time as soon as one vehicle move to region of next RSU connection is ended automatically due to acceleration, so applying security approaches depending on verifying identities is hard [9]. (3) Network Scale: VANETs consist of a large number of vehicles; and this strength affects their functions if there is no robust confidential system, which has the ability to distribute cryptographic keys for that large number [1]. Therefore, a detail study is needed before deploying VANETs to be sure of its scalability for any changes in number of communicating vehicles. (4) Liability: Vehicle information is accessed is for investigation purpose, it should be available while tracking and extracting any information [5]. (5) Wireless Link use: in VANETs wireless communication take place whether in V2V or in V2R and requires robust security mechanisms to maintain confidentiality and network integrity. (6) Without Infrastructure: VANETs architectures vary with vehicles position in communication [10]. Therefore, no routers or central server is used, and then a trust relationship should be established among vehicles. (7) Delay-Sensitive Applications: some VANETs applications related to passengers safety are time sensitive, they have values of delays with certain tolerance [8][5]. The routing techniques perform their functions with message of small overhead and low processing delays. (8) Multi-hop connection: VANETs communications depend upon multi-vehicles to send information from source to destination by passing received messages to possible neighbours in its range [5][12].

III. CLASSIFICATION OF ATTACKS IN VANETS DUE TO DIFFERENT NETWORK LAYERS

3.1. Security threats in application layer

The application layer contains important vehicle's information related to some protocols such as Hyper Text Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP) [8][5]. The application layer deals with vehicle data, attacker can handle some applications to capture and analyze specific Information (e.g. location, and vehicle packet loss characteristics [1,8]) about vehicles found in a VANET. This information can help malicious vehicles in detecting future behaviors of other trusted vehicles [14]. The two famous attacks are generally performed by malicious vehicle in application layer such as repudiation attacks and malicious code attacks [9]. An efficient connection is required for non safety applications with the remote vehicles during communication [2][16].

3.1.1. Repudiation attacks

A repudiation attack adopts controls to properly track and log users' actions, thus attempting malicious activities or forging the identification of new actions in a similar scheme [9]. Spoofing mail messages and general data manipulation in the name of others, data is considered as invalid when this attack takes place [13].

3.1.2. Malicious code attacks

Here malicious vehicles like spywares, Trojan horse and virus to attack other vehicle or remote base station, these activities the system services, destroy vehicles application, and gain information about trusted vehicles send the malicious code. Countermeasures on application layer attacks firewall programs can provide protection against, spywares worms, Trojan horses and viruses [9]. Outgoing packets are filtered and incoming packets are authenticated. Anti-spyware is be used to detect spywares and malicious programs [5]. Application layer has the capability of detecting DoS very quickly than other layers. Application aware control scheme and unidentified routing scheme [17] to register the applications periodically and for the secure routing of application.

3.2. Security threats in transport layer

The transport layer deals with some security topics such as securing end-to-end communications, packet corruptions and loss Authentication, and handling delays. The transport layer used with VANET should support end-to end connection like TCP protocol in the internet model. Now we will discuss possible attacks during transport layer in VANET.

3.2.1. SYN flooding attack

This Attack is considered as Denial of Service (DoS) attack where a large number of half-opened TCP connections are created between two communicating vehicles in a VANET [15]. The TCP connection depends on three handshake messages, where a sender sends a SYN message Initial Sequence Number (ISN) to the receiver. Receiver acknowledges the received SYN message with an ACK message, which contains its own ISN. After that, the connection is established. The malicious vehicle sends flooding of SYN messages to a specific remote station or a vehicle, remote vehicle spoofs return addresses of SYN messages, that the received vehicles store many SYN messages and wait for ACK messages, more received SYN messages by victim vehicle and its system may be out of service for a period of time.

3.2.1. TCP ACK storm

In order to perform TCP ACK storm attack, firstly session hijacking is performed [9]. The malicious vehicle sends session data with certain sequence number to a vehicle; then that vehicle acknowledges these data to another vehicle. Afterward, the last received vehicle is confused with the received sequence number. Then it acknowledges and resynchronizes the TCP connection with the malicious vehicle by sending the required sequence number packet [16]. The last step is repeated many times and this represents the TCP ACK storm.

3.2.3. Session hijacking

In this attack, the malicious vehicle pretends to be a legitimate vehicle and make use of a session establishment feature where no authentication is required in beginning. To perform Denial of service attack, IP addresses of legitimate vehicles are spoofed and correct sequence numbered is inserted. So, legitimate vehicles became unavailable for a period of time [2].

3.2.4. Countermeasures on transport layer attacks

Data encryption is a main concern to achieve end-to-end communication confidentiality in the transport layer. TCP does not fit MANET; therefore, it is not fit VANET. In addition, Ad-hoc Transport Protocol (ATP) [1] and Ad-hoc Transmission Control Protocol (ATCP) are deployed for MANET and do not overcome security issues in MANET, which also will not be suitable for VANET. Transport Layer Security (TLS), and Secure Socket Layer (SSL), to provide a secure channel based on public key cryptography [13]. These protocols make immunity against rollback, replay attack, man-in-middle and masquerade.

3.3. Security threats in network layer

VANET posses topological network nature due to movements of vehicle, in such a scenario it is big challenge to maintain a route, the communicating vehicles can work as routers in order to communication capabilities to other vehicles and to establish optimal route for broadcasting information [6]. So, network layer security plays a vital role in the network. Any attack in routing phase may interrupt the overall communication and the entire network can be paralysed [4][10]. MANETs and VANETs share similar characteristics such as low bandwidth, self-management networks Self-organized and short communication range. Hence, most routing protocols applied for MANETs can be applied for VANETs [14]. To provide secure Communication and remove defects in the existing protocols are the main target of the routing protocols. Some of these protocols such as SRP, Ariadne, endairA, S-AODV, ARAN, SEAD, SMT can be classified into the following categories [5][12].

A. Proactive Routing Protocols:

Here the nodes keep updating their routing tables by periodical messages. This can be seen in Topology Broadcast based on Reverse Path Forwarding Protocol (TBRPF) and Optimized Link State Routing Protocol (OLSR). When one or more tables are used to store routing information changes in network topology then is called Table Driven routing protocol. In the similar manner to maintain a consistent network environment, Some common examples are (SPAAR) Secure Position Aided Ad hoc Routing protocol, HSR (Hierarchical State Routing) protocol, Dynamic Destination-Sequenced Distance Vector routing protocol (DSDV) are the methods to protect position information in a high-risk environment [5][16].

B. Reactive or On Demand Routing Protocols

As per the name of the protocol on demand routing, the routes are created only when they are needed. The application of this protocol can be seen as follows: on-demand protocols are Anti-based Routing Algorithm for Mobile Ad-Hoc Networks, Dynamic Manet On-demand Routing (DYMOR), Admission Control enabled On demand Routing (ACOR), Dynamic Source Routing (DSR), On-Demand Anonymous Routing (ODAR), Ad-hoc On-demand Distance Vector Routing Protocol (AODV), in Ad Hoc Networks to enable complete anonymity of nodes and source routing paths [11].

C. Other routing protocols

Hierarchical and Hybrid are the two other protocols. The hierarchical protocols include scalable routing strategies and create a hierarchy. Distributed Dynamic Routing Algorithm (DDR), Hierarchical State Routing (HSR), OORP Order One Routing Protocol (HSR) are examples of hierarchical protocols. The hybrid routing protocol is a combination of proactive and reactive scheme. Hazy Sighted Link State routing protocol (HSLS) and Zone Routing Protocol (ZRP) are hybrid protocols [2]. VANETs with high mobility and low node density to deliver messages with minimized high reliability and delivered delay [2]. Recently, a novel Cross Layer Weighted Position based Routing (CLWPR) [12] was proposed following the minimal weight hop based routing periodically broadcasted by each node. This protocol calculates the distance to be travelled to reach the destination. To make this possible, e-maps are to be imported on the vehicles. Selection of the path for nodes traversing in the direction of the destination can be identified. Xiang et al.[18] propose a Geographic Stateless VANET Routing protocol (GeoSVR). This protocol consists of two main algorithms namely restricted forwarding algorithm (RFA) and optimal forwarding path algorithm (OFPA). RFA is used to identify the next hop node to forward the data [18]. OFPA eliminates the problem of sparse connectivity by considering the vehicle density. Here optimal forwarding path cannot be calculated using traffic information so the map is considered as the weighted graph. Dijkstra algorithm is applied to this graph to fine the optimal forwarding path with minimum weight, there is a possibility of more than one route with minimum weight. GeoSVR calculates the derivation of the each path and chooses the one with lowest value in order to determine best and optimal forwarding path [18].

D. Ad-hoc On-demand Distance Vector (AODV)

AODV routing algorithm is a reactive algorithm that routes data across wireless mesh networks [12]. Here attacker may advertise a route with a smaller distance metric than the original distance or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes [11]. Another version of AODV was proposed (Secure AODV) to provide more secure authentication and integrity in AODV through multi-hop connection. Advantages of AODV is that it requires less memory, straight forward nature and does not create additional traffic for communication along existing links.

E. Dynamic Source Routing (DSR)

Like AODV protocol, DSR protocol is also a forms route on-demand protocol. In DSR packet is forward on hop-by-hop basis. Attacker can modify the source route listed in the RREQ or RREP packets [11]. If a node is deleted from the list, then appending a new node into the list is difficult in DSR. The difference between AODV & DSR is the use of source routing instead of relying on the routing table at each intermediate node.

F. Authenticated Routing for Ad-hoc Networks (ARAN)

ARAN is an on-demand routing protocol which authenticate routing of packets, detects and protects against malicious actions [14]. This protocol introduces various security features like message integrity, non-repudiation and authentication. ARAN is designed to enhance ad-hoc security [17].

G. ARIADNE

ARIADNE is an on-demand secure ad-hoc routing protocol based on DSR which follows highly efficient symmetric key cryptography. Message authentication code (MAC) is used to provide point-to-point authentication and a shared key between the two communicating parties [16]. Cache poisoning attack, wormhole attack and rushing attack are not applicable on ARIADNE.

H. Secure Efficient Ad hoc Distance vector routing protocol (SEAD)

Specifically, SEAD builds on the DSDV-SQ version of the Destination Sequenced Distance Vector (DSDV) protocol. It deals with attackers that change routing information and with replay attacks and makes use of one-way hash chains rather than execute expensive asymmetric cryptography operations [4]. The system uses two different approaches, which are used for message authentication to prevent the attackers.

ATTACKS FACED BY ROUTING PROTOCOLS

Attacks on ad-hoc routing protocols can be generally classified into active and passive attacks. An Active Attack injects arbitrary packets and tries to interrupt the operation of the protocol in order to limit accessibility, gain authentication, or grape packets destined to other nodes [13]. A Passive Attack does not disrupt the process of the protocol, but tries to discover precious information by eavesdropping the traffic. Passive attacks involve obtaining essential routing information by sniffing network [4]. Such attacks are usually difficult to detect; therefore, defending against such attacks is complicated. Attacker tries to attract all packets for analysis or to disable the network. Such attacks can be detected and the nodes can be identified. The following list includes some of the attacks that face the routing layer and some of the routing protocols [8].

A. Routing table over-flow attack:

In order to update the routing information periodically, proactive routing algorithms are used. In this attack, routes are created to reach the non-existent nodes which are present in the network, Attacker forwards extreme route announcements in-order to over-flow the target system's routing table [14]. Attacker accesses all possible routes, creation of new routes is prohibited.

B. Routing cache poisoning attack

This attack occurs when information stored in routing tables is altered, either deleted or injected with false information. For example, malicious node A wants to poison routes to node B. Node A have to broadcast spoofed packets with source route to B via A itself, when neighbouring nodes receive the packet, they add the route to their route caches.

C. Rushing attacks

Rushing attacks results in denial-of-service when used against all previous on-demand ad hoc network routing protocols. All these protocols such as DSR, AODV, ARAN and Ariadne are unable to discover routes longer than two hops when subject to this attack. In this type of attack, attacker quickly forward route requests to all the legitimate users and try to impersonate them and increase the probability of accessing the discovered route rather than other valid routes [10]. Major dangerous features of this attack are the weak attacker [9] can perform it. A proposed defence mechanism against this attack is named as rushing attack prevention (RAP).

D. Byzantine attack

Byzantine attack can be launched either by a group of nodes that work in cooperation or by a single malicious node. A set of compromised intermediate nodes works in collusion to form attacks. The compromised nodes may create routing loops, forwarding packets in a long route instead of optimal one, even may drop packets [18]. This attack degrades the routing performance and also disrupts the routing services.

E. Wormhole attack

In the wormhole attack, attacker records packets at one location in the network, tunnels them to another location, and retransmits them there into the network [2]. It is applicable where two or more nodes may collaborate to exchange messages between them along existing data routes. This exploit gives the opportunity to the nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

F. Black hole attack

This attack is performed in two steps, in first step; the malicious node exploits the routing protocol such as AODV. With the intention of intercepting the packets form the node, attacker advertises itself as having a valid route to a destination node, even though the route is spurious. In second step, the attacker receives and consumes the packets and never forwards. Actually attacker suppresses or modifies packets originating from some nodes while leaving the data from the other nodes unaffected. So in this way, attacker misguides the neighbouring nodes that monitor the ongoing packet [5][17].

3.4. Security threats in Data link layer

The VANET is a multipoint peer-to-peer network where link layer protocols preserve node connectivity among the neighbour's nodes. The IEEE 802.11 MAC protocol use distributed contention resolution mechanisms, which are based on two different coordination functions [9]. One is centralized access protocol named Point Coordination Function (PCF). For resolving channel contention among the several wireless hosts and other is Distributed Coordination Function (DCF) that is completely distributed access protocol. DCF uses a carrier sense multiple access with collision avoidance or CSMA/CA technique. Wireless medium access control (MAC) protocols have to organize the transmission of the nodes on the regular communication or transmission medium [15].

3.4.1. Threats in IEEE 802.11 MAC

The IEEE 802.11 MAC is used to detect to DoS attacks. To start the DoS attack, the attacker may use the binary exponential back off scheme. For example, the attacker may disregard the ongoing transmission or may damage frames easily by adding some bits. In all the competing nodes last winner is decided by the binary exponential method and direct it to the capture effect. Some harmful nodes may take the benefit of capture effect weakness. All the neighbours nodes need to update their NAV field with respect to time that they overheard for transmission duration. The attacker in the local neighbourhood also knows the duration of the current transmission and in order to cause errors a few bits within this period are transmitted Using wireless interference [15].

3.4.2. Threats in IEEE 802.11

WEP IEEE 802.11 standards provided the Wired Equivalent Privacy (WEP). It is known that WEP is exposed to probabilistic cipher key recovery attacks, message integrity and privacy attacks. WEP was designed to grant security for WLAN. But it bears many design problems. Presently AES in 802.11i take over WEP. Some of the limitation of the WEP is described below.

1. Key management is not specified in the WEP protocol.
2. The use of stream chipper with non-cryptographic integrity algorithm is a security hazard and may cause message integrity and message privacy attacks.
3. It is a 24-bit field named as initialization vector (IV) used in WEP is sent in clear the probabilistic cipher key recovery attack.

3.4.3. Countermeasures on link layer attacks

The security concerns that are closely related to link layer reprotecting the wireless MAC protocol and providing link-layer security support. binary exponential back-off scheme is the major weaknesses of Data link layer [10]. To overcome this security extension to 802.11 was proposed. Resource consumption is still an open challenge, some techniques have been proposed such as ERA-802.11. To improve the strength of wireless security, Robust Secure Network / Advanced Encryption Standard Cipher block Chain Message authentication code Protocol (RSN/AESCCMP) are also being developed.

3.5. Security threats in physical layer

Physical layer security is vital for securing VANET as many Attacks can occur in this layer. The physical layer must adapt to quick changes in link characteristics. The most familiar Physical layer attacks in VANET are denial-of-service; jamming and eavesdropping are most familiar physical layer attacks in VANET. The common radio signal in VANET is easy to jam. Pulse and random noise are the most frequent type of signal jamming [9]. An attacker can eavesdrop or disrupt the service of wireless network physically. Eavesdropping is the reading of messages and conversations by not deliberate receivers. The nodes in VANETs allocate a wireless medium and the wireless communication using RF spectrum and broadcast, which can be simply intercepted with receivers adjusted to the proper frequency. So transmitted message can be eavesdropped as well as false message can be injected into the network [14]. Batch Mode Multicast MAC (BMMM) protocol is used to overcome problem of collisions by using control frame for sending multiple data in the same time.

3.5.1. Countermeasures on physical layer attacks

The physical layer of VANET is protected from DoS attack, signal jamming. Intrusion Detection Systems (IDS) can be used to detect jammed signal. Spread spectrum techniques are used detect signals. Direct Sequence Spread Spectrum (DSSS) symbolizes each data bit in the original signal by multiple bits in the transmitted signal through 11-bit Barker code. Frequency Hopping Spread Spectrum (FHSS) makes the signal incoherent period impulse noise. Spread spectrum techniques changes frequency and spreads it to wider spectrum. These mechanisms are secure only when the hopping pattern or spreading code is unidentified to the eavesdropper [9].

IV.CONCLUSION

VANETs are infrastructure-less networks comprising mobile communicating entities with intermittent connectivity. VANETs characteristics lead to security vulnerabilities related to the various networking layers in the traditional Internet protocol stack architectures. In this paper, we have overviewed VANETs clarifying their security requirements and challenges. Also, we have provided attack classification which categorized security threats to VANETs with respect to each operating layer in the five protocol layered stack model. Additionally, we have discussed countermeasures on attacks facing each layer.

V. REFERENCES

[1]. F. Li, Y. Wang, Routing in vehicular ad hoc networks: a survey, Veh. Technol. Mag., IEEE, pp 12-22, 2007.

[2]. Dahlia sam, v. cyril raj," a time synchronized hybrid vehicular ad hoc network of roadside sensors and vehicles for safe driving", journal of computer science 10 (9): issn: 1549-3636,pp: 617-1627, 2014.

[3]. S. Yousefi, et al., Vehicular ad hoc networks (VANETs): challenges and perspectives, in: ITS Telecommunications Proceedings, 2006 6th International Conference, pp. 761-766, 2006.

[4]. X. Ma, J. Zhang, X. Yin, K.S. Trivedi, Design and analysis of a robust broadcast scheme for VANET safety-related services. IEEE Trans. Veh. Technol. 61(1), pp:-46-61, 2012.

[5]. K.C. Lee, et al., Survey of routing protocols in vehicular ad hoc networks, Advances in vehicular ad-hoc networks: developments and challenges, pp. 149-170, 2010.

[6]. Kokuti, V. Simon, Adaptive multi-hop broadcast protocols for ad hoc networks, in International Symposium on Communication Systems, Networks & Digital Signal Processing, pp. 1-6, 2012.

[7]. X. Li, B.J. Hu, H. Chen, J. Ye, A distance-aware safety-related message broadcasting algorithm for vehicular networks. Int. J. Distrib. Sens. Netw. 2014(6), pp:1-11, 2014.

[8]. G. Xiao, H. Zhang, Z. Huang, Y. Chen, Decentralized cooperative piggybacking for reliable broadcast in the vanet, in 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), pp. 1-5, 2016.

[9]. B.Wu, et al., A survey of attacks and countermeasures in mobile ad hoc networks, in: Wireless Network Security, ed: Springer, pp. 103-135. 2007.

[10]. X. Sun, et al., Secure vehicular communications based on group signature and ID-based signature scheme, in: Communications, 2007, IEEE International Conference (ICC'07), pp. 1539-1545, 2007.

[11]. K. Katsaros, et al., CLWPR-A novel cross-layer optimized position based routing protocol for VANETs, in: Vehicular Networking Conference (VNC), 2011 IEEE, pp. 139-146, 2011.

[12]. P. Nithya Darisini, N.S. Kumari, A survey of routing protocols for VANET in urban scenarios, in: Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference, pp. 464-467, 2013.

[13]. Y. Qian, N. Moayeri, Design of secure and application-oriented VANETs, in: Vehicular Technology Conference, 2008. VTC Springer 2008. IEEE, pp. 2794-2799, 2008.

[14]. E. Meriam, N. Tabbane, VANET adaptive and reliable broadcast protocol, in International

Wireless Communications and Mobile Computing Conference, pp. 237-243, 2014.

[15]. H.A. Omar, W. Zhuang, L. Li, On multi-hop communications for in-vehicle internet access based on a TDMAMAC protocol, in IEEE Conference on Computer Communications, pp. 1770-1778, 2014.

[16]. Y.-W. Lin et al, Routing protocols in Vehicular Ad Hoc Networks: a survey, J. Inf. Sci. Eng., pp 913-932, 2010.

[17]. G. Al-Kubati, et al., Fast and Reliable Hybrid routing for Vehicular Ad hoc Networks, in: ITS Telecommunications (ITST), 2013 13th International Conference, pp. 20-25, 2013.

[18]. Y. Xiang et al, GeoSVR: A map-based stateless VANET routing, Ad Hoc Networks 11 (2013) 2125-2135, 2013