A Survey on Vehicular Ad-hoc Networks (VANETs)

Mahendri[1], Neha Sawal[2]

M-Tech Student[1] Assit. Prof.[2] &Department of CSE & NGF College of Engineering &Technology
Palwal, Haryana, India

***Abstract*— Vehicular ad hoc networks (VANETs) are the specific class of Mobile ad hoc networks (MANETs). Since vehicles tend to move in a high speed, the network topology is rapidly changed. It is a promising approach for the Intelligent Transport System (ITS). There are many challenges to be addressed when employing VANET. It has a very high dynamic topology and constrained mobility which makes the traditional MANET protocols unsuitable for VANET. The aim of this review paper is to give an overview of the vehicular ad hoc networks, its standards, applications, security issues and the existing VANET routing protocols.**

Keywords: VANET, ITS, dynamic topology, mobility, routing protocols.

I. INTRODUCTION

In todays prospective the sheer volume of road traffic affects the safety and effectiveness of traffic environment. Millions of people are killed around the globe every year in the road accidents. It's been a challenge to stop these accidents and deliver safety of people. Safety applications are vital in nature and straightly associated to users and their lives. One promising way is to offer the traffic statistics to the vehicles so that they can use them to scrutinize the traffic situation. That can be accomplished by switching the information of traffic situation among vehicles. With the progress of microelectronics, it becomes possible to integrate node and network device into single unit and wireless interconnection.
VANET is an exciting application of mobile ad-hoc network (MANETs). VANET is the influential technology that can deliver realistic vehicle to vehicle (V2V) and vehicle to roadside infrastructure (V2I) communication. VANETs are self-configuring system where nodes are vehicle and WIFI technologies are used to form these networks.
VANETs are permitted to build intelligent transportation system (ITS) that emphases on road safety, traveler wellbeing and traffic efficiency. The accomplishment of VANETs relies on the crucial element such as statistics routing amid nodes and the entrance to the internet. Deprived of any powerful routing methodology, the power of VANETs will be constrained. Vehicular Networks (also known as VANETs) are a foundation of the projected Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well to safer and more effective roads by providing appropriate statistics to drivers and concerned authorities. The stimulating research area of Vehicular Networks is where ad hoc systems can be brought to their full potential.

the repeated interchange of such kind of data on the network clearly point toward the role of the security. For safety programs, the statistics not only needs to be accurate but also securely communicated from a source to destination. Hence security is a vital issue which can't be ignored. Attackers can generate difficulties by receiving full access of system therefore any effective attack can cause loss of lives or financial lose. Hence the security of the data in VANET is critical.

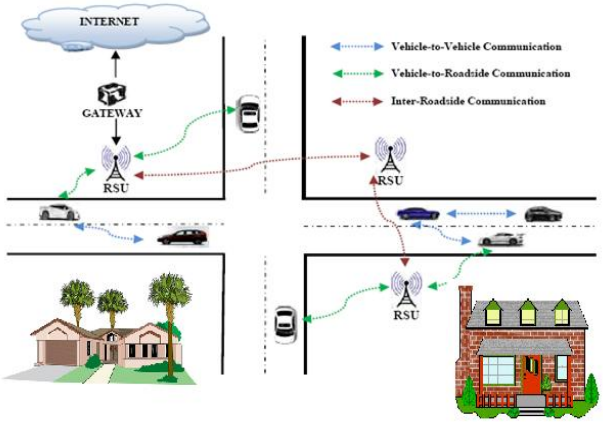

Figure1. Vehicular Ad hoc Network

II. ARCHITECTURE AND STANDARD

Vehicular Ad hoc Network (VANET) system architecture comprises of three types of domains such as in-vehicle, ad hoc, and infrastructure domains and numerous specific components like application unit, on-board unit, and road-side unit. Brief description of this architecture's is given below:

A. In-Vehicle Domain

The in-vehicle domain is composed of an on-board unit (OBU) and one or multiple application units (AUs). The connections between them are usually wired and sometimes wireless. Applications Units (AUs) is an in- vehicle entity, several AUs can be integrated with a single OBU and share the OBU processing and wireless resources. An OBU is used for giving the vehicle-to-infrastructure and vehicle-to-vehicle communication. An OBU is fitted with a single network device based on IEEE 802.11p radio technology; basically network device is used for sending, receiving and accelerating the safety and non-safety messages in the ad hoc domain.

B. Ad hoc Domain:

The ad hoc domain is composed of vehicles equipped with OBUs and roadside units (RSUs). An OBU can be seen as a

ISSN: 2278 – 1323

mobile node of an ad hoc network and RSU is a static node likewise. An RSU can be connected to the Internet via the gateway; RSUs can communicate with each other directly or via multi hop as well. The key purpose of RSU is to deliver the internet connectivity to the OBUs. On-Board Units (OBUs) form a mobile ad hoc network that permits communications between vehicles without the need for a centralized coordination occurrence.

C. Application Units (AUs):

An Applications Units (AUs) is an in-vehicle entity, multiple AUs can be plugged in with a single OBU and share the OBU processing and wireless resources. An Application Unit (AU) interacts exclusively via the On-Board Unit (OBU), which manages all mobility and networking utilities on the Application Unit (AU) behalf. The difference between an Application Unit (AU) and an On-Board Unit (OBU) is only logical and an Application Unit (AU) can be physically co-located with an OBU [29].

D. On-Board Units (OBUs):

The function of On-Board Unit (OBU) is vehicle to vehicle communications and communications with vehicle to infrastructure or road side unit. It is also used to deliver communication services to the application units and forwards data on behalf of other On-Board Units (OBUs) in the ad hoc domain. An On-Board Unit (OBU) is furnished with at least a single network device based on IEEE 802.11p standard.

E. Road-Side Units (RSUs):

A Road-Side Unit (RSU) is a device that is situated at stationary positions along roads and highways, or at permanent locations such as parking places, hospitals, shopping complexes, restaurants etc. A Road-Side Unit (RSU) is equipped with at least a network device based on IEEE 802.11p. Internet connectivity to the OBUs is the main function of RSUs.

III. VANET NETWORK ARCHITECTURE TYPES

The network architecture of VANETs can be divided into three categories: Cellular/WLAN, Pure Ad hoc, and Hybrid. Brief description is given below:

A. Cellular/WLAN Network Architecture:

WLAN/WiMAX access points are used in this type of network architecture. In order to connect to the Internet, fixed and cellular gateways are used. VANET can association both WLAN and cellular network to introduce such type of network so that a WLAN is used where an access point is accessible or a 3G connection can be used.

B. Ad hoc Network Architecture:

The cost for cellular/WLAN network architecture is very high as it is using fixed gateways, access points and other devices to build the network. So to overcome these problem vehicles and all the roadside units (RSUs) or roadside wireless devices can build an ad hoc network among themselves.

C. Hybrid Network Architecture

Hybrid network architecture is a mixture of both cellular/WLAN network architecture network and ad hoc network .This is also a conceivable solution for VANET. Better coverage can be provided by hybrid architecture new issue is faced like seamless transition of the communication among different wireless systems.

IV. STANDARDS FOR WIRELESS ACCESS IN VANET

Different communication standards are supported by Vehicular environment that communicate to wireless accessing. These standards are as follows

A. Dedicated Short Range Communication (DSRC)

It gives a communication range from 300m to 1Km. The V2V and V2R communication occurs within this range. DSRC uses 75MHz of spectrum at 5.9GHz, which is assigned by United States Federal (FCC). This provides half duplex, 6-27 Mbps data transferring rate. FCC does not charge for usage of DSRC spectrum. The DSRC spectrum is ordered into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channels is kept for safety communication. For critical safety of life and high power public, two channels are used and remaining of the channels is used as service channels.

B. IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE)

It is also recognized as IEEE 802.11p. It provisions the ITS applications, for a small range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz frequency range. It gives real time traffic statistics improving performance of VANET. It also profits the transport sustainability. It comprises the standard of IEEE 1609. This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques for division of signal into various narrow band channels.

V. SECURITY ISSUES

Due to the open nature of the wireless medium used in VANET, there is possible number of attacks by which VANET is exposed to. Some of the attacks mentioned below.

A. Denial of Service

Denial of service is one of the most severe attacks in vehicular network. The main objective of DOS attack is to prevent the legitimate users to access the network services.

Jamming- This attack refers to block the communication channel in order to prevent the flow of any information. It is initiated by malicious node after determining the frequency of the channel.

SYN Flooding- An attacker sends large number of SYN requests to a victim node in an attempt to consume enough server resources to make system unresponsive to legitimate traffic.

Distributed DOS attack- This attack is more severe because it is in distributed manner where the impact is dispersed in the network.

B. Black hole attack

A malicious node, exploiting the flooding based routing protocol; falsely advertise itself as having an optimum route to the destined node. If the malicious node replies to the requesting node before the reply of actual node, then a bogus or forged route will be created. In this attack, the attacker node drops out to form a black hole; all routes it involved in are broken down leading to a failure to propagate messages. Therefore, the data packets are not forwarded to the legitimate vehicle nodes, instead, the malicious node intercepts the packets, drop them or forward them to unknown address and thus, absorb network traffic.

C. Gray hole attack

Gray hole attack is the specialized type of black hole attack in which the malicious node's behavior is totally unpredictable, it may first act as an honest node during route discovery process and then may change its state to malicious and vice-versa. It drops the packets selectively either on probabilistic distribution or dropping all UDP packets while forwarding TCP packets. Detection of gray hole attack is not an easy task due to congestion, overload and ability of changing states. A Gray hole attack is an event that disturb route discovery process and degrade the network performance by intentional malicious activity.

VI. NETWORK SIMULATORS

Network simulator is a kind of software or hardware that predicts the behavior of the network without an actual network being present. Most of the simulators are graphical user interface driven while others require input scripts or commands. Trace file is the important output of the simulations.

A. NS-2

NS-2 (Network simulator-2) is a discrete event simulator used for networking research developed at Berkeley. NS-2 was built in C++ and provides the simulation interface through OTcl. The combination (C++ and OTcl) proves to be very effective because C++ is used to implement the detailed protocol and OTcl is used to control the simulation scenario for users and schedule the events.

Features

a. The event scheduler keeps track of simulation time and release all the events in the event queue by invoking appropriate network components.
b. Efficient, NS-2 separates control path implementation from data implementation.

B. OPNET

Optimized Network Engineering Tool (OPNET) is a simulator built on the top of a discrete event system, which means it simulates the behavior of the system by modeling each event in the system and processes it by user-defined processes. It can be used to study communication networks, devices, application and protocols. OPNET also provides programming tools for users to define packet format of the protocol.

FEATURES

Lot of component library with source code
Hierarchical modeling environment
Supports Grid computing

C. QUALNET

Quality Networking (QUALNET) simulator is used for large heterogeneous network that supports both wired and wireless network protocol.

FEATURES

It uses highly detailed standard based protocol models.
It can connect to various hardware and software applications e.g. OTB, real networks.

FEATURES	QUALNET	NS-2	OPNET
Language supported	Parsec C++	C++/ OTcl	C++/JAVA
License	Commercial	Open source	Commercial
GUI Support	Excellent	Poor	Excellent
Platform	Linux window	Unix, mac-os, Microsoft window cygwin	C, C++, opnet modeler software
Time taken to learn	Very easy	Long	Long
Scalability	Good	Poor	Good
Network visualization tool	✓	✓	✓
Interaction with real system	✓	✓	✓
Fast simulation capabilities	✓		✓
Possibility to design and modify scenarios	✓	✓	✓
Latest version			
Communication with other modules	✓		✓
Availability of analysis tool	✓	✓	✓

VII. ROUTING IN VANET

Routing is the mechanism of transmitting data from source to destination with the least rate via multi-hop steps. Due to unpredictable and dynamic nature of VANET because of high mobility of nodes, large network size, intermittent communication between vehicles and infrastructure, makes routing even harder. Vehicles do not have any prior knowledge about topology, therefore, they have to acquire the network topology and store it in a data structure called routing table and distribute it in order to find an efficient and feasible route. Routing is a big challenge to find an efficient strategy that guarantee the maximizing reliability, minimum delays and timely exchange of information while designing architecture for vehicular communication. The primary aim of routing protocol must be to find an optimal route that has minimal overhead and consume minimum bandwidth.

ISSN: 2278 – 1323

A. PROACTIVE ROUTING PROTOCOL

Proactive (table-driven) protocols allow a network node to maintain the routing table to store topology information about all other nodes, each entry in the table contains the next forwarding hop node used in the path to the destination irrespective of the fact that whether they are presently participating in the communication or not. The table is updated periodically to reflect the changes in the network topology and should be broadcast to the neighbors. After analyzing all routes, the shortest route will be chosen through shortest path algorithm to each possible destination in the table. Examples are FSR (Fisheye State Routing Protocol), DSDV (Destination Sequenced Distance Vector Routing Protocol), and CGSR (Cluster Head Gateway Switch Routing Protocol).

Advantage

Destination route is already stored in the background.

Disadvantage

It may fail in VANET due to high bandwidth consumption and large routing table.

B. REACTIVE ROUTING PROTOCOL

Reactive (On-Demand) protocols do not continuously exchange routing information with the neighbor nodes, instead a route is determined on a demand and maintain only those routes that are needed in current communication. When a source node needs to find a route to the destination node, it starts a route discovery process in which the query packets are flooded into the network for the path search. The destination node responds for establishing a route and this phase completes when route is found. Examples are AODV (), DSR (), TORA ().

Advantages

No distribution of routing information

Effective in route maintenance and less bandwidth

Disadvantages

Higher time for route discovery

Network congestion due to excessive flooding of messages Vanet covers a great range of potential applications with high diverse requirements. It ranges from road safety to multimedia delivery.

VIII. VANET APPLICATIONS

Communication between the vehicles has led to the development of a number of applications and provides a wide range of information to drivers and travelers. This has increased the road safety and comfort of the passengers. Applications can be classified into two, on the basis of their purpose.

A. Safety Application

These applications focus on improving road safety and in avoiding accidents by using the wireless communication between the vehicles or between vehicles and infrastructure

Table 1: Safety Oriented Applications

NAME	DESCRIPTION
Electronic brake warning	Broke down vehicle or vehicle performing sudden brake broadcasts messages to approaching vehicles
Lane change warning	Safe lane change can be performed by drivers
Road hazard condition	A vehicle detecting hazard (landslide, presence of fluid) warns other approaching vehicles
Intersection violation warning	Vehicles exchange messages to make a safe crossing
Post crash notification	A vehicle involved in an accident would broadcast messages about its position to trailing vehicles for taking decision in time
Traffic vigilance	Cameras installed at RSU can work as input and act as tool in low and zero tolerance campaign against driving offenses
Blind crossing	Vehicles can corporate with each other in a crossing when there is no traffic lights

B. Non Safety Oriented

It includes commerce and convenience applications which provides the entertainment and services to drivers and also deals with traffic management to enhance traffic efficiency.

Table 2: Non Safety Oriented Applications

NAME	DESCRIPTION
Congested road notification	Detect and notify about congested road, so route and trip planning can be done
Value added advertisement	Announcements like petrol pumps, highway restaurants to lure the drivers to their stores within communication range
Electronic toll collection	Payment can be done electronically through toll collection point without stopping
Parking availability	Helps the drivers to find available slots for parking in certain geographical area
Internet access	Vehicles can access internet through RSU where RSU works as a router
Media or map download	Highway or urban area map can be downloaded to avoid traffic jam

IX. VANET LITERATURE REVIEW

AUTHOR NAME	YEAR	PAPER TITLE	WORK
Shaikhul Islam Chowdhury et.al	2011	Performance evaluation of reactive routing protocols in VANET	Here, the author compared performances of reactive routing protocols i.e. AOMDV, DSR, AODV in VANET by using NS-2.34.After simulation, the author showed that DSR has better PDF and lesser routing overload and

			AOMDV has better performance in end to end delay.
Hua-Wen Tsai	2011	Aggregating data dissemination and discovery in vehicular adhoc network	This paper proposed an aggregating data dissemination and discovery algorithm in vehicular ad-hoc network by using NS2. After simulation, author concluded that ADD algorithm can decrease aggregation and dissemination cost in communication and the user can get data quickly when they need.
Vijaylaxmi S.Bhat et.al	2012	Performance comparison of adhoc VANET routing algorithms	Here, the author proposed a rate adaptation algorithm that behaves as Auto Rate Fallback and evaluated the performance of this algorithm and compared this with other algorithms. the result showed that AODV provides quick adaptation .
Jagdeep Kaur et.al	2013	Performance comparison between unicast and multicast protocols in VANETs	In this paper, author showed the performance comparison b/w unicast and multicast routing in VANETs and calculated the efficiency of unicast routing protocols (AODV,DSR) and multicast routing protocols (ADMR, ODMRP) by using NS-2.34. The author compared the protocols efficiency for result.
Sheeba Memon et.al	2014	Performance evaluation of MANET's Reactive and proactive routing protocols in high speed VANETs	In this paper, the author evaluated the performance of two MANET routing protocols –AODV and DSDV in high mobility VANET by using NS2 simulator. After evaluation author observed AODV has better performance as compared to DSDV which has low performance in even un-stressed conditions.
SUNXi et.al	2011	Study of the feasibility of VANET and its routing protocols	Here, the author studied the application of VANET to city road traffic control by using NS2 simulator. After the simulation, author concluded that reactive routing protocols more suitable for VANET.
Josiane Nzouonta et.al	2009	VANET routing on city roads using real-time vehicular traffic information	In this paper, the author implemented a reactive protocol RBVT-R and a proactive routing protocol RBVT-P and compared them using NS-2.30.The result showed that distributed applications can use RBVT-R when throughput is required and RBVT-P if they are delay-sensitive.

X. CONCLUSION

VANET is a promising technology and with the substantial advancement in wireless technology, vehicles are becoming a vital part of global network. VANET will not only provide life saving applications but will also become a powerful communication tool for users. Here, focus is paid on basic architecture of VANET, routing , simulation, attack and application. Fulfilling the requirements and facing challenges will result in an efficient communication tool which can also provide life saving tools to the users [6]. If improved it can give better results than other mobile ad hoc network. Vehicles can be designed in a way that they possess learning abilities so as to have perception of potential dangers and to modify vehicle's behaviour consequently. It can help vehicle to take decisions from it's past experience.

REFERENCES

[1] Biswas, S., & Misic, J to Privacy-preser. (2013). "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192

[2] Pradweap, R. V., & Hansdah, R. C. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Information Systems Security (pp. 314-328). Springer Berlin Heidelberg.

[3] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[4] Grzybek, A.; Seredynski, M.; Danoy, G.; Bouvry, P., "Aspects and trends in realistic VANET simulations, *Wireless, Mobile and Multimedia Network, 2012 IEEE International Symposium on a* , vol., no., pp.1,6, 25-28 June 2012

[5] Jie Li, Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs" , IEEE Transactions on Parallel and Distributed Systems, 2012

[6] Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Li, V.O.K., "VSPN: VANET-Based Secure and Privacy-Preserving Navigation," *Computers, IEEE* Transactions *on* , vol.63, no.2, pp.510,524, Feb. 2014

[7] Yen-Wen Lin; Guo-Tang Huang, "Optimal next hop selection for VANET routing," *Communications and Networking in China (CHINACOM), 2012 7th International ICST Conference on* , vol., no., pp.611,615, 8-10 Aug. 2012

[8] Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survay and taxonomy," *Communications Surveys & Tutorials, IEEE* , vol.11, no.4, pp.19,41, Fourth Quarter 2009

[9] Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," *Wireless communication, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on* , vol., no., pp.1,4, 12-14 Oct. 2008.

[10]Performance Comparison Of AODV and DSDV Routing Protocols in Mobile Ad Hoc Networks, Aditi Sharma,Sonal Rana, Leena Kalia, International Journal of Emerging Research in Management and Technology, ISSN:2278-9359 Volume-3, Issue-7, July 2014.

[11] Ait Ali, K.; Baala, O.; Caminada, A., "Routing Mechanisms Analysis in Vehicular City Environment," *Vehicular Technology Conference, 2011 IEEE 73rd* , vol., no., pp.1,5, 15-18 May 2011

[12] Bhoi, S.K.; Khilar, P.M., "A secure routing protocol for Vehicular Ad Hoc Network to provide ITS services," *Communications and Signal*

ISSN: 2278 – 1323

Processing (ICCSP), 2013 International Conference on , vol., no., pp.1170,1174, 3-5 April 2013

[13] Pathre, A.; Agrawal, C.; Jain, A., "A novel defense scheme against DDOS attack in VANET," *Wireless and Optical Communications Networks (WOCN), 2013 Tenth International Conference on* , vol., no., pp.1,5, 26-28 July 2013

[14] Hamieh, A.; Ben-othman, J.; Mokdad, L., "Detection of Radio Interference Attacks in VANET," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE* , vol., no., pp.1,5, Nov. 30 2009-Dec. 4 2009

[14] Lyamin, N.; Vinel, A.; Jonsson, M.; Loo, J., "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks," *Communications Letters, IEEE* , vol.18, no.1, pp.110,113, January 2014

[15] Yeongkwun Kim; Injoo Kim; Shim, C.Y., "A taxonomy for DOS attacks in VANET," *Communications and Information Technologies (ISCIT), 2014 14th International Symposium on* , vol., no., pp.26,27, 24-26 Sept. 2014

[16] Verma, K.; Hasbullah, H.; Kumar, A., "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.550,555, 22-23 Feb. 2013

[17] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on* , vol.3, no., pp.261,265, 25-27 May 2012

[18] Pooja, B.; Manohara Pai, M.M.; Pai, R.M.; Ajam, N.; Mouzna, J., "Mitigation of insider and outsider DoS attack against signature based authentication in VANETs," *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on* , vol., no., pp.152,157, 10-12 Feb. 2014

[19] Durech, J.; Franekova, M.; Holecko, P.; Bubenikova, E., "Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modelling," *ELEKTRO, 2014* , vol., no., pp.424,429, 19-20 May 2014

[20] Nafi, N.S.; Khan, R.H.; Khan, J.Y.; Gregory, M., "A predictive road traffic management system based on vehicular ad-hoc network," *Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian* , vol., no., pp.135,140, 26-28 Nov. 2014

[21] Kumar, A.; Sinha, M., "Overview on vehicular ad hoc network and its security issues," *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on* , vol., no., pp.792,797, 5-7 March 2014

[22] Mehta, K.; Malik, L.G.; Bajaj, P., "VANET: Challenges, Issues and Solutions," *Emerging Trends in Engineering and Technology (ICETET), 2013 6th International Conference on* , vol., no., pp.78,79, 16-18 Dec. 2013

[23] Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," *Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian* , vol., no., pp.1,6, 7-9 Nov. 2012

[24] Shuai Yang; Rongxi He; Ying Wang; Sen Li; Bin Lin, "OPNET-based modeling and simulations on routing protocols in VANETs with IEEE 802.11p," *Systems and Informatics (ICSAI), 2014 2nd International Conference on* , vol., no., pp.536,541, 15-17 Nov. 2014

[25] Sadeghi, M.; Yahya, S., "Analysis of Wormhole attack on MANETs using different MANET routing protocols," *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on* , vol., no., pp.301,305, 4-6 July 2012

[26] Jhaveri, Rutvij H.; Patel, Ashish D.; Dangarwala, Kruti J., "Comprehensive Study of various DoS attacks and defense approaches in MANETs," *Emerging Trends in Science, Engineering and Technology (INCOSET), 2012 International Conference on* , vol., no., pp.25,31, 13-14 Dec. 2012

[26] C. Sommer, Z. Yao, R. German, and F. Dressler, "On the need for bidirectional coupling of road traffic micro simulation and network simulation," in Mobility Models '08: Proceeding of the 1st ACM SIGMOBILE workshop on Mobility models. New York, NY, USA: ACM, 2008, pp. 41–48

[27] Zhao and G. Cao, "Vadd: Vehicle-assisted data delivery in vehicular ad hoc networks," Vehicular
Technology, IEEE Transactions on, vol. 57, no. 3, pp. 1910 –1922, may 2008.

[28] Q. Chen, D. Jiang, and L. Delgrossi, "Ieee 1609.4 dsrc multi-channel operations and its implications on vehicle safety communications," in Vehicular Networking Conference (VNC), 2009 IEEE, oct. 2009, pp. 1 –8.

[29] Y. H. Choi, R. Rajkumar, P. Mudalige, and F. Bai, "Adaptive location division multiple access for reliable safety message dissemination in vanets," in Wireless Communication Systems, 2009. ISWCS 2009. 6th International Symposium on, sept. 2009, pp. 565 –569.

[30] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen,Angela Irwin, Aamir Hassan," *Vehicular Ad hoc Networks(VANET):Status, Results, Challenges*". Springer Science, Business Media.2010

[31] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan *Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.*

