Vehicular Ad-Hoc Network Communication Domains and Challenges

Babangida Zubairu[1], Dr Savita Shiwani[2]

[1]Research Scholar, [2]Associate Professor
Jaipur National University
Jaipur, Rajasthan State, India

Abstract **: In a prospective era of artificial intelligence and advancement in the wireless technology, some of the challenges militating the existing system of driving and road safety will soon be relieved, hence, caution and messages related to a warning, traffic condition, information about approaching vehicles before reaching driver's vision and road status, would reach drivers before the occurrence of incidence. These tremendous benefits can be achieved from vehicular networks, which is a brand of wireless technology intends to hence safety and comport of driving system. The paper examined the current trend of the technology and identifies the vulnerabilities and the challenges of the technology. Different models of the communication in vehicular ad-hoc network were present with the challenges in each model. The vehicular ad-hoc network would be one of the building blocks for smart cities deployment around the globe.**

Index Terms: artificial intelligence, wireless, technology, vehicular networks, vulnerabilities

1.0 INTRODUCTION

The technological shift and advancement in the wireless technology will rapidly influences the transportation sector; the traditional transportation system will soon be changed with a new brand of wireless technology known as Vehicular Ad-hoc Network. The development comes from the rapid speed of innovations in the auto industries, research efforts from academia across the globe and the need to enhance safety in the transportation system. The rate of the developments in the wireless technology reveals that the deployment of Intelligence Transportation System (ITS) and emotional cars moving on the roads will soon be actualised [**1**]. Various research efforts are ongoing to speed up the deployment of a wireless network based on short-range communications between moving vehicles [**2**], these efforts contribute tremendously in the new innovations and the paradigm shift towards modernising transportation system of the present generation and beyond [**3**]. Vehicular Ad-hoc Network (VANET) is a new brand of wireless network intends to enhance drivers' safety as well as the passengers and provides support for safety-related applications such as collision warning and traffic control [**4**] . As such, VANET becomes a key component of Intelligent Transportation System (ITS) [**5**]. According to Amita Meshram (2014) VANET technology is symbolized by higher speed, limited connectivity and rapidly varying topologies, the technology provides real-time information about road conditions as well as traffic status and allows the vehicles to react on time when a need arises. The vehicles represent mobile nodes that move on hundreds of kilometres per hour. The number of nodes keeps changing dramatically in a large scale, this demands frequent and constant update on the node information, incurring a large amount of communication and control overhead, the technology allows Vehicles to communicate with each other, send and receive information in real time basis [**6**].

2.0 VEHICULAR NETWORK TECHNOLOGY (VNT)

VANET emerge as one of the most promising and challenging technology, integrating ad-hoc networks consisting of two or more nodes **[**7**]**. The technology support V2X communication, with this technology, the vehicles can directly communicate with each other in ad-hoc mode branded as Vehicle-to-Vehicle communication (V2V); the technology enables vehicles to communicate with Road Side Units (RSU) known as Vehicle to Infrastructure communication (V2I) **[**8**]**. The RSU, in turn, connects the vehicular network to the internet via a central control called the Trusted Authority (TA) **[**9**]**. The TA hosts the application services provided by servers at the backend **[**10**]**. Each vehicle is equipped with On-Board Units (OBUs), The OBU resides within the vehicles and provides communication capabilities support, the OBU is made up of a set of devices such as sensors and processors for collecting data, Global Positioning System (GPS) for vehicle speed, direction and position, as well as Event Data Recorder (EDR) responsible for recording events activities **[**9**]**.

3.0 TAXONOMY OF VEHICULAR AD-HOC NETWORK

A Vehicular Ad-hoc Network is a brand of mobile Ad-hoc network mainly intended for moving vehicles to support the wireless communication [**11**]. According to M.Sindhuja (2015), VANET network consists of moving vehicles as the nodes, each node can be equipped with On-Board Units (OBU) to access the remote services provided by the network on the road through the RSUs. The infrastructure of the network consists of the Road Side Unite (RSU) and Trusted Authority (TA). The TA serves as a getaway and provides central management of the network [**12**]. The backbone support RSUs integrations as well as network connection to the internet is provided by TA, The RSUs connect to TA as shown in Fig. 1, the communication between the vehicle to vehicle, or between vehicles to RSUs is achieved through a wireless medium called Wireless Access in Vehicular Environments (WAVE) [**13**].

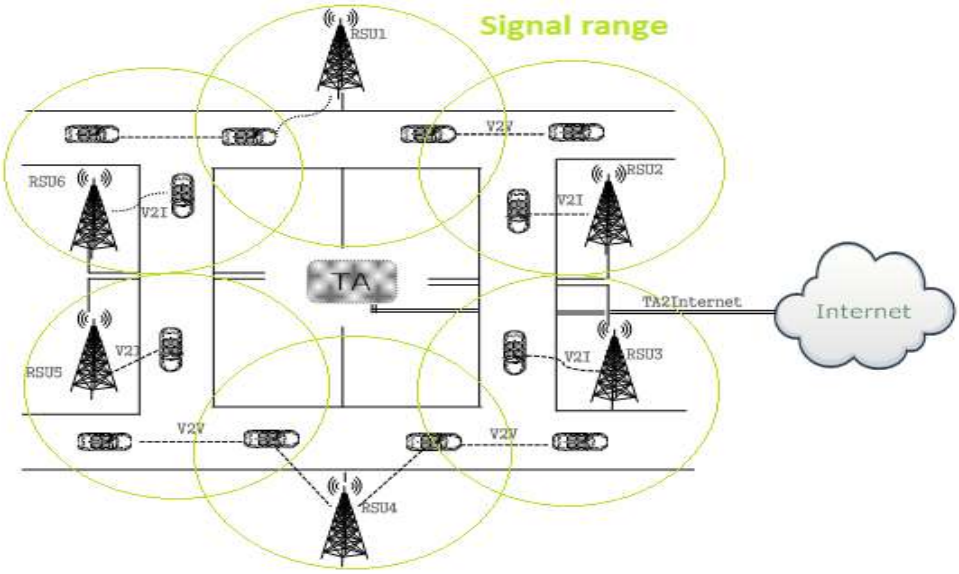

Figure 3 Vehicular Ad-hoc Network model

4.0 VEHICULAR AD-HOC NETWORK

Vehicular Ad-hoc Networks is one of the significant components of Intelligent Transportation System, the vehicles are the nodes that send and receive traffic information via wireless communications channels. The aims of VANETs are to enhance passenger comfort, traffic efficiency, the safety of passengers and provide support for safety-related applications such as collision warning and traffic control **[4]**. Vehicular Network communication occurs in two modes, the first is infrastructure less and self-organised network for Vehicular to Vehicle (V2V), this type of network required no central control or a gateway. The second is infrastructure based on Vehicle to Infrastructure (V2I) communication that relies on gateway such as Access Point (AP). The nodes are characterised by higher mobility which leads to rapid changes in the network topology and frequent network fragmentation due to short connection lifetime.

5.0 VEHICULAR NETWORKS COMMUNICATION MODELS

The technology supports either peer-to-peer communications using ad-hoc mode where a vehicle communicate with another vehicle directly or dependence on the network infrastructure like client/server approach for message sending and receiving [**14**]. The communication pattern can be in form of Vehicle to Vehicle (V2V) where the vehicles communicate among themselves or Vehicles to Infrastructure (V2I) that relayed on a gateway device such as AP. The communication supports both stationary and moving nodes [**15**]. Network delay is the major concern in V2I communication. Hence, the message passes from vehicle to Infrastructure and then infrastructure to destination vehicles (V2I - I2V). Though, in V2V communication, this constraint is not an issue, since the communication is infrastructure less. The connectivity and security are the major pressing issues in V2V, since, the nodes are mobile and the network may contain active and passive nodes, however, due to the higher mobility of the nodes, the network suffer from short communication lifetime and defragmentation of the network topology [**16**]. The main communication models supported by this technology as described by [**17**] and [**18**] are the V2V, V2I, and R2R.

5.1 Vehicle to Infrastructure (V2I) communication

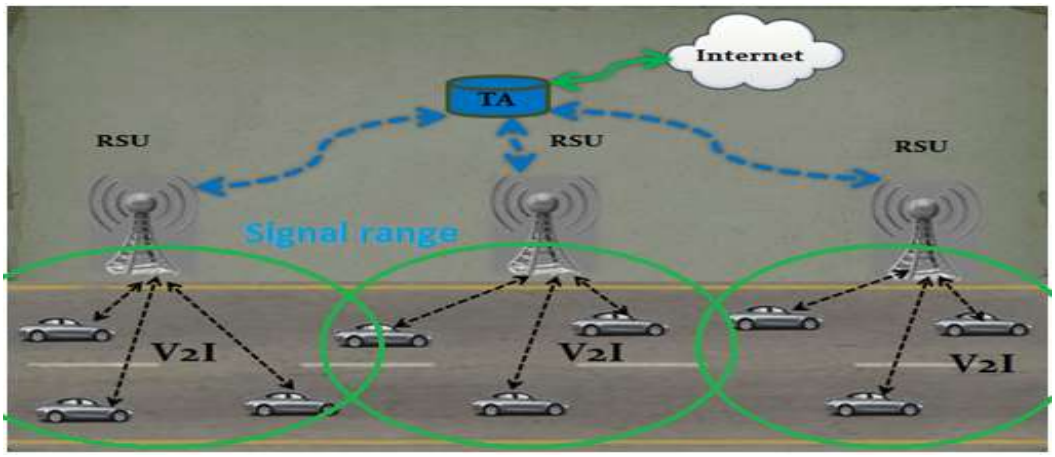

Figure 2: Vehicle to Infrastructure (V2I) communication

In V2I Fig. 2, the vehicles communicate with one another via the Road Side Unit (RSU) [8]. RSU is a static device that can be placed at some distances along the roadside; the RSU is part of the infrastructure that enables connections between the vehicles and the Trusted Authority (TA) [10]. The application servers reside on the backend of TA for central control and management of the network [18]. During a communication, the vehicles send messages to RSU and the RSU broadcast the message to target vehicles. The RSU works as a relay device between senders and receivers, hence this type of communication is not suitable for time-critical or emergency messages since the process of communication introduces delay in message propagation, but has advantages of covering large areas.

5.2 Vehicle to Vehicle (V2V) communication

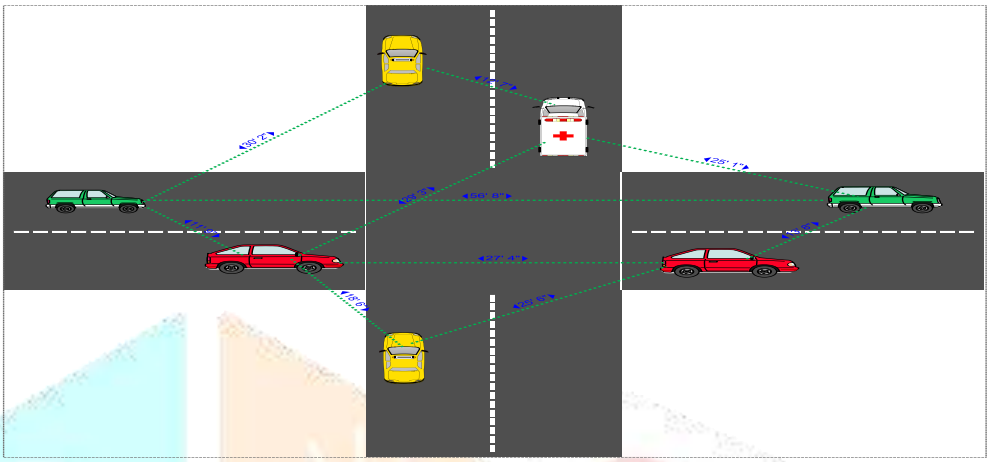

Figure 3: Vehicle to Vehicle (V2V) communication

In the V2V model, the vehicles communicate wirelessly with one another via a wireless medium [19], V2V communication is pure wireless communication between vehicles in ad-hoc mode see Fig. 3; the technology provides data exchange platform for the vehicle share information with other vehicles within a communication range [15]. In V2V communication, each vehicle is a node and can work as a source, a destination and/or a router to re-transmit traffic-related information to other vehicles. The use of V2V communication reduces the delay introduced by RSU in V2I communication. The vehicles communicate either directly or indirectly, this means, the nodes within the same signal range communicate directly and but to communicate with other nodes out of the same signal range, the communication occurs via an intermediate nodes by establishing routes for transmissions in multiHop mode [20], this enables forwarding of data to an individual or group of node [21]. The communication between nodes is achieved by means of Dedicated Short Range Communications (DSRC) [18] . The DSRC technology work in the range of 5.9 GHz with the bandwidth of 75 MHz and transmission range of 0 to 300m, $0 \leq D < 300$, where D represents the distance separating the two vehicles [16].

5.3 RSU-to-RSU (R2R)

Beside V2V and V2I communication, VANET supports RSU to RSU communication known as R2R communication [22]. This type of communication provides backbone support to vehicular networks; the RSUs are static and can be placed along the roadside after a fix distance interval [23].

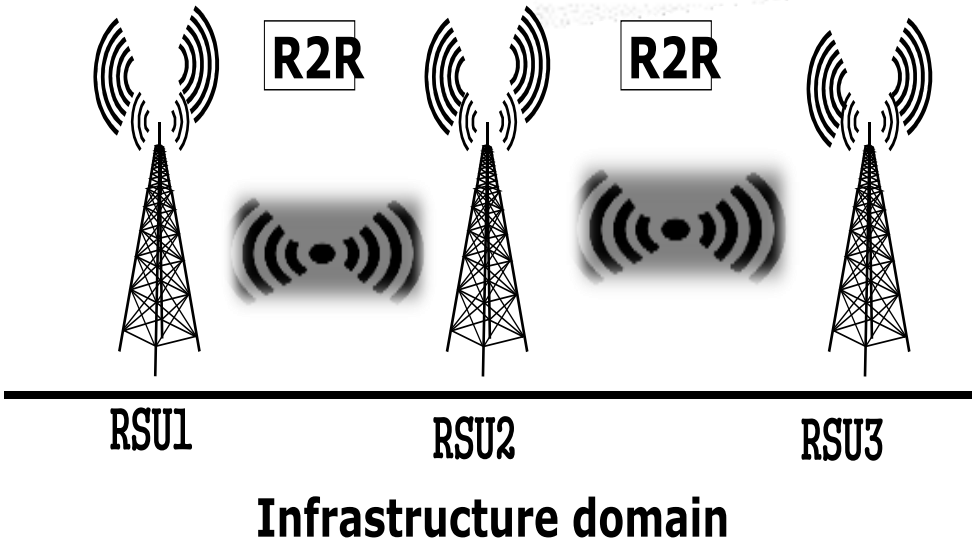

Figure 4: RSU-to-RSU (R2R)

The RSUs can be connected through wired or wireless medium technology such as Cellular/ WiMAX (see Fig. 4) while in turn connects vehicular networks to the Wide Area Network (WAN) via the TA **[**24**]**. The distance between RSU to RSU as proposed in **[**23**]** is between 300m to 1km, this range will enable effective communication among RSUs **[**25**]**.

6.0 SERVICES OFFERED BY VEHICULAR AD-HOC NETWORK

Vehicular Ad-hoc Network as described by **[**26**]** provides the following services:

6.1 Road safety applications

The safety application service offered by VANET improves driving conditions and reduces the possibility of a road accident. The ad-hoc network enables information sharing amongst vehicles or between vehicles and RSU. The precise means of reflecting the value of ITS, is to guarantee the security of the applications and network performance, such as collision warning as well as the emergency warning. However, minimal reduction of accidents rate and fatalities that occurs day and night on the roads are among the goals of ITS.

6.2 Intelligent Traffic Management System (ITMS)

Another application service supported by VANET is to provide real-time information and update to drivers about the road's traffic condition in advance when there is traffic jam along the road so that the driver can decide to choose an alternate route to avoid the traffic jam. The information updates from a vehicle can be periodic or real-time transmission to its neighbouring vehicles. Intelligent traffic management helps in disseminating real-time update between vehicles and road users on traffic flow and road status. Therefore, ITMS reduces driver's travel time and traffic delay, risk of accident and fuel consumption; hence, reductions in the fuel consumption will have a significant effect on environmental population control.

6.3 Internet applications

Vehicular network services include internet application in a form of on-demand services. The vehicles can provide support to the internet services so that the passages on the vehicles can connect, access and share information while the vehicles are on moving along the road.

6.4 Location services

The mobile nodes in the networks can be used as information gathering device and a spy tool that can provide support for services such as location information via the inbuilt hardware. However, other services include Global Positioning System (GPS) and Enhance Global Positioning System (EGPS) receiver that enables information sharing about vehicle location with other vehicles.

7.0 VULNERABILITIES IN VEHICULAR AD-HOC NETWORK

According Bharti (2016) Vehicular Ad-hoc Network is vulnerable to several security threats, a vehicle to vehicle communication is infrastructure less and lack centralized control, these have made it becomes vulnerable to malicious activities [**27**]. Data transmission passes in an open path through a wireless medium and the openness natures of communication are exposed to security threats [**28**]. Below are the identified threats in vehicular networks.

7.1 Denial of Service (DOS) attacks

In DOS attack the malicious nodes prevent legitimate and authorised vehicle for accessing the network and resources. In this attack, the path of the network is jammed by malicious node so that no authorised vehicle can access the network. This attack is serious, since, the infected vehicle will not be able to communicate with the other vehicles **[**11**]**. DOS attacks in vehicular networks as mentioned by **[**29**]** can be implemented from one of the following techniques:

- Jamming mode: In this approach, the malicious vehicle senses the physical channel of the communication and gets the information about the frequency at which the vehicle receives the signal. The malicious vehicle re-transmits the signal on the channel so that the channel is jammed by making the channel busy executing unnecessary tasks, this will make the channel overwhelm and stop executing necessary tasks.

- Distributed mode: In this approach, the attack executes in distributed manner from multiple malicious vehicles at different locations, by preventing the victim vehicle for accessing the network resources and services. The malicious vehicle may use different time slot for executing the action by sending threat messages at a variable time, the aim is to slow down the network and prevent the network from operating properly. The execution of this threat as described by **[**11**]** is achievable against vehicle to vehicle or vehicle to infrastructure communication.

- Sybil Attack: As described by [**11**] is a threat in which multiple messages from one node are sent to multiple nodes with different identities. This creates confusion in the network that can lead to collision problems in the network.

7.2 Threats in Routing

The goal of routing attacks as described by [**29**] is to exploit the vulnerability of network layer of the routing protocol by either dropping the packet or disturbs the routing process of communication. The most common routing attack in the vehicular network is black hole attack. In this type of attack, the malicious vehicle attracts the active vehicles to transmit the packet through itself. However, the malicious vehicle keeps sending false route continuously claiming to be an active route. This threat has the characteristics as follows:

- Packet dropping: In this type of security threat, the malicious vehicle attracts and convinces the active vehicles to broadcast the packet through itself by sending fake route request, claiming to be an active route, the active vehicle broadcast the packet through the malicious vehicle route, when the packet reaches the malicious vehicle, then the packet is drop [**11**]. This type of attack reduces network throughput and increases packet drop ratio significantly and can lead to collapse or suspension of the communication channel [**30**]. However, According to [**31**] packets can also be dropped due to congestion, corruption or fault from the channel of communication and overflow of transmission queue. Bharti (2016) highlighted packet drop attack as one of the security threats that affect the performance of VANETs, this treat is potential to cause catastrophic consequences of violating routing protocol and vital segments of vehicular networks to develop serious problem and malfunctions [**32**]. However, packet drop leads to poor network performance such as excessive network delay, suspension of communication route or even generating erroneous information between nodes [**33**].

- Route flooding: In this threat, the malicious vehicle floods the network channel with generated forge Route Requests (RReg) addressed to an unknown destination in the network. The malicious vehicle does not intend to receive a reply, but to flood the network and creates congest. As results of this, the network resources are exhausted and increase unnecessary bandwidth consumption, as well as disruption of operational performances of the routing protocol operations [**34**].

- Wormhole attack: In a vehicular network, the wormhole attack occurs with the presence and support of two or more malicious nodes. The malicious nodes create a secret tunnel which, if a packet comes to one of them, it guides the packet to another pair of the malicious nodes in the network and this action creates a short path control by the malicious nodes. The malicious nodes re-broadcast the packet through the network. Hence, they control all Packets that come to them and threaten the safety of data within packets, by implication; this action can disturb the network operations [**35**]

- Gray hole attacks: This threat works in a similar way like the packet drop with exception in the attack process, the malicious node behaves like a malicious node in packet drop attack but it drops the packet selectively instead of entire received packets.

8.0 INFORMATION TRANSMISSIONS IN VEHICULAR NETWORK

Nodes in vehicular networks are of equal status; this implies that, each of the nodes can transmit information from itself to another node within a network signal via a network channel, the channel is the mechanism responsible for the transmission and guided by the routing protocol. Hence, the consistency of the channel is among the vital issue in vehicular communication, since nodes are mobile and demand regular information updates of their neighbours' identities and location. Moreover, Security remains a significant issue in vehicular network deployment **[**36**]**. Safety in VANET is essential, since it affects the life of people, it is essential that the message traverses between nodes reaches the right destinations **[**37**]**.

The communications in vehicular networks are exposed to signal interference as the vehicles may move in different environmental setting, physical objects such as buildings, trees, moving trucks, construction work on the sides of the road, topography area can hinder with the radio signals, however, the threat in the communication like packet drop can affect the network performances and quality of services **[**38**]**. Hence, improving and enhancing information transmission in vehicular networks is essential for smooth running of intelligent transportation system. It is also a vital issue to safeguard the vehicular network communication for reliable information exchange among the moving vehicles **[**39**]**. The message traverses on the network may contain crucial information for driver's decisions making, thus, it is inevitable to maintain credibility of the information so that the data cannot be altered or deleted by a malicious node **[**40**]**. Information exchange plays significant role in vehicular networks and provides guides and references for safety **[**41**]**.

9.0 CONSEQUENCES OF VULNERABILITIES IN VEHICULAR NETWORKS

- Safety in VANET is crucial because it affects the life of people; it is essential that modification or deletion of vital information should not be allowed
- A threat like packet drop is very dangerous for a vehicle can claim to be in different positions at the same time, thereby creating chaos and huge security threats in the network.
- Threat in the network topologies leads to the communication channel performance degrading and higher bandwidth consumption.
- Security threats can compromise and disturb the application functionality and increase the chances of road accident
- Any change in the network information by a fraud vehicle may cause great harm for the vehicle, drivers and passengers, as well as partitioning the network and reduce the performance of the entire or a segment of the network.

10.0 CONCLUSION

Vehicular Ad-hoc Network is a brand of wireless technology intends to enhance the transportation sector and is among the components of Intelligent Transportation System, the technology enables vehicle to communicate with each other by sending and receiving information frequently. The V2X technology operates on wireless technology and enables vehicle to connect to another vehicle and other devices, access and analyse the data about related objects surrounding the road infrastructure such as signs and traffic lights, as well as information sharing on the speed of vehicles, location and direction. Moreover, the technology support real-time information dissemination about road conditions as well as traffic status and support vehicles to react on time when a

need arises. Despite these tremendous advantages offered by the system, the technology is symbolised with some challenges, which were presented in the paper.

REFERENCES

[1] Buban Chales. (2017, January) MotionCars. [Online]. http://motioncars.inquirer.net/47744/trends-transform-auto-industry

[2] Arindam Ghosh, Vardhan Paranthaman Vishnu, Mapp Glenford, and Gemikonakli Orhan, "Exploring efficient seamless handover," EURASIP Journal on Wireless Communications and Networking, vol. 1, no. 227, pp. 1-19, 2014. [Online]. http://jwcn.eurasipjournals.springeropen.com/articles/10.1186/1687-1499-

[3] P. Papadimitratos, L. EPF, La Fortelle A. D., Evenssen K., and Brignolo R., "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation ," IEEE Communications Magazine, vol. 47, no. 11, pp. 84 - 95 , 2009.

[4] Bhed B. Bista, Gongjun Yan, and Stephan Olariu Danda B. Rawat, "Vehicle-to-Vehicle Connectivity and Communication Framework for Vehicular Ad-Hoc Networks," in International Conference on Complex, Intelligent and Software Intensive Systems, Birmingham, UK, 2014, pp. 44-49.

[5] Ram Shringar Raw, Kumar Manish, and Singh Nanhay, "Security Challenges, Issues And Their Solutions For VANET," International Journal of Network Security & Its Applications (IJNSA), vol. 5, no. 5, pp. 95 -105, 2013.

[6] Guangtao Xue, Luo Yuan, Yu Jiadi, and Li Minglu, "A novel vehicular location prediction based on mobility patterns for routing in urban VANET," EURASIP Journal on Wireless Communications and Networking, vol. 222, no. 1, pp. 2012-2222, 2012. [Online]. http://jwcn.eurasipjournals.springeropen.com/articles/10.1186/1687-1499-

[7] Dhami Anil Kumar and Agarwal Neha, "Challenges in Securing VANET: The Intelligent Transportation System," International Journal of ComputerScience and Security (IJCSS), vol. 6, no. 6, pp. 366-375, 2012.

[8] Ramazani, Tahereh Mohammadi , Wathiq Mansoor, Mansoor Vahdat-Nejad Hamed Azam, "A survey on context-aware vehicular network applications," Elsevier:Vehicular Communications, vol. 3, no. 1, pp. 43–57, 2016.

[9] L. Wischhof, A. Ebner, and H. Rohling, "Information dissemination in self-organizing intervehicle networks, Intelligent Transportation Systems," IEEE Transactions, vol. 6, no. 1, pp. 90 - 101, 2005.

[10] N.Jayalakshmi, "Designing of Regional Trusted authority With Location Based Service Discovery Protocol In VANET," International Journal for Reasearch in Applied Science and Engineering Technology (IJRASET), vol. 1, no. 1, pp. 1-8, 2013.

[11] Anil Kumar Supinder Kaur, "Techniques to Isolate Sybil Attack in VANET A Review," in International Conference on Electrical, Electronics, and Optimization Techniques , 2016, pp. 720-726.

[12] Xiaodong Lin, Xiaohui Liang, Xuemin Shen Rongxing Lu, "A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs," in IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS , 2012, pp. 127-139.

[13] Moath M. Al-Doori, Ali H. Al-Bayatti, Hussien Zedan Saif Al-Sultan, "A comprehensive survey on vehicular Ad Hoc network," Journal of Network and Computer Applications, vol. 37, pp. 380-392, March 2014.

[14] Khalil El-Khatib Jesse Lacroix, "Vehicular Ad Hoc Network Security and Privacy: A Second Look," in The Third International Conference on Advances in Vehicular Systems, Technologies and Applications, 2014, pp. 6-15.

[15] Mohamed Watfa, Advances in Vehicular Ad-Hoc Networks:Developments and Challenges, 1st ed., Kristin Klinger, Ed. New York, USA: IGI Global, 2010.

[16] Danda B. Rawat Gongjun Yana, "Vehicle-to-vehicle connectivity analysis for vehicular ad-hoc networks," Science direct: Ad Hoc Networks , pp. 1-11, 2016.

[17] Akhilesh Singh, Rakesh Kumar Rashmi Mishra, "VANET Security: Issues, Challenges and Solutions," in International Conference on Electrical, Electronics, and Optimization Techniques, 2016, pp. 1050-1055.

[18] S.M. Yiu, Lucas C.K. Hui,Victor O.K. Li T.W. Chim, "Secure and privacy enhancing communications schemes for VANETs," in Ad Hoc Networks: Elsevier, 2011, pp. 189–203.

[19] Elias C. Eze Si-Jing Zhang En-Jie Liu Joy C. Eze, "Advances in Vehicular Ad-hoc Networks (VANETs):Challenges and Road-map for Future Development," International Journal of Automation and Computing: Springer, vol. 13, no. 1, pp. 1–18, JANUARY 2016.

[20] Arun Kumar KA, "Worm Hole-Black Hole attack Detection and Avoidance in Manet with Random PTT using FPGA," International Conference on Communication Systems and Networks, pp. 21-23, 2016.

[21] Dr.M.Yuvaraju M.Sindhuja, "CONGESTION CONTROL USING ON-BOARD DATA UNITS IN VANET SCENARIOS," International Journal of MC Square Scientific Research, vol. 7, no. 1, pp. 1-9, November 2015.

[22] Tushar Singh Chouhan, P.Vetrivelan Rajvardhan Somraj Deshmukh, "VANETS Model: Vehicle-to-Vehicle, Infrastructure-to-Infrastructure and Vehicle-to-Infrastructure Communication using NS-3," International Journal of Current Engineering and Technology, vol. 5, no. 2, June 2015.

[23] Saroj Kumar Biswal, "On Board Unit Based Authentication for V2V Communication in VANET," National Institute of Technology, Rourkela, Rourkela, India, Dissertation 2014.

[24] Sharifah H. S. Ariffin , Norsheila Fisal Shereen A. M. Ahmed, "Overview of Wireless Access in Vehicular Environment

(WAVE) Protocols and Standards," india Journal of Sciencce and Technology, vol. 6, no. 7, pp. 4996-5001, July 2013.

[25] C., & Falko, D Summer, Vehicular Networking, 1st ed. United Kingdom: Cambridge University Press, 2015.

[26] Shailendra Mishra, Narottam Chand Vishal Kumar, "Applications of VANETs: Present & Future ," Communications and Network, pp. 12-15, 2013.

[27] Shikha Agrawal,Sanjay Silakari Uzma Khan, "Detection of Malicious Nodes (DMN) in Vehicular Ad-HocNetworks ," Procedia Computer Science, pp. 965-972, 2015.

[28] M. Hussin, N. Manshor R.A. Raja Mahmood, "Performance evaluation of time-based black hole attack detection in mobile ad hoc networks," in International Conference on Computational Science and Technology (ICCST), Kota Kinabalu, 2014, pp. 1-6.

[29] Bharti and D. P. Dwivedi, "Performance Analysis of Black Hole Attack with AODV using Different No. of Nodes in VANET," International Journal of Science and Research, pp. 1956-1959, 2016.

[30] Farid Nait Abdesselam, and Zonghua Zhang Soufiene Djahel, "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges," in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2011, pp. 658 - 672.

[31] Venkatesan Balakrishnan and Vijay Varadharajan, "PACKET DROP ATTACK: : A SERIOUS THREAT TO OPERATIONAL MOBILE AD HOC NETWORK," in International Conference on Networks and Communication Systems , 2005, pp. 89-95.

[32] Stefan Savage, Keith Marzullo Alper T. Mizrak, "Detecting Malicious Packet Losses," in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2009 , pp. 191-206.

[33] Martin Euku and Richard Ssekibuule Kennedy Edemacu, "P ACKET D ROP A TTACK D ETECTION T ECHNIQUES IN W IRELESS A D HOC N ETWORKS : A R EVIEW," International Journal of Network Security & Its Applications (IJNSA), vol. 6, no. 5, pp. 75-86, September 2014.

[34] 2 Dinesh Goyal Kshitij Bhargava, "PACKET DROPPING ATTACKS IN MANET: A SURVEY," Journal of Advanced Computing and Communication Technologies , pp. 14-18, 2014.

[35] Ali Movaghar , Misagh Mohammadizadeh Seyed Mohammad Safi, "A novel approach for avoiding wormhole attacks in VANET," in First Asian Himalayas International Conference on Internet, Kathmandu, Nepal, 2009.

[36] Shahzad F., Qayyum A., Mehmood R Gillani S., "A Survey on Security in Vehicular Ad Hoc Networks," in Springer, Berlin, Communication Technologies for Vehicles, Heidelberg, 2013, pp. 59-74.

[37] Kiho Lim and Manivannan D., "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," Elsevier Inc: Vehicular Communications, vol. 4, no. 1, pp. 30–37, 2016.

[38] Osama Abumansoor and Boukerche Azzedine, "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET," IEEE transactions on vehicular technology, vol. 61, no. 1, pp. 275 - 285, 2012.

[39] T.W. Chim, S. Yiu M., and Hui.K. Lucas C., "SPECS: Secureand privacy enhancing communications schemes for VANETs," Science Direct, vol. 9, no. 2, pp. 189-203, 2011.

[40] Kotramma Mathada, Mamatha P, Latha N.R Sindhu J., "A Survey on Detection of Packet Drop Attack and Data Forgery using Dictionary Based Provenance in WSN," International Journal of Computer Science and Information Technology & Security, vol. 6, no. 2, pp. 122-126, March 2016.

[41] Jinna Hu, Jianfeng Zhang, Canding Sun, Liqiang Zhao, Zhiyuan Ren Chen Chen, "Information Congestion Control on Intersections in VANETs: A Bargaining Game Approach," in Vehicular Technology Conference , IEEE , Nanjing, China, 2016.