RESEARCHERID
THOMSON REUTERS

ISSN: 2277-9655
[Rani * *et al.*, 6(12): December, 2017] Impact Factor: 4.116
IC™ Value: 3.00 CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

VEHICLE ADHOC NETWORK TECHNIQUES-A REVIEW

Pooja Rani*
*Research Scholar, Singhania University, Rajasthan, India

DOI: 10.5281/zenodo.1116688

ABSTRACT

Accidents have increased in the country's accidents in the world and there is no involvement in death. Due to the traffic / hostility of the vehicles around us, new technologies are related to vehicle advertising hacks. Communication in vehicles is very important because technology has been developed. Implementation of enterprise and investigation systems and implementation will improve the safety of road users and improve the comfort and traffic efficiency of the same passenger, drivers and other road users. This research paper examines the current and current security issues associated with VANET, and potential problems in this area expose any recession among them to light the potential potential.

KEYWORDS: VANET, applications, routing, VANET security, vehicles to vehicle communication. component.

I. INTRODUCTION

Over the past few years, countries around the world are implementing ventures, it is more entertaining and exciting, WANANET is also known as the vehicle communication path. VNET is a harsh approach because it has a low maintenance cost [3] due to the rapid increase in the number of vehicles, we need to install VNET [1]. If each vehicle falls under a communication network, then we can reduce the proportion of the accident which is moving towards the day. During communication, they will send messages to their neighbors. On the road, the vehicles become neighbor to each other for a few seconds [5] VANET also helps us in informing us about the situation of interest. VNAT not only communicates V2V communication, but infrastructure communications vehicles are also possible. [4] If there is a problem on a particular road, then transfer of messages to other vehicles starts providing information on the condition of the roads. VNATET not only works for the basic MMA transmission, but the driver works for the rest [2] Manufacturing vehicle provides services for vehicle communication with the objective of security. [4] Use of custom version of Ventet IEEE 802.11, i.e. IEEE 802.11b, can be setup on the basis of macrotron and physical layer protocol [4].

II. SYSTEM ARCHITECTURE

Such communication networks between V2V and V2i [6] Road accidents increase with speed of speed between different vehicles so that if we want to avoid it, then we need to communicate with the vehicles. Venture architecture is divided into three separate domains [6] Maintain the integrity of the specifications.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

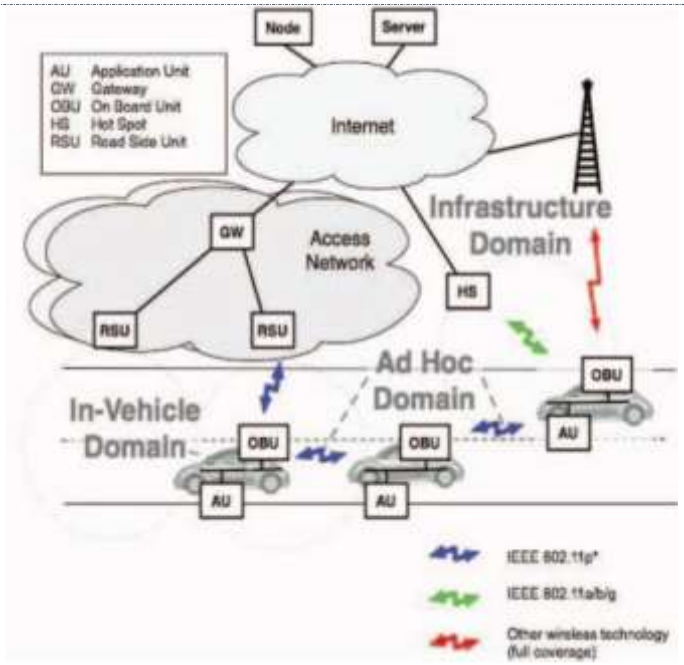

Figure 1: Architecture of VANET[11].

a) Ad hoc Domain: Vehicles establish a communication link with RSU. Different OBU helps to setup a link between RSU and Vehicles.
b) Infrastructure Domain: RSU helps to setup a link for OBU to communication with remote host using internet for the purpose of non safety applications.
c) In Vehicle Domain: A OBU which is a part of vehicle which helps to establish a communication link beween AU then vehicle can start applications.

III. VANET APPLICATION

V2V and V2I communication helps to create applications for the better understanding of driver and traveller[7]. With the help of vehicular ad hoc network data message and safety message can transfer from vehicle to another entity.

A. Safety Oriented: It includes safety related applications such as collision on road, road condition, information about road traffic and so on. Safety applications are divided into two parts : one is informational and another is warning message transmission. Warning message transmission provides information about road condition, traffic, post crash and any obstacle on the road[7].

Informational message provide full details about speed limits, work zone , lane navigation and so on[7]. For example, sometime if you apply brakes on your vehicle then a message will be generated and will be sent to all the vehicles which are behind your vehicle. The message transmission should be very fast in order to reduce transmission delay and to reduce crashes

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

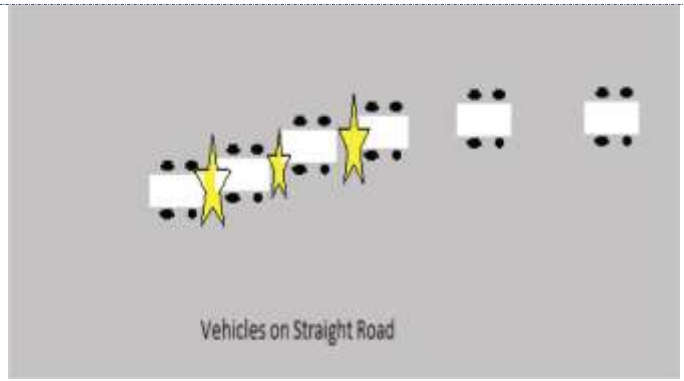

Figure 2: Problem Figure: when one vehicle apply brakes then crash can occur.

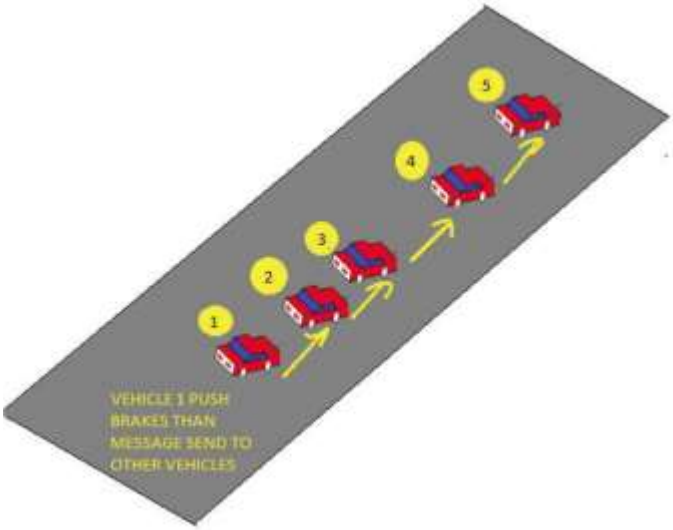

Figure 3: Solution Figure: This figure helps to avoid crashes between vehicles.

Vehicle Advertising Hack Network (Ventet) used vehicles to create a mobile network as a node node [13]. Vehicles work as a mobile node with the same network. The main objective of VNET is to improve and improve communication between our roads and road users, the comfort of passengers, and the vehicles and roadside equipment. Enterprise communication has been established on the mid-node (vehicle) [11] As shown in Identity 1, the communication of each vehicle is a wireless network card which facilitates the flow of communication between vehicles and roadways. Identity 2 displays various domains in the VANET mobile domain (car and mobile device) such as PDAs, smartphones, and laptops etc. Nodes and servers, such as general domains (Internet infrastructure and private infrastructure), while infrastructure networks (Road infrastructure or units and central infrastructure) such as RR, which talk to the car along the road, and the management center that interacts with the Internet Mobile Domain Infrastructure Domain and Infrastructure Domain Talk, Common Domain and Data Flow Dialogs Between Different Domains To Provide Road Effective And Efficient Use By Road Users Since the communication VANET is provided in 2 different ways, there are certain fixed nodes present in the form of road side units or devices that enable VANET simplicity to serve as Internet gateway and enable access to geographical data counting. Is [14]. In each VANET, each node only does not participate in data transmission. Communication limits allow cars to each other in the area of 100 to 300 meters, and create a network widely, since the car emits from the signal range and exits from the network, join the vehicles in other vehicles so that the vehicle To be connected to each other so that mobile internet is ready. According to the Figure 3, the vanate component is the ship unit and road side units. How we can see communication

The ship unit and vehicle communication vehicle are also taken from road to road, it makes better part of the information between vehicles, unlike vehicles, acts as VANET nodes, vehicles which will go on predefined road traffic signals and Signals are required and depending on their speed depending on their speed, [9] Supported by ventilation inside the vehicle [16] - [20] Wireless devices such as wikis Individuals digital assistants (PDAs),

remote cable entry devices, mobile phones, laptops and more. Increasing causes of mobile wireless devices, vehicle-to-vehicle (V2V), vehicle to road side (VRC), and vehicle-related infrastructure (V2I) communication are increasing rapidly [20]. There are two types of communication available by VNET; The first wireless wireless network is communication without communication without communication. Second, communication between the vehicle and road side unit [14] IEEE details for setting up WEEEET is standard 802.11 or 802.16 (VIMA). Due to the relatively fast speed nodes (vehicle) in Veneton and in particular place the cartridge of the vehicle, at this time a very large network is known due to the communication standard dedicated low-distance communication due to each node freedom (DSCCC) problem solving Was ready to do this Under the Road Side Units (RSU), communication standards are used explicitly, which are installed along the road as infrastructure and nodes (vehicle) and gate in reverse. DSRC interacted with 5.9 GHz band and used 802.11 access methods. The United States allocated 75 MW spectrum in 5.9 GHz, while Europe DSP allocated spectrum of 30 MW in 5.9 GHz band for RC, it should be used by Intelligent Transportation System (IT). As shown in Table 1, there are 7 MHz wide channels. There are four service channels used for protective and non-secure applications, and a control channel (CCC) that is used to control the channel. There are two secure channels (172 and 178) in future security applications. The channel is special for 172 accessibility and high non-functional while the channel 178 high power is specific to public safety applications..

IV. LAYERED ARCHITECTURE FOR VANET

The OSI model group is one of the same logic functions in the seven logical layers [23] - [25] In the enterprise, the session and presentation layers are removed, and in the table, the specific layer in the form described below has sub-layers in the WANnet architecture Can be broken or broken in [25] VANET construction can be converted into different areas, and protocols and interfaces will also be different. As shown in Table 3, protocols for dedicated short border communication (DSRC) in the United States [24], various protocols can be used in various layers, some of which are still under development [26] The IEEE 802.11 standard is approved, which is the IEEE 802.11p standard, which adds wireless access to the VNET Vehicle Environment (YAV). It is basically focused on the physical layer and mac

Protocol stick sub-layer The IEEE 1609 standard is the quality of a higher protocol than IEEE 802.11p. The IEEE 1609 works on the middle layers of the standard protocol stack and it supports satisfactory security applications in VENAT. While the disliked application is supported by various protocols. Transport services for unusual applications in the network are provided by VENET IPv6, TCP, and UD or [27] - [2].

V. VANET APPLICATIONS

There are two categories of applications that is associated with the VANET; safety and user based applications [30].

Safety Related Applications

Safety related applications are used for the development of road safety and applications such as roads: transmission protection, cooperative driving, and traffic improvements. Avoid Conflict: Some studies show that 60 percent of road accidents can happen before traffic accidents, [31] - [33] - [33] in an application to avoid transmission, if there is an accident Any other signal or node is broadcasted on other nodes, so that other vehicles can be connected. Cooperative driving: An ineffective / secure journey can be obtained through transmission warning signal such as the speed of the lane, speed limit, a turn or a curve etc. Drivers are practically responsible and are involved in this application because there are many accidents due to lack of money. For collaboration between drivers [34] [35] Cuffe Reform: Vehicles work as VANET's data collections. When there is a vehicle or road obstacle, signs sent to the vehicles sent to Jim (acne) etc., so that they can improve the traffic and save time. For example, if there is a brooch on the lane, the information about it can be moved to the front street or transferred by car, so it can move rapidly towards the crowd. Has been given a lot of time to choose alternate routes for incoming vehicles [36]

User based application

First of all comes before the road and other services can be added. Information about information (information and entertainment) is also provided by VNET, such as: Monday to Monday Applications: The ability to use these apps in the network to share music, videos, etc. Internet connectivity: VNET provides Internet users with Internet connectivity Other services: Geographic location, payment services, etc. are provided by non-protective applications by VAENET.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

VI. FEATURES OF VANET

As previously mentioned, VENET is a subtitle subnet, but it has its own respectable characters: High Mobility: Because the car moves fast, it is difficult to guess the position of the node and it is also the information of privacy that protects the problem. Speed-transposed network topology: Due to the speed of the node (vehicle), it is difficult to ensure the position of the node and its condition often changes frequently. Therefore, network topology often changed Wanet. Exposed network size for reasons: The size of the VNET network is not limited to a specific region or area, it can be applied to the city or more. Vent is geographically limited. Exchange information immediately: Information between cars and road side units can be changed (RSU), Wanat's ADP died in nature. It frequently repeats and updates the information Wireless communication: VANET-run technology is wireless technology, so the nodes are connected and the information exchange is done through the wireless communication channel. The importance of time: the limitations of time are sent to each information packet The ones that have been sent or received, have the right to provide information at the right time, to enable abnormal delay and to avoid the same node for decision Land. Accordingly, enough energy can be made: Negroos has a big power source, because cars run on their batteries. There is no limited power supply working for the related components, due to this, there is a demand for the students used by VNET, such as RSA, ECC etc. Better physical protection: Because Vannat is nodded to vehicles, more physically safe. It makes it harder to physically settle the venetette node and reduce physical attack on the infrastructure.

VII. VANET MODEL

Although there are various units involved in enterprise deployment, majority nodes (other units) are however other units or institutions that maintain core operating operation in the network. Due to the large and complex system model, it is divided into four sub-models i.e.: driver and vehicle model, traffic flow model, communication model, and application model [37] - [39]. Driver and car model: This shows the behavior of the same vehicle. In this model, two factors are considered as follows: Different driving styles and car features. For example, a driver driver or passenger and a sports car [3 9]. Traffic Flow Model: This model demonstrates the interaction between vehicles, drivers and infrastructure to create a good road network [3 9] [40]. Communication model: This road shows data or data between users or data [41]. Application Model: This indicates interest in behavior and quality of cooperative VANET applications. [41] Figure 4 defines VANET units and institutions that make VANET models, and are defined below in descriptions of the description.

General vent unit and institute

Infrastructure and advertising environment: Wanet usually has two different environments.

Basic environment

In this environment, units or institutions can be permanently linked. Inside this environment, there are mainly institutions that access variable traffic and external services. This is known within this enviroment of the VANET model, because they typically identify each vehicle during the manufacturers. Legal authority is also in the Vent Model of this environment, various rules which can be promoted to countries, vehicle registration and crime reporting can be done. There is also a trusted third party (TTP) in this environment [42] They offer various services from time to time and reliable management. Manufacturer and Authority related (TTP) because services are required, for example, issuing electronic certificates [42]. Service providers are also in the environment, because they provide services which can reach VANET, such services are 'Location Based Services (LB)' or Digital Video Broadcasting (DDI). [42].

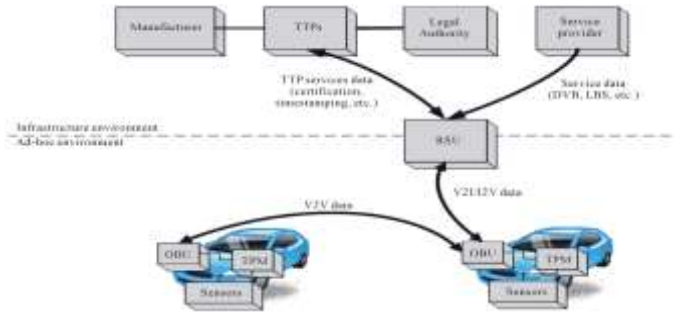

Figure 4. VANET units and entities.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Ad-Hoc Environment

This environment creates ad-hoc communications from vehicles. The vehicles are equipped with 3 different devices namely; On-Board Unit (OBU) that enables the Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication [23]. The Ad-Hoc environment also have a set of sensors to their status and its environment e.g. (Fuel Consumption, Slippery Road, and Safety Distance). The data gotten can be shared among other node to improve and increase road safety. A Trusted Platform (TPF) is always installed on the vehicles, such devices are for security purposed and also for computation and reliable storage [43].

It creates advertising communications with environmental vehicles. Equipped with vehicles, 3 different devices; Onboard of Board (V2V) vehicle enables vehicle-infrastructure (V2I) communication [23]. Their environment in the advertising environment and their environment involves a set of sensors. (Fuel consumption, slip-road and safety distance). The data can be obtained in other nodes to improve road safety and improvements. A trustworthy platform (TPF) is always installed on vehicles, such devices are used to clarify security and ensure serious and reliable storage. [43]

VIII. VENTETTE COMMUNICATION PATTERN

Using VANET Enables several applications for safe use of unsafe applications. This app discusses messages over VANETs and is used for their various purposes. There are four separate communication patterns in their identity in Wanette [44] [45] although there are other communication methods (multimedia access, location-based services, etc.).

Car Vehicle (V2V) Warning Transmission

This communication pattern is useful in an exceptional or multicultural situation where the message has been sent to a particular group or group of vehicles. For example, and an emergency vehicle is approaching, a message can be sent to send incoming vehicles, it will make an easy way for emergency vehicles, or when a crash is detected, a message can be sent is. That they should be sent for vehicles and to increase safety of the road, it is shown below in size 5.

Vehicle Vehicle (V2V) Group Communications

In this communication model, the same feature sharing feature can participate in the same communication. Such characteristics can be nature or dynamic nature, in which only one device or enterprise (static nature) or vehicle that is a special time lag [47] [48]. This is shown in the ID below 6.

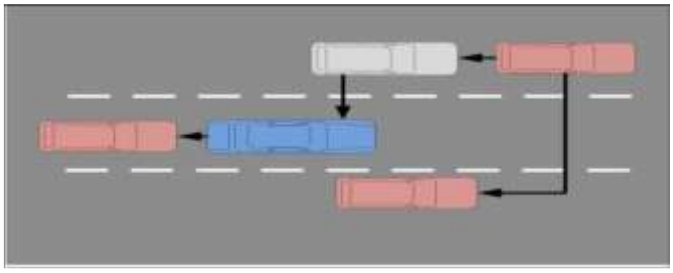

Figure 5. V2V warning broadcast

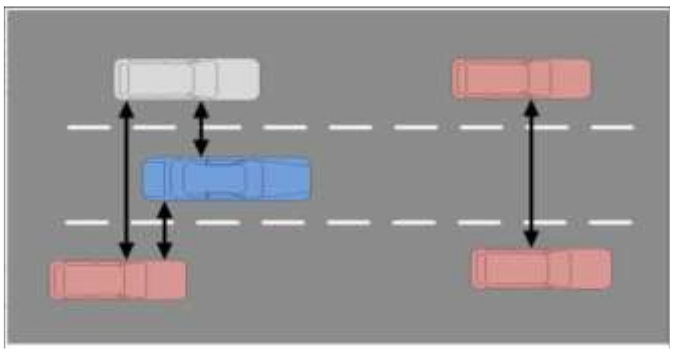

Figure 6. V2V group communication

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Car Vehicle (V2V) Baking

Under this method, the messages are sent from time to time which are nearby. These messages change by using sender or transmission car, superficial, current speed, conversation etc. As shown in Figure 7, V2Vbanking communication messages are sent to a 1-stop communication vehicle, which is not forwarded to the post after receiving. It is helpful because the message enables you to find and access the best neighbor for finding vehicles and via a message path [49] - [51].

Infrastructure to indicate two vehicles / vehicle infrastructure

Messages either convey basic messages from roadside units (archive), or vehicle to archive, when a vehicle or device encounter a potential risk. For example, an alert message can be sent by aresio or to reach a moving entrance that may be possible ticker. This communication model is very useful for increasing road safety [52] [53]. Figure 8 shows how to tell the warning message in different nodes to avoid the collision.

IX. ROUTING IN VENT

In the last few years, the way in Vienna has been widely studied [42] [52] - [54] However, there is a high-functional topology for frequent connectivity due to the features of Vitaliane, commonly used routing The protocol that has been applied for the menu has been tested for use in the WNAT environment and is used [55] Nodes involved are based on the number of sending and receiving routes, can be rated in three types of ventures. Is; geocost / broadcaster, multicast, and unicast approach.

Jacob / Broadcast

This protocol is very important in VANETs. [56] Various geocost / broadcast protocols have been reviewed on VANET, such as:

- Superior Aerial Packet Routing Algorithm (This protocol is capable of evaluating holes in the capology and regulating geographical forwarding).
-

SHDV (This helps to find the best way to send a protocol to a protocol)

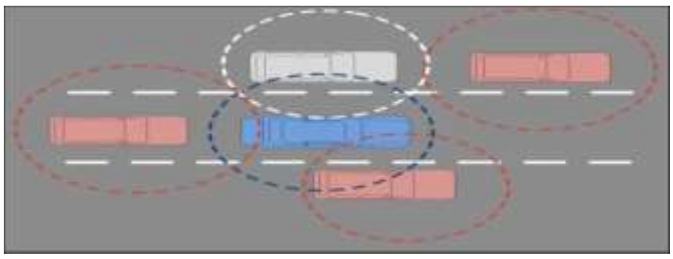

Figure 7. V2V beaconing.

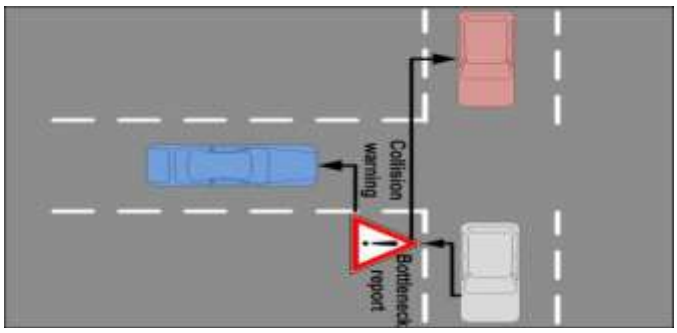

Figure 8. I2V/V2I warning.

- Interface Awake Routing Scheme (this enables the node with a multichannel radio interface and switches the channel based on the SIR evaluation).
- FROV (this selects the retransmission and spans further node to rebroadcast a message).
- Multi-hop Broadcast Protocol (this protocol segments the road and choose the vehicle that is far in a nonempty segment).

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Other protocols such as; V-TERADE, UMB, AMB, MHVB, and MDDV have been proposed by other researchers [56].

Multicast protocol

The country is important among some vehicles such as the movement of vehicles in the road block, high traffic density or culture accidents, road posts, bad road conditions etc. [56], the Multilext Protocol was divided into two categories, 1) Topology-based approach like ODMRP (this creates a source-based multestat network and is based on the group address), MAODV (this creates a group based multi-valley tree), and GHM Ups based Mltest makes trap). 2) location-based approach, such as P BMW (which is based on the location of all 1 hop neighbors and individual sites), SP BMW (presenting its vertical group membership are present), LMB (This Multetast area used as destination information Does for multicast canned), and RBM and IVG (which describe a multi-population capability for security alert messages).

Unicast Protocol

Universal communication protocol for the ventil is in three ways (as shown in Table 4): Greedy in this protocol, the nodes forward the vehicles or nodes, which come from their destination far away, such as (GYTAR).
Opportunistic nodes use the "carrying" technique, where this figure is used to transport the resources related to the destination, as is done for the supply of land assistants, ground stand worship etc.
Transferring based: Nodes set such routes that will take to the potential destination and provide data from the nodes, which is one of the intricate routes, as soon as the transformer-based data forwarding (TBD) [55] [56]

X. VAN SAFETY ISSUES

Security is always a challenge for any structure used in communication. Due to the involvement of human life, security is very much in VNET, during the design of VANET architecture, safety challenges or issues are necessary [53] - [55] [56], the author divided the invaders into three types or dimensions , Internal vs. Internal, Unfortunately fair targets, and Passive versus Disabled Ventet related issues are based on security issues, such as Danger, three major groups, available The following 3 sections will explain these issues in detail, reliability and privacy.

Risk availability

There are risks for vehicle access for vehicle and road access communication:

1) Denial of service service: This type of attack can be done by internal or external networks in the network, a reason for this kind of attack is not available to authentic users of high-volume synthetic messages, floods and blocked reasons. Due to the vent components such as nude board units and roadside units, there is no excessive requirement.
2) Targeting: This attack is done internally, it shows fraud protection messages in the VANET to harm users or harm users. An accident can occur when an attacker adds traffic to a particular route.
3) Malware: Operation initiated in the virus or VENET can cause operation interference. This attack is often done internally by foreigners and the firmware is updated when it can be downloaded on the network
4) Spamming: Transmissions in spam messages in the ventet can be due to non-functionality. It is more difficult to control because there is no central administration.
5) Black hole attack: Because of this kind of attack, the network is refused to participate in the network or when the node exits from the network, when all this is the communication path and before that it is already connected Will be broken message for Posted

Threats to Authenticity

VANET is very important in delivering authenticity. It includes the protection of legitimate legal validity nodes with fake "counterfeit internal or external" threats, such as:

6) Assessment: This attack is different from others and it is easy to release. The attacker joins the network to get the unit working on the network and is near a valid vehicle in the attacker network, false orphanage can be made for various types of attacks and Make black holes
7) Global Positioning System (GPS) Spfing: Global positioning system maintains a place table, which identifies all vehicles on geographic location and network. GPS GPS using GPS satellite simulator can be used to create a false position on the GPS system in the network, which makes the vehicle feel that it is the right place at the same place. This is because GPS satellite simulators can produce such signals that are more powerful than generating authentic or real satellite.

8) Attack on the Rapley: In this attack, the invaders already used the nodes in the network, then poisoned the noodle table by running bacon. Although working in this framework work is protected from the attack, but in order to maintain security, a clear source of time should be kept and managed to maintain cash messages of recent messages. Is
9) Tunneling: In an event, a vehicle goes through the tunnel on the other side to obtain positioning position when the vehicle uses a long loss of a positioning system. The attacker is injected fast. To understand this node, the wrong position information or data in the unit on the node's plane

Received is valid

10) Counterfeit positioning: In venture, vehicles are responsible for the details of their position or location information. The unsecured communication link is almost impossible to change or the channel can create a blind spot where the attacker can quickly edit or position their positions or other vehicles, as well as known as additional identities. Is. Important and authentic protective messages, or to prevent vehicles.

11) Fixing message: To respond to request requests or other nodes by applicants, the message has been modified or edited to contact the vehicle from the car or the car to the roadside. .

12) Under the message / construction / change: the invading physically disables the communication of the communication between vehicles or changes the application so that the vehicle does not send or receive the bacon.

13) Sybil Attacks: In VANET, periodic messages are 1-hop broadcast, this is for securing the physical layer. When the network is not secured an attacker can partition the network and make delivery safety message impossible.

Threats to Confidentiality

Messages that are exchanged between nodes (vehicles) in VANET are open to confidentiality threats or attack with techniques such as illegitimate collection of messages through eavesdropping and passive attacks which are stated in the literature by the researchers.

XI. RESULT

VANET is an area of research in which future future and vehicles promise to be a future promise. However, there are its challenges in its safety prospects: Venture aims to reduce accidents on our roads and increase the flow of information between car and road users. Vent's unique nature creates problems like illegal tracking and blocking of the network. In this letter, we introduced venture, its construction, components, communication systems and problems in our security. During this research, we used routing protocols in VNEET, in which users are able to send and receive messages properly, such as: Geocost / Broadcast, Multestaste, and Unicast Protocol. In addition Vienna communication patterns, institutions and features include high mobility, rapid transformation, network capology, synchronized network size, information frequent exchange, wireless communication, time-critical, sufficient energy and better physical security. . Features of VANET exposure to utility and performance in VANET. With more research on VANET's security issues, I believe that the vanity will cause a change in technical change and road users. Interchangeable information can be changed to our future road loss and accidents. Future research will be conducted compared to the performance of various data mechanisms and their performance measurements

XII. REFERENCES

[1] Kadum, A. (2013) A Survey on Vehicular Ad Hoc and Sensor Networks (VASNET).
[2] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security
Mechanism. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, **3**, 79-94. http://dx.doi.org/10.5121/ijasuc.2012.3306
[3] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of*
Communications, Network and System Sciences, **8**, 19-28. http://dx.doi.org/10.4236/ijcns.2015.83003
[4] Sivasakthi, M. and Suresh, S. (2013) Research on Vehicular Ad Hoc Networks (VANETs): An Overview. *Journal of*

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Applied Sciences and Engineering Research, **2**, 23-27.

[5] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications*, *Society for Science and Education, United Kingdom*, **2**, 1-6.

[6] (2011) Vehicular Ad Hoc and Sensor Networks—Principles and Challenges. *International Journal of Ad Hoc, Sensor & Ubiquitous Computing* (*IJASUC*), **2**..
Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. *IEEE Vehicular Technology Magazine*, **2**, 12-22.

[7] Sari, A. and Necat, B. (2012) Impact of RTS Mechanism on TORA and AODV Protocol's Performance in Mobile Ad Hoc Networks. *International Journal of Science and Advanced Technology*, **2**, 188-191.

[8] Li, F. and Wang, Y. (2007) Routing in Vehicular Ad Hoc Networks: A Survey. *IEEE of Vehicular Technology Magazine*, **2**, 12-22. http://dx.doi.org/10.1109/MVT.2007.912927

[9] Saha, A.K. and Johnson, D.B. (2004) Modelling Mobility for Vehicular Ad Hoc Networks. *ACM International Workshop on Vehicular Ad Hoc Networks*, Philedelphia, 91-92.

[10] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372. http://dx.doi.org/10.4236/ijcns.2014.79038

[11] Manvi, S.S., Kakkasageri, M.S. and Mahapurush, C.V. (2009) Performance Analysis of AODV, DSR, and Swarm Intelligence Routing Protocols in Vehicular Ad Hoc Network Environment. *International Conference on Future Computer and Communication*, Kuala Lumpar, 3-5 April 2009, 21-25.

[12] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. *Proceedings of the* 6*th International Conference on Security of Information and Networks* (*SIN* '13). Aksaray, 26-28 November 2013, 454-456. http://dx.doi.org/10.1145/2523514.2523586

[13] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 5*th International Conference on Computational Intelligence, Communication Systems and Networks* (*CICSyN*), Madrid, 5-7 June 2013, 334-337. http://dx.doi.org/10.1109/cicsyn.2013.79

[14] Bernsen, J. and Manivannan, D. (2008) Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service. *The* 4*th International Conference on Wireless and Mobile Communications*, Athens, 27 July-1 August 2008, 1-6. http://dx.doi.org/10.1109/icwmc.2008.15

[15] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N. and Nemoto, Y. (2007) A Stable Routing Protocol to Support ITS Services in VANET Networks. *IEEE Transactions on Vehicular Technology*, **56**, 3337-3347. http://dx.doi.org/10.1109/TVT.2007.906873

[16] Sari, A. (2014) Economic Impact of Higher Education Institutions in a Small Island: A Case of TRNC. *Global Journal of Sociology*, **4**, 41-45.

[17] Hartenstein, H. and Laberteaux, K.P. (2008) A Tutorial Survey on Vehicular Ad Hoc Networks. *IEEE Communication Magazine*, **46**, 164-171.

[18] Sari, A. and Onursal, O. (2013) Role of Information Security in E-Business Operations. *International Journal of Information Technology and Business Management*, **3**, 90-93.

[19] Eichler, S., Ostermaier, B., Schroth, C. and Kosch, T. (2005) Simulation of Car-to-Car Messaging: Analyzing the Impact on Road Traffic. *IEEE ASCOTS*, 507-510.

[20] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. http://dx.doi.org/10.4236/ijcns.2015.83004

[21] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. http://dx.doi.org/10.4236/jis.2015.62015

[22] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. http://dx.doi.org/10.4236/ijcns.2015.87026

[23] Gerlach, M. (2006) Full Paper: Assessing and Improving Privacy in VANETs. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=84FC4EF0852B23FBF15CF35E16E0450D?doi=10.1.1.84.8167&rep=rep1&type=pdf

[24] Dahiya, A. and Chauhan, R. (2010) A Comparative Study of MANET and VANET Environment. *Journal of Computing*,**2**.

[25] Sesay, S., Yang, Z. and He, J.H. (2004) A Survey on Mobile Ad Hoc Network. *Information Technology Journal*, **3**, 168-175. http://dx.doi.org/10.3923/itj.2004.168.175

[26] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial
[27] Data Interconnect. 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), Konya, 9-11 May 2013, 579-582. http://dx.doi.org/10.1109/TAEECE.2013.6557339.

CITE AN ARTICLE

Rani, P. (n.d.). VEHICLE ADHOC NETWORK TECHNIQUES-A REVIEW. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(12), 274-284