

# A Systematic Survey on VANET: Routing Protocols, Harmful Attacks, and Security

Ajay Kumar<sup>1\*</sup>, Raj Shree<sup>2</sup>

<sup>1</sup>Department of Information Technology Babasaheb Bhimrao Ambedkar University, Lucknow, India

<sup>2</sup>Department of Information Technology Babasaheb Bhimrao Ambedkar University, Lucknow, India

\*Corresponding Author: dynamicajay1988@gmail.com, Tel.: +919971126451

Available online at: [www.ijcseonline.org](http://www.ijcseonline.org)

Accepted: 10/Jul/2018, Published: 31/Jul/2018

**Abstract:** VANETs privacy and security have attracted a lot of attention over the last couple of years. VANETs are being used to boost road safety and empower a wide variety of services like internet, Emergency Message etc. The Vehicular Ad-hoc Network is a collection of smart devices with their vehicle interface. It can play a significant role in the routing process and provide better Security. An increased number of vehicles can raise a number of accidents. That can be part of life loss. So it is the need for smart vehicles that can establish interpersonal communication and warn each other for safety and security. On the other hand, many forms of attacks against VANETs have emerged recently that attempt to compromise the security of VANET networks. Such security attacks on VANETs might cause harmful results. Therefore, making VANETs security has become a key objective for VANET designers. To modify and deploy secure VANET infrastructures remains a significant challenge. The authors portray the different routing protocol by using Octopus diagram, number of attacks and its solution in VANET. With the help of safety and road traffic info among vehicles and related network attacks which improve security under possible attacks in VANETs.

**Keywords:** VANET, Attacks, Security, Routing Protocol, Authentication, RSU, and DSRC.

## I. INTRODUCTION:

These days transportation takes an important part in our regular day to day life. From the latest couple of year's network-based transportation called as VANET. It's abbreviated as Vehicular Ad-hoc Network. A vehicular specially appointed system (VANET) uses a vehicle node as convenient center points as in MANET to make a flexible network [01]. A VANET changes each taking an intrigue auto into a remote switch or hub, allowing vehicle around 100 to 300 meters of each other to interface and, in this manner, make a network with a wide range. As a vehicle drop out of the defined range will drop out of the networks, the same as when any vehicle come within the range work as part of the network. Communicating vehicles to each other shows that a compact network is made. It is assessed that the vital structures that will consolidate this advancement are police and fire vehicles to talk with each other for security purposes. Vehicle associations like General Motors, Toyota, Nissan, DaimlerChrysler, BMW, and Ford propel this term [01]. In VANET each center point works as vehicle mode, which can move transparently inside the network range and stay

related to the roadside unit. It constitutes of short-range radio that is presented inside vehicles and roadside units (RSUs) [02, 03] and central forces which are reliable of character selection and organization [04]. The security in VANET is a more fundamental issue in light of the way that the information is caused in an open access environment. VANET's are introduced to various risks and dangers for your life. It is fundamental that each one of the data which is transmitted should not be changed by the attackers. The assailant may be the approved customer of the network that has unobtrusive component data of the network that can be used for cognizance the blueprint and design of the network protocol [05]. The possible ambushes that can occur in the VANET are thoroughly sorted into three essential social occasions firstly those that represent a danger to Accessibility [03]. Moreover, those that speak of a danger to legitimacy and those that stance risk to the driver. In figure1 the flow diagram describing how to communicate the emergency message within the Ad-hoc network [06].

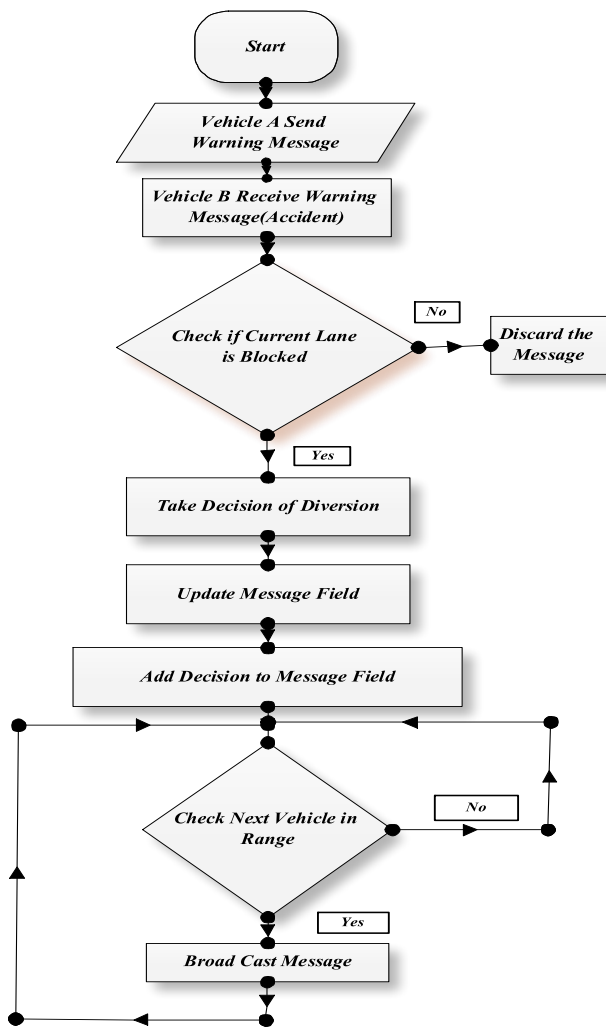


Figure1. The Flow diagram of V2V communication which shares the emergency message

## II. RELATED WORK AND PROJECT:

Dedicated Short Range Communication (DSRC) [01] it is developed by the USA and is a short to medium range communications service that is used for V2I and V2V communication. The United States Federal Communications Commission (FCC) had allocated 75 MHz of spectrum, i.e. from 8.5 GHz to 9.25 GHz to be used by DSRC [09, 10]. DSRC spectrum has 7 channels with each channel 10 MHz wide. Out of 7 channels, six channels are used for service purpose and remaining one for control purpose. The following Table2 shows the bandwidth allocation of DSRC Spectrum [11].

VANET Projects across the World with the advent of wireless technology and underlying VANET architecture, there are several Intelligent Transportation System [07] projects, which have been undertaken in various countries mostly in the USA, the European Union and Japan. Some

of them are sponsored by automobile industries and others by the government. Early developments in VANET focused on an underlying VANET architecture such as communication standards, wireless protocol infrastructure, standardization of 802.11p, WAVE [04, 05] and DSRC. Those are considered as phase 1 development in VANET. But now various projects in VANET are mostly concerned with real-life implementation by field trials, called phase 2 where the verification of protocols developed during phase 1 is also conducted. A brief summary of various research projects from 2004 is given below.

### A. In the European Union:

- Car-to-Car Communications Consortium (C2C-CC) [01]: The Car2Car Consortium, a non-profit organization, sponsored by various European automobile manufacturers that are open to research organizations, equipment providers, and other partners. The aim was to improve driving assistance, active safety application deployment.
- SEVECOM: Secure Vehicle Communications is an EU-funded project that focuses on providing a full definition and implementation of security requirements for vehicular communications [08].
- FleetNet: An early European Union-sponsored trial, aimed at identifying problems inherent in V2V communications.
- Network on Wheels [01]: An initiative by major European manufacturers and supported by the Federal Ministry of Education and Research, Germany. The aim was to solve the key technical issue of communication protocols and security of V2V communications.
- PReVENT: PReVENT, an EU project regarding safety applications using sensors, maps, and communication system.

### B. In the USA:

- Wireless Access in Vehicular Environments (WAVE): It is a set of standards released in 2004 and again revised in 2006, which enabled the practical trials for V2V and V2I communications and became the foundation for other projects.
- Vehicle Safety Communications (VSC, VSC-2): Goal was to improve critical safety situations with the help of positioning systems and DSRC, Evaluate the minimum safety requirement and various performance parameters.
- Vehicle Infrastructure Integration (VII): Aim was to provide coordination between different automobile manufacturers.
- Clarion: Clarion A consortium of hi-tech automobile companies from both Japan and USA.

**C. In the Japan:**

- o ASV 2 [12]: stands for Advanced Safety Vehicle. It is extended to ASV-3 in 2001 and ASV-4 in 2005 by providing an automatic collision avoidance system and a navigation system. It is supported by Toyota, Honda, Mitsubishi, and Suzuki.
- o DEMO [11] started in 2000 for providing cooperative driver support system. It uses a band of 5.8 GHz and CSMA protocols for communication.

- o JARI [13] stands for Japan Automobile Research Institute, which conducts many trials for the projects and it evaluated the USA projects and European Union Projects. It mainly focuses on security and safety.

Table2.DSRC bandwidth allocation

	Reserved				Control channel			High Power Public Safety
Frequency (MHz)	5850-5855	5855-5865	5865-5875	5875-5885	5885-5895	5895-5905	5905-5915	5915-5925
Channel Number	Grand Band	172	174	176	178	180	182	184
			175			181		
Channel Usage		SCH	SCH	SCH	CCH	SCH	SCH	SCH

IEEE Fact Sheet was written on Sept 25, 2009. The status of the IEEE 1609.1, 1609.2, 1609.3 and 1609.4 standards was Trial Use Published and draft Standards under development. Status of 1609.0 and 1609.11 was Under Development. Status of P802.11p was Active Unapproved Draft.

Wireless Access in Vehicular Environments (WAVE), the IEEE 1609 family of standards consists of five standards which are as follow:

- o IEEE P1609.1 Standards —WAVE Resource Manager defines the basic application platform and includes application data read/write protocol between RSU and OBU,
- o IEEE P1609.2 Standards —WAVE Security Services defines the 5.9-GHz DSRC Security, anonymity, authenticity, and confidentiality,
- o IEEE P1609.3 Standards —WAVE Networking Services defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange, and
- o IEEE P1609.4 Standards —WAVE Multichannel Operations provides DSRC frequency band coordination and management, where it manages lower-layer usage of the seven DSRC channels, and integrates tightly with IEEE 802.11p

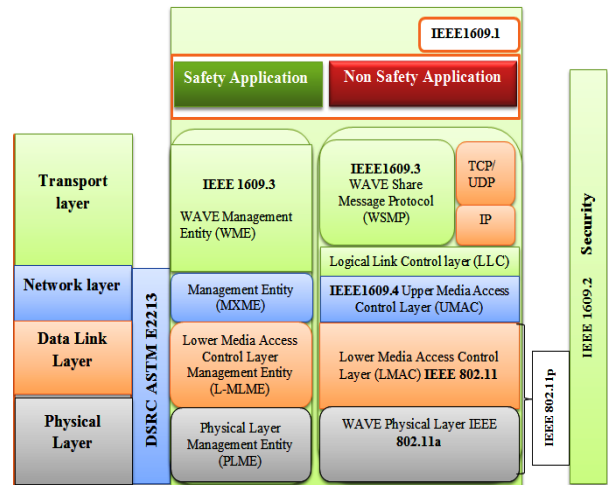


Figure2. WAVE (1609.0) protocol Stack Diagram.

- o IEEE P1609.11 Standards Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS) will define the services and secure message formats necessary to support secure electronic payments.

Wireless Access in Vehicular Environment (WAVE) (IEEE 802.11p) November 2004, American Society for Testing and Materials (ASTM) sets ASTM-DSRC which was totally based on the 802.11 MAC layer and IEEE

802.11a physical layer [10]. The main problem with IEEE 802.11a with Data Rate of 54 Mbps is it suffers from multiple overheads. Vehicular scenarios demand high-speed data transfer and fast communication because of its high topological change and high mobility. For this, the DSRC is renamed as IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) by the ASTM 2313 working group [10]. This works on MAC layer [14] and physical layers. WAVE consists of Road Side Unit (RSU) and On-Board Unit (OBU) [15]. WAVE uses OFDM technique to split the signals. The following Figure2 shows the WAVE, IEEE 802.11p, IEEE 1609 and the OSI model [50].

### III. ROUTING PROTOCOLS USED IN VANET:

Routing protocols play an essential role in vehicular ad hoc network communication. Designing a network protocol must be appropriate for the network design to ensure high performance. Messages among the vehicles should be spread efficiently without delay [16]. Emergency messages ought to be transmitted in time with the goal that it is useful to the travelers and drivers to take necessary actions as a move to the bypass road. Various routing protocols have been developed for vehicular ad-hoc network communication and all are listed in Figure3 [51, 52, 18].

#### A. Topology-based routing protocol:

Route selection is the fast undertaking of sending messages amongst source and destination [12]. In topology based routing, it considers how the Route is chosen for building up the connection amongst source and goal to exchange the information. This topology based routing conventions can be ordered into proactive, receptive and hybrid.

##### 1. Proactive routing:

In the proactive routing scheme, every node in the network topology keeps up at least one directing tables which are refreshed at a consistent periodical interim. To get a fresh table of information each node broadcasts a message to the nearby node and gets updated if there is any change in the network. The various lists of available proactive routing protocols are mentioned in the Figure3 This Routing information has the following drawbacks which are as follows [17].

- It takes the extra overhead cost to maintain the up to date information.
- Slow reaction on restructuring and failures.
- The throughput of the network may be affected.

##### 2. Reactive routing:

As according to the reactive routing each node discovers a route based on demand, it is not active all time [16, 17]. This routing methodology floods a control message to all

nodes by global broadcast during discovering a route. As soon as the route is discovered then the available bandwidth of the ad-hoc network is used to transfer the messages. The fundamental advantage of this routing protocol is it needs less memory storage during routing information [02]. The various available reactive routing protocols are listed in Figure3 However, it has the following disadvantages.

- During route discovery, it produces huge control packets
- Latency time is high in route finding.
- Excessive flooding can lead to network, overloading

##### 3. Hybrid routing:

A Combination of both proactive and reactive routing protocols is called as Hybrid routing protocol [18, 19]. In this routing protocol, the route of the control message is firstly established with the proactive routing protocol concepts and later the route may be established with the reactive routing protocol concepts based on the demand. Listing of topmost available hybrid routing protocols is in Figure3. This hybrid routing has the following disadvantages [20]. It depends on a number of other nodes activated. According to the gradient of traffic volume, the reaction of traffic demand depends. The difference between Proactive, Reactive and Hybrid routing protocol with properties are as in table3.

#### B. Clustering based routing:

In cluster based routing protocol [21] whole network topology is divided into a various number of a group based upon the density of the vehicle nodes in an area. For each group, one node is chosen as the cluster head (CH). Cluster head controls the flow of control message transmission between the vehicle nodes in its group [22]. All the other vehicle nodes are connected to the CH. Any message exchange should be possible through the CH only. Whenever the CH reaches the cluster limit boundary the new CH should be elected and after that, all the control and information of the old CH need to be transferred to the new CH. The various lists of available clustering based routing protocols are listed in Figure3. This clustering routing has the following drawbacks [13].

- Extra overhead cost due to CH election and switching.
- Poor memory use as all the CH is putting away the repetitive information.
- Communication is only possible for CH.

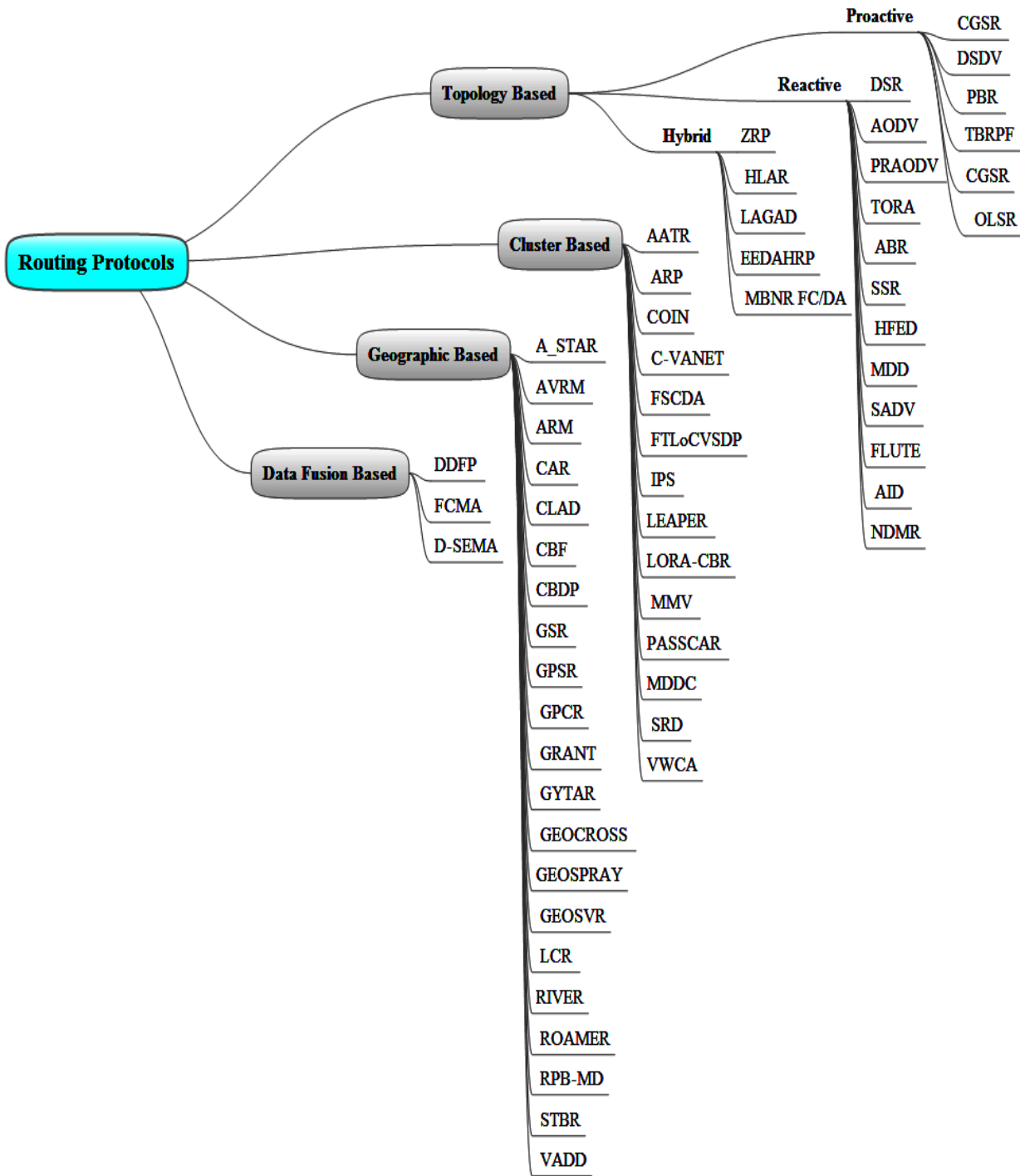



Figure3. Different Routing Protocol by using the Octopus diagram.

Table3. Difference between Proactive, Reactive and Hybrid Routing Protocol.

S.no.	Routing Properties 	Proactive	Reactive	Hybrid
1.	Routing structure	Flat	Mostly flat except CBRT	Mostly hierarchical
2.	Routing accessibility	Always reachable	Active when needed	Depends on the locations of the destination
3.	Traffic control unit	Usually high	Low	Mostly lower than proactive and reactive
4.	Mobility in handling the effect	At fixed interval updates occur based on mobility	ABR introduced LBQ AODV uses local route Discovery	Usually, more than one part may be available
5.	Storage requirement	High	Usually lower than proactive protocols	Usually, depending on the size of each cluster
6.	Delay level	The small route is pre-determined	Higher than Proactive	For local destination small, since inter Zone maybe as large size reactive protocols
7.	Scalability level to perform efficiently	100 nodes (Maximum)	Source routing protocol up to few 100 nodes point to point may scale higher	Node $\geq$ 1000

### C. Position-Based Routing (PBR):

Position Based Routing is also called Geographic routing or routing Protocol [23, 24]. It uses the principle of geographic position information to route the control information. Instead of using the network address, the source sends a message to the geographic locations of the destination. In PBR each node should be able to know its own location through this source should know the location of the destination. Without the knowledge of network topology or a prior route discovery, a message can be a route from source to the destination with the use of PBR. With the help of Global Positioning System (GPS) or through periodic beacon messages the position of each node can be identified. Listing of available geographic routing protocols is in Figure3.

### D. Data fusion routing (DFR):

Data fusion [25] can be circulated into the network and executed on vehicle nodes, which lowering the data from redundant nodes. It fuses the message from complementary nodes to get the complete structure of the message to cooperative nodes. Consequently, only the inference of interest sends the important

message to the other node. Listing of variously available data fusion routing protocols is as in

Figure3. Research on security issues the broadest research in vehicular ad hoc network communication is security issues [26]. Similarly, the proposed advance VANET communication system should prevent the various security threats. It should be noted that all the harmful attacks are also possible in the VANET communication system as web technology is merged in vehicular ad hoc network. Here, we would like to discuss some of the key security concerns of the advanced VANET model.

## IV. POSSIBLE ATTACKS ON VEHICULAR AD-HOC NETWORK

In a vehicle, Ad-hoc network security is the top priority. Know how important security is to make VANET secure. We first know about the possible attacks which make signal jam and provide wrong information about the node. The researcher describes the different type of attack, its structure, working, effects and possible solution [27]. With the help of attack, attackers will know the whole information about the nearby nodes. This will help to modify the rules and the protocol of the existing node and after modification, the attackers do whatever he wants to do [28]. The number of a possible attack which reduces the QoS and efficiency are as follows.

### A. Sybil attacks:

Sybil attack is a very harmful attack on the vehicle Ad-hoc Network because of this attack vehicle claim to be in a different position at the same time with the different identities [29, 30, 31]. This shows that vehicle is one, but it has N numbers of different positions through this the vehicle network gets broken down and creates confusion, as a result, the network will take more bandwidth to communicate with the neighbor nodes. The attacked vehicle sends multiple messages to the other vehicle node. Due to multiple messages sent to the other vehicle nodes and it assumes that there is heavy network traffic ahead. As shown in the Figure4 the vehicle Y claims to be in different locations at the same time and it sends multiple messages to the other vehicles with different identities.



Figure4: Sybil attack by the same identity and have a different location.

There were three types of defense mechanisms proposed against Sybil attack [31]:

- 1) Name registration,
- 2) Position verification and
- 3) Radio resource testing.

Name registration is not good enough to stop malicious nodes [32, 33] because it creates multiple identities by node information stealing. Each vehicle gets strict registers in a network center. Then it is possible to reduce the privacy-stealing.

The position of each node is verified according to the position verification mechanism. The goal of the mechanism is to make certain that each physical node refers to one and only one ideal identity.

All the physical nodes are limited in resources in radio testing [34]. Sybil attack is additionally doable in VANET design and this attack can increase the network information measure heavily in VANET. This attack can harm the topology and also the connections among the nodes.

### B. Bogus information attack:

This attack is attempted by the nodes for private benefits. The node sends the false (Bogus) [35] message to the opposite nodes like “heavy traffic is ahead, taking diversion” so as to divert the nodes to the opposite routes in order that the route is obvious to the wrongdoer. This attack can produce significant network traffic in denser areas and create the network busy and also the communication gets a block. The illustration of the fake info attack is shown in Figure4.1.



Figure4.1: Bogus information attack by Vehicle(X)

As pictured within the colluding attacker's ahead vehicle air the imitative info to have an effect on the choice of alternative vehicles (X). Once the receipt of false info the vehicle X assumes that the received info is correct and it takes the choice route and also the route is obvious for the wrongdoer (Y). This imitative info attack can cause several kinds of security issues and it'll have an effect on the topology. This kind of attack also will produce a collision which is able to cause surprising accidents. A special care should be shown in detection [36] and interference of this sort of attack. In VANET design this imitative info attack ought to be prevented and for identifying a secure algorithmic program ought to be developed to watch the behavior of the nodes within the configuration.

### C. Impersonation attacks:

In the Ad-hoc network each node can be identified with the help of its IP and MAC address. Similarly, in VANET architecture, each node is uniquely identified by IP and MAC addresses [35]. However, these two identities are not sufficient enough to authenticate the nodes in the network topology. A malicious node can spoof the IP and MAC addresses in order to get the identity of the other nodes so that it can hide in the network. The malicious node can make use of the identity of other nodes to communicate with other nodes. In this attack, the malicious node can broadcast the false information such as heavy traffic, accidents and so on with the identity of other nodes. For

instance, a malicious node can spoof the identity of an emergency vehicle and it can request for the priority lane and even it can demand the RSU to turn the green signal on. An efficient algorithm needs to be developed to identify the malicious node that has the spoofed identity. Moreover, attempting a strict authentication will lead to privacy issues because the driver of the vehicle has the right to prevent the disclosure of his driving routes. A novel and secure algorithm are needed obviously to defend the impersonation attack in the VANET communication model.

#### D. Timing attack:

The fundamental aim of Vehicular Ad-hoc network communication is to prevent the accidents. For the same emergency, messages need to be broadcast at the right time to avoid the accidents. However, in this attack mode when the attacker receives an emergency message does not forward the message at the normal time rather adds more time slots in order to create delay [37]. Thus, the nearby vehicles of the attacker receive the message after the moment when they should receive the message actually. If the vehicle receives the message at the right time it may take the different lane to avoid the accidents. This type of attack is known as Timing Attack.

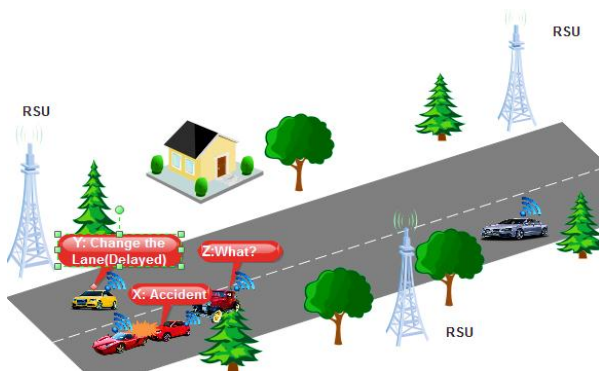


Figure4.2 Vehicle Y sends delayed emergency Message to Vehicle Z

The Figure4.2 depicts the timing attack that is attempted by the attacker. As depicted in the Figure4.2 there is an accident between the two vehicles the vehicle Z was informed about this accident. However, the vehicle Y did not forward the message in time to the other vehicle Z by adding extra time slots to delay the message. If the node Z received the message in time it would have taken the different lane, but due to the delay, it received the message after it has received the accident position. This attack model is known as a timing attack. This attack collapses the entire communication process of the vehicular ad hoc network communication. As we know the fundamental aim of VANET communication is to disseminate the emergency messages in time. This timing attack will be the

biggest challenge to the researchers. In VANET every message should be transmitted in time without further delay to achieve the better communication performance [38]. For the same an effective algorithm need to be modeled to prevent the timing attack in VANET architecture.

#### E. Illusion Attacks:

In this attack model, the attacker attaches sensors to produce the wrong sensor readings regarding the traffic information. The traffic monitoring system may receive the incorrect traffic information because of the wrong sensor readings and that incorrect traffic information can be broadcasted to the nodes. This type of attack model is known as an illusion attack. In vehicular ad hoc network communication scenario many types of data are received from the vehicles and those data are disseminated to the other nodes as it is requested by the nodes. When a node sends a data to the server, that data must be trustworthy because those data are going to be used by other nodes. Attaching wrong sensors to the vehicles will send the incorrect information to the server and will be the security threat forever. Those incorrect data will be broadcast to the other nodes and believing the received data the nodes may take different routes. This may lead to a collision at the particular location and it will also create accidents. This kind of illusion attack must be prevented to provide trustworthy communication [39, 40] among the nodes. All the data received at the server end need to be checked for its trustworthy. However, checking all the data received at the server end will lead to extra overhead and it will be a difficult task to complete it. Hence, this illusion attack also needs to be prevented in VANET communication model and to do so an efficient algorithm needs to be modeled.

#### F. ID disclosure:

A malicious node reveals the identity of the neighboring nodes so that the vehicles can be tracked to know its current location. Once the identity of the vehicle is revealed, the particular vehicle can be misused for various malicious activities. The attacker sends a malicious virus to the list of nodes to identify the target node. Once a node is attacked by the virus, it will send the ID of the victim node to the attacker [41]. Once the identity of the node is revealed the traveling route of the victim can be traced by the attacker and the victim node can be misused widely. An attacker can make use of the victim's identity to broadcast the false information among the nodes. This kind of ID disclosure will also lead to privacy issues. The identity of each node should not be revealed. If identity knows that identity can be used by malicious nodes to collapse the vehicular ad hoc network communication. In the proposed VANET communication architecture this type of attack should be avoided and for the same, a secure algorithm should be developed.



### G. Denial of Service (DoS) and Distributed Denial of Service (DDoS):

Denial of Service (DoS) [42, 43] is the process by which a node sends many dummy messages from different identities to the server as well as to other nodes. When the server receives multiple dummy messages continuously, the server will become busy and the performance of the network will be slow [44]. Due to this, the server may not be able to send the required information to the legitimate users. Similarly, sending many dummy messages like “Lane is closed ahead” to the legitimate vehicle causes the vehicle to take an alternate route.

The Denial of Service (DoS) is represented in the Figure4.3. As shown in the Figure4.3 the malicious vehicle sends many dummy messages with different identities to the legitimate vehicle and to the server [45]. The aim is to prevent the legitimate vehicle not to get the service form the server. When the server gets many dummy messages it will become busy as well as the efficiency of the entire network will be poor. This Denial of Service (DoS) attack is the most harmful attack on the every network communication architecture.

Distributed Denial of Service (DDoS) [46] attack is more advanced than the DoS attack. In this DDoS attack number of malicious vehicle attacks a legitimate node from different locations at different time slots in a distributed manner.

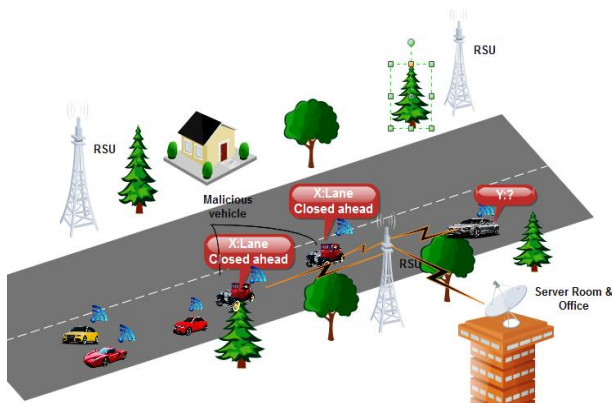


Figure4.3 Denial of Service (DoS)

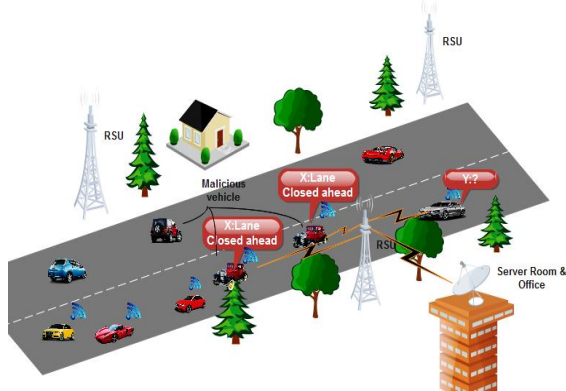


Figure4.4 Distributed Denial of Service (DDoS)

The Figure4.4 illustrates distributed denial of service (DDoS) attack. As demonstrated in the Figure4.4 malicious three vehicles attack a target legitimate vehicle A by sending many dummy messages such as “Accident Ahead”, “Lane Closed Ahead” from different locations and time slots. The aim of this attack is to stop the victim vehicle not to communicate with the other vehicles. The victim vehicle will be isolated from the network communication due to this attack. A novel and secure algorithm should be modeled to prevent the DoS and DDoS attacks in VANET communication architecture.

### H. Virus Attack:

The virus is a malicious software program which is more harmful to any network communication architecture [47]. In VANET, this virus is spread out from one vehicle to another vehicle when the user sends or downloads the information in the network architecture. In the VANET architecture, all the vehicles are connected to the internet and the communication [35] is carried out through the web. When the user sends a data from one vehicle to another vehicle or when the user downloads a data from the internet this virus can attach itself in the existing program and it can move to the particular vehicle to infect it. Virus program needs an existing program to move from a node to another node. If a node is vulnerable in the network, then the victim will be infected by a virus and the communication will be collapsed. Once a node is infected by the virus in the network architecture, it is also possible for other nodes to get infected by the virus as the nodes receive the files from the infected node. All the nodes in the VANET communication architecture should not be vulnerable to avoid virus infection. In VANET communication all the communication is carried through the internet and every vehicle will upload and download the information from the server. Hence, it is possible for a node to get infected by the virus attack. A secure virus attack detection and prevention algorithm must be developed to enhance the communication performance of VANET communication architecture.

### I. Worm attacks:

The worm is another type of malicious software code [35] which is more damageable to the network. The worm does not need an existing program to propagate from a node to another node like a virus. The worm will scan for the vulnerable nodes in the network architecture. As soon as a victim is found the worm will propagate to the victim node to infect it. After infecting a node, it will start the scanning process to find out the other vulnerable nodes in the network. Once another victim is found, it will propagate to the victim and infects it. Similarly, the worm propagates to all the vulnerable nodes in the network architecture [48]. This type of worm propagation will infect and collapse the entire network communication process. All the nodes in

the network must not be vulnerable to avoid worm attack. Normally this worm will be silent during the scanning process. So that worm cannot be identified by the worm scanning process. In the proposed VANET architecture this worm attack will be the biggest challenge. Any malicious user in the network can spread out the worm in order to collapse the entire network communication. An effective and secure worm propagation detection and prevention algorithms should be developed to enhance the VANET communication model.

#### **J. Trojan attacks:**

The Trojan attack is derived from the Greek mythology. Trojan looks harmless at the beginning. However, it will leave a node unprotected in the network architecture. It will enable the hackers to steal the sensitive information from a node. Initially, the Trojan will look like useful information to the nodes so that the node will install it. This will be similar to the social engineering attack. In VANET communication process the attacker may send the Trojan to the list of neighbors to attack them. Once a node is attacked by the Trojan it will leave the node unprotected and it will transfer the control of the victim node to the attacker. The attacker can steal the sensitive information about the node and that information can be misused for various nuisance activities. Normally a Trojan can perform the following actions [35].

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of the networks

In VANET communication model every node will store many data in it and these data can be used for the various communication purposes. This Trojan will delete the information stored on the victim node. Once the data is deleted the victim node may not be able to communicate in the network topology. Similarly, the Trojan can block the data that is being sent from a node to another node. The Trojan will block the emergency message that is being disseminated in the network. Emergency messages should be broadcasted at the correct time without delay, but the Trojan may block the information that is being broadcasted on the network. Another serious issue of the Trojan is modifying the data. That is, the Trojan can change the original data with the false information and the false information will be sent to the nodes in the network which will collapse the network communication. All the data stored in a node should be kept secret and that should not be copied without the consent of the authorized user. However, the Trojan will copy the data stored in a node

without notifying the user and it will send the sensitive information to the attacker. This Trojan will disrupt the communication performance of the entire network in the VANET communication model. A secure and effective algorithm should be developed to protect the proposed VANET communication model from the Trojan attack.

#### **K. Spyware attacks:**

The Spyware is installed on a node without the consent of the node when a file is downloaded. The aim of Spyware is to monitor and gather the information about the node and report it to the attacker. This Spyware would reset the auto signature, read and delete the files of a node. Even this Spyware [35] will format the data storage (hard drive) of a node. Vehicle to Vehicle communication depends on the huge amount of data. However, this spyware would read the secret data of the node and then sends that information to the attacker and even the files exist on the victim node can be deleted by this spyware [49]. In addition to that, the spyware can format the data storage (hard drive) of a node. Once the hard drive of the node is formatted, the node will be isolated and the communication in the particular network will be collapsed. This Spyware attack will be a real task to the defenders to defend against them. In VANET, this spyware needs to be prevented to secure the communication among the nodes.

#### **L. Spam attacks:**

The spam attack is similar to E-mail spam attack. In this attack, a malicious node sends more unwanted messages to the network, which consumes more network bandwidth. Also, this type of attack will create latency in the network scenario. This spam attack will make the server busy and the server will be slow in responding to the legitimate nodes. Sending unwanted data to a node will divert the communication of a node and even the unwanted data will contain malicious viruses to infect the node [35]. This attack will consume more network bandwidth and the network performance will be reduced obviously. In VANET communication architecture, this attack will degrade communication performance. Hence, a secure algorithm should be modeled to prevent these kinds of attacks. So far, we have reviewed the various types of security attacks that are possible for the secure VANET communication model. Recently introduced secure VANET communication model should prevent the various security attacks that are aimed at the attackers.

Overall summary of attacks on VANET is described as bellow in table4 which includes the type of attacks, attacker's type, security attributes, and requirements, do Physical Access require? and communication type.

Table4. Summary of different attacks in VANET

S. No.	Type of Attacks	Attackers type	Security Attributes and requirements	Requires Physical Access?	Communication types
1.	Sybil	Insider	Authentication, Privacy	Yes	V2V
2.	Bogus Information	Insider	Data Authentication	No	V2V
3.	Impersonation	Insider	Privacy, Confidentiality	Yes	V2V
4.	Timing	Malicious, insider	Data Integrity	No	V2V/V2I
5.	Illusion	Insider, Outsider	Authentication, Data Integrity	Yes	V2V/V2I
6.	ID Disclosure	Malicious, insider, network attack	Confidentiality, Data Integrity	Yes	V2V
7.	DoS [42] and DDoS	Malicious, active, insider, network attack	Availability,	Yes or No	V2V/V2I
8.	Virus	Insider, network attack	Data Integrity, Privacy	Yes	V2V/V2I
9.	Worm attacks	Outsider, Malicious, monitoring attack	Authentication, Confidentiality	Yes or No	V2V
10.	Black Hole(BH)[53,54]	Passive, outsider	Availability	Yes	V2V
11.	Trojan	Malicious, insider, network attack	Confidentiality, Data Integrity	Yes	V2V
12.	Spam	Insider, Network attack	Data Integrity, Privacy	Yes	V2V/V2I
13.	Malware	Malicious, insider	Availability	No	V2V/V2I
14.	Man-in-the-middle	Insider, Monitoring attack	Data Integrity, Confidentiality, Privacy	Yes	V2V
15.	Social Attack	Insider, e.g. "You a Donkey"	Data Integrity, Trust	Yes or No	V2V

○ Privacy-Preservation and Non-Repudiation Authentication

## V. AUTHENTICATION

Authentication is the process of making sure that all the nodes within the network are verified. Each node that enters the communication network must be authenticated efficiently [55, 56]. In VANET architecture each node is communicating through the internet technology, which could be attackable by the unauthorized nodes to exchange the false messages within the network. These kinds of unauthorized nodes may create accidents and collision among the nodes. Hence, each node that enters the VANET architecture must be authenticated. Here, the lists of available authentication mechanism are reviewed.

- Password-based authentication
- Privacy question-based authentication
- Mobile and E-mail authentication
- Efficient Privacy-preserving Authentication
- Dual Authentication and Key Management Techniques
- Cooperative Message Authentication
- The TESLA Broadcast Authentication
- On Joint Privacy and Reputation Assurance

### A. Password-based authentication Password based:

Authentication is the mostly used validation mechanism in an internet-based service. The password can be created by the user at the time of account creation with the combination of alphanumeric characters. It should be noted that purely character-based password can be attacked by the hackers easily. Highly complicated passwords [57] need to be created to avoid hacking. These complicated passwords may not be remembered always for the original user also. There are many techniques that attempt by the attackers to crack the passwords such as password guessing attack, cracker programs, Brute force attack or dictionary attack [58]. Even the malicious software known as Keylogger can be injected into a node to monitor the keystroke of a victim to hack the password. From the above views, it can be concluded that the password-based authentication mechanism cannot be the apt one for VANET communication. Hence, a novel authentication mechanism needs to be developed especially for securing [59,60] the VANET.

### B. Privacy question-based authentication:

Another way of authenticating a user in the internet based application is privacy question-based authentication mechanism. In this approach, a privacy question and its answer are set by the user at the time of profile creation [10]. Special care needs to be taken in framing an answer to the question as the answer could be easily guessable. As described in the previous section various cracking and Keylogger software can be used to hack the answers. Hence, this authentication mechanism is also not sufficient enough to get adopted in the VANET communication model.

### C. Mobile and E-mail authentication:

Mobile and E-mail based authentication mechanism is proposed to validate the user originality at the time of suspicious unauthorized access [57]. When an unauthorized access is suspected for an account, the account will be locked temporarily and the lock will be released after the successful verification of the user. In order to verify the user originality the generated random number either will be sent to the mobile number of the user added in the profile at the time of account creation or to the E-mail account that is registered with the user profile. However, this mechanism has the various limitations when we try to adopt this mechanism into the VANET communication model.

- This authentication procedure completely depends on Mobile and E-mail service provider.
- This mechanism does not make use of any of the VANET communication data to authenticate the node.
- Depending on another service provider will be always a security threat and the VANET communication architecture cannot function independently.

From the above observation, it is clear that a secure authentication mechanism is needed to authenticate nodes in the VANET communication model and the authentication mechanism should be under the characteristics of VANET.

### D. Efficient Privacy-preserving Authentication:

In Efficient privacy-preserving authentication scheme, Xiaoyan Zhu et al. [61] introduce a group signature for vehicular ad-hoc networks (VANETs) security. Although a group signature is widely used in VANETs to realize anonymous authentication and tackle with defining attacks, the scheme in literature is also based on group signatures which suffer from long time delay in the signature verification process and in the checking of Certificate Revocation List (CRL), leading to high message loss. As a result, they cannot meet the requirement of verifying define the number of messages/second in VANETs. Efficient privacy-preserving authentication scheme first divides the precinct into different sections, in which roadside units (RSUs) are responsible for distributing

group private keys, public keys and managing vehicles for best secure communication. To avoid time-consuming CRL checking and to ensure the integrity of messages before batch group authentication the Hash Message Authentication Code (HMAC) were used. Finally, the author also introduces cooperative message authentication among different entities, in which every vehicle solely needs to verify a small length of messages, thus greatly alleviating the authentication burden. According to the author, the analysis of security and performance in VANET prove that the scheme is much more efficient in terms of vehicle speed while keeping conditional privacy in VANETs.

### E. Dual Authentication and Key Management Techniques:

To boost the network environments, security and intelligent decision are two important problems need to be addressed. In Pandi Vijayakumar et al. [62] technique a trusted authority (TA) is designed to provide a variety of online internet based premium services to customers. Therefore, it is important to maintain the security of the bases confidentiality and authentication of messages exchanged between the TA and the OBU. Eliminating the security problem by focusing on the TA classifies the users into primary, secondary, and unauthorized users. In a 1<sup>st</sup> level, a dual key authentication scheme is to provide a high-level security in the vehicle to stop the unauthorized vehicle entry into the network. In the 2<sup>nd</sup> level, the author proposed a dual group key management scheme to distribute a group key to the users and update group keys during the users join and leave operations from time to time. The main goal of proposed dual key management is that adding/revoking users in the VANET group can be performed in a computationally efficient manner by updating a small amount of info. Through comparative analysis, the results of the proposed dual authentication and group key management scheme are much efficient as compared with all other existing literature.

### F. Cooperative Message Authentication:

According to Wenlong Shen et al. [63] VANET is described as a very complex cyber-physical system with the intricate interplay between the physical and cyber domains. In the physical domain, vehicles need to frequently broadcast their geographic information. The safety message broadcasting in an area with a high density of vehicles tends to incur a large data traffic rate that should be properly processed in the cyber domain. This is to deal with the difficulty of enormous computation overhead caused by the security message authentication. Especially, a cooperative message authentication protocol (CMAP) is developed to alleviate vehicles computation burden. With CMAP, all the vehicles share their verification results with each other in a cooperative way,

so that the number of safety messages that each vehicle needs to verify reduces significantly. Furthermore, Author study the verifier selection algorithms for a high detection rate of invalid messages in a practical 2-D road scenario. Another important contribution of the technique is use full for an analytical model for CMAP and the existing probabilistic verification protocol [03], considering the hidden terminal impact.

#### **G. The TESLA Broadcast Authentication:**

Perrig et al. presented a Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol, which uses symmetric keys instead of using asymmetric keys. The symmetric key systems are faster than signature-based authentication, the Denial of Service (DoS) attack is avoided in this system. However, it is hard to attain non-repudiation with symmetric key-based approaches. Digital signatures provide the best way for authentication with non-repudiation. Whereas one of the main challenges of securing broadcast between vehicles [64] is source authentication. The sender did not retransmit lost packets due to source authentication problem which gets complex by mutually unauthorized receivers and unreliable communication of the network. The technique TESLA broadcast authentication protocol, which proves that TESLA is an efficient protocol with respect to low communication and computation overhead. With this, it increases the large numbers of receivers and tolerates packet loss. This authentication depends on loose of time synchronization within the sender and the receivers. One of the limitations of TESLA is that it gains systematic properties while using purely symmetric cryptographic functions (MAC functions). In this technique, PKI application based purely on TESLA, assuming that all network nodes are loose time synchronized.

#### **H. On Joint Privacy and Reputation Assurance:**

According to Zhengming Li and Chunxiao (Tricia), Chigan [65] describe privacy protection in VANET. It is a challenging task to maintain a long-term reputation of any node. While reputation the management of information requires reputable certification at risk of easier vehicle tracks. Author projected JPRA to reconcile these difficult conflicts and support the synergistic beings of each indispensable scheme in VANETs. JPRA is for a localized reputation management model with the help of behavior evaluation, reputation manifestation and reputation aggregation this collectively performed by a node and its neighbor node. In the JPRA model, novel algorithms are designed to support secure and efficient reputation management in the face of node mobility and privacy protection. Furthermore, a Conditional Reputation Discretization Algorithm ensures privacy-preserving reputation manifestation for the honest nodes.

#### **I. Privacy-Preservation and Non-Repudiation Authentication:**

According to Jie Li et al. [66] authentication is an essential security service for both OBU and vehicle roadside communications. Vehicles must be shielded from the abuse of their private information and the attacks, as well as to be capable of being investigated for accidents or liabilities from non-repudiation. Under this authentication, the author looks into the issues with non-repudiation and privacy preservation in VANETs. The author proposes a novel privacy framework with Conditional Privacy-preservation and Non-repudiation (ACPN) to protect from attacks in VANETs. In the novel framework of ACPN, Author introduces the public-key cryptography (PKC) to the pseudonym generation. This pseudonym ensures third parties certification to achieve the non-repudiation of vehicles by obtaining vehicles' real IDs. The self-generated PKC-based pseudonyms also are used as identifiers rather than vehicle IDs for the privacy conserving authentication, whereas the update of the pseudonyms depends on vehicular demands. The existing ID-based signature (IBS) scheme and the ID-based online/offline signature (IBOOS) scheme are used, for the authentication between the Road Side Units (RSUs) and vehicles, and the authentication among vehicles, respectively. The overall performance analysis has been conducted using two efficient schemes, i.e. IBOOS and IBS schemes. The authors proposed ACPN is feasible and adequate to be used efficiently in the VANET environment.

#### **VI. CONCLUSION:**

In this paper, the researcher's aim was to provide a holistic view of previous works in VANETs which is divided into different parts. First part, researcher describes the previous work and the project. In Second part, routing protocols with octopus diagram. In Third part, explanation of the dangerous attacks with the possible diagram in Vehicular Ad-hoc Network and in last part, summary in table4. The techniques used in the attacks showed that the attackers generally exploit network and application layer operations. Researcher point out authentication solutions for security in VANET with respect to the methods used, infrastructure, reputation, and response mechanisms. Possible solutions are discussed, and open issues outlined for future research. In conclusion, attack/misbehavior detection in VANETs is a complex and challenging one and, protocol stack-wide and adaptive detection techniques, computational intelligence-based approaches are promising areas that could be explored in future studies as a means to make VANETs more secure.

## REFERENCES:

- [01] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", *Telecommun Syst* 50: 217, 2012. doi:10.1007/s11235-010-9400-5.
- [02] Duarte, P. B. F., Fadlullah, Z. M., Vasilakos, A. V., & Kato, N., "On the partially overlapped channel assignment on wireless mesh network backbone: A game theoretic approach", *IEEE Journal on Selected Areas in Communications*, 30(1), 119–127, 2012.
- [03] Shivaldova, V., Paier, A., Smely, D., & Mecklenbra'uker, C. F., "On roadside unit antenna measurements for vehicle-to-infrastructure communications", In 23d IEEE international symposium on personal, indoor and mobile communications (PIMRC) 2012.
- [04] J. Bernsen, D. Manivannan, "RIVER: A reliable inter-vehicular routing protocol for vehicular ad hoc networks", *Comput. Netw.* 52 (17), 3795–3807, 2012.
- [05] Liao, Cong, Jian Chang, Insup Lee, and Krishna K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", In *Wireless Vehicular Communications (WiVeC)*, IEEE 5th International Symposium on, pp-1-5, 2013.
- [06] Kumar, N., Chilamkurti, N., & Rodrigues, J. J. P. C., "Learning automata-based opportunistic data aggregation and forwarding scheme for alert generation in vehicular ad hoc networks". *Computer Communications*, 39, 22–32, 2014.
- [07] Xiang, X., Qin, W., & Xiang, B. "Research on a DSRC based rear-end collision warning model", *IEEE Transactions on Intelligent Transportation Systems*, 15(3), 1054–1065, 2014.
- [08] Sheng, Z., et al. "A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities." *IEEE Wireless Communications*, 20(6), 91–98, 2013.
- [09] Isaac, J.-T., Camara, J.-S., Zeadally, S., & Marquez, J.-T. "A Secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks", *Computer Communications*, 31(10), 2478–2484, 2012.
- [10] K.-Y. Ho, P.-C. Kang, C.-H. Hsu, C.-H. Lin, "Implementation of WAVE/DSRC Devices for vehicular communications", *Int. Symp. Computer Communication, Control, and Automation*, vol. 2, May 2010.
- [11] Xiang, X., Qin, W., & Xiang, B. "Research on a DSRC based rear-end collision warning model", *IEEE Transactions on Intelligent Transportation Systems*, 15(3), 1054–1065, 2014.
- [12] Zhang, X. M., Zhang, Y., Yan, F., & Vasilakos, A. V., "Interference-based topology control algorithm for delay-constrained mobile Ad hoc networks", *IEEE Transactions on Mobile Computing*, 14 (4), 742–754 2015.
- [13] S.S. Wang, Y.S. Lin, "PassCAR: A passive clustering aided routing protocol for vehicular ad hoc networks", *Comput. Commun.* 36 (2), 170–179, 2013.
- [14] Xiao, Y., Peng, M., Gibson, J., Xie, G. G., Ding-Zhu, D., & Vasilakos, A. V., "Tight performance bounds of multihop fair access for MAC protocols in wireless sensor networks and underwater sensor networks", *IEEE Transactions on Mobile Computing*, 11(10), 1538–1554, 2012.
- [15] C. Ou, "A Roadside Unit-based Localization Scheme for Vehicular Ad Hoc Networks", *International Journal of Communication Systems*, vol. 27, pp. 135-150, 2014.
- [16] Dua, A., Kumar, N., & Bawa, S., "A systematic review on routing protocols for vehicular ad hoc networks", *Vehicular Communications*, 1, 33–52, 2014.
- [17] A.M. Malla, R.K. Sahu, "A review on vehicle to vehicle communication protocols in VANETs", *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 3 (2), February 2013.
- [18] M.A. Rabayah, R. Malaney, "A new scalable hybrid routing protocol for VANETs", *IEEE Trans. Veh. Technol.* 61 (6), 2625–2635, 2012.
- [19] L.V. Minh, Y.M. Chuan, G. Qing, "End-to-End delay assessment and hybrid routing protocol for vehicular ad hoc network", *IERI Proc.* 2, 727–733, 2012.
- [20] Meng, T., Wu, F., Yang, Z., Chen, G., & Vasilakos, A. V., "Spatial reusability-aware routing in multi-hop wireless networks", *IEEE Transactions on Computers*, PP (99), 1–13, 2015). doi:10.1109/TC.2015.2417543.
- [21] O.A. Wahab, A. Mourad, H. Otrok, J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks", *Expert Syst. Appl.* 50, 40–54, 2016.
- [22] Manju Bhardwaj, "Faulty Link Detection in Cluster based Energy Efficient Wireless Sensor Networks", *International Journal of Scientific Research in Network Security and Communication*, Vol.5, Issue.3, pp.1-8, 2017.
- [23] Sandonis, V., Calderon, M., Soto, I., & Bernardos, C. J., "Design and performance evaluation of a PMIPv6 solution for geonetworking-based VANETs", *Ad Hoc Networks*, 11, 2069–2082, 2013.
- [24] A. Fonseca, T. Vazao, "Applicability of position based routing for VANET in highways and urban environment", *J. Netw. Comput. Appl.* 36 (3),961–973, 2013.
- [25] L. Zhang, D. Gao, W. Zhao, H.C. Chao, "A multilevel information fusion approach for road congestion detection in VANETs", *Math. Comput. Model.* 58 (5–6), 1206–1221, 2013.
- [26] Zhou, J., et al. "Secure and privacy-preserving protocol for cloud-based vehicular DTNs", *IEEE Transactions on Information Forensics and Security*, 10(6), 1299–1314, 2015.
- [27] Viriyasitavat, W., Boban, M., Tsai, H.-M., & Vasilakos, A. V., "Vehicular communications: Survey and challenges of channel and propagation models", *IEEE Vehicular Technology Magazine* x, 10(2), 55–66, 2014.
- [28] A.Vani, "Detection and Elimination of Wormhole Attacks in a MANET", *International Journal of Scientific Research in Computer Science and Engineering*, Vol.5, Issue.5, pp.35-40, 2017.
- [29] J. Grover, M.S. Gaur, V. Laxmi, N.K. Prajapati, "A Sybil attack detection approach using neighboring vehicles in VANET, in *Proceedings of the 4th International Conference on Security of Information and Networks*, pp. 151–158, 2011.
- [30] X. Feng, C. Li, D. Chen, J. Tang, "A method for defending against multi-source Sybil attacks in VANET", *Peer-to-Peer Netw. Appl.* 10 (2), 305–314, 2017.
- [31] B. Yu, C.-Z. Xu, B. Xiao, "Detecting Sybil attacks in VANETs, *J. Parallel Distrib.* 73 (6) 746–756, Jun 2013.

- [32] U. Khan, S. Agrawal, S. Silakari, "Detection of malicious nodes in vehicular ad-hoc networks", *Procedia Comput. Sci.* 46, 965–972, 2015.
- [33] A. Daeinabi, A.G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks", *Multimed. Tools Appl.* 66 (2), 325–338 2013.
- [34] D. Kushwaha, P.K. Shukla, R. Baraskar, "A survey on Sybil attack in vehicular ad-hoc network", *Int. J. Comput. Appl.* 98 (15), July 2014.
- [35] Zeadally, Serali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", *Telecommunication Systems* 50, no- 4 pp- 217-241, 2012.
- [36] H. Sedjelmaci, S.M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks", *Comput. Electr. Eng.* 43, 33–47, 2015.
- [37] Zeng, Y., Xiang, K., Li, D., & Vasilakos, A. V., "Directional routing and scheduling for green vehicular delay tolerant networks", *Wireless Networks*, 19(2), 161–173, 2013.
- [38] Y. Liu, J. Niu, J. Ma, L. Shu, T. Hara, W. Wang, "The insights of message delivery delay in VANETs with a bidirectional traffic model", *J. Netw. Comput. Appl.* 36 (5), 1287–1294, 2013.
- [39] N. Kumar, N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs", *Comput. Electr. Eng.* 40 (6), 1981–1996, 2014.
- [40] M.Ch. Chuang, J.F. Lee, "TEAM: trust-extended authentication mechanism for vehicular ad hoc networks", *IEEE Syst. J.* 8 (3), 2013.
- [41] Biswas, Subir, Jelena Mistic, and Vojislav Mistic, "ID-based safety message authentication for security and trust in vehicular networks", In *Distributed Computing Systems Workshops (ICDCSW)*, 31st International Conference on, pp- 323-331, 2011.
- [42] K. Verma, H. Hasbullah, A. Kumar, "Prevention of DoS attacks in VANET", *Wireless Person. Commun.* 73 (1),95–126, 2013.
- [43] L. He, W.T. Zhu Mitigating, "DoS attacks against signature-based authentication in VANETs", *IEEE Int. Conf. Comput. Sci. Automat. Eng. (CSAE)* 3, 261–265, 2012.
- [44] Abubakar Bala and Yahya Osais, "Modelling and simulation of DDOS Attack using SimEvents", *International Journal of Scientific Research in Network Security and Communication*, Vol.1, Issue.2, pp.5-14, 2013.
- [45] A.M. Malla, R.K. Sahu, "Security attacks with an effective solution for Dos attacks in VANET", *Int. J. Comput. Appl.* (ISSN 0975-8887), 66 (22), 2013.
- [46] S. Biswas, J. Mistic, V. Mistic, "DDoS attack on WAVE-enabled VANET through synchronization", in: *Global Communications Conference (GLOBECOM)*, pp. 1079-1084, 2012.
- [47] J.T. Isaac, S. Zeadally, J.S. Cámara, "Security attacks and solutions for vehicular ad hoc networks", *IET Commun.* 4 (7), 894, 2010.
- [48] Shree, R., Khan, R., "Wormhole attack in wireless sensor network", *Int. J. Comput. Netw. Commun. Secur.* 2(1), 22–26, 2014.
- [49] V. La Hoa, A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey", *Int. J. Netw. Syst.* 4 (2), April, 2014.
- [50] A. Kumar, R. Shree, "Study of Wireless Technologies Related to Vehicular Ad-hoc Sensor Network for Intelligent Control and Security", *International Journal of Innovations & Advancement in Computer Science*, ISSN No. 2347 – 8616 Vol. 4, 2015.
- [51] M. Joe, and B. Ramakrishnan, "Review of Vehicular Ad hoc Network Communication Models including WVANET (Web VANET) Model and WVANET Future Research Directions", *Wireless Networks*, Springer, vol. 22, no. 7, pp. 2369-2386, 2015.
- [52] M. Joe, and B. Ramakrishnan, "WVANET: Modelling a Novel Web-Based Communication Architecture for Vehicular Network", *Wireless Personal Communications*, Springer, vol. 85, no. 4, pp. 1987-2001, 2015.
- [53] V. Bibhu, R. Kumar, B.S. Kumar, D.K. Singh, "Performance analysis of black hole attack in VANET", *Int. J. Comput. Netw. Inf. Security* 4 (11) 47, 2012.
- [54] S.Sharma, Rajshree, R.P.Pandey, V.Shukla, "Bluff-Probe Based Black Hole Node Detection and Prevention", *IEEE International Advance Computing Conference (IACC)*, pp. 458-462, March 2009.
- [55] S. Biswas, J. Mistic, "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs", *IEEE Trans. Veh. Technol.* 62 (5), 2182–2192 Jun, 2013.
- [56] Ram Shringar Raw, Manish Kumar, Nanhay Singh, "Security Challenges, Issues And Their Solutions For Vanet", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.5, No.5, pp- 95-105, September, 2013.
- [57] K. Lim, D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks", *Veh. Commun.* 4, 30–37, 2016.
- [58] R. Raiya, Sh. Gandhi, "Survey of various security techniques in VANET", *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* 4 (6), June 2014.
- [59] J.-P. Hubaux, S. Capkun, J. Luo, "The security and privacy of smart vehicles", *IEEE Security Privacy Mag.* 2, 49–55, 2004.
- [60] U. Korupolu, S. Kartik, GK. Chakravarthi, "An Efficient Approach for Secure Data Aggregation Method in Wireless Sensor Networks with the impact of Collusion Attacks", *International Journal of Scientific Research in Computer Science and Engineering*, Vol.4, Issue.3, pp.26-29, 2016
- [61] X. Zhu, S. Jiang, L. Wang, H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks", *IEEE Trans. Veh. Technol.* 63 (2), 907–919, 2014.
- [62] P. Vijayakumar, M. Azees, A. Kannan, L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks", *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015-1028, Apr. 2016.
- [63] Shen, W., Liu, L., Cao, X., Hao, Y., & Cheng, Y., "Cooperative Message Authentication in Vehicular Cyber-Physical Systems". *IEEE Transactions on Emerging Topics in Computing*, 1(1), 84-97, 2013.
- [64] A. Perrig et al., "The TESLA Broadcast Authentication Protocol", *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.
- [65] Z. Li and C. Chigan, "On joint privacy and reputation assurance for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2334–2344, 2014.
- [66] Jie Li et al., "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, No. 4, pp.938-948, April 2015.

### Author's Profile

---

**Ajay Kumar:** He received a Master Degree (M. Tech.) in Information and Communication Technology from School of ICT, Gautam Buddha University, G B Nagar in 2013. He is currently, a Ph.D. scholar in Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India. His current research interests include, ad hoc networking and its Security.



**Raj Shree:** She has completed her master degree (M. Tech.) in Computer Technology & Application from Rajiv Gandhi Prodyogiki Vishwavidyalaya, Bhopal, and Ph.D. from Department of Information Technology, BBAU, Lucknow. Currently, she is working as Assistant Professor in the Department of Information Technology, in Babasaheb Bhimrao Ambedkar University, Lucknow, India. Her research interest includes Mobile Computing, Software Engineering, Image Processing & Wireless Sensor Network. She has published various research papers in national, international journals & conferences.

