International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 30th Jul 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue= Spl Issue 06

DOI: 10.48047/IJIEMR/V11/SPL ISSUE 06/21

Title A Survey: Issues and Challenges of Vehicular Ad Hoc Networks (VANETs)

Volume 11, SPL ISSUE 06, Pages: 107-116

Paper Authors

D.Rakesh, K.Srinu,M.Dharani,P.Swaran, RadhaKrishna Karne

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Survey: Issues and Challenges of Vehicular Ad Hoc Networks (VANETs)

D.Rakesh[1], K.Srinu[2],M.Dharani[3],P.Swaran[4], RadhaKrishna Karne[5]

[1,2,3,4]UG Scholar, Department of ECE, Balaji Institute of Technology & Science, Narsampet, Warangal, Telangana, India

[5]Assistant Professor, Department of ECE, Balaji Institute of Technology & Science, Narsampet, Warangal, Telangana, India

Abstract:A broad and developing field of research in vehicle communication technology is the Vehicular Ad-hoc Network (VANET). A network without infrastructure is the VANET. It is used to improve driving comfort and safety for certain applications. In order to share secure data while driving on roads or highways, VANET connects automobiles. Applications for the VANET are being created for cities around the globe. VANET offers an identity recognition technology that has a significant impact on improving activity administrations and reducing traffic accidents. The construction of a vehicle safety and security environment is the main objective of this technology. In recent years, numerous structures, algorithms, and protocols have been implemented to improve the efficiency of moving vehicles. The writers of this research study examine current issues including developments, exploitation, safety, security issues, and the newest plans running consecutively in diverse environments. They offer the simulator-related data required to run the VANET. This paper's main goal is to analyse and come up with a fresh notion for vehicular communication.

Keywords: VANET, Protocols, Routing, Security, Simulation Model

1. INTRODUCTION

The Vehicular Ad hoc Network (VANET) is a technology that enables communication between vehicles and roadside units (RSUs) within a short range of between 100 and 300 metres. To solve the accident problems is the primary goal of the deployment of VANET [1]. It can be used for a wide range of purposes related to human safety and good driving on urban roadways. Because the number of vehicles on the road is growing along with the accident rate, it is essential that all vehicles adopt the VANET system. For illustration, suppose that a vehicle A is travelling ahead of a vehicle B when suddenly A collides with a thunderstorm and experiences brake problems. In order to prevent B from experiencing the same problem, vehicle A's sensors repeatedly activated the signal and sent it to the roadside unit, which then broadcast a warning to other vehicles. B accepts the notice message and moves the vehicle backward [2]. Therefore, effective and trustworthy vehicle-to-vehicle communication is necessary when driving on the roadways.

A component and subset of Mobile Ad hoc Network is Vehicular Ad hoc Network (VANET) (MANET). The purpose of VANET is to provide communication between vehicles and nearby infrastructure (RSU). This communication strategy aims to enhance both safety-related and non-safety related applications in moving vehicles. Real-time position data must be accessible for the vast majority of VANET applications. According to the World Health Organization (WHO), statistics on road traffic injuries across all countries show that fatal accidents are a major cause of death. To solve this problem, a traffic system is therefore required. The VANET is a driven network that focuses on intelligent and smart transportation systems (ITS). It gives end-user vehicles access to resources for speedy information exchange and health. VANET uses unique protocols like DSRC and WAVE for quick and simple information communication [3]. For direct, dedicated short-range communication, the US FCC has set aside 75 MHz of the 5.9 GHz spectrum (DSRC). Seven 10 MHz channels make up the DSRC range. It is suggested to use one of these seven channels as a control channel, mostly for safety applications. There are two different types of safety-related communications that are sent over the control channel in VANET: the first is event-driven messaging, which is sent to a destination vehicle when a hazardous situation has occurred, and the other is periodic beacon messaging, which is used by vehicles to communicate vocational information to other nearby vehicles, such as their position and speed [4]. These beacon messages serve a vital safety function by providing drivers with a precise and comprehensive map of the vehicles that are immediately around them. Based on the graph, security and safety applications have largely evolved into cooperative alertness programmes that can reduce accidents by warning drivers about the upcoming dangerous states.

In recent years, research has concentrated on developing secure VANET systems to prevent mishaps caused by various cruel or harmful elements and circumstances that impair network performance. Numerous active and passive features target the VANET system to lower vehicle efficiency. To protect the system from these malware attacks, numerous secure and safe medium access control (MAC) mechanisms and routing are being created. Numerous initiatives are being carried out in numerous nations to improve human safety and security as well as the conditions for driving vehicles. The projects being carried out in the USA and other nations offer the end customers a variety of services such safety alarm systems, sensor devices, broadcasting, media downloading, etc.

The major goal of this essay is to examine the difficulties that drivers experience nowadays when travelling by vehicle. These difficulties are numerous, and drivers need safety. Vehicular Ad hoc Network deployment is not widespread due to numerous problems with moving organisations and the WHO. Additionally, people need to be aware of the conditions relating to vehicle safety, and it is becoming a research area for scientists to interface between the vehicles and provide safety for people. End users can access a variety of services through VANET, including e-health resources, multimedia, security, and safety [5]. Many researchers are currently attempting to create and enhance the VANET system while also concentrating on issues including traffic management, routing, broadcasting, security, and vehicle safety.

The review and survey of VANET systems are described in the parts that follow in this study. A thorough explanation of the VANET architecture is provided in Section 2. The purpose of VANET communication in the real world is presented in section 3. The routing techniques used in the VANET system are illustrated in Section 4. Section 5 discusses the privacy and security issues that the VANET system faces. It also emphasises the VANET system's safety applications. The system model of the VANET architecture and the simulation tools used in VANET environments are described in section 6. Section 7 presents the conclusion and future directions for VANET system research.

2. VANET DESCRIPTION

2.1 VANET Architecture

The architecture of the VANET system is described in this section. The primary components of the VANETs system are first introduced. Presented the intersection portion after that, followed by an explanation of how the vehicular ad hoc network communicates. Additionally, it gives a fundamental overview of the layered architecture of the vehicle system. The three domains of the VANET system architecture are the transportation domain, the mobility domain, and the fundamental domain [6]. Automobiles and mobile devices made up the second division of the mobile domain. Every sort of vehicle, including vehicles, trucks, and buses, is included in the automobile domain. All transportable gadgets, such as personal navigational devices, cell phones, and mobile phones, are included in the mobile device domain. Road infrastructure and central infrastructure, also known as the transportation domain, make up the infrastructure domain. Roadside unit items like traffic signal data are included in the roadside infrastructure domain. The vehicle management centres and traffic management centres (TMCs) are examples of central infrastructure that is maintained by the central infrastructure unit [7]. Aside from this domain region, each region has its own deployment and development of the VANET system architecture. The vehicles, on board units (OBU), road side units (RSU), and transportation systems are all included in the VANET system design. VANET operation is carried out using a particular wireless standard (e.g. IEEE 802.11p). In a VANET system, the road side unit (RSU) serves as a router and has a far wider coverage area than a vehicle. The automobiles have a on board unit chip implanted for communication. Vehicles are equipped with global positioning systems (GPS) that allow them to track other vehicles in addition to determining their own location. Electronic License Plates (ELP) are now put in automobiles for identification purposes as a further improvement. These elements improve the speed and effectiveness of the VANET system. For the purpose of supplying information on vehicles, the light amplification/Radio detection and ranging (RADAR) by simulated emission by radiation (LASER) approach is used. The design includes a trusted certified authority to simplify the vehicle. The architecture of the VANET system is shown in Figure 1.

2.2 Transportation System

The infrastructure architecture known as an intelligent transportation system (ITS) enables a vehicle to function as a sender, collector, and switch for data broadcasting. As previously stated, the VANET system includes RSUs, and vehicles are equipped with OBU, GPS, and ELP, among other things. Vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) or infrastructure to vehicle (I2V) communication are the two methods of communication

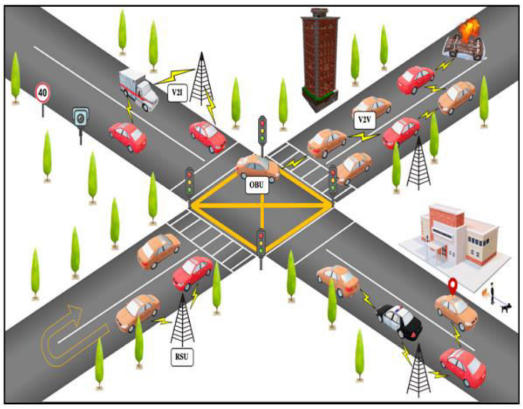

Figure.1. VANET Communication architecture

that ITS chooses for the vehicular ad hoc network. The task of information transfer through vehicle to vehicle (V2V), vehicle to infrastructure (V2I), or infrastructure to vehicle (I2V) communication is performed via multicasting or broadcasting communication [9]. There are two types of correspondence that take place between vehicles: the first is called guileless telecom and involves messages that are constructed on demand, while the second is called cunning telecom. The risk of a crash occurring during the process can be reduced by using the information transmission method. Single-jump correspondence is used in vehicle-to-vehicle (V2V) communication (RSU transmits message to vehicles in range) . A wide range of connections between the vehicles and the RSUs were included. When the RSU determines that the vehicle speed has exceeded the limit, the RSU transmits a message as a clear warning signal [10].

3. OBJECTIVE OF VANETs

3.1 Description

When travelling by vehicle today, massive and quick changes took place in every area of the planet. Due to increased traffic congestion and vehicle accidents, the streets are becoming more hazardous. According to the National Road Safety Observatory's survey, which was published in recent reports, there were 65000 more accidents in 2012 than there were in 2011. Secure traffic is therefore not only necessary, but also a fundamental duty. The goal of the intelligent transportation system (ITS) is to provide an appropriate solution for both the problem of traffic congestion and the safety of drivers and passengers on the road. By integrating information technology into transportation networks, they improved comfort and driving conditions as well. A node in an intelligent transportation system (ITS) could be a vehicle with a wireless short-range radio system, or it could be a piece of roadside equipment that connects mobile ad hoc points to network infrastructure. The Ad hoc Network is made up of vehicles that are connected via sensors, on board units (OBUs), and ELP chips. The infrastructure also includes the manufacturer, third-party on-board units and service providers, and governmental agencies. Between the network and infrastructure components, the road side unit acts as a liaison.

3.2 Smart Vehicle

According to [8], an intelligent transportation system is essentially a collection of sensors that work together to produce relevant environmental data that, in most cases, the driver cannot detect on their own. GPS (global positioning system) is used by this intelligent vehicle to determine its location, which is important for positioning and providing driving support. A multi-rate communication system and an event recorder, which serves the same purpose as an aircraft's black box, are integrated into smart vehicles.

3.3 VANET Standards

Standardization and institutionalisation in communications and data innovation aid in ensuring interoperability and the speedy implementation of new developments in addition to the benefits of the generating process, the reduction of costs, and the reduction in time to market. These VANET standards are used to enhance the transportation of vehicles and to assist clients in verifying and contrasting the products. The dedicated short range communication protocol (DSRC)and wireless access in vehicle environments (WAVE), as well as IEEE 802.11p, are only a few of the protocols that are used in the VANET system.

3.3.1. DSRC Protocol

The USA established the DSRC standard, both V2I and V2V communication use it for short-range communication benefits. The US government, represented by the federal communication commission (FCC), establishes 75 MHz of range at 5.9 MHz for the specialised short range Communication in order to achieve the highest level of interoperability and for the purpose of institutionalising the frequencies with which the

VANETs operate. The DSRC band is subject to stringent action of utilisation rather than a permit for use. Seven channels of 10 MHz each, with unique numbers 172, 178, 176, 174, 182, and 184, make up the DSRC band range. The control channel is channel 178, while the administrative channels are channels 6 through 8. Benefit channels 184 and 172 are each held to HALL standards for high power and open security as well as for high accessibility and low idleness. The European Telecommunication Standards Institute (ETSI) has standardised the DSRC band in Europe, and only channels 180 of CCH and 174, 172, 178, and 176 of SCH are used.

3.3.2. Wireless Access in Vehicular Environment (WAVE)

The WAVE IEEE 1609 family (standard for wireless access in vehicular environment) explains a design and a matching set of service, standardised protocols, and interface that permit all WAVE stations to activate in a vehicular environment and set up vehicle to Infrastructure (V2I) and vehicle to vehicle (V2V) communications, based on the most recent smart transport system fact sheets published by IEEE in. The security of transfer messages is also created by the WAVE architecture. WAVE standards are used in the transportation sector based on the effectiveness of a wide range of applications, including traffic management, automatic toll collection, vehicle safety and security, and diverse applications. The WAVE IEEE 1609 standards family is divided into the following categories:

IEEE P1609.0:For the design of Wi-Fi access in a VANET context, this protocol is the star (WAVE). It explained how the 1609 standards' collective services and cooperative efforts enable multi-channel dedicated short-range communication devices to operate in a very mobile environment.

IEEE Std. 1609.1:The WAVE system architecture's fundamental components are defined by this resource manager, which also serves as a vehicle for command messages and storage data formats. It outlines the kind of devices that the OBU can support (on board unit).

IEEE Std. 1609.2:It offers management messages and application security services. It is primarily used for structuring and processing secure messages sent via the DSRC and WAVE networks. Additionally, it outlines the characteristics needed to provide message security and vehicle privacy.

IEEE Std. 1609.3: This standard implements the network and transport layer services, which are addressed with the aid of cloud computing and WAVE secure information sharing. It offers a precise alternative that is tailored to the WAVE system and supports IP applications directly. Additionally, it offers the WAVE protocols group's management information base (MIB).

IEEE Std. 1609.4: To support WAVE, this standard uses a modification to the 802.11 MAC protocol. It describes WAVE architecture-based IEEE 802.11p wireless multi-channel radio operations.

Draft IEEE P1609.5& 6:The communication management services for V2V and V2I communication for the Wave Environment are presented in this Draft IEEE P1609.5, which was developed through a process. Draft P1609.6 is also in progress; it focuses on the remote management service, which manages interoperable services. This draught offers WAVE device remote administration and identification services (OBU and RSU). For additional facilities, it provides an additional middle layer between the application and transport layers.

IEEE Std. 1609.11:For the usage of a secured electronic payment sample, it delivers secure and safe messages.

IEEE Std. 1609.12:This application defines the identification value that has been allocated for use by the WAVE system (Provider service Identifier Allocations (PSID)).

3.3.3 IEEE 802.11p

The IEEE has expanded its collection of IEEE 802.11 protocols by adding 802.11p to fit vehicle systems, as per the DSRC band, in addition to the IEEE 1609 specifications. The IEEE 802.11p-2010 standard, which modified the PHY and Medium Access layers of the IEEE 802.11-2007 to be suitable for automotive systems, establishes the MAC and physical layers for vehicular ad-hoc networks. In terms of the PHY layer and QoS, IEEE 802.11p primarily focuses on IEEE 802.11 and IEEE 802.11e, respectively. The OFDM (Orthogonal Frequency Division Multiplexing), which has stream rates of 3, 4, 5, 6, 12, 24 and 27mbps and a channel width of 10 MHz, is the foundation of IEEE 802.11p PHY.Ten times per second, the WAVE hardware in a vehicular ad-hoc network alternates between SCH and CCH channels. The MAC layer of IEEE 802.11 uses EDCA (Enhanced Distributed Channel Access), a replacement for DCF (Distributed Coordination Function), which was previously used in the majority of IEEE standards. EDCA uses the protocol known as carrier sense multiple access with collision avoidance (CSMA/CA) to obtain a communication channel.

3.4 VANETs Characteristics

VANET is a wireless network where the hubs are stationary street devices or incredibly adaptable/mobile vehicles. In foundation mode, hubs communicate with fixed hardware on the streets and with each other in an ad hoc manner. As a result, the characteristics of remote mediums mixed with those of various topologies in both ad hoc and foundation modes make up the VANET system. The characteristics of VANET architecture are as follows:

High mobility: The key characteristic of VANET hubs is their high degree of adaptability. Hubs are travelling in different directions and at variable speeds during the crucial hub communication process. The system's complicated architecture is made possible by hubs' great degree of adaptability. Compared to MANET, VANET has a greater mobility range. Numerous academics are working hard to focus on the impact of adaptability in specially designed systems, especially for vehicle systems.

Dynamic topology: The topology of the VANET is dynamic, unstable, and ever-changing. In instance, the association time between hubs travelling in opposite directions is constrained. This structure makes it more difficult to find malfunctions and facilitates an attack on the entire system.

Frequent extrications: The topology of the VANET is dynamic, unstable, and ever-changing. In instance, the association time between hubs travelling in opposite directions is constrained. This structure makes it more difficult to find malfunctions and facilitates an attack on the entire system.

Transmission medium Accessibility: The transmission medium in the VANET system is air. Despite the fact that the general openness of this remote transmission medium, which is one of the major attractions of IVC, also serves as the source of some security concerns.

Limited bandwidth: It is possible to think of the formalised DSRC band for VANET as restricted; its entire transmission capability range is 75MHz. Some countries' restrictions on usage suggest that not all of these 75 MHz ranges be allowed. The maximum fictitious throughput is 27 Mbps.

Attenuations: With such frequencies, the DSRC band also has transmission problems such diffraction, reflection, scattering, various types of blurring Doppler Impact, mishaps, and spread deferrals due to multipath reflections.

Restricted transmission control: The WAVE system limits the transmission power, which limits how far the information may travel. Up to 1000 metres separate these two points. Additionally, it is permitted to broadcast with a higher power in specific circumstances, such as public safety and emergencies.

4. ROUTING PROTOCOLS

A significant component of MANET and VANET communication systems is routing. In ad hoc systems, there are numerous routing protocols created for communication between the vehicles. Routing is a common process in vehicular systems due to its high mobility. Even though VANETs can enable a wide range of innovative applications, the design of effective vehicular communications continues to be difficult. In VANETs, vehicles often enter and exit the network, causing persistent way interferences. Because of the temporal differences in vehicle density, topology frequently changes, making it challenging to safeguard a route. brings about low throughput and excessive routing overhead for this case. Low packet reception rate is caused by the well-known hidden terminal issue, which alters the way VANET system operates. Interference problems, such as routing loops and sending data down the wrong path, cause delays in VANET systems. System administration, frequent information interchange, traffic management, topological change, broadcasting mobility, and quality of service are only a few of the core system concerns that call for routing. These are the difficult parts that call for expert routing methods. Following are the main divisions that may be made between VANETs routing communication. The authors of this section examine the advance routing communications used in VANET systems. The taxonomy of the routing protocols in the VANET system is shown in Figure 2.

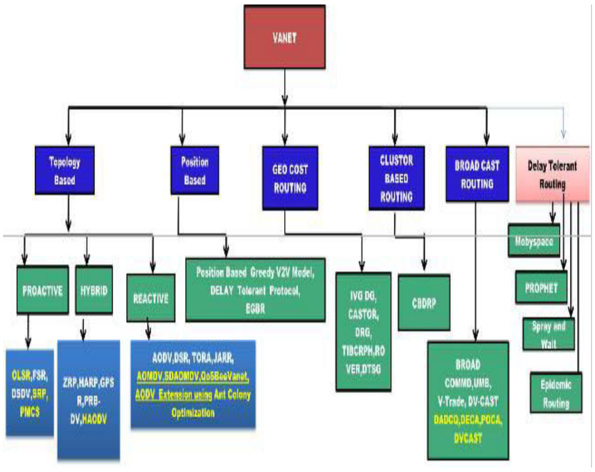
VANET
Topology Based
Position Based
GEO COST ROUTING
CLUSTOR BASED ROUTING
BROAD CAST ROUTING
Delay Tolerant Routing
PROACTIVE
HYBRID
REACTIVE
Position Based Greedy V2V Model, DELAY Tolerant Protocol, EGBR
IVG DG, CASTOR, DRG, TIBCRPH,ROVER,DTSG
CBDRP
Mobyspace
PROPHET
Spray and Wait
Epidemic Routing
OLSR,FSR, DSDV,SRP, PMCS
ZRP,HARP,GPSR,PRB-DV,HAODV
AODV,DSR, TORA,JARR, AOMDV,SDAOMDV,QoSBeeVanet, AODV Extension using Ant Colony Optimization
BROAD COMMD,UMB, V-Trade, DV-CAST DADCQ,DECA,POCA, DVCAST

Figure.2. Routing Protocols in VANET

4.1 Unicast Routing Protocols

Information packets are sent from a single source to a single destination using unicast routing methods.

They mostly support specialised corporate applications and consumer applications like online networks and multimedia access. In particular ad-hoc conditions, unicast routing protocols are the most important protocols and serve as the foundation for many sorts of protocols. Additionally, unicast routing methods are divided into topology-based, hybrid position-based and cluster-based protocols.

4.1.1 Topology Based Routing Protocols

Topology-based protocols use data from around the world about network topology and information about communication channels to make routing decisions. There are two different types of routing protocols: one is proactive and the other is reactive. No route discovery occurs in the proactive routing protocol because the path is already known. Supporting underused paths and routes increases network system and load, which reduces network execution . Topology dissemination based on reverse path forwarding (TBRPF), fisheye state routing (FSR), wireless routing protocol (WRP), cluster head gateway switch routing (CGSR), optimised link state routing (OLSR), destination sequenced distance vector (DSDV), etc.These protocols function independently of the present communication requirements and network conditions and discover network topology data through recurrent control packets. Reactive routing protocols are planned, in which the path finding occurs on request, but proactive routing systems suffer from the impacts of system load and increased bandwidth consumption. As a result of only the recently utilised route adjusting with minimal packet overhead, the network load decreases. Ad hoc on-demand distance vector (AODV), border gateway protocol (BGP), temporary ordered routing algorithm (TORA), dynamic source routing (DSR), and some more reactive routing protocols are examples of reactive routing protocols. Utilizing a hybrid routing strategy, which has the advantages of both proactive and reactive routing protocols, helped the VANET run better. It uses the routes between the different zones to overcome network load. Intra-zone and inter-zone routing are used proactive and reactive protocols respectively.

4.2 Routing Protocol based on position

Position-based routing locates geographic information to choose the next hop where the data will be transferred. Beaconing is used to transmit the information. There is no routing involved in this process, and no route tables are maintained. Area is used as a message in this operation to route the packets to the nodes. This uses an onboard unit (OBU) for information delivery together with GPS, road maps, and services. Because of the high level of mobility, the topology changes dynamically frequently, and if topology-dependent routing is used, the performance may suffer as a result of increased network load. Routing protocols that depend on position include those that use the distance routing impact algorithm, greedy edge stateless routing for mobility, connection awareness, geographic source routing, and anchor-based road and traffic.

4.3 Cluster Routing Protocols

Because it can scale more easily and is preferable for broadcast systems, cluster-based routing is used. A group of vehicles is referred to as a cluster, and each group contains a cluster head that relays information to various vehicles. Cluster based area routing, Cluster based routing, clustering for open IVC network, and several other cluster based routing therefore with respect to are a component of the routing protocols depend on cluster are the primary problems with group based systems.

4.4 -Routing protocol based on Geo Cast

This Geo Cast-based routing is a multicasting service; it uses multicasting to send messages to a certain area . These routing methods are more beneficial for applications involving VANETs. For data transmission, flooding is used within a region or a range. It is also possible to transmit messages without inundation. As parcel overhead is corrupted, it reduces crashes. Geo cast for query distribution in VANET, heading-based Geo cast routing, inter-vehicle, distributed robust geo cast, robust vehicular routing Dynamic Time-stable Geo Cast routing protocol is one of the subroutine protocols included in Geo Cast routing protocols.

4.5 Routing protocol based on Broadcast

This method of routing messages between the vehicles, between the vehicles and the infrastructure, and between the infrastructure and the vehicles is quick. Additionally, a huge system network results in several problems, including excessive bandwidth usage, high packet and crash overhead, which lowers system performance. In order to solve this problem, we used a specific sending strategy. The communication-based routing protocols are required for vector-based tracing recognition, distributed vehicular communication protocols, BROADCOMM, and urban multi-hop communication protocols.

4.6 Infrastructure Based Routing

Infrastructure-based routing refers to RAR and SADV, which are utilised as relays in static network nodes and is an in-clouding routing mechanism that was created primarily for infra-structured networks.

5. VANET SECURITY AND SAFETY

In VANETs, security is more important, and before they can be deployed, they must adhere to a number of tight requirements. User and data authentication, privacy, liability, and secure broadcast transmission are some of these criteria. It is challenging to meet these requirements in highly dynamic and mobile VANETs, but it is crucial since a compromised VANET could lead to the loss of human life. In the age of cyber dangers, security in VANET systems is a difficult problem for scientists to solve. A hacker who creates a performance weakness in the system may be able to intercept or hack the information that is being transmitted from one vehicle to the next. Numerous sorts of attacks, such as position duping, ID deceiving, GPS data stealing, message manipulation, etc., target the network system in vehicular communication. Malicious drivers disrupt the flow of traffic, which results in accidents. The vehicles must therefore employ safety and security features to combat these dangerous scenarios. In this section, we look at the applications for security and safety in VANETs.

5.1 Security Issues in VANETs

A crucial component of the VANET architecture is security authentication. There are a number of challenges to availability that could influence the performance standards for vehicle systems. The following list of often occurring concerns to accessibility is discussed:

Denial Attacks: Vehicles inside or outside the VANET can launch denial-of-service assaults. In these situations, the attackers disrupt services by severing and breaking the main lines of communication between vehicles. However, only authorised clients were able to access the service.

Jamming Attacks: In this attack, the perpetrators use an overpowered signal in the same frequency range to interrupt radio wave channels in the vehicle system. This reduces the message signal quality till the clients' frequency band becomes unstable or separated.

Malware Attacks: Software elements used to implement the RSUs and OBU can be used to deliver the malware (virus) attack into the vehicular system. Malware could stop the vehicle system from being generally useful.

Broadcast Altering Attacks: Genuine users may participate in this assault as insiders and send false security alarm signals to the VANET. To authorised clients, this may include the proper security messages, which may lead to strict mishaps. Additionally, it affects the VANET system's overall performance.

Black hole Attacks: The Black hole attack typically happens when a real VANET client cooperates with outside sources for a variety of reasons. Through this vehicle, a packet is transmitted, but instead of sending the packet to its intended recipients, it silently crashes.

Greedy Behaviour Attacks:In this "greedy behaviour" attack, the MAC layer of IEEE 802.11 is targeted by the perpetrators. In an effort to increase data transmission at the expense of other vehicles, the malicious vehicles purposely handle the MAC protocol incorrectly. The major goal of these attacks is to prohibit other vehicles from using the VANET's support and services. In their hungry nature, malicious drivers also make an effort to reduce the time required to gain access quickly. The wireless medium may experience collision issues as a result, adding to service delays for the actual user.

Spamming Attacks: This kind of attack injects unwanted spam messages. For instance, VANET system advertisements consume bandwidth needlessly and cause volunteer crashes

Movement Analysis Attacks: The traffic analysis attack is not a dynamic attack in the VANET design. Attackers can listen in on data broadcasts in this attack and then examine the frequency and duration of messages being sent. Unwanted users can identify the nature of communication from the study and attempt to gather the most crucial data for their own advantages.

Social Attacks: Drivers become confused and irritated as a result of the attackers' immoral and unprincipled messages. The attacker's primary goal is to make sure that the appropriate vehicle clients react negatively to these kinds of signals, which will affect the way the vehicle drives in the VANET system.

Tunnelling Attack: An example of a wormhole attack is the tunnelling attack. By using a tunnel as a second communication route, the outside wormhole attackers connected two remote elements of the vehicular system in this attack. As a result, system users who are far away can communicate with those who are nearby.

Global Position System (GPS) Issues: The location database is maintained by a GPS satellite, which also holds the geographic location information for each vehicle connected to the VANET. With the aid of a GPS satellite tracking system, an attacker can fabricate misleading readings about the vehicle's location rather than providing accurate information, leading the vehicle to believe it is inaccessible in another area.

Replay Attacks: Replay attacks, also known as playback attacks, occur when accurate information is purposefully or untruthfully retransmitted or delayed to have an unintended effect. The VANET requires a time source with cache memory to compare the most recent messages received with those now being received in order to prevent replay attacks.

Key and/or Certificate Replication: In this instance, the attackers use duplicate keys and vehicle endorsements as a form of validation to raise suspicions, but doing so makes it difficult for TAs to identify a particular vehicle. The purpose of these attacks is to confuse TAs and alarms that confirm vehicle clients in hit-and-run incidents.

Message Altering: In this attack, the attackers modify the messages sent during vehicle-to-vehicle or vehicle-to-infrastructure connection in order to pretend to be sending requests for certain applications or pretending to be receiving responses.

5.2 Security based Challenge in VANET

The following are some of the significant difficulties encountered when implementing safety and security systems in vehicular ad-hoc networks:

Validation: The numerous messages that were transmitted, starting with one protest and continuing with the next, must be confirmed. The central authority must confirm each vehicle in the system.

High Mobility: Due to the vehicle's high mobility, a number of problems, such as disruption problems and handshaking loss, developed as it moved more quickly. As a result, the vehicles are not prepared to work together and establish secure communication.

Area Based Schemes: We can locate other automobiles by using beacon messages. However, handling allows sensors, GPS, and Laser to pinpoint the precise location of the vehicles.

Real Time System: Real-time systems cannot be developed in areas with high mobility. As a result, sending alarm messages to other devices in time for the deadline is a challenging undertaking.

6. VANET SIMULATION

A collection of guidelines for describing arbitrary system topologies using test systems make up the portability model. It performs a few operations and workouts between the vehicles while creating linkages between them. Another adaptable exhibit that organises the vehicles according to their portions is the cluster-based model. It offers unique plans, as seen by the portability on both a small and large scale. The limitation of this model's inefficiency is that it struggles to reproduce complex movement scenarios, as evidenced by its difficulties with scaffolds, passageways, etc.

6.1 VANET Test Systems

Systems that measure viability and heartiness are used to implement VANET. The age of a useful and potent versatility display is the basic element in VANET reproduction. The basic building blocks that join the portability show and the system test system together are perception device, yield, stage, and class. The authors in this section go through numerous activity test systems, different vehicle models, inserted vehicle models, and advanced vehicle versatility models.

6.1.1 Network Simulator

Organize test systems play a significant role in managing and controlling the system components. These are offered on the market as both business and open source options. These tools, which include OMNet++ , OPNET, QualNet, and VANET, are free to use for academic purposes, but a licence is required for more commercial uses. Open source test systems include ns-2, which is mostly utilised in the MANET environment.

6.1.2 *Traffic Simulator*

For mobility analysis of vehicle movement on public roads and expressways, traffic simulators are used. This method is useful for tracking the movement of vehicles. Major traffic simulators for the vehicle activity test include TRANSIM, VISSIM, VANET MobiSim, MOVE, and others. These test platforms are trusted and employed in order to provide precise portability models. The main limitations of movement test systems are that they require more time for planning and transportation, which increases the complexity of the time. End users need a permit in order to use these test systems. Today, a variety of open source development test frameworks, like SUMO (Simulation of Urban Mobility), are available to manage extensive development. Draws generated by SUMO are used by the test systems.

6.1.3 Vehicular Model based on Isolated

The mobility models with no apparent communication with the test systems are isolated based on vehicular models. It is divided into four pieces: increased movement limitations, improved activity generator, enhanced movement requirements, and enhanced movement generator. Legacy portability display is one of the portions.

The legacy portability presentation combines the Gauss-Markov demonstration, the random walk model, and the vehicle following model. It includes tools like the STRAW (Road Irregular Way point) device, the TSM (Movement sign Model), the VANETMobiSim, and others.

6.1.4 Embedded Model

For the most part, the implanted model implies a combination of modules for systems administration and portability. The main tool for providing embedded vehicular mobility demonstrations is Groove Sim. The wander is Groove Net, and the model for showing is GrooveSim. It is anticipated that the urban demonstration simulators will be used to introduce, run, and test routing protocols. Then, Installed VANET engineering focuses on regaining the accurate position of the vehicle hub. A simulator called Auto Mesh, which includes a radio spread piece, driving, and system test system, was also created by for the article. Propelled versatility models, which offer higher system administration services and movement features, are comparable to some other portable models. Additionally, it is divided into open source and commercial models. Along with NS-2 and SUMO, open source network models make up the Trans instrument. After using the notification messages, another project called VGrid is also launched to conduct research on vehicle collisions.

7. CONCLUSIONS AND FUTURE SCOPE

7.1 Conclusions

Due to its security and safety-related and non-security and safety-related services for user satisfaction, Vehicular Ad hoc Network (VANET) is quickly becoming the most challenging and promising research subject in wireless communication systems. In this research study, we looked at the basic uses of the vehicular ad hoc network, as well as its standards, architecture, security difficulties, routing problems, projects, cutting-edge VANET applications, and potential future research topics. Scientists from all over the world are attempting to address the current VANET system problems, such as routing, broadcasting, security, safety, implementation, etc. to expand the VANET system's region.We have covered secure MAC and routing techniques in this paper, which protect messages and vehicles. Due to multiple recent attacks, VANET may soon face significant challenges to operation. Future researchers can learn approaches for vehicular ad-hoc network security thanks to this survey. This essay also includes a description of current projects being undertaken globally, including in the USA, Europe, and Japan. We have also provided comparisons of the systems used to test VANETs, assisting scientists in selecting the optimal system for VANET road situations.We have distilled all security breaches and associated solutions to address security concerns. Researchers will be able to learn more about VANET with the aid of this VANET study.

7.2 Future Scope

As automobiles are growing quickly, automotive innovation is gaining traction. For many uses and forms of safety, this progress system must function. To provide end users with security and safety, several analysts are working in this area. To develop novel tactics and provide services to customers, it is necessary to study a variety of research areas.

Bandwidth:A few plans are needed for managing the amount of information delivered to the system due to the channel's bandwidth. To accurately ascertain the communication needs of vehicular applications and deduce the appropriate parameter tuning of the communication system is a crucial task for the future.

Mobility Model:General mobile ad hoc network mobility models are unable to account for the portability of the VANET architecture; therefore, unique mobility models utilising the activity stream hypothesis must be created. In VANETs, a routing protocol's implementation is highly dependent on the mobility models, driving circumstances, and many truths. In any event, it is required to have a general solution for all VANETs application scenarios or a set assessment standard for routing protocol in VANETs.

MAC Layer:Giving rapid information swaps is a crucial part of MAC layer protocol implementation. The IEEE 802.11p protocol is used in the WAVE standard for wireless communication. The IEEE 1609.3, IEEE 1609.2, IEEE 1609.1, and IEEE 1609.4 are all part of the WAVE series and provide administrations such resource allocation, security, safety applications, and system services. Consequently, a strong and efficient MAC protocol is required.

Simulation:Simulation techniques must be improved because experimental evaluation of VANETs is expensive. Human behaviour models are necessary in order to simulate the impact of VANETs on traffic safety and efficiency because they help us understand how drivers will respond to information provided in advance by VANETs.

Security:Because many applications will have a direct impact on life or death decisions, security is a crucial problem for routing in the VANET system. Accurate data sharing and dissemination in

VANETs is a challenge for routing. The incorporation of security and privacy measures into routing protocols, as well as the priority routes for emergency and safety communications, are further areas that could use improvement.

REFERENCES

[1] RadhaKrishna Karne, Dr TK. "COINV-Chances and Obstacles Interpretation to Carry new approaches in the VANET Communications." *Design Engineering* (2021): 10346-10361.

[2] Karne, RadhaKrishna, et al. "Simulation of ACO for Shortest Path Finding Using NS2." (2021): 12866-12873.

[3] RadhaKrishna Karne, Dr TK. "Review OnVANET Architecture And Applications." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12.4 (2021): 1745-1749

[4] RadhaKrishna Karne, Dr TK. "ROUTING PROTOCOLS IN VEHICULAR ADHOC NETWORKS (VANETs)", International Journal of Early Childhood Special Education (INT-JECS) ISSN: 1308-5581 Vol 14, Issue 03 2022

[5] Karne, Radha Krishna, et al. "GENETIC ALGORITHM FOR WIRELESS SENSOR NETWORKS."

[6] Karne, RadhaKrishna, et al. "Optimization of WSN using Honey Bee Algorithm."

[7] Vaigandla, Karthik Kumar, Radha Krishna Karne, and Allanki Sanyasi Rao. "A Study on IoT Technologies, Standards and Protocols." *IBMRD's Journal of Management & Research* 10.2 (2021): 7-14.

[8] Vaigandla, KarthikKumar, Nilofar Azmi, and RadhaKrishna Karne. "Investigation on Intrusion Detection Systems (IDSs) in IoT." *International Journal* 10.3 (2022).