REAL-TIME TRAFFIC CONTROL WITH COGNITIVE RADIO ENABLED VEHICULAR NETWORKS

Abstract

Wireless communications are expanding their applications globally thanks to cognitive radio (CR). By interacting with the environment, cognitive radio can modify the transmission parameters and confirm the availability of the electromagnetic spectrum. Opportunistically occupying spectral bands while causing the least amount of interference to other users or apps is the aim. In the automotive industry, a recent development is cognitive radio for Vehicular Ad hoc Networks (CRVs or CR-VANETs). Vehicles of the present and the future will be furnished with features that allow for the transmission of intra-vehicular orders and dynamic access to wireless services while the vehicle is moving. The cognitive radio technology and its signal processing implications for the automotive business are discussed in this article.

Keywords: Cognitive Radio, vehicular ad hoc network, vehicular command, LI-FI, WAVE Communication, IoT based CRVENET, Vehicular Cloud Networking, Vehicular Information Network, PIC16F877A, SWaP.

Author

Pranay Ghosh
B. Tech Student
Maulana Abul Kalam Azad University of Technology
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology
Kolkata, India.
tubaighosh967@gmail.com

Riddhi Mitra
B.Tech Student
Maulana Abul Kalam Azad University of Technology
Department of Electronics and Communication Engineering
Guru Nanak Institute of Technology
Kolkata,India.
riddhimitra2703@gmail.com

Dr. Soumik Podder
Assistant Professor
School of Computer Science & Artificial Intelligence
SR University
Hasanparthy, Hanamconda, Warangal
Telangana, India.
scientist.soumik@gmail.com

I. INTRODUCTION

Intelligent cars have been made possible by recent changes in Intelligent Transport System (ITS). The car is now collecting data from the adhoc vehicular environment and exchanging it with other infrastructure, drivers, and Internet of Vehicles (IoV) apps to help with safe driving.

We are going to suggest a dynamic system that will supply the smart solution to the traffic congestion in light of the significant traffic congestion throughout the day's peak periods in addition to during various festival times. If there are any additional routes where cars may be automatically redirected, it will offer an ioptimum path based on the shortest distance.

The environmental pollution level has also been taken into account in this project to build an eco-friendly traffic management system that is optimized. Here, the Air Quality Index (AQI) is used as a criterion to lessen the pollution that is produced as a result of traffic congestion. Now, if the AQI level of one route is high, the cars must turn around and use a different, shorter path to go to their destination.

However, if it looks that the shorter route is congested, we must choose a route that is neither the shortest nor has the least amount of traffic.In such a scenario, fuel economy of cars would decrease and the AQI level along that route will begin to rise, which is a worrying development for an environmentally friendly traffic management system.

By using a spectrum allocation approach, each vehicular node may use the ISM band to send information to a local coordinator about its present location and destination. Central Coordinator (CC) and Local Coordinator (LC) will exchange messages. The central coordinator will offer the optimum route in every way after obtaining information from the other LC.

Another important problem is safety hence an IoT-based smart transportation system has been implemented to address this. This method relies on sensors built into cellphones to collect the essential data from the automobiles. Since the sensors are connected to IoT-enabled devices, appropriate algorithms must be used to analyze the acquired data. Finally, the site of the accident will receive the required assistance based on the computational analysis with a shorter reaction time.

II. COGNITIVE RADIO

A cognitive radio (CR) is a radio that may be dynamically designed and adjusted to utilize the best nearby wireless channels to reduce user interference and congestion. To support more wireless communications in a particular spectrum band at a single place, such a radio automatically discovers available channels in the wireless spectrum and modifies its broadcast or reception characteristics as necessary.

The cognitive engine is able to set radio-system parameters in response to the operator's orders. Waveform, protocol, operating frequency, and networking" are some of these factors. In the communications environment, this performs as an independent unit, sharing environmental data with the networks it accesses and other cognitive radios (CRs). In addition to "reading the radio's outputs," a CR also "monitors its own performance continuously." Using this data, a CR can "determine the RF environment, channel conditions, link performance, etc." and "adjust the radio's settings to deliver the required quality of service subject to an appropriate combination of user requirements, operational limitations, and regulatory constraints.

With opportunistic access, cognitive radio increases the spectral efficiency for the local frequency bands that are accessible. When a spectral opportunity is found, CR keeps an eye on the available spectrum and modifies its transceivers to operate in that frequency range.Users of the spectrum are classified into two categories: primary (or licensed) users and secondary (or cognitive) users. While secondary users lack a grant to transmit and receive in that frequency range, licensed users are permitted to operate in that frequency band.

A cognitive user should keep an eye on the frequency spectrum to see if any authorized users are using it or if there is a spectral opportunity.Spectrum sensing is used by cognitive users to confirm the existence or absence of spectrum gaps. Spectrum holes are described as momentarily underutilized spectrum channels that cognitive users can access when they have the opportunity.

The cognitive user can opportunistically utilize a channel if it is accessible, but when a priority user is present, the CR will not be permitted to use that frequency band.An essential component of a cognitive radio network is spectrum sensing (SS). Observations of increased bandwidth and decreased transmission error rates may be made by keeping an eye on channel occupancy.

Cognitive networks can use a variety of spectrum sensing methods: Additional approaches that enhance spectral identification include energy detection, matched filtering detection, cyclostationary (or feature) detection, and others. Hybrid sensing, which combines two or more spectrum sensing approaches, is another novel approach in recent studies.

III. VEHICULAR Ad Hoc NETWORKS (VANETs)

Wireless network nodes that connect with one another without a central control station or infrastructure network to coordinate the communication are referred to as MANETs (Mobile Ad Hoc Networks). Nodes (or users) are able to receive data supplied by neighbouring devices via wireless transmission in ad hoc mode.

Multihop techniques are used in a MANET to increase the transmission range of the data. Specific networking solutions are favoured by the absence of a coordinating node or a particular architecture. The most popular MANETs1 applications are Wireless Sensor Networks (WSNs) and Vehicular Ad hoc Networks (VANETs), which are used for a variety of purposes including traffic management, environmental monitoring, installations in smart buildings, and military uses.

VANETs are sensor-based networks that can connect to other nodes (or moving vehicles) in a given area and communicate with them.

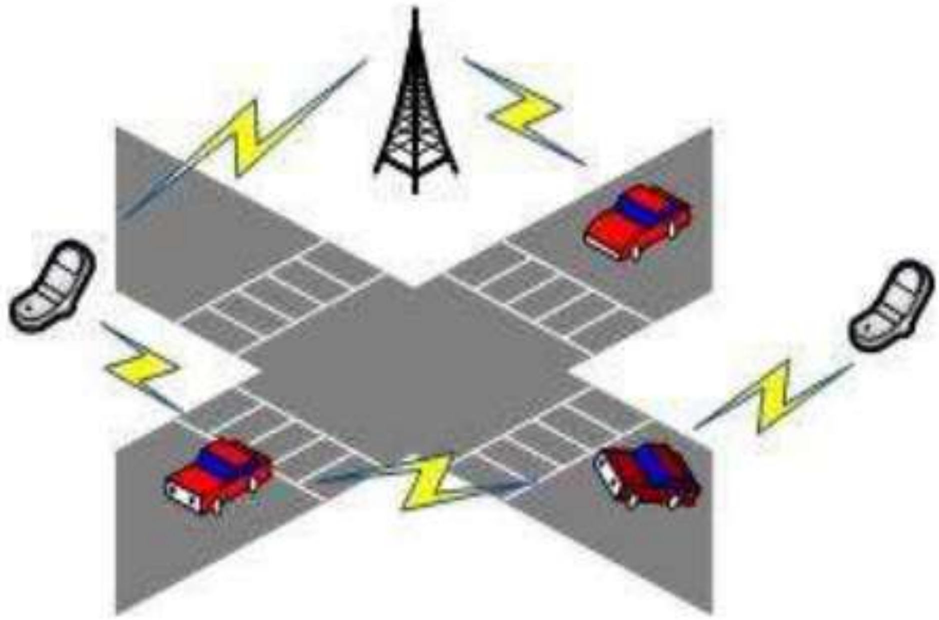

Figure 1: Vehicle-to-Vehicle Links Via Radio Can Enable A High Capacity Communication Network.

Figure 1 illustrates how radio connections between vehicles might provide a large capacity communication network.The advancement of Intelligent Transportation Systems (ITS) and Wireless Access in Vehicle Environment (WAVE)14 has sparked interest in VANETs. By installing transceivers in the cockpits, ITS and WAVE hope to lower traffic jams and accidents.

These systems may also provide non-safety applications (such as entertainment, Internet connectivity, or electronic communications). Any car will be able to update real-time information (such as traffic conditions or weather conditions) and alert other drivers to prevent collisions and accidents thanks to wireless transceivers.

1. **CRAVENET (Cloud Enabled Cognitive Radio Ad hoc Vehicular Networking):** Cloud enabled CRAVENET architecture is a type of computing architecture that enable access of multiple sources on the internet on demand basis. For connecting worldwide companies, it is more appealing. Many businesses all around the world provide cloud computing architecture based solutions that users may access, install, and upgrade as needed. Through the internet, cloud-based businesses provide their customers cost-effective services and server maintenance. Multiple services, including Software as a Service (SaaS), Hardware as a Service (HaaS), and Data as a Service (DaaS), are made possible by the cloud-enabled CRAVENET architecture. These services are combined to form Platform as a Service (PaaS). It is a cutting-edge transportation system technology. Using multi-hop adhoc networking, CR equipped numerous vehicles connect and exchange their gathered data regarding traffic, weather, driver behavior, and street views . Cloud-enabled CRAVENET offers a more effective technique than the conventional method of collecting traffic information from road-side traffic cameras for obtaining real-time data in cars utilizing V2V(Vehicle to Vehicle) communication. The local

CRAVENET cloud network (LCCN), wide CRAVENET cloud network (WCCN), and central CRAVENET cloud network (CCCN) make up this architecture's three parallel cloud networks.

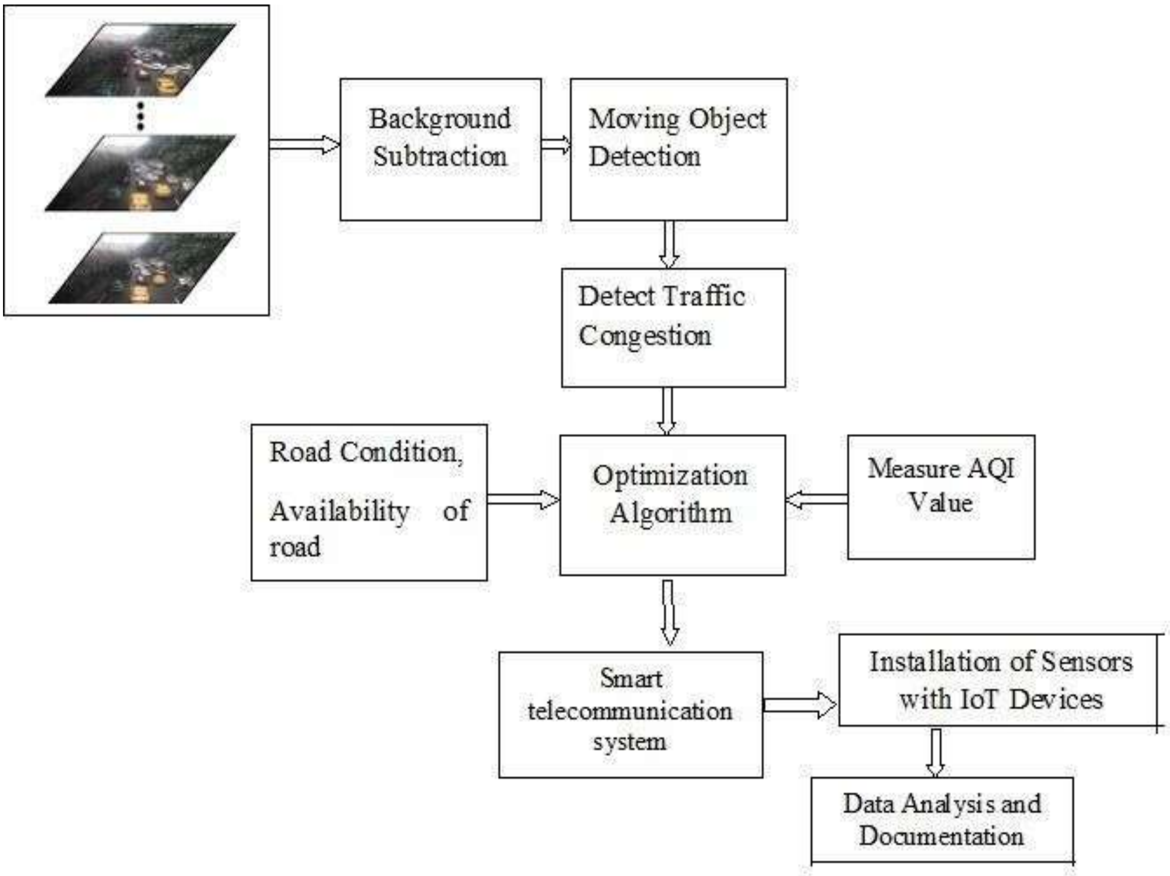

Figure 2: Block Diagram of VANET

- **Local CRAVENET Cloud Network (LCCN):** A few miles away, an LCCN was created between several CRAVENET-capable vehicles. The vehicles in a set create an LCCN by being perceived as moving local cloud positions. They share their computing, storage, and spectrum resources among their local fleet of vehicles, improving resource efficiency. Each vehicle can access cloud services as needed for specific purposes.

- **Wide CRAVENET Cloud Network (WCCN):** A WCCN formed by the internet, Wi-Fi, or dedicated short range communications (DSRC) between a group of LCCN cars. Other CRAVENET cloud networks are connected to specialized LCCN servers. By using V2V communications, a vehicle may reach a cloud site that is inside the CR service region. It is a reliable cloud network with enough of resources that provides cloud services to cars that skip traffic. A vehicle can select a WCCN option for updating, customizing, and sharing big volumes of data related to their system setup.

- **Central CRAVENET Cloud Network (CCCN):** A CCCN created through the internet between a number of WCCN servers. A CCCN is obtained by a vehicle via cellular communications. For detailed calculations and difficult global policy judgments, a CCCN has greater resources. For the provision of cloud services, there are several commercial software platforms available, including Amazon Web Services, Microsoft Azure, IBM, Google Cloud Platform, Salesforce.com, Adobe, Oracle cloud, SAP, Rackspace, and Workday.

The three parallel cloud networks' physical resources are better used thanks to the cloud-enabled CRAVENET design. The CRAVENET cloud network includes the calculation and storage of resource data. All CRAVENET vehicles can retrieve data from all three cloud networks. This design enables all vehicles to correctly retrieve all parallel cloud network layers. Despite this, the design is cutting edge and works with many different wireless communication protocols, including DSRC and long-term evolution (LTE). These three cloud networks can all be rapidly and easily established to support numerous services.

2. **Applications of CRAVENET:** The CRAVENET applications must consider user comfort, safety, and access to local resources.

- The comfort-based program offers warnings for parking availability, no-parking zones, the next toll, traffic congestion, adverse weather, petrol stations, and rest areas.

- An application based on local resources informs users about restaurants, parks, attractions, historical sites, zoos, shopping malls, designer shops, service centers, supermarkets, theaters, fitness centers, book stores, gaming centers, body care facilities, and hospitals based on their interests.

- Safety-based application: It offers Pre-Collision Notifications (PCN), Emergency Notifications (EN), Traffic Aware Notifications (TAN), and Road Hazard Notifications (RHN) in addition to real-time road monitoring services.

The enhancement of driver and passenger safety through the optimization of vehicle-to-vehicle communication is the main goal of VANETs and CRVs. The development of Driving Safety Support Systems (DSSS) aims to improve driver awareness while lowering traffic accidents. Vehicles converse with one another. As well as the infrastructure next to the roads and motorways. international manufactures like Toyota and Nissan creating remedies for new automobiles.

3. **Performance Evaluation of CRAVENET:** We go into simulations and analysis of the suggested system employing the secure IEEE 802.11 protocol in this part. We presume that each vehicle in the CRAVENET-based communication scenario must rely on its own resources to secure communications. Every car in the area must broadcast messages to the other vehicles.

The Basic information is broadcast by each vehicle. Basic information includes the spectrum bands that are available, authenticated user lists, data on how their activity was analyzed, and user traffic at certain geographic locations. Any CRAVENET-authorized vehicle can modify its route using the outcome of the study in order to increase the effectiveness of the communication system and the utilization of the transportation system.

We make the assumption in our simulations that every vehicle is using a unique set of spectrum band channels. We use the fundamental IEEE 802.11 settings for each channel. Basic data rate is 10 Mb/sec, slot time is 25 milliseconds, RTS/ACK size is 120/112 bits, frame header size is 224 bits, preamble size is 48 bits, minimum window size is 31, maximum window size is 1023, packet size is 150 bytes, average time interval is 5 milliseconds, and retry limits are 10. These are the main parameters.Message mutation attacks, sybil attacks, spectrum supply and demand attacks, service message attacks, and acknowledgment message attacks are created in the simulation models at a frequency of six per millisecond and are aimed at the transmission of messages to the end vehicles.

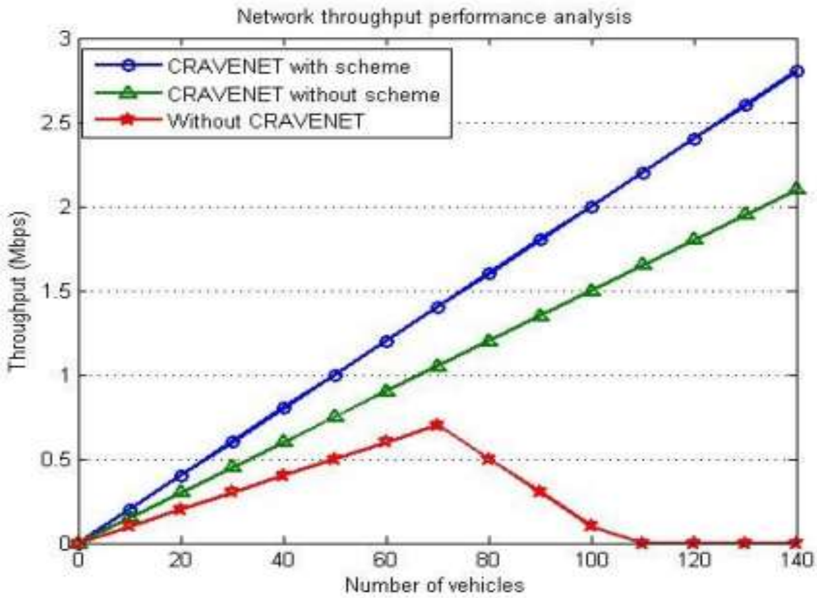

Figure 3: Numbers of Vehicles Vs Network Performance Analysis

The suggested scheme's behavior is displayed in Fig. 3 as network throughput vs the number of cars in the system. As the number of vehicles rises and more are able to effectively deflect assaults, we discover that throughput increases linearly in the CRAVENET system that incorporates the proposed approach. Additionally, we note that CRAVENET without the scheme performs similarly to CRAVENET with the scheme, but is vulnerable to assaults that result in loss of spectrum access, which lowers network performance.Additionally, we see that the network without CRAVENET performs the worst and is subject to the most attacks, with throughput initially increasing linearly as the number of vehicles increases but rapidly decreasing as the number of vehicles increases past a certain point owing to the loss of spectrum access.

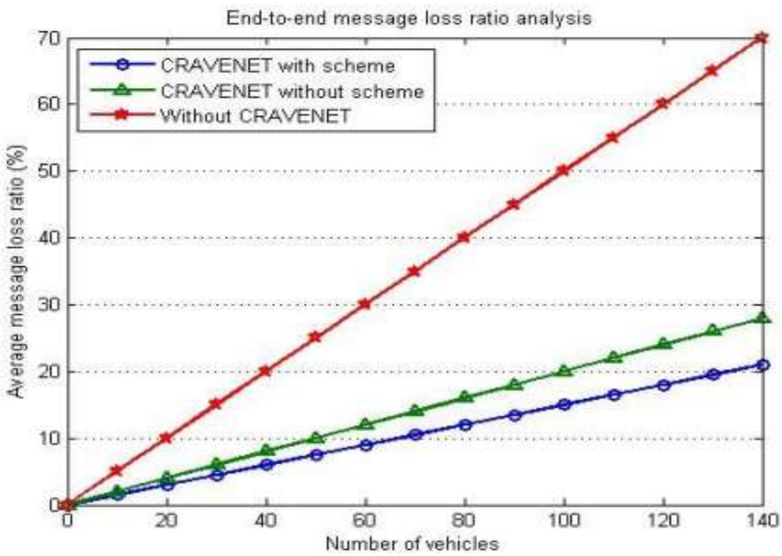

Figure 4: Number of Vehicles Vs End-To-End Message Loss Ratio Analysis

The suggested scheme's study of the number of cars vs end-to-end message latency is displayed in Fig. 4. As the number of cars rises, we see that CRAVENET, which incorporates the suggested strategy, experiences the least increase in message latency and is best suited to successfully prevent assaults.This suggests that the method not only incorporates security and privacy but also sends messages to end users with the lowest possible chance of message loss. We also see that without CRAVENET, if the number of cars rises and is subject to assaults that produces theoutcome in the form of message loss or retransmission due to message delay, the average message latency exponentially grows.

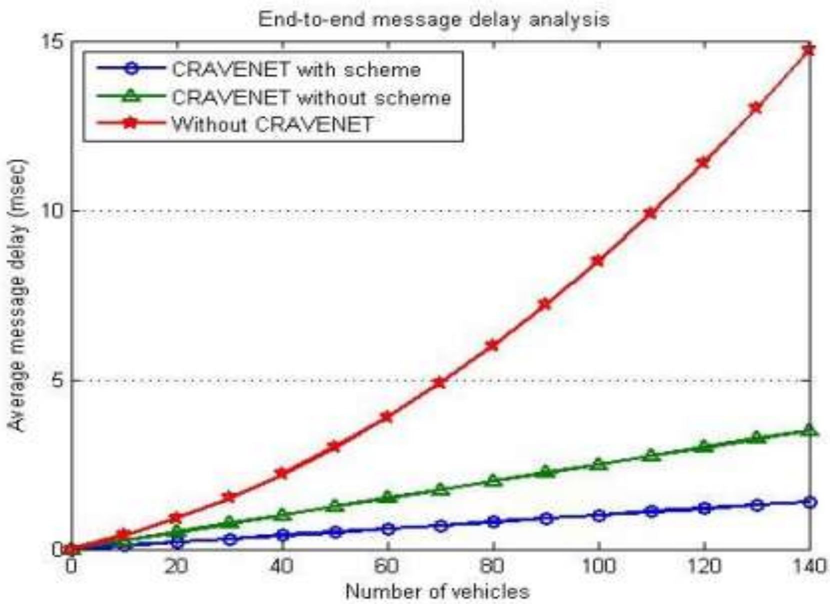

Figure 5: Number of Vehicles Vs End-To-End Message Delay Analysis

Since there are more vehicles within each vehicle's communication range, Fig. 5 demonstrates how the three methods behave in terms of end-to-end message loss ratio. Among the methods simulated in the figure, we note that CRAVENET including the suggested strategy has the lowest message loss ratio and can effectively repel various attacks.The average ratio between the total number of messages received by receiver R per 25 millisecond and the number of messages discarded every 25 millisecond as a result of several assaults is known as the end-to-end message loss ratio.

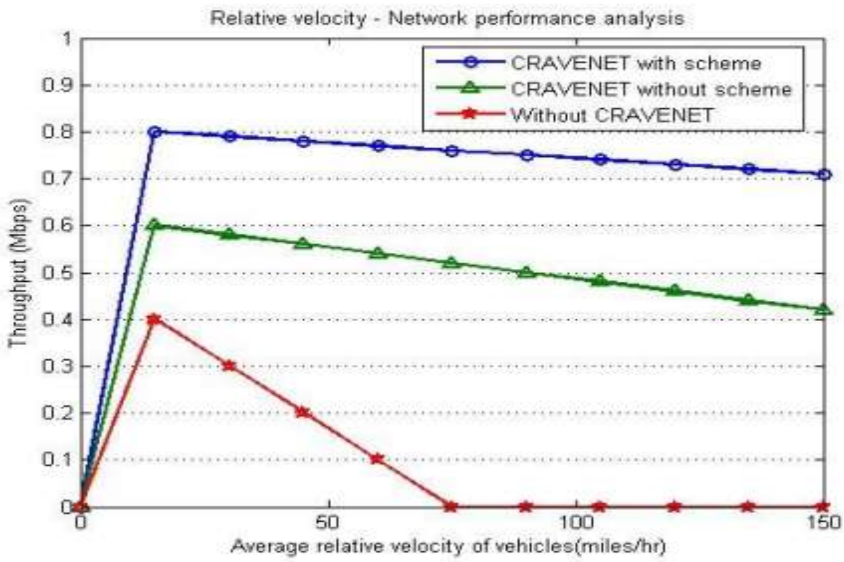

Figure 6: Average Relative Velocity of Vehicles Vs Network Performance Analysis

As the average relative velocity of the vehicles rises, Fig. 6 presents how the schemes behave in terms of network throughput. We note that, among the schemes simulated here, CRAVENET containing the suggested method demonstrates the greatest performance and is able to successfully resist attacks with regard to network throughout as a function of the average relative velocity of vehicles.

This advocates that the suggested plan has widespread support while also offering the right level of security and privacy under a range of traffic flow scenarios.Without the suggested plan, CRAVENET performs poorer and is subject to several assaults that result in message retransmission and loss of spectrum access, lowering network throughout.

In either instance, when the average velocity rises to around 15 mph and then falls, the throughput increases linearly. Once more, the decline is the smallest for the suggested plan.Without the CRAVENET design, the system as a whole progressively degrades and becomes increasingly vulnerable to assaults as the average velocity rises. Only 10% of the throughput is achieved at 60 mph.At around 60 mph, the throughout is roughly 77% and 55% with CRAVENET and with and without the proposed method, respectively.

IV. THE WAVE COMMUNICATION MODEL

IEEE WAVE, a U.S. vehicle communication standard, combines the IEEE 1609 protocol family with 802.11p. The physical layer and lower MAC layer are defined by the IEEE 802.11p standard, which has been incorporated into IEEE Std 802.11-2012, while the top layers are covered by the IEEE 1609 family of standards.

Figure 7: WAVE Communication Protocol

Fig. 7 displays the WAVE communication protocol stack tailored for the vehicle context.Six service channels (SCHs), each with a 10 MHz capacity, and one control channel (CCH) make up the 75 MHz spectrum designated for vehicle communications. In order to operate alternatively on the CCH and one of the six SCHs, the IEEE Std 1609.4-2016 provides an addition to the IEEE Std 802.11-2012 MAC layer.

The channel access time is split into two 50ms repeated intervals that are made up of a CCH interval and a SCH period according to the standard. Single radios may now listen to CCH during CCH intervals and switch to a chosen SCH during SCH intervals thanks to this channel cooperation.The networking services necessary for the functioning of a WAVE system are defined by IEEE Std 1609.3-2016.The protocol supports WAVE Short Message Protocol (WSMP)-based messages that are suited for the driving environment as well as Internet Protocol version 6 (IPv6) traffic. WAVE Short Message (WSM) data and a WSMP header make up WSMP messages. While any of the seven channels may be utilized for WSMP messages, high volume IP traffic carrying data for general application purposes is only allowed on the SCHs. The provider role and user role are the two WAVE device roles that are defined by the IEEE1609.3 standard.

Service providers (SPs) are WAVE devices that deliver data services on one or more channels. The SPs emit WAVE Service Advertisements (WSAs) to signal their readiness for data exchange. WSAs are sent using the WSMP and are included within WSM data. You can send a WSA either secured or insecurely.

Figure 8: WAVE Service Advertisement

In Figure 8, the WSA packet format is depicted.When new WSAs emerge, service users (SUs) who are interested in accessing SP services can allocate the SCHs they include.

V. IoT BASED INTELLIGENT TRANSPORTATION SYSTEM

Internet of Things (IoT)-based Intelligent transportation systems (ITS) are growing in popularity and may be implemented into a smart traffic management system to avoid traffic risks and accidents. Road accidents can have various causes, some of which include driver irresponsibility brought on by sleepiness, drunk driving, over speeding, etc. According to certain research, factors like fog, rain, and strong winds might affect how serious an accident is. Reduced reaction time after an accident may be an efficient way to reduce traffic risks and save priceless lives.

In the past, researchers have employed a variety of strategies to this end, including automatic accident detection, the identification of drunk drivers, the detection of over speeding cars, etc. Data is gathered for each situation, including the number of vehicles in each zone, the speed of vehicles in certain lanes, etc., and choices are then made in accordance with that data. For extracting important characteristics for collision detection models, data from different sensors and event logs is used. To find accidents, several sophisticated computational models are employed.

The suggested Systems emphasized performing preventive actions in addition to accident detection, such as limiting speed, verifying driver identification, etc. The approach suggests analyzing the data utilizing cellphones' pressure and vibration sensors, GPS, and GSM along with the appropriate machine learning algorithms.

The procedure of detecting the parameters, corresponding with wireless IoT protocols, and logging in the cloud platform is demonstrated in Figure 9. All of the sensors in this instance are serving as IoT network nodes.Different wireless protocols are applied for communication in the Wireless IoT. These technologies are Bluetooth Low Energy (BLE), LoRaWAN, Near Field Communication (NFC), ZigBee, 6LoWPAN, and Z-Wave. One of them is the Low Power Long Range Wide Area Network (LoRaWAN), which has sufficient capacity and communication range while using less power and spending little money. It provides fundamental IoT needs like mobile access, secure communication, etc. This makes it a viable IoT communication protocol.

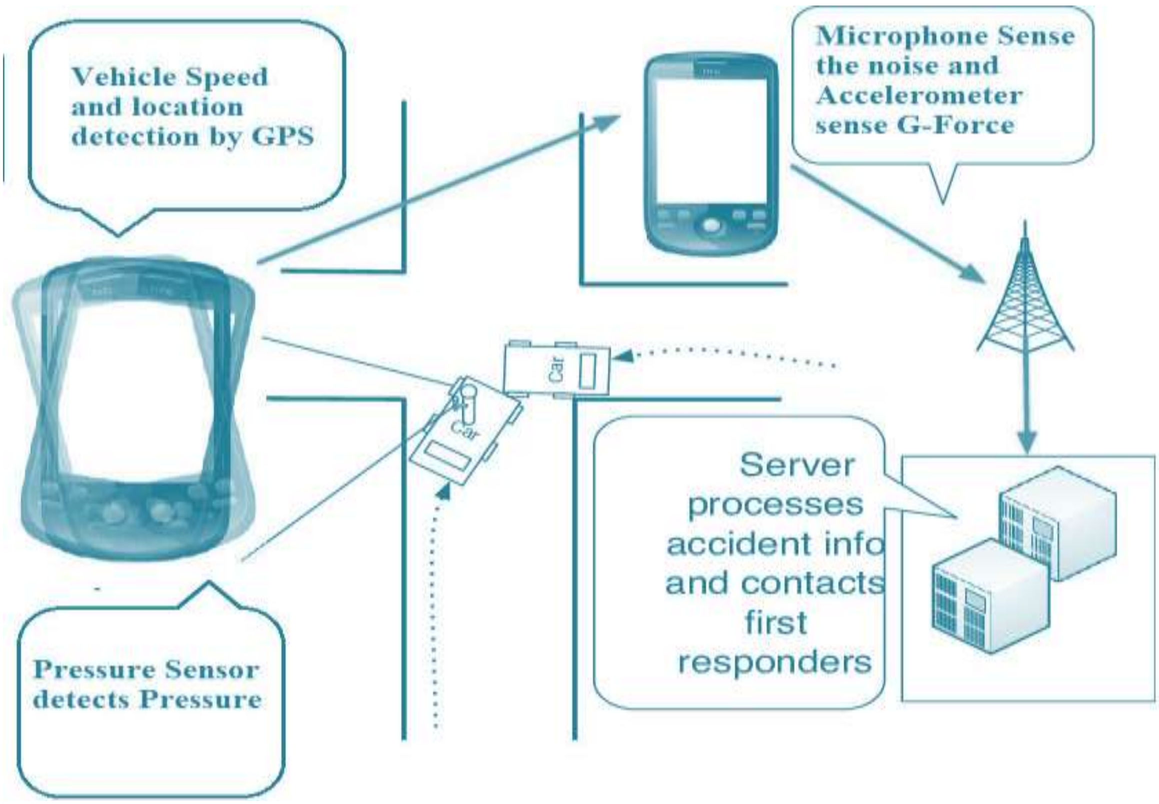

Figure 9: Method of Detection of Accidents on The Street

VI. VEHICULAR CLOUD NETWORKING

Architecture And Design Principles Numerous research projects have been focused on vehicular adhoc networks (VANETs) during the last few decades, including everything from physical layer communications to networking issues in the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) modes. With the development of technology, VANETs offer convenience and safety to drivers and passengers, as well as new uses for entertainment and environmental monitoring. With new paradigms, vehicular communication is set to change.

1. **Emerging Applications on Wheels:** Applications for in-car communications have included everything from convenience and safety to entertainment and business services. Three standout traits seen in developing VANET applications are covered in this subsection. Application content validity in time and place Vehicles generate a lot of content while also consuming it. Thus, they are transformed into rich data "presumptive." These materials have a number of characteristics, including explicit lifespan, local interest, and local relevance and validity. Local validity suggests that consumer-utilitarian vehicle-generated content has a distinct geographical reach.

   The development is being driven by the fundamental qualities of VANET contents and how VANET applications use the contents.The fact that a speed-warning sign at a sharp bend is only valid for incoming cars, say during the explicit lifespan, in safety applications, for example, underscores the reality that vehicle content has its own temporal scope of validity. This implies that the material must be accessible for the duration of its existence. For instance, while a roadwork notice is good until the task is complete, information about traffic congestion may only be valid for a short period of time. Local interest suggests that the majority of likely content consumers are local cars.In order to differentiate between the range of consumers, this notion is further expanded. For instance, all of the nearby automobiles are interested in receiving safety alerts, while only a small percentage are interested in commercial adverts.

2. **Content-Centric Distribution:** Applications for vehicles are more concerned with the content itself than with where it came from. VANETs have this memoryless quality as a defining feature. When using the fixed Internet, one goes to a preferred service site to assess the level of traffic. In other words, the explicit site's URL ensures access to a wealth of trustworthy information. Vehicle apps, in contrast, send out a flood of inquiry messages to a local region rather than to a single vehicle and accept replies regardless of who sent the material.In actuality, the answer can come from a nearby car that has, in turn, indirectly obtained such traffic information from nearby vehicles. Whoever began the transmission in this instance is irrelevant to the vehicle. This trait is primarily brought on by the fact that the information sources (vehicles) are mobile and dispersed geographically.

3. **Vehicle Collaboration Sharing Sensory Data:** Emerging car applications collaboratively utilize a significant quantity of sensor data. That is, a variety of physical occurrences are captured by several sensors that are put on cars. Such sensor recordings are gathered by car apps, even from nearby vehicles, to create value-added services. For instance, with Mob Eyes, automobiles employ a limited number of sensors (such as a video camera) to capture all surrounding occurrences while driving, such as auto accidents. Then, as part of their inquiry, Internet agents and/or mobile agents (like the police) search the vehicular network for witnesses.Using the Car Speak application, a car may access nearby vehicles' sensors in the same way that it can access its own. Then, without knowing who made what, the car uses the sensor data to execute an autonomous driving program.

4. **Vehicular Cloud Computing:** Vehicle contents are produced locally by nearby vehicles and sensors. The nearby residents store, seek, process, and consume these materials over the course of their lifespan. In order to take these factors into consideration, Gela has unveiled a brand-new computing a paradigm called vehicular cloud computing (VCC). A variation of mobile cloud computing (MCC), known as VCC, starts with a traditional cloud computing concept. The Internet cloud provides network connectivity for both accessing limitless computer resources on the Internet and storing/downloading stuff to/from the Internet to mobile nodes with restricted resources.

   However, it is too expensive and time-consuming to upload all material to the Internet cloud and to search for and retrieve useful stuff from the cloud. In addition, most of the data collected by automobiles is only relevant locally and therefore best retained locally. The majority of driver inquiries in VCC are about our immediate surroundings (i.e., local relevance), and automobiles are the finest sensors of this setting. VCC uses a self-organized model of the local environment to answer the inquiries.In other words, cars act as a sort of cloud where services are created, managed, and used. VCC builds a cloud utilizing the collection of computing resources from cars, with the primary goal of enhancing the capability of interactions among vehicles, in order to implement the model by leveraging the growing processing and storage capacity of vehicles.

5. **Vehicular Cloud Networking:** New VANET applications and services require both computing and networking models, which are effectively provided by VCC and ICN, respectively. This makes combining VCC and ICN the best option, and we call this notion vehicular cloud networking (VCN).

6. **Information-Centric Networking:** ICN was once envisioned as an all-encompassing communication infrastructure to facilitate effective content delivery via the Internet. ICN prioritizes what (content) above where (host). This is done in order to satisfy the main needs of both publishers and consumers, who are simply interested in the information itself and aren't concerned about where it came from. In order to do this, incuses uses node or data properties (such as content name, geolocation, or context) rather than a specific node address (i.e., IP address) to route traffic.As a result, the material is separated from the publishers. In this view, ICN types can be categorized as content-based routing, geo-routing. Data-oriented network architecture (DONA), named data networking (NDN), publish-subscribe Internet routing paradigm (PSIRP), and a network of information (Netting) are a few of the newly suggested architecture ideas in the context of the Internet.

VII. NECESSITIES OF VEHICULAR INFORMATION NETWORK AND APPLICATION SCENARIOS

There are more than 1 billion automobiles and moveable devices worldwide. In addition, there are a billion "things" linked to the Internet, a large fraction of which will be automobiles. The adequacy of the supporting transportation and communication frameworksin addition to the application design methodologies will be put to the test as cars and the gadgets carried by their occupants and drivers become more Internet-linked and run more sophisticated apps.

The vehicle information network is a component of a developing ecosystem of human-centric sensing applications that leverage crowdsourced data collecting on a small- and large-scale in communities. The growth of cost efficient,superior-performance sensor devices has driven this type of information ecology.

These include active RF identification devices (RFIDs), smart residential wireless power meters, in-vehicle GPS units, sensor-enhanced entertainment platforms (like Wii-fit), and activity-monitoring sportswear (like the Nike + iPod system), which are now available to regular consumers. Today, the growing applications' information ecosystem analyzes and distills the many data kinds produced by the abundance of devices into information that may be used. In the case of the vehicular information network, the data that is typically collected includes GPS trajectories to keep an eye on traffic flow, pollution traces to assess environmental impact, measures of vehicle fuel efficiency to identify routes that use less fuel, pollution measures to evaluate the effects on the environment, and health information to track the physical health of the driver or passenger.. Vehicles are being developed which are capable of communicating with more of the said applications and to enable smooth integration with additional information devices (such as GPS, sensors, and MRs). When on the road, vehicles and drivers can utilize this information. Vehicles are also capable of publishing the data they feel around them, including images and movies.

High-precision travel estimation, avoiding pollution hotspots, and/or providing time-varying road feature and hazard notification are all features of route planning and turn-by-turn navigation that incorporate traffic congestion detection. These features also maximize use of road while lessening risk. For the benefit of the owners of the cars, manufacturers now have private access to billions of data points thanks to programs for predictive vehicle maintenance. The manufacturer can access data gathered by in-car sensors to give the vehicle with real-time maintenance assistance.

It is possible to provide local/microenvironment data on air quality or civic and cultural activities.

Applications for emergency response can leverage data from automobiles to help during emergencies or after accidents. When a crisis strikes, these technologies may be used to trace missing persons using tracking data, monitor passenger health using medical information, identify possible accident risks, and send out timely alarm messages that are pertinent to the situation.

In light of these developments, we must create a revolutionary vehicular information network design that can accommodate increased vehicle mobility and efficiently handle a large volume of information items.

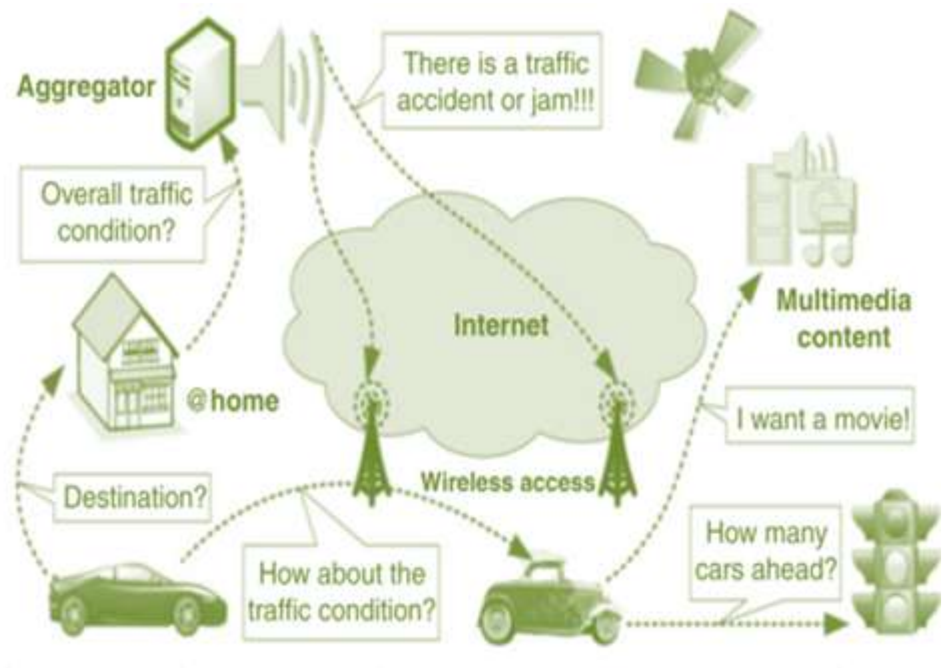

Figure 10: Vehicular Information Network Infrastructure based on Named Data Networking (NDN)

Figure 10 depicts a few example potential application scenarios for the automobile information network. The car has sensors to gather weather and temperature data, GPS to determine its recent location and time, and MR to enable Internet connection, particularly for passengers short of Internet access capabilities.Vehicles can communicate with other neighboring vehicles ad hoc or through the communication set-up to obtain or transmit traffic, street condition information, or multimedia data. Vehicles can propagate sensed data or multimedia data using the network using push- or pull-based techniques.

Data is gathered and processed using an aggregator (like a server), which is also used to deliver processed data to further vehicles on demand. The goal of this task is to create a novel network architecture that supports high mobility, ad hoc networking, and communication systems to back the various application scenarios previously presented, based on the aforementioned communication necessities for the vehicular information network. We pay special attention to how to make it possible for many devices to communicate in the automotive environment.

VIII. NATIONAL & INTERNATIONALSCENARIO OF THE OFFERED SCHEME

Road congestion has emerged as one of the most aggravating issues in recent years, negatively affecting road securityin addition to costing money, time, and fuel. For the avoidance of congestion, for traffic planning, and for the decision-making by traffic control systems, accurate and quick detection of traffic congestion is crucial. There are essentially two unlike strategies for traffic detection. The first is built around stationary equipment, and the second around floating vehicles. For fixed equipment, cameras are the primary tool for spotting traffic jams.The second technique uses a mobile device or a global positioning system to identify traffic bottlenecks. This second approach has the advantage of being able to cover a bigger region. However, this method's accuracy in heavily populated metropolitan regions is relatively poor. Kalman filter and Hungary algorithm-based and IOT-based recent efforts on traffic congestion detection are two examples.

Traffic congestion has emerged as a severe problem in most major cities due to the quick growth in the number of automobiles. It is anticipated that route planning using real-time traffic information would be a successful solution to resolve such a predicament. The two main kinds of existing path planning systems based on vehicular ad hoc networks (VANETs) are infrastructure-less systems and infrastructure-based systems. The only elements in the former that self-organize in a dispersed fashion are the cars.As a result, each vehicle autonomously chooses the projected quickest way after gathering traffic data through interactions with others. When compared to the latter, the traffic data across with the potential assistance of additional tools or infrastructure (such as cellular base stations (BSs)), the entire network is aggregated into a single server.

However, given the dynamicThe model-based and reinforcement learning-based models struggle to make wise judgements under complicated traffic circumstances. In the vehicular cloud network, an intelligent virtual network functions selection technique that utilizes deep neural networks to separate service behaviors has recently gained favor.It proposes a multiagent recurrent deep deterministic policy gradient method for traffic light management in land traffic. Each agent makes decisions on their own, evading the low performance brought on by an unsteady environment. To reduce network congestion, the software defined network (SDN) architecture and coupled cache, network, and compute resource optimization are proposed for IoT-based vehicle network topology.

Different methods were previously deployed for this necessity by researchers to give safety measures on the road, such as automatic accident detection, recognizing drunk drivers, cars traveling at excessive speeds, etc.VANET (Vehicular Ad-hoc Network), in which every moving vehicle functions as a node, can be used in this situation. The alarm signals are conveyed through RF (Radio Frequency) module in the event of an accident. Another method employs limit switches to detect accidents, GSM (Global System for Mobile Communications) is used to send alarm messages, and a GPS (Global Positioning System) module is used to track the accident's position.Another option is to use an android app on a smartphone to detect car collisions.

These systems use accelerometer sensors to assess tilt angle change, GPS receivers to calculate speed, and inform users when an accident is detected. Because saving lives is the ultimate aim, some systems place a strong emphasis on prevention. This technology specifically monitors for drowsiness in the driver and prioritizes the safety of two-wheelers.

One method makes advantage of the accelerometer sensor by keeping track of the vehicle speed and reporting an accident as soon as it drops below the threshold. Another strategy involves fitting alcohol sensors to the steering wheel and forbidding drunk drivers from operating a vehicle by monitoring the amount of alcohol in their bloodstream.

A system that employs a helmet as an equipment for accident detection and reporting has been proposed for two-wheelers. The system is constructed using sensors, CPUs, and cloud computing infrastructure. Using a cloud-based service, information about accidents is provided to the emergency contacts. Vehicle position is tracked using GPS. The helmet has a tri-axial accelerometer, a microprocessor, and a GPS. By continually tracking the location of the helmet and head's direction, the likelihood of an accident is determined.Pre-trained surveillance cameras placed on roadways can also find accidents.

IX. ADVANTAGES OF COGNITIVERADIOENABLEDVEHICULARNETWORKS

So far it is clearly understandable that the Cognitive Enabled Vehicular Network is very helpful in the traffic networking now a days. There are so many advantages in CRVANET. Some are like-

1. **Overcome Radio Spectrum Scarcity:** Cognitive radio enabled vehicular network may transmit on unoccupied radio spectrum while still avoiding interference with the primary licensee's operation by detecting spectrum use (regardless of channel allotment).

2. **Avoid Intentional Radio Jamming Scenarios:** Cognitive radios enabled vehicular network can avoid jamming by proactively and dynamically switching to higher quality channels by detecting channel availability and even anticipating the jammer's strategies.

3. **Switch to Power Saving Protocol:** Cognitive radio enabled vehicular network preserve power when slower data rates are sufficient by switching to protocols that trade off reduced power consumption for lesser bandwidth.
4. **Improve Satellite Communication:** Cognitive radio enabled vehicular network boost communication quality at crucial times and places by anticipating rain fading and adjusting transmitters and receivers for the best bandwidth.

5. **Improves Quality Of Service(QOS):** Cognitive radio enabled vehicular network can choose frequency channels with a greater Signal to Noise Ratio (SNR) by detecting ambient and unintentional man-made radio interferences.

X. DISADVANTAGES OF COGNITIVERADIO ENABLE DVEHICULAR NETWORKS

So far we can comprehendthe the Cognitive Radio Enabled Vehicular Network is very helpful and also a advanced technology but there are various disadvantages as well. The disadvantages are as follows:

- No process is entirely automated, and all adjustments must be carried out with user involvement.
- It always requires multi band antenna.
- Compared to conventional wireless networks, cognitive radio technology providesbetterprospects for attackers. Without warning, the data might be changed or intercepted. The enemies may have clogged or misused the channel.
- QoS (Quality of Service) in Cognitive radio is affected due to its adverse effects.
- Translation of observations into actions is a big test in cognitive radio.

XI. EMERGENCY TRAFFIC MANAGEMENT DEPLOYING LI-FI TECHNOLOGY

1. **Introduction to Li-Fi:** Li-Fi is the abbreviation for Light Fidelity. It is a quick pace, wireless communication technique that deploys light in visible region of electromagnetic spectrum. The word Li-Fi was first devised by Professor Harald Haas at the University of Edinburgh in his TED Talks on Visible Light Communication. It is one of the optical wireless communication techniques where data communication takes place with the aid of LED bulbs whose intensity fluctuates.Digital communication occurs based on this fluctuation.

2. **Working Principle of Li-Fi:** In Li-Fi, the digital datais conveyed using LED bulbs with flickering intensity controlled by fluctuating currents. There is alight emitter or LEDat one end. On switching the LED on, a digital ‘1’ is conveyed and on switching the LED off, a digital ‘0’ is transferred. This is received by a photo detector at the other end that detects the variations of the LED light and converts light photons into an electrical signal. The receiver device will receive the data after it is processed, amplified and converted back to its original format.

3. **Modulation Techniques of Li-Fi:** Diverse modulation methods are applied to transfer data using Li-Fi. Some of them are: ON-OFF keying (OOK), Pulse Amplitude modulation (PAM), Pulse Position Modulation (PPM), Orthogonal Frequency Division Multiplexing (OFDM), Color-Shift Keying (CSK).

4. **Application of Li-Fi In Traffic Management:** Li-Fi can be utilized in developing the Vehicle to Vehicle (V2V) communication. Li-Fi is beneficial since it connects a very big area with more network security and better data rates. Various Emergency vehicles like Ambulances, Fire-fighting trucks, Police cars, and other vehicles can implement Li-Fi to travel at a greater pace through the congested roads using this V2V Communication. A vehicle's headlight and tail light vehicle is designed in form of Li-Fi transmitter and receiver respectively. On activating the traffic signal, the system will receive a notification about the emergency vehicle and the traffic signal would instantly turn green.

5. Block Diagram: There are 3 main nodes

- Ambulance (Emergency Vehicle)
- Non-Emergency Vehicle/s
- Traffic Signal Control

Figure 11 represents the 3 main nodes as a block Diagram.

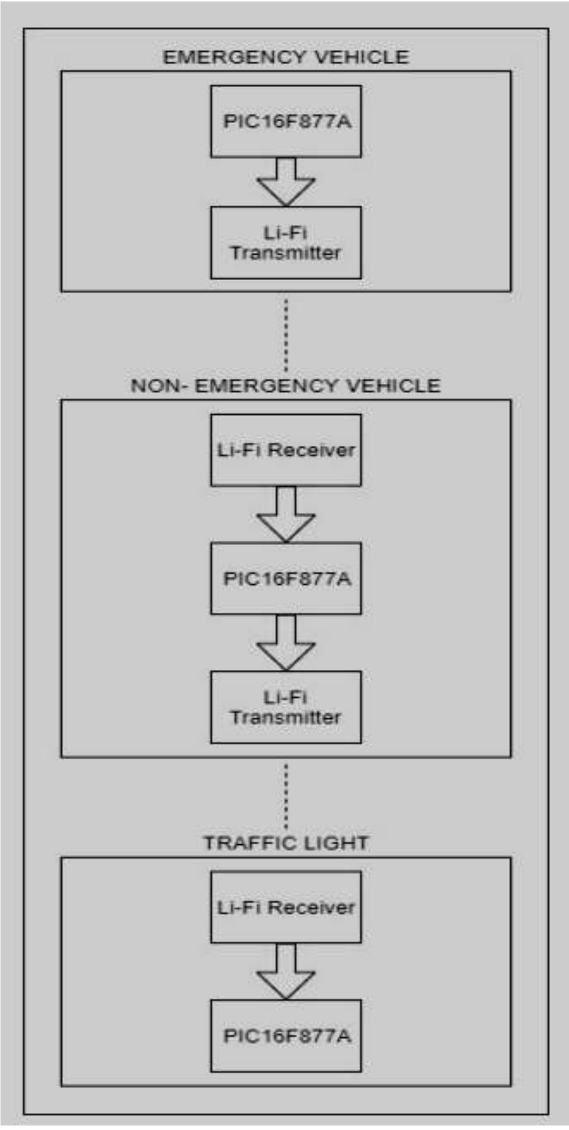

Figure 11: Block Diagram of Traffic Control using Li-Fi

6. Implementation of Li-Fi in Traffic Management: Let's imagine a situation as shown in Figure 12, where an emergency vehicle has come into a lane that has a large number of non-emergency vehicles ahead of it in a busy lane. Additionally, the lane's traffic signal is red. The emergency vehicle' siren is the only method to signal its presence in a lane with heavy traffic under the current arrangement. The light for the street will only turn green if the siren is audible to the traffic signal operator. This procedure is cumbersome and ineffective.

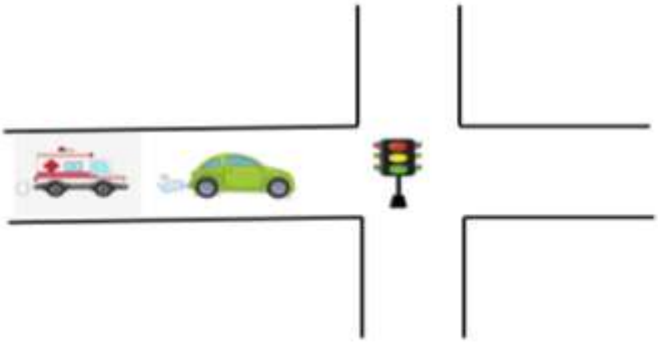

Figure 12: Pictorial Illustration of the Scenario

A Li-Fi transmitter is installed in the emergency vehicle and used in conjunction with the headlight. Itemits a warning signal like "EMERGENCY" when it enters a busy traffic lane. The alertnotification will be picked up by the non-emergency car's transceiver if there is a non-emergency ahead of it. The driver of the non-emergency vehicle will be notified via the in-car infotainment system when the alert notification is received. It will simultaneously communicate the alarm message to the traffic signal control or, if a car is ahead of it, to that vehicle. Upon receiving the alarm message, the signal control will become green.

Any number of automobiles can be crossed before the alert notification reaches the traffic signal control. As a result, the alert notification will quickly arrive at the traffic signal control, regardless of how long the traffic jam lasts.

7. **Components of The Li-Fi Based Traffic Control System:** The Ambulance contains a PIC microcontroller and a Li-Fi transmitter. The non-emergency vehicle containsaPIC microcontroller accompanied by a Li-Fi transceiver and the traffic light control consists of a PIC microcontroller with a Li-Fi receiver. The Li-Fi transmitter for the non-emergency vehicle and ambulance can be employed using the vehicle's headlights and the Li-Fi receiver can be attached anywhere near the vehicle tail lights.

   - **PIC16F877A:** An LED and a photodiode are utilized to construct a Li-Fi transceiver unit utilizing the PIC16F877A as shown in Figure 13. It is a cheap, energy-efficient microcontroller. It comprises a UART module that can support baud rates of up to 57.6 kbps.

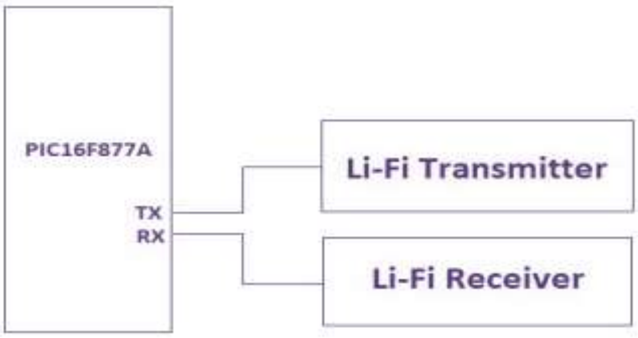

Figure 13: Li-Fi Transceiver Block Diagram Using PIC16F877A

- **Li-Fi Transmitter:** In the CE configuration, a BC547 NPN transistor serves in form of a current amplifier. Depending on the LED light that needs to be driven, several current amplification circuits or signal power amplifying circuits can be employed. A 2.4 kbps data stream is applied to regulate the intensity of the LED bulb using the N-channel power MOSFET STP55NF06. The 'Tx' pin of the Li-Fi transmitter unit is linked to the UART transmitter pin of the PIC16F877A. By linking it to the circuit (as shown in Figure 14), any LED-based headlight that is currently on the market, can be converted into a Li-Fi transmitter.

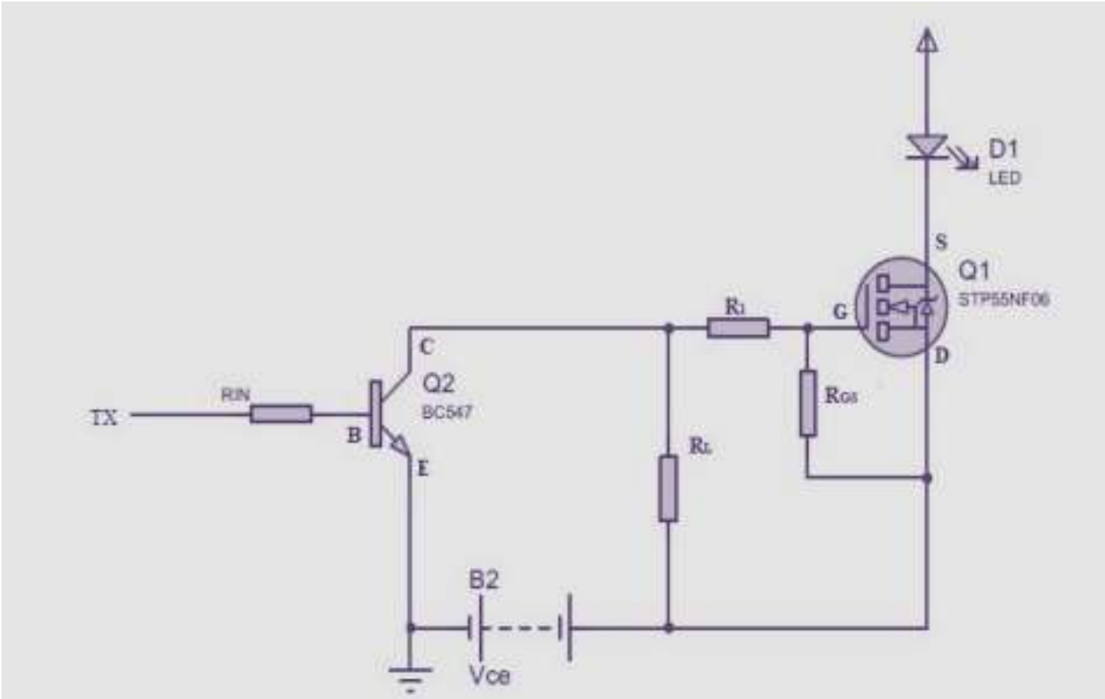

Figure 14: Li-Fi Transmitter Module's Circuit Diagram

- **Li-Fi Receiver:** The receiver circuit is shown in Figure 15 which includes a photodiode, operational amplifier LM358N, a potentiometer, and resistors. The potentiometer is linked to the op-amp's inverting terminal, and the output of the photodiode is attached to its non-inverting terminal. The op-amp will either establish the output to the maximum positive voltage or maximum negative voltage depending on how the input voltage from the photodiode compares to the reference voltage set using the potentiometer. The op-amp distinguishes between logic 1 and logic 0 of the propagated bit stream in this manner.

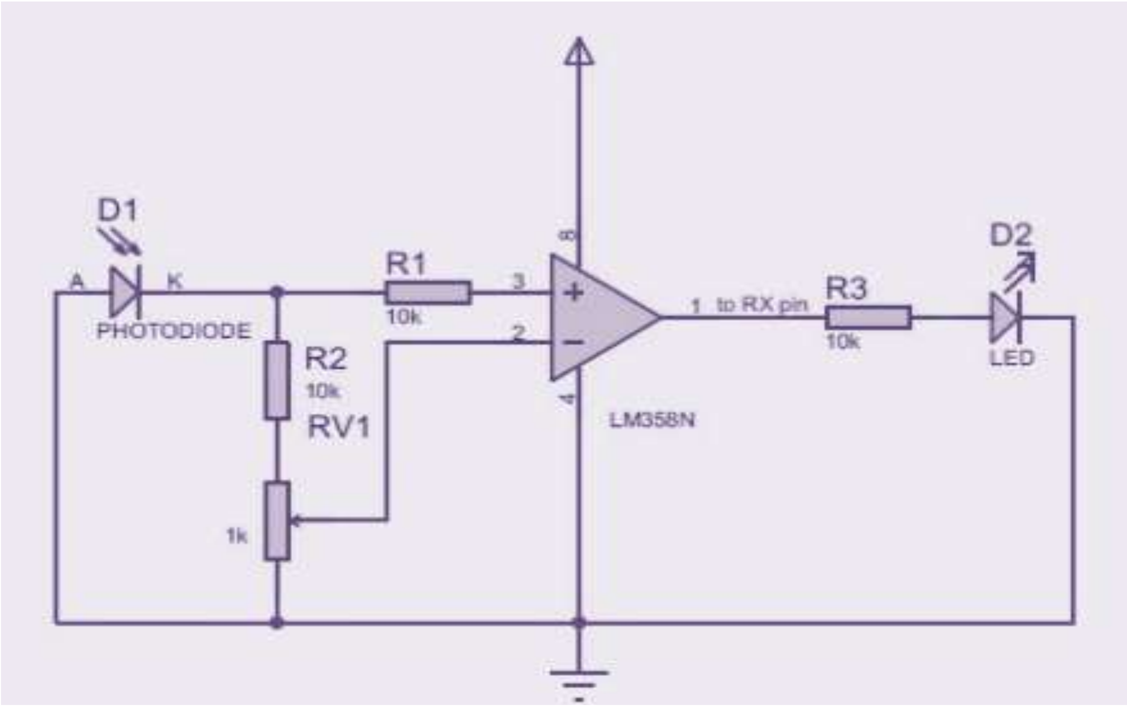

Figure 15: Li-Fi Receiver Module's Circuit Diagram

8. **Advantages Of Li-Fi Based Traffic Management:** The numerous benefits of Li-Fi based Traffic Management are listed below

- Li-Fi employs the visible light spectrum, which ismuchgreater than the radio spectrum, for communication.
- Any vehicle's LED headlights and taillights can be applied in this system to transmit and receive data. So, in this case, availability is not a problem.
- Any LED bulb might be converted for affordable prices to function as a Li-Fi module. Hence, it is cost effective.
- Visible light spectrum, which is what Li-Fi uses, has no negative health impacts on human body. Hence it is absolutely safe to use.

9. **Disadvantages of Li-Fi Based Traffic Management**: Despite its advantageous nature, there exist some barriers which requires to be overcome for a smooth communication.

- Functioning of Li-Fi needs the headlights and taillights of the car to be always be ON, even during the day.
- If both the transmitter and receiver are in Line of Sight, Li-Fi operates effectively. Any departure from this stance may result in miscommunication.
- Intense sunshine during daytime may obstruct Li-Fi communication. Additionally, other light sources like regular light bulbs could stop the communication.

XII. SECURITY ISSUES IN CRAVENET

CRAVENET is subject to a number of security attacks. In this study, we describe nine distinct types of assaults that aim to disrupt message transmission to the final vehicle.

1. **Active Level Attack:** This attack comes into action when an attacker alters the existing active population of CR users in a certain area, which may impact the supply requirements of spectrum bands and lead a user astray.

2. **Acknowledgment Message Attack:** This attack occurs when an existing acknowledgement message is modified right before delivery. There is no such defense against acknowledgement messages in basic 802.11 security. An assault like this might make the CR user confused and keep them from obtaining important data.

3. **Message Modeling Attack:** This assault comes into action when a perpetrator sends a CR user misleading information.

4. **Message Mutation Attack:** This attack takes place when an attacker modifies an already existing message, which may cause a delay in message delivery to the target and may lead the final CR user astray.

5. **Message Voiding Attack:** This attack comes into action when an attacker removes a specific message packet that contains important information or a warning before the information is delivered to the final user. It could influence a driver's choice, which might result in amishap.

6. **Service Message Attack:** This assault takes place when the attacker seizes control of the CRAVENET communication channel utilized by the end vehicle, which might result in the final driver being engaged in adisaster. This issue could be resolved by the CR device on the car with secured ID functioning at random numerous frequency bands.

7. **Spectrum Demand Attack**: When an attacker modifies an existing demand for spectrum bands, it results in an attack that might cause a delay in the scanning of spectrum bands and end-user communication.

8. **Spectrum Supply Attack:** This attack takes place when an attacker modifies a list of currently accessible spectrum bands, which might cause a delay in establishing communication.

9. **Sybil Attack:** This attack occursif a hacker creates several pseudonymous identities on CRAVENET to fabricate identities and undermine the reliability of CRAVENET operation. The invader can persuade the real users to choose a different route by creating the fake scenario whereby there are more CR users on the road than in reality and that there are no more available spectrum bands for communication.

XIII. SECURITY GOALS OF COGNITIVE RADIO ENABLED VEHICULAR NETWORK

1. **Vehicle Privacy:** Users' information, including the identity of the vehicle and its position, is released during vehicular communication. Unregistered automobiles can be tracked, which poses a threat to the privacy of the vehicle.Pseudonyms are utilized to defend against invasions of privacy. Pseudonyms have been the subject of multiple publications in presenttime that have both guaranteed vehicle privacy and addressed various

techniques to preserve users' conditional privacy.Pseudonyms can preserve the privacy of the car. However, it suffers when there is a dearth of confidence among cloud members.

2. **Trustworthiness between Vc Members:** To provide protected communication in the VC, the confidence between vehicles is crucial. -Vehicles work together to do a variety of activities that are necessary to assess how reliable they are**.**

3. **Data Security**: The vehicular cloud provides a practical way to accommodate the computing and storage abilities of the vehicles. Cars are able to access and keep data on other cars if they do not take security considerations into account data must be encrypted in order to prevent illegal access.

4. **Certificate Revocation**: A strong strategy that can shield data from attackers or fraudulent input is certificate revocation. The authority cancelled the certificate when an invader certificate was found. The certificate revocation list (CRL), which manages the list of revoked certificates and instantly broadcasts the CRL across cars, is crucial to the vehicular network.

XIV. XIV.SECURITY MECHANISMS OF COGNITIVE RADIO ENABLED VEHICULAR NETWORK

The security of passengers and drivers depends critically on the safety of CRAVANETs. To achieve the safety level, major algorithms must be designed. The following are the security mechanisms:

1. **Availability:** Because it ensures that the network continues to function in the face of hostile and malfunctioning situations, availability is essential to the safety of the CRAVANET. Comparing with other security services, we can say that availability is more susceptible to harmful assaults. Therefore, CRAVANETs may be protected against these threats using trust-based and cryptographic measures.

2. **Confidentiality:** Data privacypromises that only the chosen user has access to the data, and that third parties are incapable of accessing any sensitive information relating to the chosen user.

3. **Authentication:** By shielding the CRAVANET from malevolent actors on the network, authentication is essential to ensuring its security. The validation of users and communications that move across the network is significant to protect it from hazardous assaults.

4. **Data Integrity:** Data integrity makes ensuring that the message's content isn't changed or altered while being transmitted. The public key infrastructure and cryptography cancellation mechanism can complete the mission.

5. **Nonrepudiation:** In case of a disagreement, the nonrepudiation assures that neither the sender nor the receiving entity may challenge the transmission or reception.

XV. MARKET GROWTH OF COGNITIVE RADIO ENABLE VEHICULAR NETWORK

The economics and the infrastructure of communication are intertwined in today's society. Cognitive radio will personalize the mobile communication paradigm by improving spectrum usage efficiency in many different ways. By dynamically altering the transmission settings, CR locates the open channels in the spectrum and uses them for communication, better using the channel resources.

Before the technology may be utilized in a real-world setting, certain technological challenges must be cleared. Cognitive radios must be more sensitive to distinguish between a primary signal that is fading and white space. In situations of extreme fading, a single cognitive radio employing local sensing would not be able to achieve this enhanced sensitivity since the required sensing time might be longer than the sensing period.

The enormous rise in the number of wireless smart devices need more spectrum resources. In order to better use the channel resources, CR locates the open channels in the spectrum and uses them for communication by dynamically adjusting the transmission settings.

This market has a moderate level of rivalry since just a few competitors can satisfy the demand. To help their services grow, these cognitive radio providers enter into agreements and make investments with diverse businesses. With the development of improved cognitive radio technologies, they have a wider scope of expansion as the demand for quick and reliable network connections rises.

The Thales Group, Raytheon Company, Rohde & Schwarz GmbH & Co. KG, BAE Systems PLC, and Raytheon Company are among notable businesses that provide services in this industry.

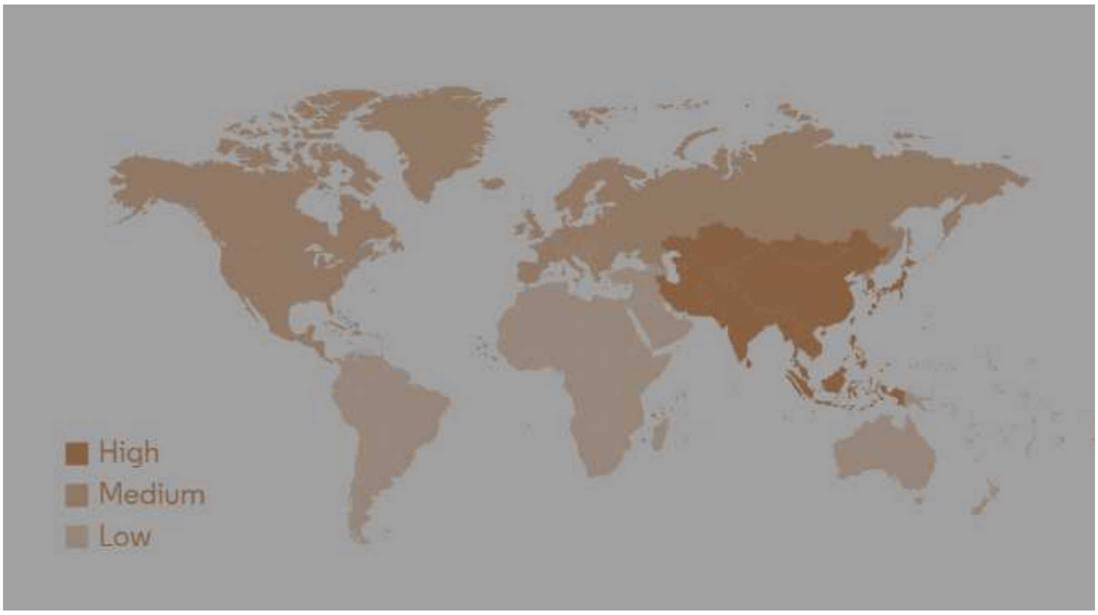

Figure 11: Market Growth of Cognitive Radio Enabled Vehicular Network by Region

The Akida neuromorphic technology from Brain Chip was chosen by Intelligence Systems Inc. in March 2023 to enhance the cognitive communication capabilities on platforms with limited size, weight, and power (SWaP), such as robots and spacecraft. In especially for cognitive radio equipment, NASA may employ Intelligence's NECR technology to increase the stability and reliability of space communication and networking.

Neva SGR, an Italian company, invested in CoreTigo in February 2023. CoreTigo gives system integrators, producers of automation equipment, and machine builders the tools they need to construct more connected, wire-free production environments that are both dependable and affordable. CoreTigo reduces industrial automation systems' complexity by rethinking conventional network and communication principles.

Ericsson intends to invest 11.9 million USD in November 2022 to improve future wireless connection capabilities in the UK. This research program is anticipated to include a range of topics, including energy efficiency, cognitive networks, artificial intelligence, and network security and resilience. It is predicted that 6G research and ground-breaking inventions will also receive attention. The firm claimed that 6G will unite the physical and digital worlds and contribute to the development of a civilization that is more intelligent, sustainable, and productive.

XVI. FUTURE PROSPECTS

1. As a key technology in4G and 5G communication systems, device-to-device (D2D)and vehicle-to-everything (V2X) communication can make our system performance improved, user experience enhanced and cellular communication applications extended.

2. This paper analyzes and organizes the literatures of DSRC and cellular parallel hybrid networking technologies for 5Gcommunication technology development from three aspects:Node Performance, local Network and Internet of Things(IoT).

3. At present, in the development of D2D and V2X,there are difficulties in which multiple interests are not easyto coordinate, making them less suitable for scale.

4. This also leads to the phenomenon that the existing D2D/V2Xresearch is out of touch with the actual application, which becomes the bottleneck for their further development.

5. In the future, research on the deployment and application of D2D/V2X architecture in real cellular networks requiresfurther practical research.

XVII. CONCLUSION

The capabilities and uses of vehicle communication networks can be expanded via cognitive radio, a developing wireless communication technology. The growth and development of vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-pedestrian communications are driven by cognitive radio. The CRVs still need to be consolidated and pertinent design problems need to be resolved, nevertheless. The unresolved problems and difficulties with CRVs will be examined in the subsequent study, along with more modern uses in the automobile industry.

In the study, we gave a general overview of the Cognitive Radio Enabled Vehicular Network and highlighted the present research status, its architecture, its different uses and advantages, and its safety and privacy. We've quickly covered the difficulties with the CRAVENET that prevent proper adoption of security and privacy in the context of security and privacy.

In addition, we have classified security and privacy threats according to the attack routes used, offered defenses, and predicted future research areas. Overall, we have emphasized that security must be an essential component of Cognitive Radio.

Hence we can conclude that Cognitive Radio Enabled Vehicular Network(CRAVENET) paradigm will take the traffic scheme to a new level that will eventually benefit the vehicle and as well as the pedestrian in the near future.

REFERENCES

[1] F.B.S.D.Carvalho, W.T.A.Lopes, M.S.Alencar, J.V.S.Filho, Cognitive Vehicular Netwroks: An Overview, International Conference on Communication, Management and Information Technology (ICCMIT 2015), Procedia Computer Science 65 (2015),107 – 114, 2015.
[2] Shanmughasundaram R., Prasanna.V.S, V.Dharmarajan, Li-Fi Based Automatic Traffic Signal Control for Emergency Vehicles, 2018 Second International Conference on Advances in Electronics, Computer and Communications (ICAECC-2018), 2018.
[3] S.Sharma, M.B.Awan, S.Mohan, Cloud Enabled Cognitive Radio Adhoc Vehicular Networking (CRAVENET) with Security Aware Resource Management and Internet of Vehicles(IoV) Applications.
[4] S.Sharma, M.B.Awan, S.Mohan, Cognitive Radio Adhoc Vehicular Network (CRAVENET): Architecture, Applications, Security Requirements and Challenges.
[5] W.Wu, Z.Yang, K.Li, Internet Of Vehicles And Applications, Ch-16, Pg-299-317.
[6] R.C.Abeywardana, K.W.Sowerby, S.M.Berber, SimuCRV: A Simulation Framework for Cognitive Radio Enabled Vehicular Ad Hoc Networks, 978-1-5090-5932-4/17/$31.00 ©2017 IEEE.
[7] M. Gerla, E. K. Lee, G. Pau, and U. Lee, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” in Proc. IEEE World Forum Internet Things (WF-IoT), Mar. 2014, pp. 241-246.
[8] Sachin Sharma and Seshadri Mohan, “Cognitive Radio Adhoc Vehicular Network (CRAVENET): Architecture, Applications, Security Requirements and Challenges,” 10th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016, Banglore, India, Nov 6 - 9, 2016.
[9] Y. Fangchun, W. Shangguang, L. Jinglin, L. Zhihan, and S. Qibo, “An overview of Internet of Vehicles,” China Commun., vol. 11, no. 10, pp. 1 15, Oct. 2014.
[10] S. Haykin, “Cognitive Radio: Brain-Empowered Wireless Communications”, IEEE Journal on Selected Area in Communications, Vol. 23, No. 2, 2005.