


# Chapter 1

## VANETs and the Use of IoT: Approaches, Applications, and Challenges

**Sandhya Avasthi**

 <https://orcid.org/0000-0003-3828-0813>  
ABES Engineering College, India

**Shivani Sharma**

Indraprastha Engineering College,  
India

**Tanushree Sanwal**

Krishna Institute of Engineering and  
Technology, India

**Shweta Roy**

ABES Engineering College, India

### ABSTRACT

*The vehicular ad-hoc network (VANET) has emerged as the most sought-after technology due to its wide range of applications. In this modern era, people are looking for intelligent systems that include intelligent transport systems, which is not possible without the use of modern techniques such as the internet of things (IoT), VANETs, and cloud computing. With the growing demand for luxury cars, and people's need for safety, the ad-hoc car network is experiencing growth. The connectivity between the vehicle is possible using sensor communication among vehicles in the network. For transmitting forthcoming traffic information in case of a vehicle accident, car connectivity plays a vital role to connect to other vehicles so that appropriate actions can be taken. In this chapter, applications, protocols, trust models, and challenges of VANETS are discussed. The purpose of this chapter is to discuss and elaborate on various aspects related to VANETs and IoT. In addition, the chapter discusses characteristics, challenges, and security concerns in VANETS-based applications.*

DOI: 10.4018/978-1-6684-4991-2.ch001

## **INTRODUCTION TO VANETs AND IOT**

Internet of Things (IoT), which is fast emerging as a powerful technology, coupled with intelligent and integrated sensor network systems and domestic sensor networks are anticipated to have an impact on people's daily lives and stimulate a significant market shortly. The Internet of Things is a network of connected things such as mobile devices, smart sensors in the vehicle, digital machines, other computing devices, and even people. IoT has expanded into the field of smart vehicles and turned into something called as Internet of Vehicles (IoV) (Ahmood, 2020). The proper functioning of IoV is based on Vehicular Ad-Hoc Network. An integral component of any "Intelligent Transport Systems" (ITS) is VANET, who's growth is accelerating fast. VANET and IoT are currently the most crucial components of the "Intelligent Transport System" (ITS). The research study in the past decade on VANET and IoT indicates that both have a significant impact on intelligent transportation systems. Road accidents, congestion, fuel consumption, and environmental pollution have all become major global challenges as the number of automobiles increases. In both developed and developing countries, traffic accidents frequently cause massive loss of property and human life. ITS formed and implemented VANETs to provide infrastructure for transportation of all types. The importance lies in dealing with prevalent issues in transportation to make the journey for everyone safer, effective, hassle-free, and enjoyable (Hossain et al., 2012).

In any Mobile ad-hoc network, an integral part is VANET and therefore, nodes operate inside the networking region and devices operating in that area. Transfer of information with one another through single-hop or multi-hop through a road-site unit (RSU) (Patel et al., 2015). VANET's advantage is to improve vehicle safety by switching caution messages among vehicles. VANET's main concern is to improve passenger safety and the exchange of security messages between locations. Security is very important for VANETs because of the scarcity of centralization, and powerful arrangement of nodes leading to extreme difficulty in recognizing nodes or network vehicles that are dangerous and, malicious (Hussain et al., 2015). Vehicles are in direct contact with some other vehicle, if in case, there exists the availability of wireless connection; it is called a single vehicle to vehicle (V2V). All the motor vehicles operating within the network are connected to Road-Side-Unit (RSU) which further expands the network vehicle communication by sending a message and getting details from them.

In VANETs, the two primary types of applications are *safety and non-safety applications*. For purpose of sending safety messages, safety applications are used such as warning messages. Warning messages help and assist vehicles on the road in case of collisions that saves a life. Messages regarding road safety include reports of car accidents, traffic jams, road construction, and alerts from emergency vehicles

### ***VANETs and the Use of IoT***

(Hartenstein & Laberteaux,2010). Non-safety applications, on the other hand, make driving easier and more comfortable. Traffic management and information and entertainment are the two types of non-safety applications. Traffic management enhances smooth traffic flow and eliminates traffic congestion by incorporating advanced applications. The applications, known as infotainment applications entertain passengers by providing Internet access, the ability to store data, stream videos, make video calls, and information related to maps through GPSs (Global Position Systems). Unlike safety applications, these applications are not required to be extremely reliable and quick. In case of crucial events, accident reports can be disseminated fast and this is reliable over VANETs. Even though VANETs can be used to disseminate event information, it is still difficult to deliver critical messages to the appropriate location and time in a dynamic vehicular setting.

### **Vehicular Ad-hoc Networks**

People in the modern world need cars more than anything else. Accidents are happening more often, even though safety devices like advanced braking systems, rear-view cameras, seatbelts, etc. are getting better and more people are using private transportation. Several studies have shown that about 60% of road accidents can be avoided if the driver gets a warning message a few seconds before the crash. Intelligent Transportation Systems (ITS) constitute the present-day world. The nodes in a VANET are highly dynamic, so the network topology changes rapidly. To provide intelligent driving, safe navigation, entertainment, and emergency applications, VANETs are being utilized in implementation. VANETs are network-dependent that makes them very different from Intelligent Transportation Systems (Shinde & Patil, 2010, Tanuja et al.,2015, Zeadally et al.,2012). Table 1 displays the various wireless access technologies that are compatible with VANET.

This chapter presents an overview of VANETS, protocols, trust model, IoT technologies, and their useful application in various aspects of life. Important aspects related to the architecture of VANETs, characteristics, protocols, and challenges have been discussed in this chapter. In addition, security and privacy issues along with future advancement is provided.

### **Intelligent Transportation Systems and Internet of Vehicle**

Integration of information and communication technologies has proved efficient in traffic management systems, these are referred to as “Intelligent Transportation Systems” (ITS). Such a system aims to provide safety, sustainability of transportation networks, and efficiency. In addition to this, ITS helps in reducing traffic congestion and improving the experiences of drivers. In addition, they hope to reduce the

**VANETs and the Use of IoT**

*Table 1. Wireless technologies and comparison*

SN	Wireless Access Techniques	Coverage	Speed	Density	Throughput	Latency	Reliability
1	C-V2X	High	High	High	High	Low	High
2	DSRC	Low-moderate	High	Low	Low	Moderate	no
3	4G-LTE	Higher	Low	High	Moderate	Moderate	High
4	WiFi	Moderate	Low	Low	Low	Moderate	No
5	UWB	Moderate	Low	Low	Low	Low	No
6	ZigBee	Low	Low	Low	Low	Low	no
7	BlueTooth	Low	Low	Low	Low	Low	no

amount of time that drivers spend stuck in traffic. The possibilities are endless and have no bounds.

Sensors, software, and the technologies that connect and exchange data among these components are all part of the “Internet of Vehicles” (IoV) (Lee,2016). IoV is an extension of vehicle-to-vehicle (V2V) communication that improves assistance systems for fully autonomous driving by raising the vehicles’ artificial intelligence awareness of their surroundings (including other vehicles and driving-related smart devices). The following components make up the IoV: vehicles (as ad hoc network nodes), roadside units (RSU), infrastructure (such as road and traffic-related sensors, signals, and smart objects), personal electronics (such as smartphones and PDAs), and people (e.g., drivers) (Kumar, 2020).

The “Internet of Autonomous Vehicles” (IoAV) is expected to develop from Vehicular Ad Hoc Networks (“VANET,” a type of mobile ad hoc network used for communication between vehicles and roadside systems). Autonomous, connected, electric, and shared (ACES) Future Mobility will be enabled in part by IoV. Real-time analytics (Avasthi et al.,2022), commodity sensors, and embedded systems all contribute to the development of road vehicles. For the IoV ecosystem to function as a whole, it requires modern architectures and infrastructures that distribute computational load across multiple network nodes (Khelifi,2019, Avasthi et al., 2021).

**VANETS AND ITS ARCHITECTURE**

An overview of the main architectural components of VANET is provided here from a domain view. Other aspects such as the interaction between components and communication architecture is explained too.

## ***VANETs and the Use of IoT***

### **Main Components**

As per IEEE 1471-2000 (Maier et al.,2001) and ISO/IEC 42010 (Maier et al., 2002) architecture standard guidelines, one can implement the VANETs system by various entities taking part in it. The mobile domain, the infrastructure domain and the generic domain are three groups into which entities are divided (Schroth et al., 2012). There are two mobile domains, the first is a vehicle and the second is a mobile device as given in Figure 1. Devices such as cars, buses, and other transport mediums generally become part of the vehicle domain. The devices like navigation devices and smartphones are part of the mobile device domain. Another category is the infrastructure domain which includes central infrastructure and roadside infrastructure. Elements like traffic signals, light posts, and roadside units are called roadside infrastructure whereas traffic management centers (TMC) and vehicle management centers are called central infrastructure (Baldessari et al.,2007).

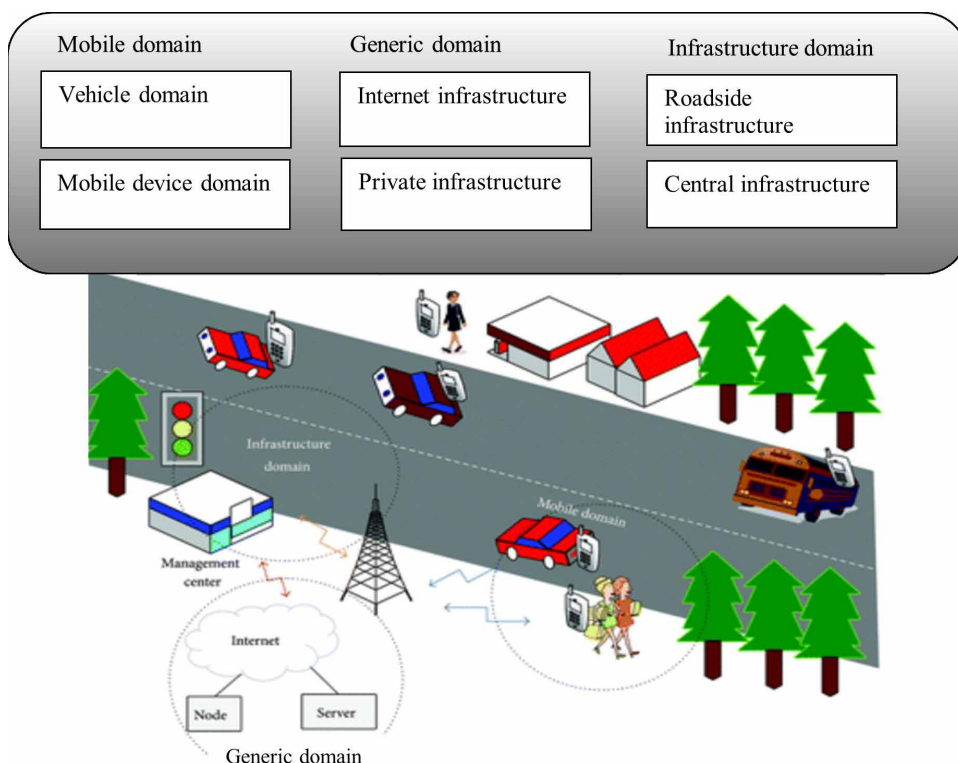
The development of VANET architecture, however, differs per region. The CAR-2-CAR communication consortium is pursuing a standard design for the CAR-2-X communication system that is a little bit different. The primary force behind vehicular communication in Europe is the CAR-2-CAR communication consortium (C2C-CC), which published its “manifesto” in 2007. The in-vehicle, ad hoc, and infrastructure domains of this system design are separated. The in-vehicle domain consists of one or more application units and an on-board unit (OBU) (AUs). They often use wired connections, although they also employ wireless connections on occasion. The ad hoc domain, on the other hand, is made up of cars carrying OBUs and roadside units (RSUs) (Faezipour et al.,2012). A RSU is a static node, on the other hand OBU is a mobile node. RSU get the connectivity through internet via gateway, these units communicate with each other directly or through multihop. In the infrastructure domain, the access is done through RSUs and hot spots (HSs). OBUs get connected to internet via RSUs and HSs and use cellular radio networks such as GSM, Wi-Max and 4G when RSUs are absent.

### **Communication Architecture**

Four categories are there in VANETs for communication types, which are closely related to components as described in Figure 2. This figure explains and illustrates the key functions of each communication type. The term “in-vehicle communication” refers to the in-vehicle domain, which is an increasingly vital component of research into VANETs. An in-vehicle communication system is essential for driver and public safety since it can monitor a vehicle’s performance, notably driver fatigue and drowsiness. Drivers can exchange information and warnings via vehicle-to-vehicle (V2V) communication for providing support to the driver. Another category is

**VANETs and the Use of IoT**

*Figure 1. Different parts of VANET systems*



Vehicle-to-road infrastructure (V2I). In this type of connectivity, drivers can receive weather and traffic information in real-time, as well as environmental sensing and monitoring. In Vehicle-to-broadband cloud (V2B) communication, automobile interacts via a wireless broadband network for example 3G or 4G. The information of traffic and monitoring activity and infotainment is stored on the cloud. Due to this connectivity is imperative for providing assistance to driver and keeping track of vehicle.

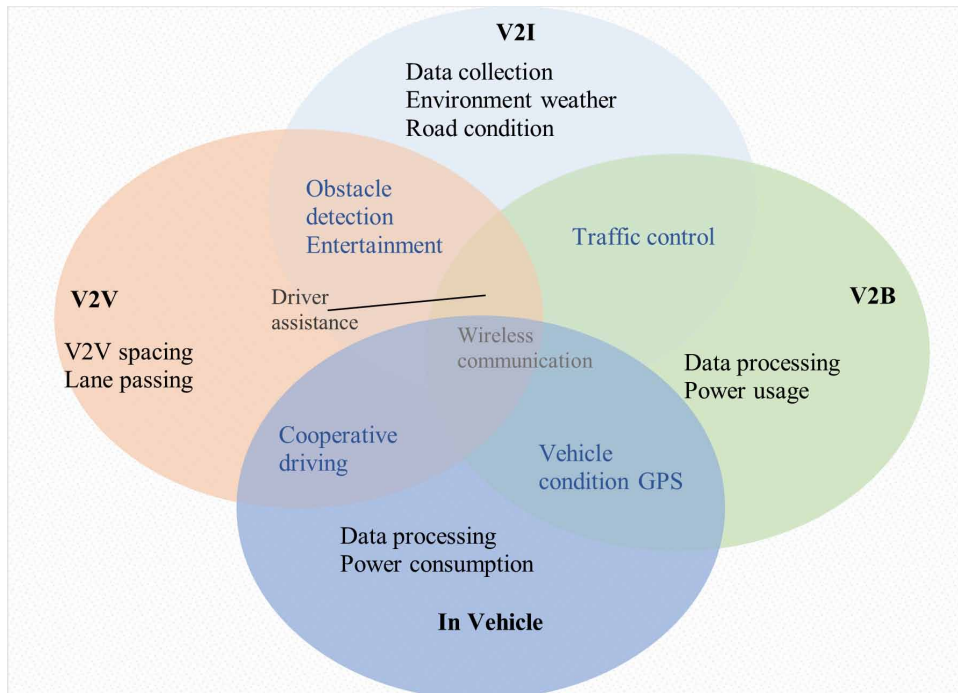
**Layered Architecture**

The communication functions between nodes is divided into one of the seven logical levels as per the open systems interconnection (OSI) model. With this architecture, the session and presentation levels are dropped, and each layer can be further divided into sublayers. The design of VANETs can generally differ from region to region, which has an impact on the protocols and interfaces. A dedicated short-range communication (DSRC) was developed specifically for use in automobiles, along

### ***VANETs and the Use of IoT***

with a corresponding set of protocols and standards (Laberteaux & Hartenstein,2009). For DSRC communication, the US FCC has set aside 75 MHz of frequency between 5.850 GHz and 5.925 GHz. Some of the protocols are still being actively developed today, are intended to be used by the various layers.

*Figure 2. Communication types in VANETs and their key functions*



## **CHARACTERISTICS OF VANETS**

Some distinguishing characteristics of VANET in the design of communication systems that plays an important role (Kaur et al.,2012, Chen,2015) are discussed here. These are:

- *Topology*: The topology of VANETs is dynamic and, is defined by the two primary parameters of speed and route selection, i.e., how quickly a vehicle changes its route. Assume two vehicles are moving at 90 km/h (25 m/s) apart and the link between them lasts 4 seconds (200 meters) if the transmission range is approximately 200 meters.

### ***VANETs and the Use of IoT***

- *Localization Feature:* This feature transmits and sometimes determines a vehicle's geographical location, i.e., to and from one or more vehicles. Vehicle localization (estimation of location) is a global requirement. Vehicle usage is increasing in both developed and developing countries. The global vehicle fleet continues to grow on a daily and annual basis (Shinde et al.,2012, Almusaylim et al., 2020). Furthermore, the availability of position data (Davis, 2018) may enable applications such as driver safety, intrusion detection, inventory management, health monitoring, road traffic monitoring, and surveillance. Specific VANET applications, such as driver assistance systems, require a localization system with the highest accuracy, precision, and reliability. In these applications, the driver will receive information in advance in the event of an accident, allowing the driver to take precautionary measures.
- *Model of mobility:* The nodes and, their connectivity (vehicles) are determined by the node's (Vehicle's) direction, position, and velocity concerning time. The estimate of connectivity between nodes(vehicles) is extremely challenging due to the nature of the vehicle and its movement patterns. Nonetheless, effective network design requires mobility models based on vehicle speed and predetermined path models (Camp, 2015).
- *Infinite Power Source:* Since connectivity in VANET is seamless, the vehicle can continuously provide power to computing and communication nodes (vehicles).
- *Communication Situation:* the model of mobility is dependent on roadways patterns, they do not consider if they are highways, city or streets. So designing routing algorithms or vehicle prediction models need changes in roadways patterns. The mobility models for highways are simple and it is easier to perform prediction. On the other hand city mobility models are complex due to road structure. The obstacles like buildings, trees, signposts and other landmarks make predictions even more difficult.
- *Onboard Sensors for communication:* The onboard in any VANET are made up of several sensors. These sensors are capable in predicting a vehicle location and movement that provide effective routing and quality communication between vehicles.
- *Extremely Computational:* Active vehicles can communicate, sense, and compute in vehicular ad hoc networks.
- *Variable Network Size:* In vehicular ad hoc networks, the size of the network can change. It could be a country, a city, or a group of cities. Because of this, any protocol made for VANET is almost certainly ascendable.



### ***VANETs and the Use of IoT***

- *Anonymous Addressee:* The most important thing for many VANET applications is to identify vehicles in a certain region, not the specific vehicle, which could help protect the privacy of nodes (vehicles).
- *Time-Dependent Data exchange:* sending packets of sensitive data that have time constraints is part of any VANET application. So it is not a good idea to compromise on performance.
- *Infrastructure Support:* A good infrastructure is backbone of a good Vehicle-to-vehicle communication and, so VANET is better than every other network.
- *Lots of energy and computers:* Because there is a lot of energy and computers, VANET has a lot of schemes that use a lot of resources, like the Elliptic Curve Digital Signature Algorithm (ECDSA) and Rivest–Shamir–Adleman (RSA) (Preet et al., 2017).
- *Better physical protection:* Because it's hard to break into VANET Nodes (vehicles), VANET services are safer than MANET services.
- *Network Partitions:* Because Vehicular ad hoc networks are always changing, there are often big gaps between vehicles in isolated clusters of nodes (sparsely occupied scenario).
- *Hard Delay Constraints:* VANET safety applications require on-time message delivery instead of hard data delay delivery in case of accidents.

## **ROUTING PROTOCOLS IN VANETS**

Routing protocols evaluate each option before making a decision. the best for getting a point across. These paths are evaluated by the routing algorithms, which use them to select the best path leading to the destination, based on their connection, bandwidth, end-to-end delay, etc. For the sake of enhancing both road safety and passenger convenience, VANET routing involves sending data from the source vehicle to the destination vehicle over the network via a suitable path. To prepare for an impending thrust, the vehicles have access to data related to road safety (Da Cunha, 2014). High-dynamic topology and support for irregular connectivity are just two of the impressive features of this system. There are problems with inter-network communication in the initial VANET because of the lack of routing algorithms (Srivastava, 2020).

The best VANET routing protocol should include the following:

- Getting to Know Your Neighbors
- Their ability to transfer data
- Geographical information
- Predict where vehicles will be in the future

### ***VANETs and the Use of IoT***

- Consider the uneven density of vehicles in the area

The existing VANETs are categorized into three distinct types of routing protocols, namely: broadcast, geocast, and unicast. The list of routing approaches and routing protocols is given in Table 2.

- **Geocast/Broadcast.** The geocast/broadcast protocols are required in VANETs due to the requirement of disseminating messages to unidentified or unnamed destinations (Chen et al., 2011). Flooding is utilized for data transmission within a region or range. It is also feasible to send messages without being bombarded. Crash rates are reduced as parcel overhead is corrupted. Heading-based geocast for query distribution in VANET Inter-vehicle geocasting, distributed robust geocasting, and robust vehicular routing Timetable that is dynamic One of the sub routing protocols featured in Geo Cast routing protocols is the Geo Cast routing protocol. Daraghmi, 2013, reviewed the message broadcast protocols for VANETs, an interference aware routing scheme and spatially aware packet routing method. The interference aware routing equips the node with a multichannel radio interface which switches channels based on SIR evaluation and FROV. The FROV selects the retransmission. SADV finds the best path to forward the packet. This is possible by dividing the road into segments and choosing the farthest vehicle in the nonempty segment. Some other algorithms in this category are UMB, MHVB, MDDV, and V-Trade.
- **Multicast.** In driving situation such as crossroads, busy traffic, accidents, roadblocks and rough road conditions multicast is needed. In (Mchergui et al, 2020), the authors classify multicast protocols into two broad types. Topology-based approaches, such as GHM, ODMRP, and MAODV, produce group-based multicast trees and source-based multicast meshes using group addresses (which generates group-based multicast meshes). The location-based technique consists of RBM, IVG, LBM, SPBM and PBM. PBM uses the positions of all one-hop neighbors and all individual destinations respectively. The LBM utilizes a multicast area to keep destinations information for multicast packets. RMB and IVG main purpose is to handle safety warning messages by defining multicast protocols.

**VANETs and the Use of IoT**

*Table 2. Routing protocols applied in VANETs*

Routing Method	Routing Protocols
Unicast	Ad hoc on-demand distance vector (AODV) General packet railways services (GPRS) Vehicle assisted data deliver (VADD) Dynamic source routing (DSR) A-START Position based multihop broadcast Improved greedy traffic aware routing Trajectory based data forwarding Connectivity aware routing Geographical source routing Opportunistic packet relaying in disconnected vehicular ad
Broadcast	Linkage protocol for highway automation (DOLPHIN) BROADCAST COMMUNICATION protocol Distributed vehicular broadcast (DV-CAST) Packet routing algorithm
Geocast	Distributed robust geocast protocol (DRG) Robust vehicular routing (ROVER)

- **Unicast.** Three types of unicast communication protocols are studied for VANETs:
  1. *Greedy:* A node chooses its farthest neighboring node and forwards packets to the destination node which is the same as improved greedy traffic-aware routing known as GyTAR (Chen et al., 2011).
  2. *Opportunistic:* Nodes wait for the opportunity to come, and then send the data to the destination on arrival similar to topology assist geo-opportunistic routing (TAGOR) (Daraghmi et al., 2013).
  3. *Trajectory-based:* Potential paths to the destination is identified by nodes. Further nodes determine the delivery of the data through nodes by applying trajectory-based data forwarding (Senouci et al., 2018).

**ISSUES, CHALLENGES, AND FUTURE OF VANET**

The challenges and issues that exist in the field of VANETs is discussed in this section. Also, some useful applications are described. Some issues in VANET are:

- i. **Intermittent connectivity:** Management of connections and control between cars and infrastructure is a significant challenge. Because of heavy vehicle

### ***VANETs and the Use of IoT***

- movement or severe packet loss, intermittent connections in automotive networks are not considered good.
- ii. High mobility and location awareness: A high degree of mobility and location awareness will be required of the vehicles that participate in communication in future VANETs. Each vehicle in the network must know where the other vehicles are in order to respond to an emergency situation.
  - iii. Management of heterogeneous smart cars: A large number of heterogeneous smart automobiles will be available in the future; the management of their irregular connections will be a challenge.
  - iv. Security: Information about an individual's identity and whereabouts can never be completely protected. When cars talk to each other inside the infrastructure, they should be able to choose what information is exchanged and what information is kept private. Privacy can be guaranteed by analyzing sensitive data locally rather than sending it to the cloud.
  - v. Network intelligence support: One of the future VANET's goals will be to support network intelligence. The edge cloud will collect and pre-process data from sensors on vehicles in future VANETs before it is shared with other parts of the network, such as regular cloud servers.

VANETs, in contrast to MANETs, have distinctive properties that necessitate the use of wireless communication technologies, different communication paradigms, and security and privacy measures (Dressler et al., 2011). Network connections, for instance, cannot be dependable over a long period. Researchers are looking for new ways to utilize existing infrastructure (e.g., Roadside units, cellular networks) for improving communication performance. Although specific VANETs challenges have been overcome, several significant research issues are still open (Khan et al., 2019). Some common technical and societal challenges faced by Vehicular ad-hoc networks are:

- Communication: When it comes to data exchange, there are three different methods such as Unicast, Multicast, and broadcast. All three are applied to implement the fully operational mode in VANET. The highly dynamic topologies, vehicle speed, bandwidth constraints, and homogeneous as well as heterogeneous network densities create challenges in VANET.
- Trustworthiness: VANETs depend on seamless connectivity, and an error-free environment to work efficiently in full operational mode. This is possible only when proper facilities like robust hardware and fault tolerant software are available. This is one of the key research areas in VANET.
- Privacy: data exchange between devices/vehicles is done anytime, anywhere and so different safety mechanisms are required. Some common mechanisms

### ***VANETs and the Use of IoT***

are authentication, digital signature, multifactor authentication, and cryptography.

- **Cost allocation:** These days, some automobiles are equipped with more expensive built-in VANET connection systems that not every vehicle owner can afford. A cost-effective VANET communication system design is therefore required to provide VANET services to every car user. Designing a VANET communication system with minimal resources could lower the cost of the vehicle.
- **Quality of service:** A important responsibility in the VANET is to provide Quality of Service (QoS) at a particular level. Due to the topology's great dynamicity, severe latency restrictions, unpredictable connectivity, etc., it is impossible to offer various users a higher level of service. As a result, it is one of the fascinating and challenging research fields in the creation of the VANET system (Shinde et al., 2021).

To solve the various issues in VANETs, some criteria are discussed below as a possibility in future VANETs.

- **Low latency and real-time applications:** Future VANETs must have low latency so that they can be used for real-time applications. Future VANETs should be able to support real-time applications like safety messages with very low latency.
- **Great bandwidth:** Shortly, there will be a lot of demand for high-quality video streaming and other entertainment and convenience apps. Also, traffic apps like 3D maps and navigation systems need to be updated automatically regularly.
- **connectivity:** In the future, connected cars will need to be able to talk to each other perfectly for VANETs to work. Fog devices must be always and very reliably connected to connected or self-driving vehicles. It must be able to keep communication systems from breaking down during transmission.

## **VANETS AND IOT APPLICATIONS**

With the aid of IoT, the broadcasting protocol has been widely adopted in VANET for the distribution of data or messages for safety-based and non-safety-based applications to guarantee traffic efficiency (Mohamad et al.,2017). The idea of a smart city is crucial in today's technological era for enhancing the quality of services (QoS) provided to residents and, ultimately, their quality of life. Table 3 shows the

***VANETs and the Use of IoT***

*Table 3. Use of IoT in VANETs applications*

SN	VANET Application	IoT application
1	Warning in case of collision	Smart cities
2	Assistance for Lanes	Environment monitoring
3	Accident detection and alert	Energy management
4	Traffic planning	Healthcare systems
5	Overtake warning	Building automation
6	Emergency warning	transportation
7	Point of interests allocation	Social network
8	Weather information	

connection or prerequisites between VANET and IoT. One may argue that the two are related.

Using a game-theoretical approach, IoT in VANET has also been used to make real-time decisions for IoT-based traffic light control. The authors proposed a way to control traffic flow or congestion at intersections (Bui et al., 2017, Avasthi et al., 2022). Their method can find priority vehicles that need help right away, like police cars, ambulances, and fire engines. This cuts down on how long these priority vehicles usually have to wait at intersections. Since cities are getting bigger every day, this kind of system is very important.

**Safety application:** The traditional objective of safety applications is to prevent accidents, which has resulted in the development of ad hoc networks for vehicles that communicate with other connected elements of the environment. These apps provide life-saving traffic assistance to drivers on the road. Driver assistance, alert information, and warning alert are its three subcategories.

Safety applications can be grouped as under:

- Real-time traffic: this data is collected at roadside units and shared with cars. This is an important part of fixing traffic jams and bottlenecks.
- Cooperative Message Transfer: Cars that are moving slowly or have stopped work together and send messages to other cars to avoid accidents by automating applications like an emergency.
- Post-crash notification: If a car is in an accident, it sends warnings to other cars so they don't get into the same kind of trouble.
- Road Hazard Control Change: The car in front of other cars can quickly tell them how the road is, what it is made of, or if there is a landslide.
- Traffic Watchfulness: The cameras set up at roadside units will help a lot to cut down on driving violations.

### ***VANETs and the Use of IoT***

**Non-safety applications:** Non-safety uses are crucial for maintaining traffic efficiency and comfort while driving. Road users connected to VANET systems using IoT can benefit from weather information, location and current traffic movements on road networks, distance, Point of Interest (PoI) allocation, and social network (connected to the mobile network via smartphones) (Bauza et al.,2010). Commercial application is a popular category in non-safety applications. These involve value-added services (VASs) that emphasize improving passenger comfort (Eze et al., 2016). Commercial applications can be grouped as follows: -

- Remote Car: Through Personalization/Diagnostics, the download of customized vehicle settings or the upload of vehicle diagnostics from/to infrastructure is possible.
- Internet Access: Passengers can use the Roadside units (RSUs) of a VANET as routers to connect to the Internet.
- Downloading digital maps: Depending on the situation, a driver can download a local map for their own usage while visiting a new location.
- Real-time video relay: Vehicles can access and share or transfer multimedia files, including music, movies, news, e-lectures, e-books, etc.
- Value-added advertisements: the services given, such as shopping malls, gasoline pumps, gas stations, and highway restaurants, can advertise their services to all vehicles or passengers within range, even if the internet is unavailable.

Another type of non-safety application is a convenient application that provides convenience and comfort to the driver and manages traffic effectively making passenger's experience better. Convenience applications can be grouped under:

- Router Diversions: the driver can alter the route he or she intends to take in the event of traffic congestion.
- E-Toll: Electronic toll collection is an essential VANET application since it allows drivers to pay for tolls electronically at collection sites without having to stop.
- Availability of Parking: If a parking space becomes available, the vehicle will be alerted over the network when it is available.

## **TRUST MODEL AND ATTACKS IN VANETS**

VANET's wireless ad hoc environment is shared and open, so some nodes may be hacked. A security solution must be able to identify potentially hazardous nodes and

## ***VANETs and the Use of IoT***

remove them from the network. Making the right security judgments and taking the appropriate security actions are considerably simpler when trust connections are transparent in real-time. It will be important to have a trust-based model that can manage nodes and evaluate their activities in a way that doesn't require a central authority. Based on the trust ratings they get, malicious nodes can be found, and the network can stop these nodes from taking part in any network communication. So, figuring out trust values is a very important part of making the network safer and more reliable. One entity's belief in another inside a network and certainty that the other would not act maliciously is defined as trust. An entity is any device that participates in communication. The first and second groups of the trust establishment paradigm are infrastructure-based trust and self-organized trust, respectively.

### **Attacks on VANETS Devices**

Because of the enormous number of autonomous network members and the inclusion of the human component in VANETs, node misbehaviors in future vehicle networks are highly possible. Based on the layer used by the attacker, various attack types have been discovered and categorized (Balakrishnan et al., 2007). An attacker can disrupt a network at the physical and link layers by flooding the communication channel with unsolicited data. An attacker can also inject false messages and rebroadcast prior messages. On-Board Units (OBUs) can be tampered with or destroyed by some attackers (RSU). An attacker can insert fake routing messages or flood the system with routing information at the network layer. The common attacks in the network is described as follows:

1. **False Information:** The attacks are done by insiders who are smart and proactive. The attackers send incorrect information that can change how other drivers act. For example, an enemy could send incorrect information accident and a traffic jam on specific routes misguiding the traveler. This would send cars on different routes and free up a route for the enemy (Grover et al., 2013).
2. **Using information from sensors to deceive:** This is possible through a proactive and smart insider who uses this attack to change how the position, speed, and direction of other nodes are seen so that he won't be responsible for an accident.
3. **Identifier Disclosure:** An attacker is a passive and bad insider. It can keep track of a vehicle's path and use that information to find the vehicle.
4. **Denial of service:** A hacker may attempt to knock down the network by sending unnecessary messages over the channel. This kind of attack entails actions like channel blocking and delivering false messages.
5. **Dropping Packets and Relaying Them:** An attacker can drop packets that are meant to be sent. For example, an attacker could delete all alert messages that



### ***VANETs and the Use of IoT***

were meant to warn vehicles that were getting close to the accident site. In the same way, an enemy can play back the packets after the event has happened to make it look like an accident.

6. **Hidden vehicle:** In this situation, intelligent vehicles aim to reduce wireless channel traffic. For instance, a car has alerted its neighbor's and is awaiting a response. When a vehicle receives a response, it recognizes that its neighbour is better equipped to convey the warning message to other nodes, therefore it stops sending the message to those nodes. This is due to the node's assumption that its neighbour will relay the message to other nodes. The system could be completely destroyed if this neighboring node is an enemy.
7. **Attack of the Wormhole:** A malicious node can record packets at one point in the network and tunnel them to another point using a shared private network with other malicious nodes. The attack will be worse if the malicious node just transmits control messages across the tunnel and no data packets (Grover et al., 2013).
8. **Sybil Attack:** The vehicle pretends to be more than one vehicle. These fake names also make it look like there are more cars on the road. The vehicle spoofs identities, the positions or details of the nodes on that network, this attack lets any type of attack happen.

### **Trust Model**

Managing trust in vehicle ad hoc networks (VANETs) is one of the most difficult parts of setting up a safe VANET environment. Researchers have only made a few trust models to improve the reliability of information shared in vehicular networks. There are three main types of models shown: entity-oriented, data-oriented, and integrated trust models (Soleymani et al., 2015).

1. **Entity-oriented trust model:** The trust model of this kind focuses on how real cars are. Because vehicles move around a lot, trust models can't gather the important information about the sender and the vehicles around it that is needed to reach this goal. Now, the sociological trust model and the multidimensional trust management model are the most common entity-oriented models. The sociological trust model is based on a hypothetical principle of trust and confidence. It doesn't have a structure for finding different kinds of trust at the same time.
2. **Data-oriented trust model:** This model is different from the entity-oriented model that determines whether or not the participating nodes or cars can be trusted (Soleymani et al., 2015), the event-oriented model does not attempt to determine whether or not the participating nodes or vehicles can be trusted. The

### ***VANETs and the Use of IoT***

objective in this trust model is to ensure that incoming messages are authentic. Various data-based trust models, including the RMCV intrusion trust model, the reputation-based trust model, the event-based reputation system, and the roadside-assisted data-centric trust establishment, have been proposed.

3. **Combine based trust:** Uses a combination of individual node opinions and the opinions of other nodes to assess the authenticity of a message. In order for a message to be considered authentic, it must be accepted by the majority of cars. Beacon trust management approach [BTM] has been proposed (Raya et al., 2007) to address these issues.

## **MAINTAINING PRIVACY AND SECURITY OF VANETS**

VANETs continue to have serious effects on privacy. While this is happening, the chance that your private information will be stolen and used against you grows as cars share thoughtful information about themselves and their neighbor's cars. Malicious or rogue vehicles are cars that do bad things like signal sniffing, pattern sniffing, changing packet information, throwing away packets, etc. So, several intrusion detection systems (IDS) approaches based on anomalies, signatures, watchdogs, cross-layers, and honeypots are shown. However, each has its limitations that can't stop invaders, adversaries, hostiles, and rogue entities from messing with normal network activities. The majority of researchers in the field have determined that security and privacy pose the greatest difficulty when transmitting data or messages over VANETs. Due to the online data integrity of the personal information act (Eze et al., 2016, Liang et al., 2015), kinematic data of VANET components cannot be exposed to a malicious server and user collusion (Talib, 2017).

Recent research has addressed the issues of data ownership, massive data management, and legal culpability. Security architecture is essential for ensuring security and privacy to address the issue. Thus, the structure of a vehicular communication system should prioritize the provision of a communication scheme for safety-based applications, as it will generate a shared session key for secure network communication. Due to the poor security level of data clouds, roadside attackers may send bogus requests to cloud services for roads or parking, which causes confusion (He et al., 2014). Theoretical constraints and opportunities, the necessary IEEE standards, connectivity between vehicles and infrastructures, cross-layer design, mobility, validation, and cross-layer design are some other topics that have been briefly covered in VANETs study. Some security challenges are mentioned as follows:

### ***VANETs and the Use of IoT***

- Validation: All of the messages that have been sent must be checked, starting with the first protest and moving on to the next. The central authority must make sure that every vehicle in the system is real.
- High Mobility: As the vehicle moves faster, its high mobility causes several problems, such as noise problems and the loss of handshakes. Because of this, the vehicles can't work together and communicate with each other safely.
- Area-Based Schemes: Beacon messages help us figure out where different vehicles are in a certain area. Sensors, GPS, and Laser, on the other hand, can be used to figure out exactly where the vehicles are.
- Real-Time System: Real-time systems can't be made in this area because people move around a lot. Because of this, it is hard to get alert messages to other devices in time before the deadline.

## **CONCLUSION**

The goal of writing this chapter was to take a close look at the VANETs, IoT, and their applications. Future research in VANETs is now possible after comparison was drawn between the protocols currently in use and those that have recently been developed. Passenger safety, increased traffic efficiency, and entertainment are just a few of the many benefits that can be derived from using VANETs, or vehicle ad hoc networks. As technology advances and the number of smart vehicles rises, traditional VANETs are finding it increasingly difficult to deploy and manage due to a lack of flexibility, scalability, connectivity, and intelligence. To meet these demands, IoT technology is assisting VANETs in many ways in form of the Internet of Vehicles (IoV). In any case, VANETs of the next generation along with IoT will have unique requirements for autonomous vehicles with high mobility, low latency, real-time applications, and connectivity that conventional cloud computing may not be able to meet. The chapter provides an overview of VANET, the architecture of VANETS, Intelligent Transportation Systems, and the relevance of the Internet of Vehicles in implementing a better transport system for passenger safety and modern features.

## **REFERENCES**

Ahmood, Z. (2020). *Connected Vehicles in the Internet of Things*. Springer Nature Switzerland AG. doi:10.1007/978-3-030-36167-9

**VANETs and the Use of IoT**

Almusaylim, A. Z., & Jhanjhi, N. (2020). Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. *Wireless Personal Communications*, 111, 541–564. doi:10.1007/11277-019-06872-3

Avasthi, S., Chauhan, R., & Acharjya, D. P. (2022). Topic Modeling Techniques for Text Mining Over a Large-Scale Scientific and Biomedical Text Corpus. *International Journal of Ambient Computing and Intelligence*, 13(1), 1–18. doi:10.4018/IJACI.293137

Avasthi, S., Sanwal, T., Sareen, P., & Tripathi, S. L. (2022). Augmenting Mental Healthcare with Artificial Intelligence, Machine Learning, and Challenges in Telemedicine. In *Handbook of Research on Lifestyle Sustainability and Management Solutions Using AI, Big Data Analytics, and Visualization* (pp. 75-90). IGI Global.

Balakrishnan, V., Varadharajan, V., Tupakula, U., & Lues, P. (2007). Team: Trust enhanced security architecture for mobile ad-hoc networks. *15th IEEE International Conference on Networks ICON 2007*, 182–187. 10.1109/ICON.2007.4444083

Baldessari, R., Bödekker, B., Deegener, M., Festag, A., Franz, W., Kellum, C. C., ... Zhang, W. (2007). *Car-2-car communication consortium-manifesto*. Academic Press.

Bauza, R., Gozalvez, J., & Sanchez-Soriano, J. (2010). Road traffic congestion detection through cooperative Vehicle-to-Vehicle communications. *Proceedings - Conference on Local Computer Networks*, 606–612. 10.1109/LCN.2010.5735780

Bui, K. H. N., Jung, J. E., & Camacho, D. (2017). Game theoretic approach on Real-time decision making for IoT-based traffic light control. *Concurrency and Computation*, 29(11), e4077. doi:10.1002/cpe.4077

Camp, T., Boleng, J., & Davies, V. (n.d.). A survey of mobility models for ad hoc network research. *Wirel. Commun. Mob. Comput.*, 2, 483–502. <https://online.library.wiley.com/doi/10.1002/wcm.72>

Chauhan, R., Avasthi, S., Alankar, B., & Kaur, H. (2021). Smart IoT Systems: Data Analytics, Secure Smart Home, and Challenges. In *Transforming the Internet of Things for Next-Generation Smart Systems* (pp. 100-119). IGI Global.

Chen, W. (2015). *A book on Vehicular Communications and Networks Architectures, Protocols, Operations and Deployment*. Elsevier.

Chen, W., Guha, R. K., Kwon, T. J., Lee, J., & Hsu, Y. Y. (2011). A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, 11(7), 787–795. doi:10.1002/wcm.862

### **VANETs and the Use of IoT**

- Da Cunha, F. D., Boukerche, A., Villas, L., Viana, A. C., & Loureiro, A. A. (2014). *Data communication in VANETs: a Survey, Challenges and Applications* (Research Report RR-8498). INRIA. <https://hal.inria.fr/hal-00981126/document>
- Daraghmi, Y. A., Yi, C. W., & Stojmenovic, I. (2013). Forwarding methods in data dissemination and routing protocols for vehicular ad hoc networks. *IEEE Network*, 27(6), 74–79. doi:10.1109/MNET.2013.6678930
- Davis, S. C., Diegel, S. W., & Boundy, R. G. (2018). *Transportation Energy Data Book* (36th ed.). Oak Ridge National Laboratory.
- Dressler, F., Kargl, F., Ott, J., Tonguz, O. K., & Wischhof, L. (2011). Research challenges in intervehicular communication: Lessons of the 2010 Dagstuhl Seminar. *IEEE Communications Magazine*, 49(5), 158–164. doi:10.1109/MCOM.2011.5762813
- Eze, Zhang, & Eze. (2016). *Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-map for Future Development*. Academic Press.
- Faezipour, M., Nourani, M., Saeed, A., & Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communications of the ACM*, 55(2), 90–100. doi:10.1145/2076450.2076470
- Grover, J., Gaur, M. S., & Laxmi, V. (2013). Trust establishment techniques in VANET. In *Wireless Networks and Security* (pp. 273–301). Springer. doi:10.1007/978-3-642-36169-2\_8
- Hartenstein, H., & Laberteaux, K. P. (2010). *VANET: Vehicular Applications and Inter-Networking Technologies*. Wiley Online Library. doi:10.1002/9780470740637
- He, W., Yan, G., & Xu, L. D. (2014, May). Developing Vehicular Data Cloud Services in the IoT Environment. *IEEE Transactions on Industrial Informatics*, 10(2).
- Hossain, E., Chow, G., Leung, V. C. M., McLeod, R. D., Mišić, J., Wong, V. W. S., & Yang, O. (2010). Vehicular telematics over heterogeneous wireless networks: A survey. *Computer Communications*, 33(7), 775–793. doi:10.1016/j.comcom.2009.12.010
- Hussain, R., Rezaeifar, Z., Lee, Y. H., & Oh, H. (2015). Secure and privacy-aware traffic information as a service in VANET- based clouds. *Pervasive and Mobile Computing*, 24, 194–209. doi:10.1016/j.pmcj.2015.07.007
- Intelligent Transport Systems (ITS). (2012). *Framework for public mobile networks in cooperative its (c-its)s* (Tech. Rep.). European Telecommunications Standards Institute (ETSI).