DOI: 10.2478/ias-2024-0001 • JIAS • 19(1) • 2024 • 1-14

State of the Art, Reliable, and Trusted Communication in Vehicle to Everything (V2X) Networks

Wajid Ali[1], Shalini Z. Ninoria[1], Gulista Khan[2], Kamal Kumar Gola[3]

1 CCSIT, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, 244001, India; er.wajid.ali@gmail.com, halinin.computers@tmu.ac.in
2 Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, 244001, India; gulista.khan@gmail.com
3 College of Smart Computing, COER University, Roorkee, Uttarakhand, 247667, India; kkgolaa1503@gmail.com

Abstract: Transportation systems are a necessity of modern life. To achieve safe and fast transportation, the intelligent transportation system is being developed. In this system, the main base station facilitates communication between vehicles and all other roadside entities using vehicle to everything networks. Various technologies have been built to support this communication. After receiving the information, vehicles can make their own decisions. This data communication is done in real time. But, if any of these data packets are dropped, the vehicle will make inaccurate decisions, so we need to have reliable data communication. All data communication will be accomplished through a system of neighboring nodes. There may be some malfunctioning nodes that lose packets in between, so a trusted and reliable link is necessary for efficient and secure data communication among the nodes. This paper presents a survey of various algorithms designed for the reliable delivery of data packets, algorithms for secure data transfer, and various types of attacks. After that, various schemes for building trust in parties sending data packets if also presented for survey.

Keywords: Wireless sensor network, Latency, Throughput, IoT

1 Introduction

With the advancement in the Internet of Things (IoT) in the world and electric vehicles, an emerging area has been opened for researchers named VANET integrated with various technologies like GPS, Wireless sensor networks, and different types of sensors. Since people are spending most of their time in their homes, offices, or vehicles, they need connected vehicles and are willing to pay for them. This leads to incorporating the vehicles into IoT. With the increased demand for wireless communication, people are interested in new self-organizing and self-healing techniques that work independently of pre-existing and self-organizing networks. The previous transport systems had cyber-physical systems that embedded software into the vehicles. Then, after the network was built, all the devices connected to the network communicate with each other through smart devices using IoT. In general, VANET is a system in which there are a number of entities that connect to each other to provide safe and efficient communication. In V2X technology, all the entities, like vehicles, cycles, infrastructure units, and pedestrians, are interconnected, which reduces accidents and traffic. In 2015, a fully dynamic system was implemented on the German A9 highway by Siemens, resulting in 35% fewer accidents on that road [1]. Mobile phones in VANET are unstable and not secure, and there are a lot of challenges in this network; first and foremost is the continuous change in the network topology because all nodes are connected to each other for a very short time, for ex, 100 ms. So, all the message transfers must be done within 100 ms. Due to the short timeframe for data transfer, we must have efficient link quality. However, in most cases, data transfer gets disturbed by the buildings, obstacles, and large trucks on the road. We must have very good link quality that could not be affected by the obstacle that results in the guaranteed delivery. Therefore, before sending data over the network, we must ensure that the available links are quality networks, which is required by VANET to increase the PDR (packet delivery rate). Also, there are some misbehaving nodes, which are actual nodes that behave maliciously and start dropping the packets.

They are called internal attackers. Internal attackers are very difficult to find because they are actual nodes. In this paper, we focus on proposing a trust-based model for data transfer on VANET.

A strong link between the sender and receiver is required, which results in unintelligible irregular scalability and availability of the network. Generally, VANET is used to provide wireless technology equipped with onboard units. Roadside units are also used for providing real time data [2][3].

2 Literature Review

In this section, we define various communication technologies and applications. We also elaborate on various models of secure VANET proposed in the past and classify various techniques for trusted communication. Then, we discuss present research gaps and challenges in VANET.

2.1 Background on Vehicle to Everything (V2X) Technology

The modern transportation system includes collecting data via a sensor, data processing, and data communication to various vehicles, roadside users, and infrastructure units. Figure. 1 depicts the Modern Intelligent transportation system structure.

There are the following two types of networks [4, 5]:

1. An intra-vehicle network consists of sensors located on the vehicle. These sensors communicate with each other using Wi-Fi, Zigbee, or Ethernet connections.
2. Another type of network is that in which communication takes place from the vehicle to nearby devices. This consists of various devices, such as the onboard unit, roadside users, cloud servers, and RSU.
    - Onboard units consist of embedded sensors that are capable of sensing, collecting data, and communicating with nearby devices.
    - RSU units are called roadside units. It is used to provide various services to the road entities.
    - Roadside users include pedestrians, motorcycles, and cycles.
    - The cloud server is the central server that controls all the road entities, traffic, and roads.

Vehicle to everything networks consist of a connected platform that connects all entities. They also include neighboring and fixed entities to allow the sharing of information between entities on the road. Vehicle to everything networks can be categorized into five types of communication, as shown in Table 1.

- Vehicle to Sensors (V2S) sensors and vehicle communicate within the vehicle itself.
- Vehicle to vehicle (V2V) share the information between vehicles
- Vehicle to Pedestrian (V2P) communication link provides a link between the vehicle and the roadside node.
- Vehicle to Grid (V2G) involves the data communication between the vehicle and the smart electric grid in order to charge the electric vehicle.
- Vehicle to Infrastructure (V2I) creates a connection between road entities and road infrastructure nodes for communication.

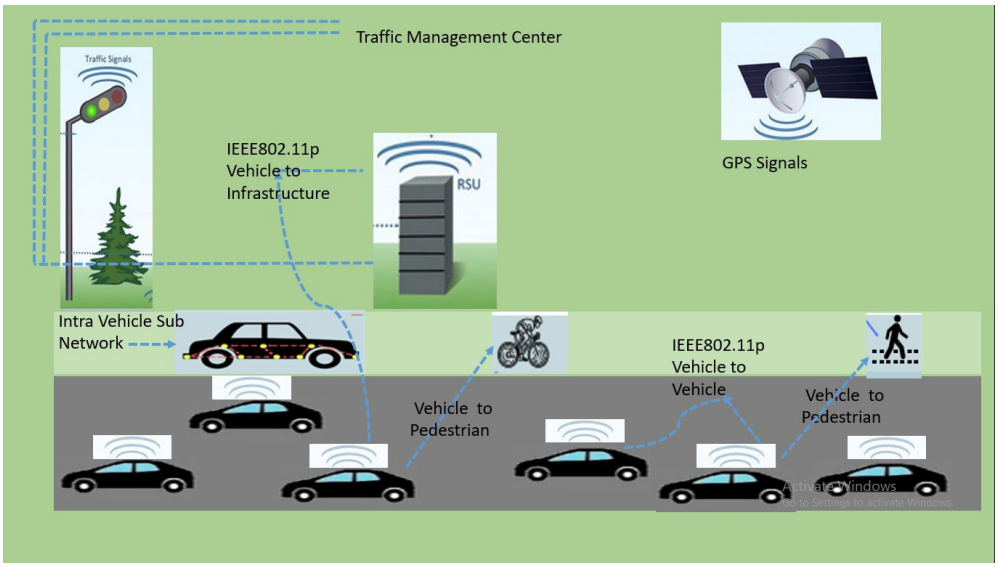

Figure 1. Intelligent transportation system structure

Table 1. Communication ranges of Vehicle to Everything

V2X connection link	Communication range
V2S	10 − 100 m
V2P	170 m (lower transmission power = 12 dBm) [5]
V2G	350 m (transmission power = 23 dBm) [6]
V2V	350 m (transmission power = 23 dBm) [6]
V2I	2000 m [7]

In a VANET, road entries are created to link and transfer the information. The information can be used for multiple types of applications, for example, safety applications, traffic applications, and entertainment information. This communicated information can be categorized among four different messages:

- **Beacon messages:** Road entities intermittently transmit messages to the next-door entities that hold information about the present status, such as the present location of a vehicle, its speed, and direction. This status is maintained periodically in intervals between 100ms and 1s. As a result, everyone can observe the local topology. Also, it can envisage and antedate disastrous conditions and high traffic congestion. These types of messages have lower priority.
- **Unicast message:** These messages are sent by road entities to the core network to access internet services. Few of these messages could contain sensitive information, so they are confidential messages.
- **Local event-triggered message:** When an event occurs, such as warning messages that affect the local area only, these messages are sent only to the nearby entities using vehicle-to-vehicle and vehicle-to-pedestrian links. This information is of local interest, so they are sent locally, not on global links. Also, these messages require low latency; messages must be received within 100 ms.
- **Global event-triggered message:** These messages are sent by road entities to the vehicle-to-infrastructure links. They consist of messages of global interest, such as road construction or congestion. So, these messages must be sent to the global range through V2I links.
- **Emergency vehicle message:** These messages support emergency vehicles. They are sent from the emergency vehicles to nearby vehicles using V2V and V2P links. By listening to these messages, nearby vehicles may clear the road to these emergency vehicles.

As technology improves, the transport system also improves, which results in various applications like traffic, safety, and infotainment [5].

2.2 Secure Protocols Built for VANET

Multiple techniques exist for the purpose of security and privacy. Related to privacy and security, two general techniques are used. One is based on anonymous certificates, and another is based on group signatures. This section elaborates on these two techniques.

2.2.1. Techniques Based on Anonymous Certificates

Authors in [7] proposed a fundamental protocol. In this, the authors use certificates known as anonymous certificates. These anonymous certificates include pseudorandom sequences. They use these certificates to hide their real identities from the attackers. Although in this scheme, real identities are hidden, and there is no information in public about real identity still, if the attacker succeeds in getting a key, then tracking the message until the identity of the sender is possible. In this way, attackers can get the knowledge of real users instead of the use of anonymous certificates. In order to prevent this attack, the techniques for the distribution of certificates must be changed so that the attacker cannot exposed. Another way proposed by the authors is that a number of anonymous certificates must be stored in a vehicle the certificates consist of public/private key pairs. By using this technique, the vehicle will use different certificates at different times so as to avoid its tractability. However, as per key exchange frequency and the speed of the vehicle, every vehicle must store a large number of key pairs. In this case, secure key exchange, management of keys, and their storage in the device will be a big issue, so this scheme is not practical.

In [8] authors tried to overcome the problem of storing many anonymous certificates. To preserve the privacy of the users, the authors assumed that vehicles and roadside units collaborate with each other. In this algorithm, each vehicle requests an anonymous certificate from an RSU unit for a short time. This request is done in a short time when the vehicle is passing the RSU in two communication messages. Its reply in the form of an issued certificate to the device from RSU must be generated in a short span of time with reliability and lower latency. Since the vehicle will be at high speed, it will require high interaction with the RSU unit, which may affect the performance of the VANET. These certificates, which are intended to be performed in a short span of time, must be frequently verified. This will also affect the performance of the VANET. According to the authors in [9] and in [10], there is a high dependency on vehicles on the RSU, which is again a big issue. Because if any RSU crashes, then the whole network will slow down.

[11] Proposed a protocol using the mix zones method. It increases vehicle anonymity, but again, this protocol depends on a large set of predefined anonymous certificates stored in the vehicle's memory.

In [12], the author proposes a technique of certificate generation that uses the HMAC that is hashed message authentication code (HMAC); this scheme uses low communication overhead. In this scheme, a vehicle sends a message to ask to obtain a symmetric key from RSU. This communication is done using the key agreement protocol. To have more security, each vehicle will communicate with the RSU using different keys at different times. Likewise, in this scheme, the vehicle must be preloaded with multiple public keys. As per the robustness concern, protocol depends on the RSU unit. If it is corrupted, then the whole network will slow down.

One ID-based certificate generation scheme is proposed by authors in [13]. This scheme does not use complicated certificates; instead of certificates, it uses ID-based cryptography. Also authors in [14] use the well-organized provisional protocol for privacy in vehicular communications in this proposed scheme. This scheme depends on the tamper-proof devices built on the vehicles. The system master key is stored in these devices and is used to generate the vehicle's identities from time to time. These identities fulfill the work of anonymous certificates. There were a few problems in this scheme. Storing the master key in all the devices will result in exposing the whole system to powerful attackers. However, the author has given the concept of powerful tamper-proof devices, which stores the master key in their memory to prevent it from attackers. However, since the master keys are involved in all the local communications, it will be traced out by calculating the energy consumption in computations. Information could also be traced out by the emitted radiation. Using statistical methods and the emitted radiation, secret information could be identified. Although this attack is expensive, it will give the attackers full control over the system if successful.

2.2.2. Techniques Based on Group Signatures

Another type of technique is known as group signatures. It was proposed by authors in [15, 16] and [17]. These techniques are alternatives to anonymous certificates. The imitation of anonymous certificates is pre-storing a large number of certificates in the vehicle memory, resulting in high costs. Alternatively, in group signature-based techniques, there is a group owner whose work is to issue and open the communication. All other vehicle nodes have the master key of the group. Any vehicle node can sign a message on behalf of the group. The verifier can verify the signature using the group public key, but he cannot trace out the vehicle that signs it. In case it is required, the group owner can identify the vehicle who signs it. The main advantage of using this technique is to save the storage and cost due to the pre-storing of multiple anonymous certificates.

Authors in [18] proposed a security framework for vehicular ad hoc networks based on group techniques. However, this scheme did not undergo an experimental analysis.

Authors in [19], presented the first experimental analysis of a scheme based on group signatures. They presented a GSIS scheme, which is based on group signatures and provides privacy-preserving VANET. In this scheme, there is a single owner who issues the secret keys to all the members. This scheme is not suitable when there are compromised vehicles on the network. Also, there is a dependency on a single node, so the scheme is not efficient enough.

2.2.3. Signature Aggregation in VANETs

There are a few problems that are still unsolved in VANET, like how to store a large number of signatures in a small storage OBU memory, how to verify these signatures in a short interval of time when the vehicle is moving fast, how to compress and store cryptographic entities as evidence, and how to avoid these conflicts of investigation and limitations of data storage in small memories.

Authors in [20] presented a solution to validate the data aggregated from the nodes. This scheme was based on the public key infrastructure scheme. These schemes focused on collecting messages instead of signatures. The idea behind this scheme is to hook the attacker and avoid the attacks over the network. The solution is considered to be tamper-proof because in this, each vehicle has to perform a few security operations and time stamping. This solution also suffers from a few limitations, such as this scheme can handle the modifications done in data and check for fake things as well, but it does not give any solutions about the data omissions. Aggregation is also not taken care of in this scheme. The main solution this scheme provides is the use of a proof device. But this again increases the cost of this additional hardware device. Also, it compromises the flexibility of the device.

Authors in [21] proposed a scheme to aggregate the signature based on BLS. They mentioned that signatures must be aggregated up to one certificate authority level only. Authors in [22] mentioned a scheme that is based on verifying the signatures as well as the PKI. They also verify the aggregated signatures. This scheme was able to verify the large number of certificates and the certificates in a short time. However, this scheme did not consider the relay of messages, which is essential in vehicular ad hoc networks.

2.2.4. Privacy-Preserving LBS Protocols

Location-based services are proven to be an attractive type of VANET. Privacy-preserving protocols focus on the security and privacy in the application designed for the VANET. Authors in [23] proposed a new scheme known as AMOEBA. This scheme provides robustness by using concept 3. By the application of the LBS protocol scheme, a group leader is selected and used as the proxy server. It forms a group of vehicles that are connected to a group dynamically. Due to its dynamic nature, it is hard to maintain a network. Again, there are a few limitations also. In this owner is compromising its location information because it is broadcasting the location information for preparing the group. Also, there is a lack of end-to-end encryption between the owner and the registered vehicle. The whole network relies on a single node that may result in a single point of failure.

2.3 Error Recovery Through Classical Approaches

ARQ and Forward Error Correction (FEC) are classically used for error recovery. These techniques are used over unreliable channels to prevent and remedy packet loss. The above techniques are defined in a further section. Their advantages and disadvantages are presented. Both schemes' qualities are not suitably fit for error recovery in VANET.

2.3.1. Error Recovery Through ARQ Approaches

Automatic Repeat Request (ARQ) [24, 25] is also known as backward error correction (BEC) schemes. This error control scheme works by calculating the error detection codes and uses positive acknowledgment when the frame is successfully received and negative acknowledgment when it is not received. It also uses timers to ensure reliability. ACK is particularly a short message that is used to ensure whether the frame is successfully received at the receiver side or not.

In this scheme, the sender is usually not receiving the ACK message, and the time out occurs. Then, it is assumed that transmission is not successful, so we need to resend the frame. It retransmits the frames again and again until they receive the ACK. ACK confirms the packet is successfully received. In other ways, frames are retransmitted when there is any failure in the reception of the packet or the sender receives the negative ACK from the receiver, indicating that the receiver does not receive the frame.

2.3.2. FEC Mechanism

In contrast to the ARQ scheme, in which we used to do data transmission awareness by means of ACK/NACK, the FEC scheme improves transmission reliability through data redundancy.

FEC is a channel coding technique used for controlling data packet transmission. In this scheme, error recovery is done by transmitting the redundant data along with the original data. This redundant data is used to correct and recover the error if there is any error on the path instead of retransmitting the frame again. It helps to recover the data from the errors due to data loss. It does not need a reverse channel because it does not use an acknowledgment system. The FEC scheme is suitable when there are retransmission are more costly than the forward channel. In the case of multicast, when there are multiple receivers but only one-way communication, the size of the redundancy, which is sent with the original data packet, is usually smaller than the error-correcting codes (ex. turbo code [26] and Reed-Solomon code [27]).

2.3.3. Hybrid ARQ Technique

This technique is the grouping of two famous techniques, that is the FEC scheme and the Automatic Repeat Request technique. In the FEC technique, the sender sends the redundant information along with the original packet messages like cyclic redundancy check codes. But in the hybrid ARQ technique, the original packet is encoded with the redundant information, and party bits are sent alongside the original packer data. Or this could be sent on demand by the receiver when there is any erroneous packet received. In the hybrid technique, the Solomon codes are typically used, which can perform the FEC and error detection. Additionally, the ARQ technique is also used to retransmit the data packets in case the errors in the packet are not correct using the error detection and correction technique of FEC. Several techniques have been used, including the HARQ technique, in the past [28, 29, 30] for efficient recovery of errors in wireless communication. They used FEC for error recovery of the packets in the path, and ARQ methods were used where NACK frames could be retransmitted when a receiver sent the request of retransmission if that packet could not recovered by the FEC scheme. No doubt HARQ outperforms both the ARQ and FEC techniques, but this results in lower throughput than the original FEC and ARQ techniques. HARQ technique could be feasible in case of: 1) the unique data packet is sent in the stream so that the source can add redundancy codes which can be used for error detection and correction, and 2) the receiver can send the NACK back to the sender so that retransmission can be possible.

However, these mentioned conditions could not be possible in a road safety environment, so the above discussion cannot be practically possible. Table 2 showing the summary of existing Error recovery techniques for VANET. Table 3 and 4 is the summarization of privacy and trust based algorithms proposed for VANET.

Table 2. Survey Summaries of Existing Studies on Error Recovery Techniques for Vehicular Networks

Ref. No.	Traffic Area	Type of Algorithm	Performance Parameters
[1]	Urban- Varying densities of Vehicles	Safety message dissemination	Reception Failure Channel Probability
[2]	Highway- Varying densities of Vehicles	Warning/ Periodic messages for Safety-Broadcast	Collision, Latency, Reception Rate
[3]	Highway- Varying densities of Vehicles	Real-time transfer of Safety message	Rate of Packet Receiving
[4]	Highway / Urban- Varying densities of Vehicles	Warning/ Periodic messages for Safety-Broadcast	Delay, Probability of Successful Delivery
[5]	Highway	Periodic messages for Safety-Broadcast	Delay, Rate of collision, Data Reception rate
[6]	Highway Varying densities of Vehicles	Safety message- Broadcast	Average delay rate, Successful delivery Probability
[7]	Highway	Safety and Reliable message	Probability of frame failure
[8]	Highway	Safety-critical message- Reliable	PDR, Throughput

Table 3. Algorithms for present security attacks

Ref. No.	Paper overview	Security dimensions	Limitations of used technology
[9]	"Gives an overview of various attacks"	Replay attacks, DOS, Routing attacks, fake information attacks.	Privacy problem
[10]	"Overview of security issues in vehicular ad-hoc networks"	Eavesdropping, Tracking of Location, ID revealing, attribute-based DOS attack	Not addressed privacy problems
[11]	"Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET".	Fake attack	Gives a solution for Fake attacks only.
[15]	"Security Analysis of Vehicular Ad-Hoc Network (VANETs)"	Replay attack, DoS attack Fabrication attack, alteration attack, replay attack, message	No solution for other attacks

Ref. No.	Paper overview	Security dimensions	Limitations of used technology
[16]	"Security challenges, Issues and their solutions on VANETs"	• Replay Attack, DoS, Attack in Routing, Masquerade attack • DOS • Node Impersonate	No solution for confidentiality.
[51]	"signature-based authentication'' in VANETs"	DOS	Not so effective
[19]	"Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks"	Node Impersonate	No solution for other attacks
[20]	"Outlier detection in ad hoc networks using dempster-shafer theory"	Node Impersonate	No solution for other attacks
[12]	"Detection and localization of Sybil nodes in VANETs"	Sybil Attack	No solution for other attacks
[13]	"P2DAP Sybil attacks detection in vehicular ad hoc networks"	Sybil Attack, Sending false info, ID Disclosure	No solution for other attacks
[14]	"Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks"	Sybil Attack, Sending false info, ID Disclosure	No solution for other attacks
[18]	"Anovelsecure communication scheme in vehicular ad hoc networks"	Sending false info, ID Disclosure	No solution for other attacks
[21]	"A group signature based secure and privacy-preserving vehicular communication framework"	Sending false info, ID Disclosure	No solution for other attacks
[6]	"Defence against Sybil attack in vehicular ad-hoc network - based on roadside units support"	Sybil Attack	No solution for other attacks
[22]	"Privacy Technique"	Node Impersonate, Sending false info	No solution for other attacks
[23]	"Distributed misbehavior detection in VANETs"	Sending false info	No solution for other attacks
[25]	DoS Detection algorithm	It records the information of the vehicle for any unusual behavior	Time-Consuming
[26]	DoS detection algorithm Using Malicious and Irrelevant Packet Detection Algorithm	Calculate the time of packet generation and detect malicious nodes	Computing the vehicle position in RSU takes maximum time
[27]	Mitigating the effect of DoS Attack in VANETs using Multiple Malicious Nodes detection technique	To detect the multiple malicious node in the network by entropy and bandwidth	Less detection rate of malicious node.
[28]	Greedy Behavior Attack Detection Algorithm	It analyses network traffic by greedy nodes behaviour	The false positive rate is maximum in case of increased greedy nodes
[29]	Dempster Shafer Theory based Denial of Services Attack detection	Prepare trace file for self-organized map (based in machine learning)	Detection of misbehavior rate is low
[30]	Extenuation of DoS attack in VANETs	It detects fraud nodes by matching signature based authentication scheme	Method will not work in case if False information sent by attacker
[31]	Denial of Service (DoS) attacks detection in VANET	It uses Bloom filter to detect malevolent vehicle	This method is not suitable for high traffic environment.
[32]	Port hopping based Dynamic Defence Strategy for VANET	It manages vulnerable service port number for V2V and V2I communication	It fails to handle the issue of hopping frequency
[33]	Detection and Extenuation of DDoS Attack in VANET	This technique isolates fraud node from other victim nodes	High bandwidth consumption and difficult to manage the control packet
[34]	Multivariant approach to mitigate DDoS attacks	Using payload tracing and frequency assessment track and detect the malicious nodes	It reduces the packet latency but not guaranteed
[35]	Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey	Using SVM it analyses the misbehavior node	The false positive rate is maximum

Table 4. Survey of the Trust Establishment Approach

Ref. No.	Description	Algorithm	Performance/ Limitations
[36]	It is working as middle layer to build trust between two nodes	SAT architecture (Situation Dari Awareness Trust)	Performance: Controlled policy and Trust enhancement network
[37]	Uses watchdog algorithm for intrusion detection	Intrusion detection using Watchdog algorithm	Increased Latency in area coverage, False negative & false positive
[38]	Dynamic Trust Token provides trust on Real Time basis	Dynamic Trust Token	Degrade latency and Integrity
[39]	ECDSA- used for authentication and verification of data transfer	Proxy Signature-based on ID	Depends on Message transfer through trusted RSU
[40]	Prevents internal attacks by quickly transfer opinion about messages	RABTM(Beacon based trust system using RSU)	Compromise to Location privacy of vehicles
[41]	Identification of malevolent and self-centered nodes which node broadcast bogus information.	TRIP	Try to identify fraud node vehicle which dispersal wrong information
[42]	Uses generation and piggybacking opinion about node reputation	VSRP algorithm	It do Event Modification, false event generation, data aggregation and data

3 Challenges and Research Gaps

Secure communication in the vehicular ad hoc networks is an open research area. VANET is the research area that allows the researchers to study and evaluate their research work. Future VANET will not be limited to the Vehicle and RSU; they will connect to the outside network through various entities. The algorithms made for traditional environments cannot work as it is with the V2X networks. Various work has been carried out in this direction. Still, there are some open areas for research. In this section, we have listed down a few open issues:

Gap 1: Attacks on VANET Security

- Traditional techniques using trust-based models in which privacy is monitored by the behavior of the neighbors. Some famous attacks are there, like whitewashing attacks, On/Off attacks, and good/back-mouthing attacks. These attacks enable this compromised node to behave as the original node so that it cannot be detected by the network. Most of the existing networks could not identify the malicious nodes. So here, we will propose a model that will consist of a few intelligent nodes that can detect the compromised nodes on the network.
- Communication inside the various trains, metros, and buses is done using wireless communication. Wired communication cannot be used in these situations. Wireless communication is more prone to attacks than the wired network. They are more susceptible to cyber-attacks. For instance, Authors in [43] proposed a secure system based on host identity protocol. It is designed to protect intra-vehicular communication from common IP-based attacks. We will try to propose an algorithm based on host identity. This algorithm will work for intra-vehicle communication for their protection from IP-based attacks.
- Traditionally, many algorithms use the RSU as the fully secured unit, which is used for many security solutions. RSU is required by the user to update security-related information. But in practice, RSU could not be available every time along the roadside. Like any other roadside entity, RSUs are also vulnerable to attacks [44]. RSU attacks have more impact on the network performance. So here, we need a secure protocol for the distribution of keys through which we can identify the hacked RSU.
- Many security algorithms we proposed in the literature were applied to the central units of the network. However, security solutions applied on central entities are not sufficient, so there must be some security which is applied at distributed places. In VANET, distributed solutions are more efficient than the centralized ones. However, we need a hybrid system that works in a centralized as well as a distributed manner.

Gap 2: Quality of Service Management

- Quality of Service is used to represent the performance level of the users. QoS level can be maintained by sufficient allocation of resources and infrastructure. Also, bandwidth, power consumption, delay in transmission, and equipment are not been controlled in the VANET because there is not any fixed topology and consistent infrastructure. In [45], Wang et al. proposed a method to have the spacing information and the density of the traffic. Some security information needs to be added to prevent the attacks. However, some security mechanisms are needed in consistency with having the QoS. This is the essential task. The security model must use all the resources efficiently in order to achieve the QoS. All the parameters, such as throughput and power consumption delay, must be considered. Most models for security cannot consider power consumption because they apply to long-life battery vehicles. But V2X includes various devices whose battery life is short, such as mobile phones. Here, we need a security model that efficiently utilizes the resources in the V2X network.
- Efficient use of the network resources, such as bandwidth, is required in order to achieve the QoS. Authors in [46] elaborate on a delay-optimal scheme for VANET, which is integrating the software-defined resource allocation into the LTE system. The model proposed in [47] wastes the bandwidth because it elaborates on sending the same information over multiple channels to achieve reliability. Models elaborated in [48, 49] increased overhead by increasing the packet size, which again did not align with the QoS. Applications used in safety need low latency time to receive the packet at the side of the receiver to have high security, but almost all encryption methods need time to do the encryption and decryption processes. Thus, the algorithms proposed for security have the capability to provide secure communication, but they have few negative impacts on the QoS.
- The solutions proposed till now are being simulated, but these simulation models do not consider the environment. Such a model is proposed in the urban and rural environment. They also did not consider propagation and mobility parameters like multipath propagation, obstacles, and signal fading. So, we need one security model that considers all these parameters.
- To ensure QoS in terms of latency. Edge computing is to be applied on the IoT devices so that data must be processed near the devices rather than running through the long route to reach the central cloud to process. It reduces the delay. Edge computing has been done in the case of VANET, which is known as V2X edge computing. This is also suitable for message that requires short latency, such as warning messages. Although we have a lot of solutions, security is still a serious challenge in vehicular edge computing [50].

Gap 3: Communication Link Quality

- As we know, VANET includes nodes that work at high speed. They have a very short connection time for data transmission. These nodes' transmission and reception may be affected by obstacles on the roads, like trucks, big vehicles, and buildings. So, they require a very good communication link. This is still a challenge in VANET. Existing models used IEEE802.11 p as a communication protocol. Which could not be used in LTE-V2X directly because this has a high data rate and low transmission power. So, practically evaluating any existing model is not possible.
- Traditionally, researchers focused on choosing a gateway node that can connect the connection between VANETs and LTE-A. It is to be noted that the selection criteria for a gateway node are different from the relying node. It may be possible that the connection may get disconnected when the second round of gateway selection criteria comes. Also, a few nodes may select the same node as the relay node to forward their packets, which can result in an overflow. In these cases, the VANET is affected negatively. So, it is an open research area to design a QoS relay node and gateway node selection.

Gap 4: Data Reliability for VANET

In VANET, all data communication is in real time. So, data reliability is very much needed to make timely decisions. If some data packets are not received in time, then many critical conditions may occur that may result in accidents. So, ensuring data reliability at the endpoint is very much necessary and an open research area for researchers.

4 Challenges in Designing VANET

Some of the peculiar properties of VANETs are listed as follows [51]:

1. **Mobility:** VANET has very high mobility. In MANET, a medium level of mobility is observed, but in VANET, generally, very high-speed node mobility is observed. On highways, the typical speed of vehicles is generally between 80 and 110 km/h. But in urban areas, the speed of the vehicles is observed to be 40- 60 km/h.
2. **Highly dynamic topology**: Multiple-lane roads are available, so along with the very high speed of nodes, they can have multiple routes, making multiple topologies possible.
3. **Non-random vehicular mobility**: In VANET, vehicular mobility is not fixed. It varies based on human driver behavior and road layouts and is subject to different traffic rules and regulations.
4. **Varying network density**: Network density is also not fixed. It is higher during rush hours and lower in rural areas than in urban areas. Also, day and night affect traffic density. At night, traffic density is much lower than in the daytime.
5. **Recurrent network fragmentation**: Frequent fragmentation in VANET is also the result of very low-density traffic, lane changes, and high mobility irregularity. Due to high speed, vehicles move from each other, disconnection with radio interfaces, and connection to others.
6. **Harsh operating environment**: In VANET, vehicles move at very high speeds. Along with this high speed, many unavoidable environmental conditions affect communication, such as buildings and trees. They cause harsh fading and shadowing effects. These may worsen the communication of wireless communication, which is naturally unreliable.
7. **Unconstrained energy capacity**: Various entities used in VANET, such as OBUs, multi-sensors, mobiles, and other electronic elements in smart vehicles, use the reserve power of the node's battery. So, power is not limited in the design of vehicular networks.

5 Problem Statement

In VANET, the safety system depends only on real-time communication between wireless entities such as RSUs, mobile nodes, and handheld devices used by pedestrians. This communication allows safe driving and prevents accidents. However, effective road safety depends on communication protocols, which must guarantee the reliable exchange of data packets. Thus, the guarantee of reliability must be ensured such that each packet of data communication carries some message related to life-saving or saving from loss of property. Currently, the IEEE 802.11p protocol is approved for use in VANET through MAC protocol (Distributed Medium Access Control Protocol). In this protocol, there is a lack of a central controller who can control all the tasks and coordinate with the other nodes for communication. Resulting in high collisions, packets could not be delivered in an error-free manner. In road safety communication systems, each vehicle has to transfer its status periodically, a minimum of one in every 100 ms, which results in collisions that may collide the whole communication system. An increased number of collisions in the absence of a central controller may result in reduced reliability of the packets, especially when there are rush hours when reliability is the foremost concern. All conventional communication systems suffer from low reliability and poor QoS. This is because of the high interference, high collisions, and absence of a controller, noise, and high mobility variations. All these things result in the loss of safety packets, which contain the information that can make the decision on life over death. Thus, we require safe and reliable communication of safety packets, which can be efficient enough for error recovery. For the same we require an error recovery scheme capable of sending reliable and secure way of packet transfer.

6 Conclusion and Future Work

Since VANET is a very vast area and very important for day-to-day life. After studying the state of the art of VANET. There are a few research areas we have identified to work on. First, we need to design novel methods for securing vehicular communications in V2X networks. Further, we can design an algorithm for reliable communication of information in VANETs. Researchers can focus on establishing a secure framework for the development of effective road traffic safety communication systems for our increasingly overcrowded highways.

References

[1] Xu, Q., Mak, T., Ko, J. and Sengupta, R. (2004). 'Vehicle-to-vehicle safety messaging in DSRC'. In: *Proceedings of 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET04)*, Philadelphia, PA, USA, pp. 19-28.

[2] Yang, L. and Guo, J. (2008). ' Increasing broadcast reliability by coded cooperative repetition in VANETs '. In: *Proceedings of First International Conference on Wireless Access in Vehicular Environments*, Dearborn, Michigan, USA, pp. 1-5.

[3] Wu, Y., Yang, L., Wu, G. and Guo, J. (2009). 'An improved coded repetition scheme for safety messaging in VANETs'. In: *Proceedings of 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom '09)*, Beijing, China, pp. 1-4.

[4] Farnoud, F. and Valaee, S. (2008). 'Repetition-based broadcast in vehicular ad hoc networks in Rician channel with capture'. In: *Proceedings of IEEE INFOCOM Workshops*, Phoenix, AZ, USA, pp. 1-6.

[5] Yang, L., Guo, J. and Wu, Y. (2009). 'Piggyback cooperative repetition for reliable broadcasting of safety messages in VANETs'. In: *Proceedings of 2009 6th IEEE Consumer Communications and Networking Conference (CCNC '09)*, Las Vegas, NV, USA, pp. 1-5.

[6] Honarvar, A. and Valaee, S. (2010). 'Selection of repetition codes for MAC in vehicular ad hoc networks'. In: *Proceedings of 2010 IEEE Wireless Communication and Networking Conference*, Sydney, Australia, pp. 1-6.

[7] Farnoud, H.F. and Valaee, S. (2009). 'Reliable broadcast of safety messages in vehicular ad hoc networks'. In: *Proceedings of IEEE INFOCOM 2009*, Rio de Janeiro, Brazil, pp. 226-234.

[8] Dang, D.N.M., Nguyen, V., Chuan, P., Oo, T.Z. and Hong, C.S. (2014). 'A reliable multi-hop safety message broadcast in vehicular ad hoc networks'. In: *Proceedings of 2014 16th Asia-Pacific Conference on Network Operations and Management Symposium (APNOMS)*, Hsinchu, Taiwan, pp. 1-6.

[9] Singh, A., Mishra, R. and Kumar, R. (2016). 'VANET security: issues, challenges and solutions'. *International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 1050-1055.

[10] Ribagorda, A., de Fuentes, J.M. and GonzalezTablas, A.I. (2010). 'Overview of security issues in vehicular ad hoc networks'. In: *Handbook of Research on Mobility and Computing*, IGI Global.

[11] Horng, S., Tzeng, S., Li, T., Wang, X., Huang, P. and Khan, M. (2015). 'Enhancing security and privacy for identity-based batch verification scheme in VANET'. *IEEE Transactions on Vehicular Technology*, 66(4), pp. 3235-3248.

[12] Xiao, B., Yu, B. and Gao, C. (2006). 'Detection and localization of Sybil nodes in VANETs'. In: *Proceedings of the 2006 Workshop on Dependability Issues in Wireless ad Hoc Networks and Sensor Networks*, pp. 1-8.

[13] Tong, Z., Choudhury, R.R., Peng, N. and Chakrabarty, K. (2011). 'P2DAP: Sybil attacks detection in vehicular ad hoc networks'. *IEEE Journal on Selected Areas in Communications*, 22(3), pp. 582-594.

[14] Zhou, T., Choudhury, R.R., Ning, P. and Chakrabarty, K. (2009). 'Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks'. *Mobiquitous*, Aug. 2009.

[15] Jyoti, G., Manoj, S.G. and Vijay, L. (2010). 'A novel defense mechanism against Sybil attacks in VANET'. In: *Proceedings of the 3rd International Conference on Security of Information and Networks (SIN '10)*, ACM, New York, NY, USA, pp. 249-255.

[16] Yong, H., Yu, C., Chi, Z. and Wei, S. (2011). 'A distributed key management framework with cooperative message authentication in VANETs'. *IEEE Journal on Selected Areas in Communications*, 29(3), pp. 616-629.

[17] Park, S., Aslam, B., Turgut, D. and Zou, C.C. (2009). 'Defense against Sybil attack in vehicular ad-hoc network - based on roadside units support'. In: *Proceedings of the IEEE Military Communications Conference (MILCOM'09)*, Boston, MA, USA, pp. 1-5.

[18] Neng, W.W., Wueh, M.H. and We, M.C. (2008). 'A novel secure communication scheme in vehicular ad hoc networks'. *Computer Communications Archive*, 31(12), pp. 2827-2837.

[19] Ameneh, D. and Ghaffar, P.R.A. (2019). 'Detection of malicious vehicles (DMV) through monitoring in vehicular ad hoc networks'. *Springer Multimedia Tools and Applications*.

[20] Wenjia, L. and Anupam, J. (2009). 'Outlier detection in ad hoc networks using Dempster-Shafer theory'. In: *10th International Conference on Mobile Data Management*, pp. 112-121.

[21] Guo, J., Baugh, J.P. and Wang, S. (2007). 'A group signature based secure and privacy-preserving vehicular communication framework'. In: *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, Anchorage, Alaska.

[22] Hawi, F.A., Yeun, C.Y. and Qutayti, M.A. (2009). *The 4th International Conference on Information Technology (ICIT)*, pp. 3-5.

[23] Ghosh, M., Varghese, A., Kherani, A. and Gupta, A. (2009). 'Distributed misbehavior detection in VANETs'. In: *Proceedings of WCNC 2009, IEEE Wireless Communication and Networking Conference*, Budapest, Hungary, IEEE Press.

[24] Roselin Mary, S., Maheshwari, M. and Thamaraiselvan, M. (2013). 'Early detection of DoS attacks in VANET using attacked packet detection algorithm (APDA)'. In: *Proceedings of IEEE International Conference on Information Communication and Embedded Systems*, pp. 21-22.

[25] Singh, A. and Sharma, P. (2015). 'A novel mechanism for detecting DoS attack in VANET using enhanced attacked packet detection algorithm (EAPDA)'. In: *Proceedings of IEEE 2nd International Conference on Recent Advances in Engineering & Computational Sciences*, pp. 21-22.

[26] Quyoom, A. and Sharma, H. (2015). 'A novel mechanism of detection of denial of service attack (DoS) in VANET using malicious and irrelevant packet detection algorithm (MIPDA)'. In: *Proceedings of IEEE International Conference on Computing, Communication & Automation*, pp. 15-16.

[27] Kamboj, S. and Singh, K. (2018). 'Detection of multiple malicious nodes using entropy for mitigating the effect of denial of service attack in VANETs'. In: *Proceedings of IEEE 4th International Conference on Computing Sciences*, pp. 30-31.

[28] Nidhal, M. and Ben-Othman, J. (2016). 'GDVAN: a new greedy behavior attack detection algorithm for VANETs'. *IEEE Transactions on Mobile Computing*, 15(6), pp. 759-771.

[29] Pooja, B., Pai, M.M., Pai, R.M., Ajam, N. and Mouzna, J. (2014). 'Mitigation of insider and outsider DoS attack against signature based authentication in VANETs'. In: *Proceedings of IEEE Asia-Pacific Conference on Computer Aided System Engineering*, pp. 10-12.

[30] Verma, K. and Hasbullah, H. (2014). 'IP-CHOCK (filter)-based detection scheme for denial of service (DoS) attacks in VANET'. In: *Proceedings of IEEE International Conference on Computer and Information Sciences*, pp. 3-5.

[31] Guleria, C. and Verma, H.K. (2019). 'Improved detection and mitigation of DDoS attack in vehicular ad hoc network'. In: *Proceedings of IEEE 4th International Conference on Computing Communication and Automation*, pp. 1-6.

[32] Hong, X., Huang, D., Gerla, M. and Cao, Z. (2008). 'SAT: situation-aware trust architecture for vehicular networks'. In: *Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture*, pp. 31-36.

[33] Hortelano, J., Ruiz, J.C. and Manzoni, P. (2010). 'Evaluating the usefulness of watchdogs for intrusion detection in VANETs'. In: *Communications Workshops (ICC), IEEE International Conference on*, pp. 1-5.

[34] Biswas, S., Misic, J. and Misic, V. (2011). 'ID-based safety message authentication for security and trust in vehicular networks'. In: *Distributed Computing Systems Workshops (ICDCSW), 31st International Conference on*, pp. 323-331.

[35] Wei, Y.C. and Chen, Y.M. (2012). 'An efficient trust management system for balancing the safety and location privacy in VANETs'. In: *Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on*, pp. 393-400.

[36] Wang, Z. and Chigan, C. (2007). 'Countermeasure uncooperative behaviors with dynamic trust-token in VANETs'. In: *Communications (ICC'07), IEEE International Conference on*, pp. 3959-3964.

[37] Gómez Mármol, F. and Martínez Pérez, G. (2012). 'TRIP: a trust and reputation infrastructure-based proposal for vehicular ad hoc networks'. *Journal of Network and Computer Applications*, 35(3), pp. 934-941.

[38] Gazdar, T., Benslimane, A. and Belghith, A. (2011). 'Secure clustering scheme based keys management in VANETs'. In: *Vehicular Technology Conference (VTC Spring), IEEE 73rd*, pp. 1-5.

[39] Ding, Q., Li, X., Jiang, M. and Zhou, X.H. (2010). 'Reputation-based trust model in vehicular ad hoc networks'. In: *Wireless Communications and Signal Processing (WCSP), International Conference on*, pp. 1-6.

[40] Wang, J., Liu, Y., Liu, X. and Zhang, J. (2009). 'A trust propagation scheme in VANETs'. In: *Intelligent Vehicles Symposium, IEEE*, pp. 1067-1071.

[41] Gazdar, T., Benslimane, A., Rachedi, A. and Belghith, A. (2012). 'A trust-based architecture for managing certificates in vehicular ad hoc networks'. In: *Communications and Information Technology (ICCIT), International Conference on*, pp. 180-185.

[42] Serna, J., Luna, J. and Medina, M. (2008). 'Geolocation-based trust for VANET's privacy'. In: *Information Assurance and Security (ISIAS'08), Fourth International Conference on*, pp. 287-290.

[43] Chen, Y.M. and Wei, Y.C. (2013). 'A beacon-based trust management system for enhancing user centric location privacy in VANETs'. *Journal of Communications and Networks*, 15(2), pp. 153-163.

[44] Chen, C., Zhang, J., Cohen, R. and Ho, P.H. (2010). 'Secure and efficient trust opinion aggregation for vehicular ad-hoc networks'. In: *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*, pp. 1-5.

[45] Sahoo, R.R., Panda, R., Behera, D.K. and Naskar, M.K. (2012). 'A trust based clustering with ant colony routing in VANET'. In: *Computing Communication & Networking Technologies (ICCCNT) Third International Conference on*, pp. 1-8.

[46] Pooja, B., Pai, M.M., Pai, R.M., Ajam, N. and Mouzna, J. (2014). 'Mitigation of insider and outsider DoS attack against signature based authentication in VANETs'. In: *2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE)*, pp. 152-157.

[47] Kumar, P.V. and Maheshwari, M. (2014). 'Prevention of Sybil attack and priority batch verification in VANETs'. In: *International Conference on Information Communication and Embedded Systems (ICICES 2014)*, pp. 1-5.

[48] Ltifi, A., Zouinkhi, A. and Bouhlel, M.S. (2015). 'Trust-based scheme for alert spreading in VANET'. *Procedia Computer Science*, 73, pp. 282-288.

[49] Li, W. and Song, H. (2016). 'ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks'. *IEEE Transactions on Intelligent Transportation Systems*, 17(4), pp. 960-969.

[50] Kerrache, C.A., Lagraa, N., Calafate, C.T. and Lakas, A. (2016). 'TFDD: a trust-based framework for reliable data delivery and DoS defense in VANETs'. *Vehicular Communications*, 9, pp. 254-267.

[51] Khan, F.A., Imran, M., Abbas, H. and Durad, M.H. (2017). 'A detection and prevention system against collaborative attacks in mobile ad hoc networks'. *Future Generation Computer Systems*, 68, pp. 416-427.

Author Biographies

Wajid Ali earned his B.E. from Vishweshwarya Technical University, Bangalore, in 2009. After that, he received an M.Tech from IFTM University, Moradabad, UP, India, in 2012. Now, he is pursuing a Ph.D. in VANET from Teerthanker Mahaveer University. He has more than 14 years of teaching experience. His subjects of interest include networks, UWSN, and VANET.

Dr. Shalini Ninoria has 16 yrs of Academic & Research Experience with 5 years of Industrial Experience. Currently, she is an Associate Professor at CCSIT, Teerthanker Mahaveer University. She was IEEE UP SSAC Ambassador 2022 & 2023 and did UG & PG from Govt. University Campus RTM Nagpur University, Nagpur. Later, she earned a Master of Philosophy by Research in Computer Science and a PhD in Computer Science from Govt. State R.D. University, Jabalpur. Working domains are Data Mining, Pattern Mining, Soft Computing, Fuzzy Logic, Algorithms, Machine Learning, AI, Applied Mathematics, etc. Official Member of several Scientific Societies: IEEE, IEEE WIE, IEEE YP, IAENG, IEDRC, SDIWC, etc. Also listed in IEEE UP SSAC Ambassador 2022. She has published research papers in many international journals, including SCOPUS, UGC Listed, UGC Care Listed, and some articles under communication with SCI and Scopus journals. Attended various FDPs, FTPs, and Workshops organized by different National Importance Institutions. She delivered Expert Sessions at different organizations.

Dr Gulista Khan has 17+ years of Academic & Research Experience and is currently an Associate Professor at FoE, Teerthanker Mahaveer University. She earned a B.Tech from Kurukshetra University, Kurukshetra, Haryana, in 2009, an M.Tech from MMEC, Mullana, Ambala, Haryana, in 2009, and a PhD. from Teerthanker Mahaveer University, Moradabad, UP, India in 2019. Working domains are Mobile Computing, Cryptography, security, networks, UWSN and VANET, etc. Official Member of different Scientific Societies like IEEE and IAENG. She has published research papers in international journals, including SCI, SCOPUS, WoS, UGC Listed, UGC Care Listed, and some articles under communication with SCI and Scopus journals. Attended various FDPs, FTPs, and Workshops organized by different National Importance Institutions. She has delivered Expert Sessions at different organizations.

Kamal Kumar Gola is an Assistant Professor at COER University, Roorkee, India. He completed his B.Tech. Degree in Computer Science and Engineering from Moradabad Institute of Technology and his M.Tech. Degree in Computer Science and Engineering from Uttarakhand Technical University. He is pursuing a Ph.D. in Computer Science and Engineering from the Indian Institute of Technology, Jodhpur. With over 14 years of university teaching experience and six months of industrial experience, Kamal Kumar Gola is a seasoned educator with a wealth of knowledge in his field. He has published more than a sixty papers in international journals and has participated in various international and national conferences where he has presented his research. He kept himself updated by attending various professional development programs, workshops, and training courses organized by esteemed institutions such as IIT, NIT, IIIT, and others. His main research interests lie in Underwater Acoustic Sensor Networks, Algorithms, and Security.