World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Privacy and security issues surrounding vehicular Adhoc networks

Emmanuel Asituha *

Jaramogi Oginga Odinga University of Science and Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 20(03), 1449–1479

Publication history: Received on 11 November 2023; revised on 18 December 2023; accepted on 20 December 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.20.3.2602

Abstract

Vehicular Ad-Hoc Networks (VANETs) is a type of mobile ad hoc network (MANET) specifically designed for communication among vehicles on the road. VANETs enable vehicles to communicate with each other and with roadside infrastructure, forming a dynamic and self-organizing network without the need for a fixed communication infrastructure. Security concerns in VANETs encompass a range of threats, including Authentication and Authorization attacks, Sybil attacks, Denial-of-Service incidents, Location spoofing, and Eavesdropping. Privacy, on the other hand, is a paramount concern in VANETs due to the sensitive nature of location-based data, Identity Disclosure, and user consent Control. The paper emphasizes the necessity for robust security mechanisms and outlines specific requirements for safeguarding VANETs. Proposed mitigation measures, including cryptographic techniques and authentication mechanisms, are critically assessed for their effectiveness and feasibility. The findings provide a comprehensive understanding of the complexities surrounding privacy and security in VANETs, contributing valuable insights for the development of resilient and privacy-preserving vehicular communication systems.

Keywords: MANET; VANETs; RSU; OBU; DOS; RBAC.

1. Introduction

Vehicular Ad hoc Networks (VANETs) have emerged as a promising technology to enhance road safety, traffic efficiency, and overall transportation systems. By enabling vehicles to communicate with each other and with roadside infrastructure, this innovation enables real-time data exchange for diverse applications, ranging from enhancing road safety to optimizing traffic flow [1]-[6]. However, the pervasive deployment of VANETs introduces a host of privacy and security challenges that demand careful consideration and mitigation. VANETs represent a specialized form of Mobile Ad Hoc Networks (MANETs) designed to facilitate communication among vehicles on the road. VANETs leverage the wireless communication capabilities of vehicles to enable real-time exchange of information, contributing to enhanced road safety, traffic efficiency, and overall transportation system performance. These networks rely on Dedicated Short-Range Communication (DSRC) technology and can operate in both infrastructure-based and infrastructure-less modes [7]-[11]. In infrastructure-based VANETs, roadside units (RSUs) play a crucial role by providing a communication backbone, while infrastructure-less VANETs enable direct vehicle-to-vehicle (V2V) communication.

One of the primary applications of VANETs is in improving road safety through the exchange of safety-related information among vehicles. This includes warnings about accidents, traffic jams, road hazards, and other critical events. Additionally, VANETs support traffic management by optimizing route planning and traffic signal control based on real-time data. The implementation of VANETs is also seen as a key enabler for the development and deployment of intelligent transportation systems (ITS), contributing to the realization of smart cities [12]-[16]. Despite the promising benefits, VANETs face several challenges, including issues related to security, privacy, and network scalability [17]-[21]. Ensuring the authenticity and integrity of transmitted messages is crucial to prevent malicious attacks and misinformation [22]. Furthermore, the integration of VANETs with existing transportation infrastructure requires

* Corresponding author: Emmanuel Asituha

careful planning and coordination. Research and development efforts are ongoing to address these challenges and unlock the full potential of VANETs for creating safer and more efficient transportation systems.

1.1. VANETs History

The history of VANETs can be traced back to the early 2000s when researchers and engineers began exploring the potential of using wireless communication technologies to improve road safety and traffic management [23]-[26]. The concept gained momentum with the advent of Dedicated Short-Range Communication (DSRC), a communication standard specifically designed for vehicular communication. DSRC operates in the 5.9 GHz band and allows vehicles to communicate with each other and with roadside infrastructure, forming the foundation for VANETs. In 2003, the Federal Communications Commission (FCC) allocated the 5.9 GHz band for Intelligent Transportation Systems (ITS) in the United States, marking a significant milestone for the development of VANETs. Around the same time, various research projects and initiatives were launched globally to explore VANET applications, protocols, and system architectures. These efforts aimed to leverage VANETs for enhancing road safety through the exchange of real-time information among vehicles, such as warnings about accidents, sudden braking, and other critical events [27],[28].

As VANET research progressed, the focus expanded beyond safety applications to include traffic efficiency, environmental sustainability, and the integration of VANETs into smart city frameworks. Standardization bodies, such as the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI), played a crucial role in defining communication protocols and standards for VANETs. The IEEE 802.11p standard, an amendment to the widely used Wi-Fi standard, specifically addresses wireless access in vehicular environments, solidifying the technological foundation for VANET deployment [29]-[33]. In the subsequent years, field trials and pilot projects were conducted to validate the feasibility and performance of VANETs in real-world scenarios. These trials helped identify challenges related to scalability, security, and privacy [34], prompting further research and development efforts to address these issues. Today, VANETs continue to evolve as a multidisciplinary field, with ongoing research aimed at unlocking their full potential in creating safer, more efficient, and connected transportation systems.

Further innovations, as from 2011; The European Telecommunications Standards Institute (ETSI) standardized ITS-G5 as a communication standard for Intelligent Transport Systems (ITS), providing further clarity for VANETs deployments. This included protocols for message exchange, data formats, and transmission mechanism, incorporates security and privacy features to safeguard the integrity of communications and protect sensitive information exchanged in vehicular networks. This is crucial given the potential risks associated with unauthorized access and malicious attacks in VANETs [35].

1.2. VANETs Architecture

VANETs are a type of ad hoc network that enables communication among vehicles (V2V), between vehicles and roadside infrastructure (V2I), and potentially with other entities such as pedestrians (V2P). The Figure 1 below illustrates the basic VANETs architecture.

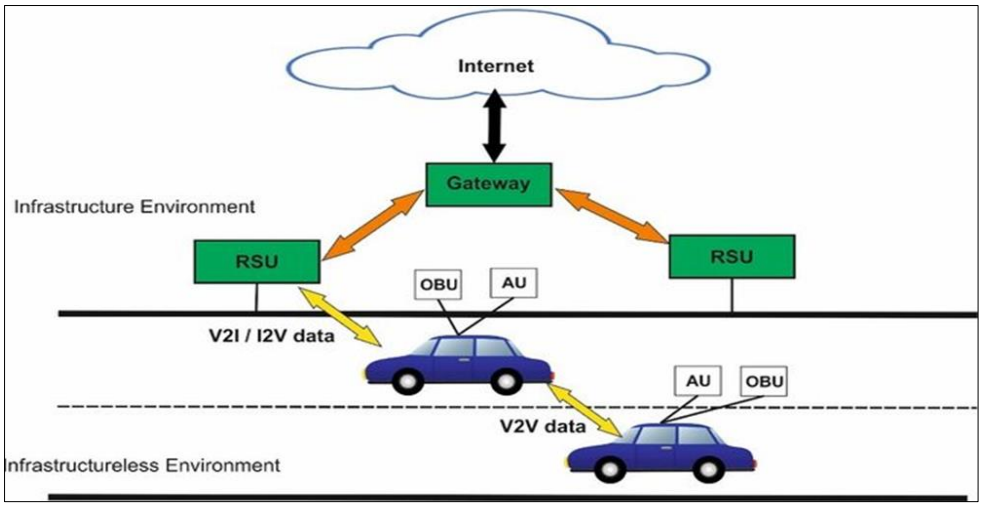

Figure 1 Basic Architecture of VANETs

The IEEE 1471-2000 and ISO/IEC 42010 standards, described that VANETs components are classified into three domains:

Mobile domain includes the vehicle and the mobile device domains. The former comprises all type of vehicles (e.g., cars, trains, buses) [36]. The latter includes all types of portable devices (e.g., smart-phones, laptop, smart watches).

Infrastructure domain incorporates the roadside infrastructure domain (e.g., traffic light, camera, etc.) and the central infrastructure domain (e.g., Traffic Management Centers (TMCs), Vehicle Management Centers) [37].

Generic domain includes the Internet and the Private infrastructures.

Authors in [35] explored the architecture of VANETs into three major domains, creating a holistic framework that integrates the ad hoc, infrastructure, and in-vehicle domains to create a connected and intelligent vehicular communication system as shown in Figure 2.

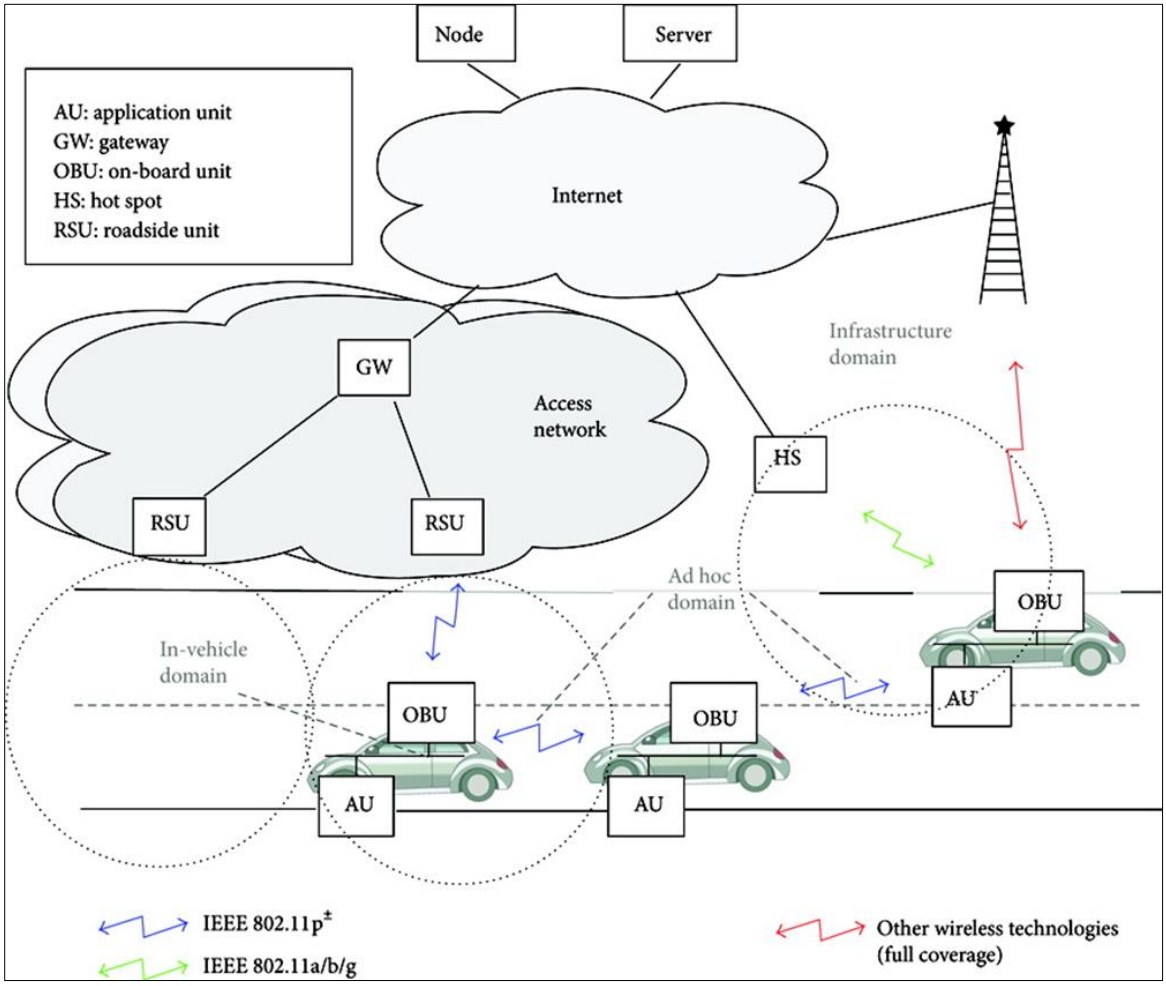

Figure 2 C2C-CC VANETs Architecture

In-vehicle domain consists multiple application units (AUs) and one On Board Unit (OBU). An AU is a dedicated device, which can be an integrated part of a vehicle or a separate portable device such as smart-phone, laptop, etc [39]. It runs one or many applications that exploit the OBU communication capabilities. The AUs and OBU are permanently connected through a wired or wireless connection.

Ad-hoc domain is composed of vehicles equipped with OBUs and stationary Road-Side Units (RSUs) deployed in specific locations along the road [40]. OBUs communicates with each other, directly or via multi-hop, using wireless short-range communication devices allowing ad-hoc communications [41] between vehicles. An RSU is a stationary device that can be connected to an infrastructure network or to the Internet. It can send, receive or forward data in the ad-hoc domain

(i.e., vehicles equipped with OBUs and RSUs), which enables to extend the coverage of the ad-hoc network. An OBU may access to the Internet via an infrastructure connected RSU, public commercial or private wireless Hot Spots (HSs) to communicate with internet nodes or servers.

Infrastructure domain access consists of HSs and RSUs. In case that neither RSUs nor HSs provide Internet access, OBUs can exploit cellular radio networks for example HSDPA, WiMax and 4G [42]. The detailed communication architectural design within the VANETs structure is shown in Figure 3 below.

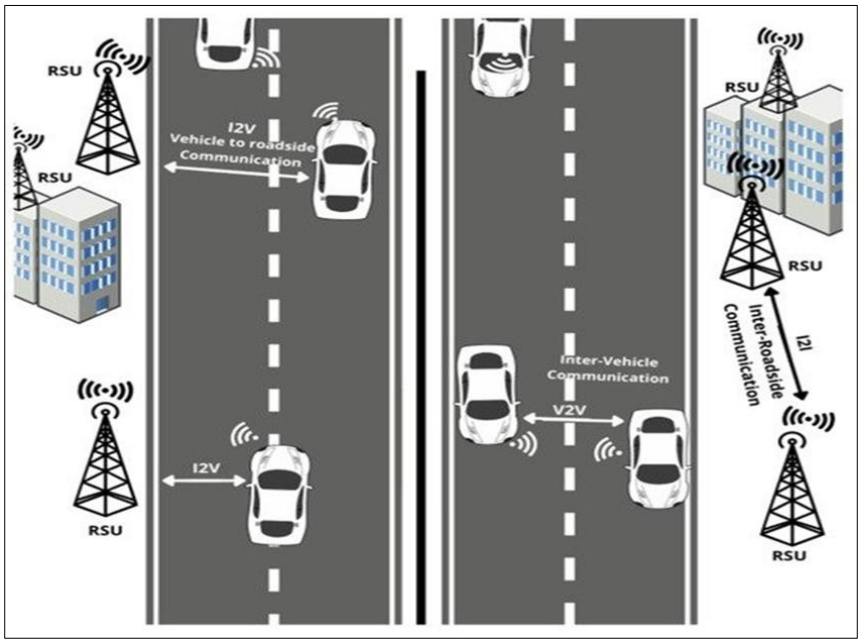

Figure 3 VANETs Communication Architecture

VANETs adopt similar concepts of connectivity and design as MANETs. VANET communication can be divided into three major categories:

- V2V communication, where vehicles can link immediately to disseminate messages to each other [43].
- V2I communication , in which the vehicle can connect with infrastructure-based networks for exchanging data wirelessly [44].
- Infrastructure-to-Infrastructure (I2I) networks to contribute to major vehicular applications [46]. A wireless connection exists between the infrastructure and nearby vehicles, where it can relay data in both directions (e.g., V2I and I2V).

The infrastructure offers up-to-date information and internet access to vehicles through this connection. As a result, they will receive major updates on current events as well as traffic on nearby highways**.**

As explained in [46], VANETs consist of several main components that work together to enable communication among vehicles and between vehicles and roadside infrastructure. These components contribute to the overall functionality and effectiveness of VANETs in enhancing road safety, traffic management, and overall transportation efficiency:

Onboard Units (OBUs): OBUs are essential components installed in individual vehicles [47]. They are equipped with wireless communication devices, such as Dedicated Short-Range Communication (DSRC) modules, GPS receivers, and sensors. The OBU serves as the communication interface for the vehicle, facilitating the exchange of information with other vehicles and roadside infrastructure. The inclusion of GPS [48] allows accurate positioning, enabling applications that rely on location data, such as navigation and cooperative collision warning.

Roadside Units (RSUs): RSUs are fixed infrastructure components strategically placed along roadways [49]. They act as communication nodes, providing a link between vehicles and the broader communication infrastructure. RSUs facilitate Vehicle-to-Infrastructure (V2I) communication, enabling vehicles to exchange data with the roadside infrastructure.

This interaction is crucial for applications like traffic signal control, congestion management, and access to centralized services [50], [51].

Vehicle-to-Vehicle (V2V) Communication: V2V communication is a fundamental aspect of VANETs, allowing direct data exchange between nearby vehicles. OBUs in one vehicle can communicate with OBUs in surrounding vehicles, sharing information such as speed, position, and status [52], [53]. V2V communication is vital for safety applications like cooperative collision warning, where vehicles collaborate to avoid potential hazards by sharing real-time data.

Communication Protocols and Standards: The communication protocols [54] and standards define how information is exchanged in VANETs. The IEEE 802.11p standard, an extension of the Wi-Fi standard, is commonly used for wireless communication in VANETs. These protocols govern channel access methods, message formats, and other communication parameters to ensure efficient and reliable data exchange [55]-[59].

Application Layers: VANETs support a diverse set of applications across different layers. Safety applications focus on real-time exchange of critical information [60] to enhance road safety, while non-safety applications include traffic management, infotainment, and environmental monitoring [61]-[64]. The architecture accommodates the specific communication needs of various use cases, making VANETs versatile in addressing different aspects of transportation.

Security Mechanisms: Security is a crucial component in VANETs due to the sensitive nature of the information exchanged. Security mechanisms include authentication, encryption, and pseudonymity [65]. Authentication ensures the legitimacy of communication participants, encryption protects data integrity and confidentiality, and pseudonymity helps safeguard individual driver privacy by using temporary identifiers [66]-[69].

Privacy-Preserving Techniques: Privacy is a significant consideration in VANETs. Privacy-preserving techniques, such as the use of pseudonyms, are employed to anonymize vehicles and protect the identities of individual drivers [70], [71]. These techniques strike a balance between the need for information exchange and the privacy concerns of vehicle owners.

These components collectively form the foundation of VANETs, enabling the seamless communication and collaboration necessary to improve road safety, traffic efficiency, and overall transportation systems.

2. Characteristics of VANETs

Understanding the features of VANETs is important in designing effective communication protocols, security mechanisms, and applications within the VANETs environment. These features make VANETs a unique and challenging domain for networking and communication research and development.

Dynamic Topology: VANETs have a dynamic and rapidly changing network topology as vehicles move in and out of communication range [72], [73]. The topology is influenced by factors such as vehicle speed, direction, and road layout.

Mobility: Vehicles in VANETs are highly mobile, leading to frequent changes in network connectivity [74]. Mobility patterns affect the efficiency of communication and network management.

Inter-Vehicle Communication: VANETs support both communication between vehicles (V2V) and communication between vehicles and roadside infrastructure (V2I). V2V communication is crucial for cooperative safety applications, while V2I communication enhances traffic management and infrastructure efficiency [75], [76].

Real-Time Communication: VANETs often require real-time communication to support safety applications, such as collision warning systems. Low latency [77] is essential for timely exchange of information between vehicles and infrastructure.

Broadcast Communication: Broadcasting is a common communication mode in VANETs, where a message from one vehicle is transmitted to all nearby vehicles [78]-[81]. Broadcasting supports applications like traffic information dissemination and emergency alerts.

Resource Constraints: Vehicles in VANETs typically have limited computational resources [82], power, and bandwidth. Protocols and algorithms must be designed to operate efficiently within these constraints [83], [84].

Secure Communication: Security is a critical concern in VANETs due to the potential impact of malicious activities on safety and privacy [85]-[88]. Authentication, encryption, and secure key management mechanisms are implemented to ensure the integrity and confidentiality of communication.

In essence, VANETs are characterized by real-time data exchange, allowing vehicles to share crucial information such as speed, position, and status with one another through Vehicle-to-Vehicle (V2V) communication. DSRC technology, often operating in the 5.9 GHz band, serves as the communication backbone, enabling low-latency and high-reliability connections. VANETs support both Vehicle-to-Infrastructure (V2I) communication, connecting vehicles with roadside units (RSUs) for additional services, and Vehicle-to-Everything (V2X) communication, encompassing interactions with pedestrians and other road users. The communication protocols, including the IEEE 802.11p standard, are designed to meet the stringent requirements of vehicular environments, and security features, such as authentication and pseudonymity, are integrated to ensure the integrity and privacy of transmitted data [85]-[94]. These characteristics collectively contribute to VANETs' role in enhancing road safety, traffic management, and creating intelligent transportation systems.

2.1. VANETs Application.

VANETs seek to connect devices contained within vehicles together to create services that are particularly relevant to a vehicular environment. They attempt to do so without relying on infrastructure devices to assist in the process of network topology management.

Authors in [95] classifies Applications of VANETs into four main categories as shown in Figure 4 below:

- Safety oriented
- Commercial oriented
- Convenience Oriented
- Productive Oriented

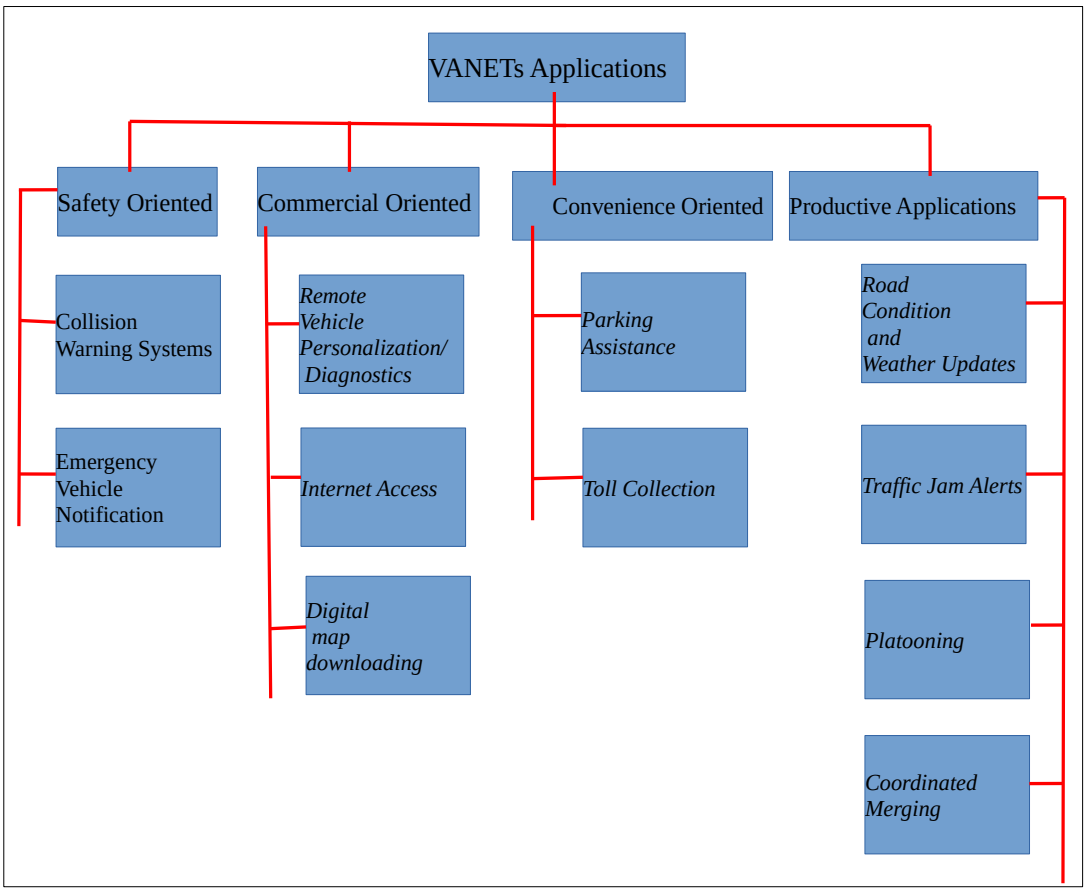

Figure 4 Applications of VANETs

2.2. Safety Oriented

VANETs safety Applications include: *Collision Warning Systems*, whereby VANETs enable vehicles to exchange information about their speed, position, and direction, allowing them to warn each other about potential collisions [96], [97]. Secondly, *Emergency Vehicle Notification* - Swift communication between emergency vehicles and surrounding vehicles can improve response times and clear paths for emergency vehicles.

2.3. Commercial Oriented

Commercial applications will provide the driver with the entertainment and services as web access, streaming audio and video. The Commercial applications can be classified as: *Remote Vehicle Personalization/ Diagnostics:* It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure. *The Internet Access, v*ehicles can access internet through RSU if RSU is working as a router [98], [99]. *Digital map downloading, contains m*aps of regions can be downloaded by the drivers as per the requirement before traveling to a new area for travel guidance.

2.4. Convenience Oriented

Equipped with *Parking Assistance Technology,* vehicles can share information about available parking spaces, helping drivers find parking more efficiently [100]. Automated toll collection systems can be facilitated through VANETs, improving the flow of traffic at toll booths.

2.5. Productive Applications

Contains the *Road Condition and Weather Updates* in which VANETs enables the dissemination of real-time information about road conditions, accidents, and weather conditions to enhance driver awareness [101], [102]. *Traffic Jam Alerts* in which vehicles can share information about traffic jams, helping others to choose alternative routes. *Platooning,* vehicles can form platoons by closely following each other, communicating to maintain a safe and efficient driving formation, reducing fuel consumption and improving traffic flow. *Coordinated* Merging in which VANETs enable coordination between vehicles when merging onto highways or changing lanes, optimizing traffic flow.

3. Security and privacy issues

Vehicular Ad-Hoc Networks, are involved in the communication between vehicles and roadside infrastructure. While these networks offer significant benefits, such as improved traffic management, increased road safety, and enhanced driver experience, they also raise various security and privacy concerns [103]-[105]. Security and privacy concerns in VANETs arise from the unique challenges posed by the dynamic and open nature of vehicular communication. One major issue is the vulnerability to malicious attacks, such as false data injection or denial-of-service attacks, which can compromise the integrity and reliability of information exchanged among vehicles. Moreover, the continuous broadcast of sensitive data, like location information and driving patterns, raises privacy issues as it can be exploited for tracking or profiling individuals. Ensuring secure and private communication in VANETs requires robust cryptographic mechanisms, authentication protocols, and intrusion detection systems to thwart malicious activities, while also addressing the need for preserving the anonymity and confidentiality of user data to instill trust among network participants.

3.1. Security and Privacy Requirements for VANETs

Security and privacy requirements for VANETs involve multifaceted considerations to safeguard the integrity, confidentiality, and availability of communication while respecting individual privacy. Figure 6 gives an illustration of security mechanism in VANETs. Robust cryptographic techniques are essential for secure message authentication and data integrity verification, preventing malicious entities from injecting false information into the network.

Privacy-preserving mechanisms, such as pseudonym changing and identity management, are crucial to mitigate the risk of unauthorized tracking and profiling of users. Additionally, secure key management and distribution mechanisms play a vital role in protecting communication channels. It is imperative to implement intrusion detection systems to promptly identify and respond to security threats. Striking a delicate balance between maintaining the security of the network and preserving user privacy is paramount in designing comprehensive security and privacy solutions for VANETs. For any system/network or architecture to be secure, it must align its principles with the CIA triad. Some sub-domains of the triad are discussed.

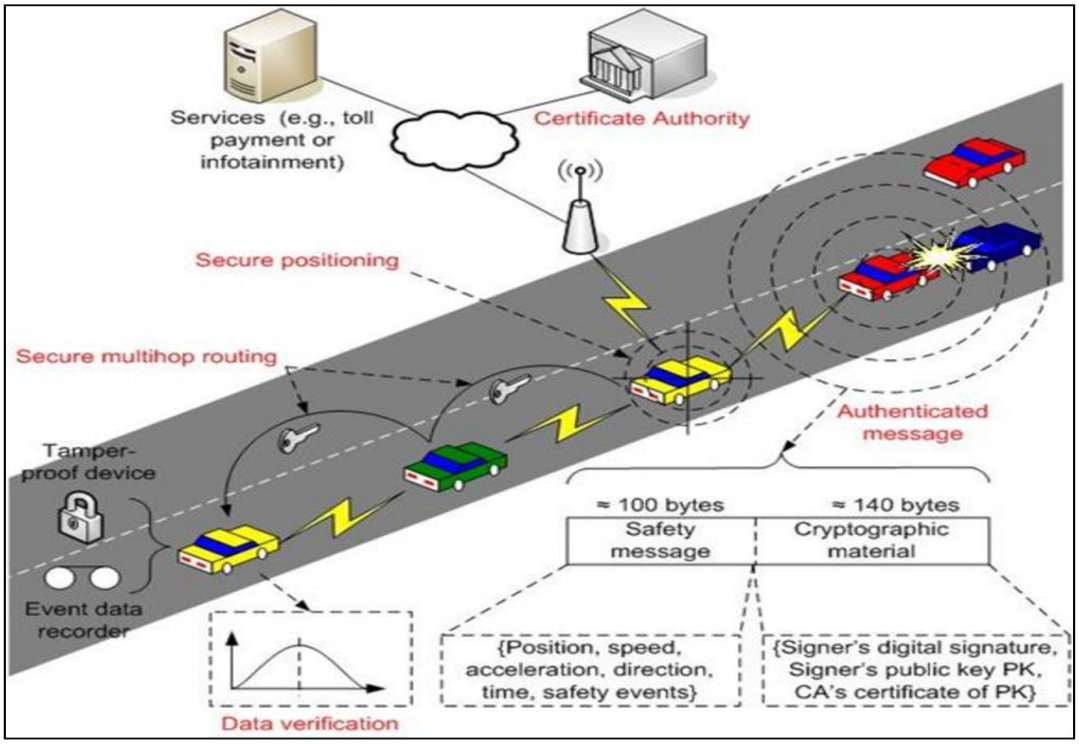

Figure 5 Security techniques in VANETs

3.1.1. Authentication

Authentication in VANETs is a crucial aspect to ensure that only authorized entities can participate in communication and to prevent malicious activities. Figure 6 illustrates some of the authentication schemes in VANETs. It is therefore clear that various authentication mechanisms are employed in VANETs to verify the identity of vehicles and entities within the network [106]-[111]. Some of the key aspects of authentication include:

Public key infrastructure: which utilizes a hierarchical system of digital certificates, public and private keys, and a certificate authority to facilitate secure communication, ensuring the authenticity of vehicles and their messages by verifying digital signatures using public keys [112], [113].

Pseudonymity and anonymous authentication. It involves the use of pseudonyms to protect the real identity of vehicles. Anonymous authentication allows vehicles to prove their authenticity without revealing their true identity [114]-[117]. Its major role in authentication is to enhances privacy by preventing the tracking of individual vehicles while still allowing for secure communication.

Group signature schemes: enables a member of a group to sign messages on behalf of the group. The verifier can confirm that the signature is from a group member but cannot determine which member, in return it supports secure communication within groups of vehicles without disclosing the specific identity of the signer [118], [119].

Efficient key management: Involves the secure generation, distribution, and revocation of cryptographic keys used for authentication and secure communication; making sure that only authorized entities possess the necessary keys, and facilitates efficient and secure key exchanges [120]-[123].

Message Authentication Codes: Cryptographic codes generated using a secret key to authenticate the integrity and origin of a message, thus protecting messages from tampering or unauthorized modifications, ensuring the integrity of the transmitted data [124]-[128].

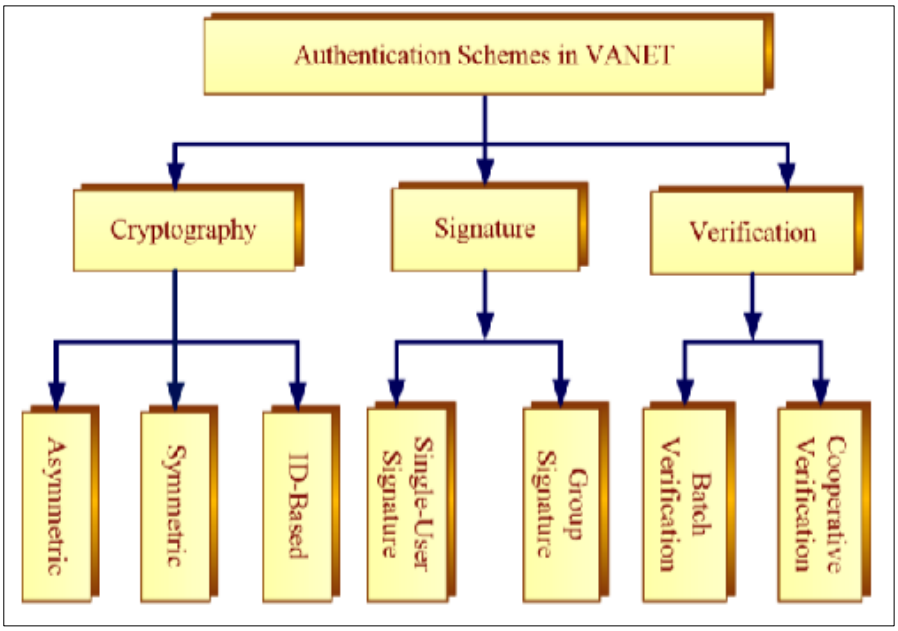

Figure 6 VANET authentication schemes

Time Based Authentication: it involves using time as a factor in the authentication process. Time-based mechanisms may include timestamps [129] or time-limited cryptographic keys, mitigating the risk of replay attacks and enhances the overall security of the authentication process.

3.1.2. Non Repudiation

Non-repudiation in the context of VANETs refers to the ability to ensure that a sender cannot deny having sent a message, and a recipient cannot deny having received the message. It is a critical security property that helps establish accountability and trust in communications. Non-repudiation is particularly important in VANETs, where reliable and irrefutable evidence of communication is essential for various applications, especially in the context of safety and security [130]-[135]. Key elements of non-repudiation include:

Digital Signatures: use cryptographic techniques to associate a unique signature with a piece of digital content as shown in Figure 7. It provides proof of the origin, identity, and integrity of the sender [136]. This serves as a cryptographic proof that a specific entity (sender) has approved the content of a message or transaction. It ensures that the sender cannot later deny their involvement.

Time stamps: records the exact time when a particular event or transaction occurs. In the context of non-repudiation, they provide a chronological record of actions [137]. This establishes the timeline of events, making it difficult for a party to deny the occurrence of an action at a specific point in time, thus enhancing the accountability and credibility of digital evidence.

Secure Time Synchronization: this ensures that all entities in a system share a consistent and accurate understanding of time [138]. It is crucial for aligning the timestamps across different components, preventing disputes, regarding the timing of events. Secure time synchronization is a critical aspect of network security, ensuring that all devices within a system maintain accurate and synchronized time. This is particularly crucial in scenarios like financial transactions, communication protocols, and distributed systems where precise timing is essential. To enhance security, time synchronization protocols need to resist various attacks, such as replay attacks or man-in-the-middle attacks, which could compromise the integrity and consistency of time across the network. Secure time synchronization often involves the use of cryptographic techniques and authentication mechanisms to verify the legitimacy of time signals and prevent malicious actors from manipulating or injecting false timing information. Implementing secure time synchronization is essential for maintaining the overall integrity and reliability of distributed systems, protecting against potential vulnerabilities that could arise from inaccurate or compromised timekeeping.

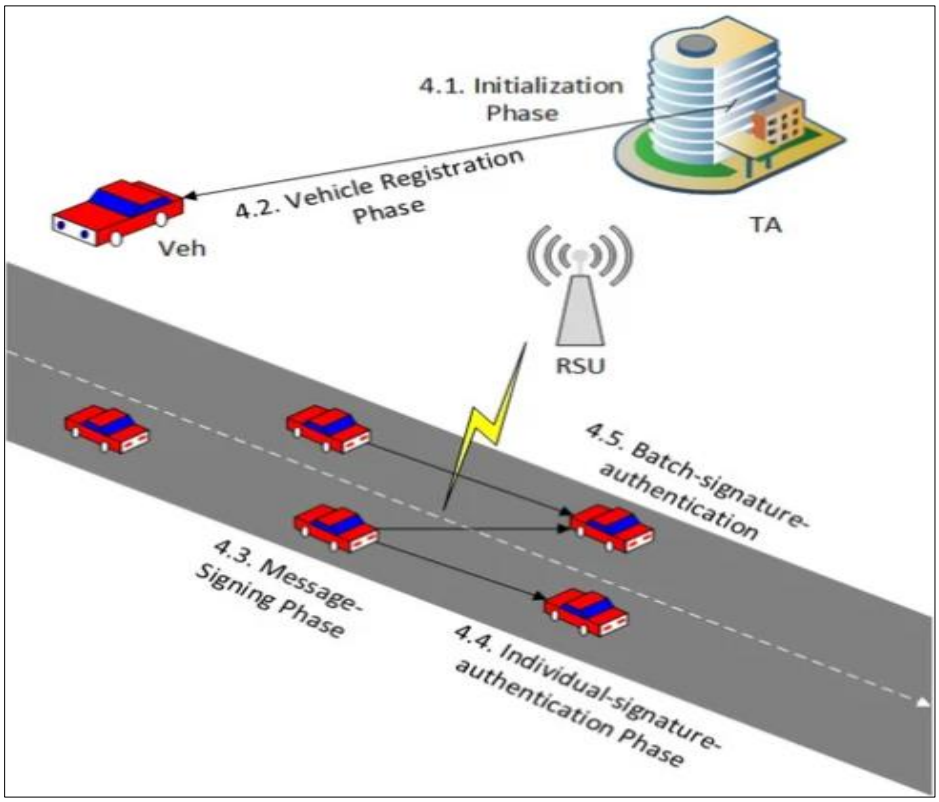

Figure 7 Signature-based authentication

Tamper-Evident Logging: are records that provide evidence of any tampering attempts or alterations to the logged information. They are designed to detect and indicate unauthorized changes. It contributes to the integrity of records [139]. If a party attempts to repudiate an action, tamper-evident logs can be used to demonstrate that the records have not been altered since the time of creation.

3.1.3. Message Integrity

Ensuring message integrity means that the content of messages exchanged between vehicles and infrastructure has not been altered or tampered with during transmission. Maintaining message integrity is essential to prevent malicious manipulation of information [140], particularly in safety-critical applications.

3.1.4. Message Confidentiality

It involves protecting the content of messages exchanged between vehicles and infrastructure from unauthorized access or eavesdropping. Confidentiality is crucial in VANETs to prevent sensitive information from being intercepted and misused by malicious entities [141], [142]. Key Mechanisms to ensure message confidentiality in VANETs include:

Encryption which involves converting the content of a message into a secure and unreadable format using cryptographic algorithms. Only entities with the appropriate decryption key can convert the message back to its original form [143], [144]. Safeguarding the content of messages from unauthorized access or eavesdropping. In VANETs, it ensures that only authorized parties can understand the information being exchanged.

Application of secure communication protocol such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), provide a secure channel for data exchange [145], [146]. These protocols incorporate encryption, authentication, and integrity checks, establishing a secure and authenticated connection between communicating entities, ensuring that messages remain confidential during transit.

Key management which involves the secure generation, distribution, and storage of cryptographic keys. It ensures that only authorized entities have access to the keys required for encryption and decryption [147], [148]. Maintaining the confidentiality of messages, preventing unauthorized entities from decrypting and accessing sensitive information by controlling access to cryptographic keys.

Selective disclosure which refers to the ability to control and limit the information disclosed to specific entities. It allows users or vehicles to disclose only necessary information to achieve a particular goal [149], [150]. By selectively disclosing information, VANETs participants can minimize the exposure of sensitive data. This mechanism helps balance the need for communication with the need to protect privacy and confidentiality.

3.1.5. Access Control

Access Control is a security framework that monitors and controls who, what, and when a subject has access to an entity or can perform actions within a system [151], [152]. In VANETs access control ensures that security and privacy of communication between vehicles.

Key aspects of Access Control include:

Vehicular communication authentication: involves verifying the authenticity of communication participants [153]. It ensures that vehicles are who they claim to be, preventing unauthorized entities from participating in the network, allowing for secure and authorized interactions.

Role based access control: assigns roles to entities based on their responsibilities or functions. Access rights are then granted based on these roles, ensuring that users have the necessary permissions to perform their tasks [154]. Helps to manage and enforce access policies by organizing participants into roles and regulating their access to resources and functionalities accordingly.

Pseudonym Management: is the use of temporary or pseudonymous identifiers to protect the real identity of vehicles. Pseudonyms are periodically changed to enhance privacy, allowing vehicles to communicate without revealing their true identities, preventing tracking and providing a degree of anonymity [155].

Selective Disclosure: allows entities to reveal only specific information to authorized parties, minimizing the amount of data shared while still meeting the requirements of a given interaction [156]. By selectively disclosing information, VANETs participants can control what data is shared, contributing to privacy preservation and access control.

Revocation Mechanisms: is the removal of access privileges from entities that no longer should have them [157]. This could be due to a change in roles, compromised credentials, or other security concerns.

Encryption for Confidentiality: encoding information in a way that only authorized parties can decipher it [158]. It ensures the confidentiality of data during transmission.

3.2. Pertinent VANET security issues

VANETs, being a wireless ad hoc network, serves its purpose completely but is prone to security attacks. Highly dynamic connections, sensitive information sharing and time sensitivity makes VANETs architecture prone to attacks. Authors in [159] classify the attacks on VANETs, grouping the attacks in the CIA triad framework as shown in the Figure 8 below.

As shown in Figure 8, attacks can compromise the CIA triad, which encompasses confidentiality, integrity, and availability. Confidentiality may be jeopardized through eavesdropping attacks, where unauthorized entities intercept and gain access to sensitive communication, potentially leading to privacy breaches. Integrity attacks involve the manipulation of data exchanged among vehicles, introducing false information or altering legitimate messages, thereby compromising the reliability of the shared information. Availability attacks target the network's ability to function smoothly, often through denial-of-service attacks that disrupt communication channels or overload the network with malicious traffic.

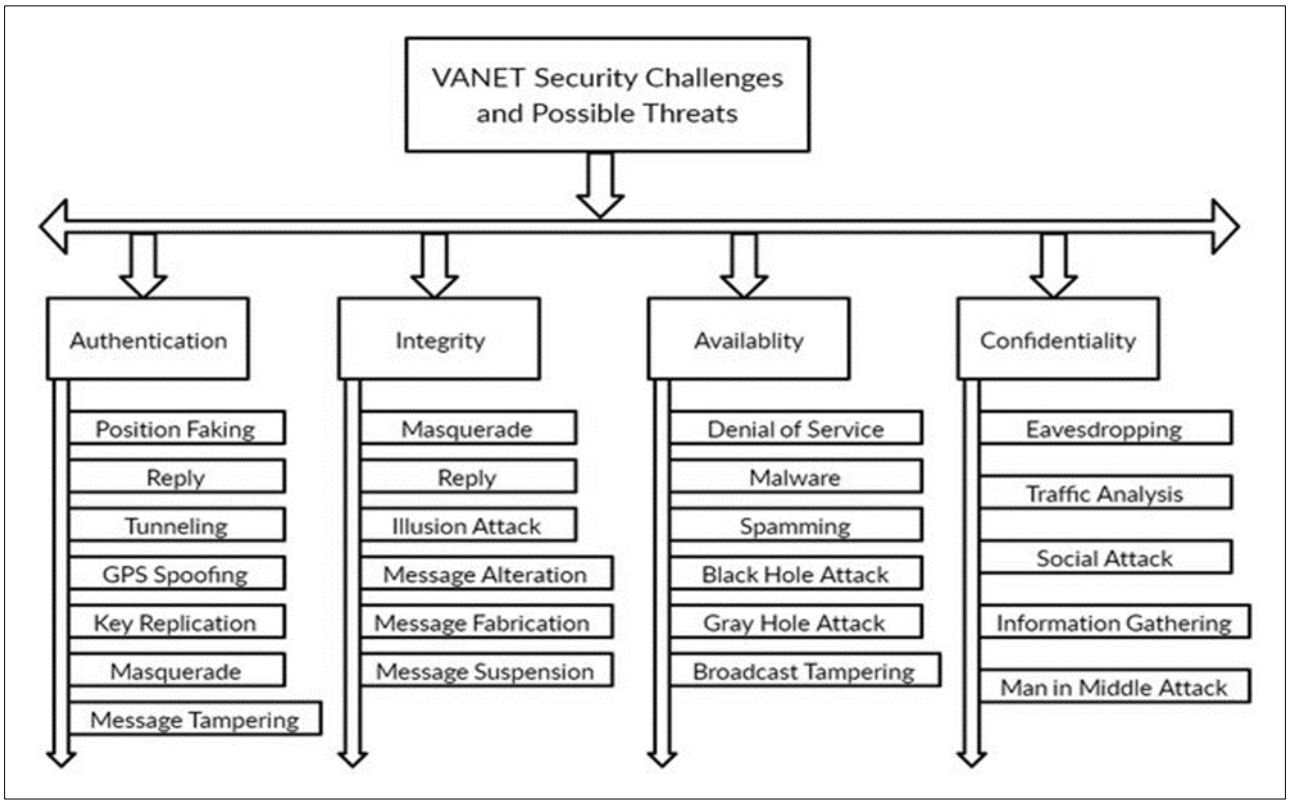

Figure 8 CIA Triad VANETs Attacks

Safeguarding the CIA triad in VANETs necessitates the implementation of robust encryption mechanisms for confidentiality, secure authentication protocols to ensure data integrity, and resilient network architectures to withstand and recover from availability threats, thus ensuring a secure and dependable vehicular communication environment. The Table 1 below represents some of the security challenges that VANETs face, its effects and probability of occurrence.

Table 1 Security Challenges in VANETs

Security Issue	**Description**	**Effects**	**Probability of Occurrence**
Authentication and Authorization	Exploits vulnerabilities in the authentication and authorization processes of systems,	Disruption of Communication, Compromised Safety, and Lack of privacy	High
Sybil Attack	An attacker creates multiple fake identities to flood the network, potentially disrupting communication and misleading other vehicles.	Impersonation of multiple vehicles, misinformation, and disruption of network services.	Medium
Denial of Services Attack	Overloading the network to disrupt services	Disruption of communication, traffic jams	Low
Location Spoofing	Involves an attacker providing false location information to other vehicles or the infrastructure, creating a deceptive representation of its position	Misleading Navigation, Traffic Congestion, and Collision Risks	Medium
Eavesdropping	Unauthorized interception of communication	Unauthorized access to sensitive information	Medium

3.2.1. Authentication and authorization attacks

Authentication verifies the identity of a subject or service, and authorization determines their access rights. The Major challenge faced is verifying the authenticity of vehicles and ensuring that only authorized entities can participate in communication. The major weakness is the open and dynamic nature of VANETs, making authentication challenging, and unauthorized entities could compromise network integrity [160]-[164]. VANETs have a highly dynamic topology as vehicles move rapidly, join, and leave the network frequently. Secondly, VANETs often lack a centralized infrastructure, making it challenging to establish a reliable and scalable authentication system. These disadvantages the authentication mechanisms to adapt to the changing topology to ensure timely and accurate verification of vehicle identities, and the Public Key Infrastructure (PKI) solutions may face difficulties in deployment and management.

3.2.2. Sybil Attacks

The primary goal of a Sybil attack in VANETs is to compromise the integrity and reliability of the network by creating numerous malicious nodes (Sybil nodes) that collaborate to disrupt communication, spread false information, or manipulate network protocols. As shown in Figure 9, Sybil attacker generates multiple fake identities, each with a unique pseudonym, to gain influence or control over the network [165], [166]. Sybil nodes collaborate to amplify the impact of malicious activities, such as injecting false traffic information, disrupting routing protocols, or causing confusion in safety applications. Sybil attacks take advantage of the lack of a centralized authority and the dynamic nature of VANETs, where vehicles frequently join and leave the network. They exploit trust and coordination mechanisms, as well as compromise the reliability of information dissemination.

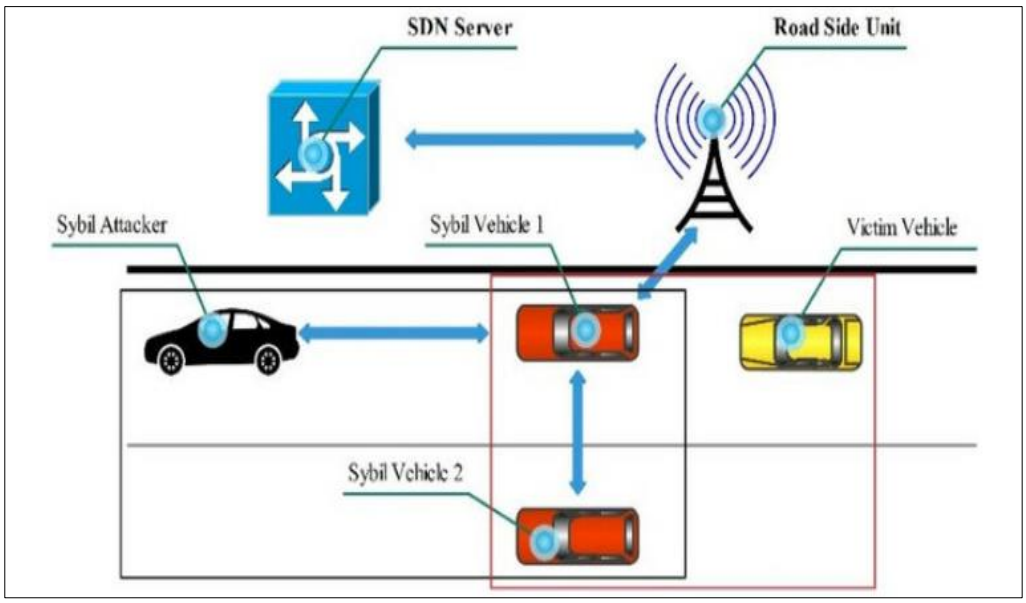

Figure 9 Sybil attackers

Sybil attacks can lead to the spread of false traffic information, causing congestion, rerouting, and potentially dangerous situations. Compromised Safety Applications: Safety-related applications, such as collision avoidance systems, can be compromised if Sybil attackers inject false data, leading to incorrect decisions by vehicles. Detecting Sybil attacks is challenging due to the dynamic nature of VANETs and the need for real-time decision-making [167], [168]. Traditional security mechanisms, such as cryptographic solutions, may be insufficient, and additional trust models or reputation systems are required for effective [169] detection. Figure 10 below, represents a more detailed graphical explanation of a Sybil attack. Car C, a single Node, creates multiple identities, and sends the information to the rest of the nodes (Car A, B,D can change route leaving car C with a free traffic road.

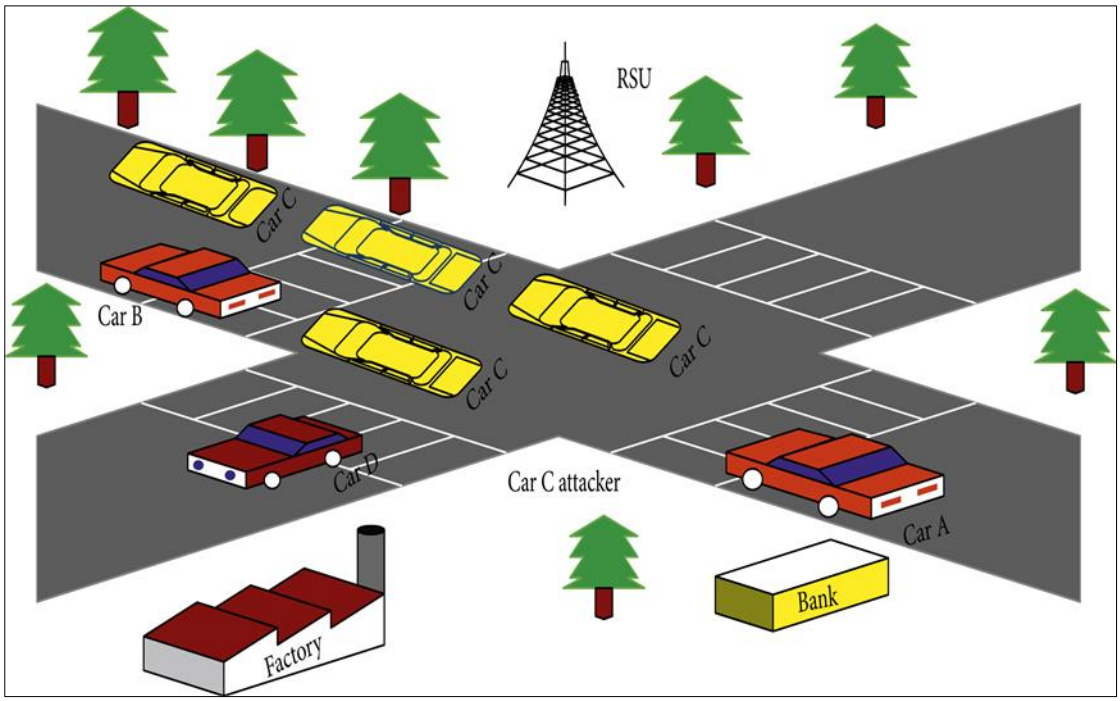

Figure 10 Sybil Attack on VANETs

3.2.3. Denial of Service Attacks

The primary goal of a Denial of Service attack in VANETs is to disrupt communication and services, causing a degradation or complete loss of network functionality. Attackers aim to overwhelm network resources, such as communication channels or processing capabilities, to prevent legitimate users (vehicles) from accessing essential services [170], [171]. Some of the attacks mechanisms includes:

Communication jamming, which involves transmitting interference signals to disrupt wireless communication channels, causing congestion and blocking legitimate messages [172].

Resource exhaustion attackers may exhaust network resources, such as bandwidth, processing power, or memory, by flooding the network with a large volume of malicious requests or traffic [173].

3.2.4. Impact on VANETs

DoS attacks can compromise safety-related applications by disrupting the timely exchange of critical information, such as collision warnings or traffic updates.

Traffic Management Disruption: Congestion caused by DoS attacks can lead to traffic flow disruptions, affecting routing algorithms and causing delays.

Service Unavailability: Legitimate vehicles may be unable to access essential VANETs services, leading to a loss of connectivity and functionality.

3.2.5. Vulnerabilities Exploited

Lack of Centralized Control: VANETs often operate without a centralized control infrastructure, making it challenging to detect and mitigate DoS attacks centrally.

Limited Security Measures: The dynamic nature of VANETs and the need for real-time communication can limit the implementation of complex security measures, making the network susceptible to attacks.

In Figure 11 below, Car Q and U compromises the RSU while Car M, N, O, and P denied the attacker Q and R. S and T, deprived of access to RSU services by the car in the attacker.

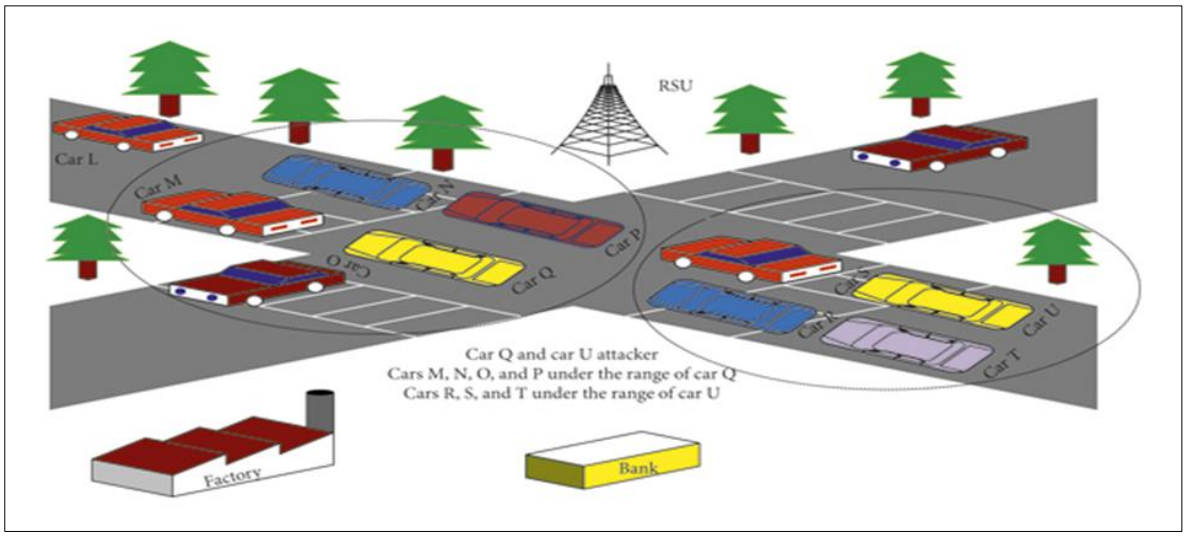

Figure 11 Denial of service attack

3.2.6. Location Spoofing

The primary goal of GPS spoofing in VANETs is to manipulate the location information of vehicles, leading to false positioning data being disseminated within the network. GPS spoofing attacks can have severe consequences for safety applications in VANETs. Misleading positioning information can result in incorrect decisions by safety systems, leading to accidents or disruptions in traffic flow. As shown in Figure 12, the Spoofer generates fake GPS signals and transmit them to nearby vehicles, fooling their GPS receivers into calculating incorrect positions [174].

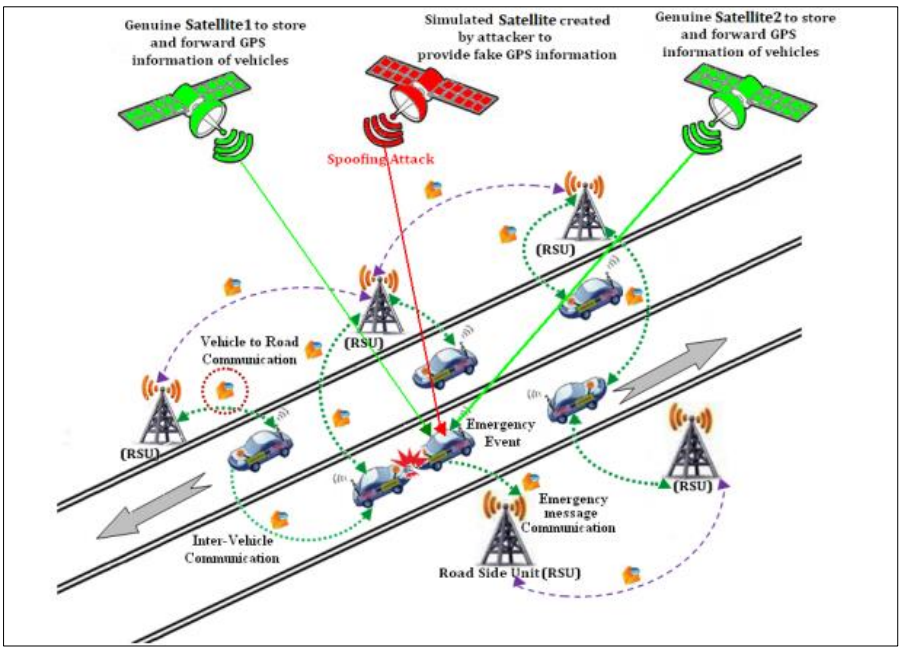

Figure 12 Spoofing in VANETs

Vehicles relying on these spoofed signals may experience inaccurate positioning, affecting safety-related applications and service. The Spoofer record legitimate GPS signals and replay them later. This can cause vehicles to believe they are at a location where they were in the past. The replay attacks [175] can lead to outdated and incorrect information being disseminated, impacting the effectiveness of safety applications.

3.2.7. Eavesdropping

The primary goal of eavesdropping attacks is to intercept and gather sensitive information exchanged between vehicles or between a vehicle and the infrastructure [176]. As shown in Figure 13, attackers aim to gain unauthorized access to information such as location data, communication patterns, or even personally identifiable information. Eavesdropping in VANETs poses a significant security concern as it involves unauthorized interception of communication between vehicles, potentially compromising the confidentiality of sensitive information.

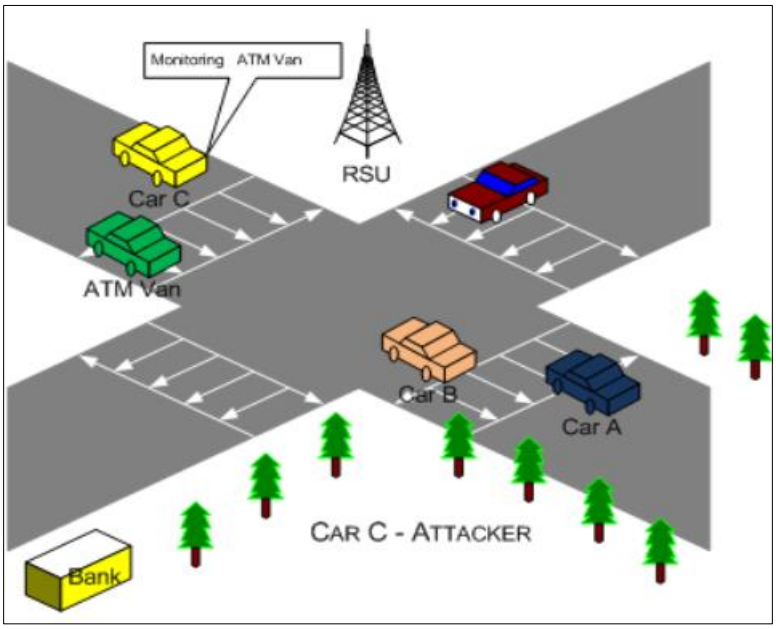

Figure 13 Eavesdropping in VANETs

Attackers may exploit vulnerabilities in the wireless communication protocols used in VANETs to eavesdrop on messages containing location data, traffic patterns, or other private details. This information can be leveraged for malicious purposes such as tracking the movements of specific vehicles or conducting targeted attacks. Mitigating eavesdropping in VANETs requires the implementation of strong encryption techniques, like secure key management and the use of cryptographic algorithms, to ensure that transmitted data remains confidential and resistant to interception by unauthorized entities. Additionally, ongoing research and development are crucial to staying ahead of evolving eavesdropping techniques and enhancing the overall security posture of VANETs.

3.2.8. Attack Mechanisms

Passive Monitoring: Attackers passively listen to wireless communication within the VANETs without actively participating in the communication [177].

Signal Interception: Eavesdroppers may intercept wireless signals between vehicles or between a vehicle and roadside infrastructure to capture sensitive data [178].

3.2.9. Data Targeted

Location Information: Eavesdropping can compromise the privacy of location-based information, revealing the movement patterns and habits of individual vehicles.

Safety Messages: Sensitive safety-related messages, such as emergency braking signals or collision warnings, can be intercepted, potentially leading to malicious exploitation.

3.3. Privacy issues in VANETs

The introduction and usage of VANETs in real world scenarios also brought by privacy concern because of the continuous exchange of location and other sensitive information among vehicles and infrastructure components. Protecting the privacy of individuals in VANETs is essential to encourage widespread adoption and prevent potential misuse of personal data [179], [180]. Vehicles should trust the sender that may have an identity or not, as well as trust

the intermediate forwarder vehicles. Thus, trade-off mechanisms are required between anonymity communication [181] and privacy with the possibility to show real vehicle identity. The Table 2 below, gives a brief summary of VANETs privacy attacks, description, effects, and probability of occurrence.

Table 2 Privacy Challenges/attacks on VANETs

Privacy Challenge/Attack	Description	Effects	Probability of Occurrence
Location Privacy	Manipulation of reported location information.	Misguides other vehicles, compromising traffic flow, safety applications, and coordination mechanism	High
Identity Disclosure	Unauthorized exposure of a user's real identity.	Compromises user privacy, may lead to tracking, profiling, and potential misuse of personal information.	High
Data Minimization	Inadequate efforts to limit the collection of unnecessary data.	Increased risk of privacy breaches, exposure of sensitive information, and potential misuse of collected data.	High
User Consent and Control	Lack of mechanisms for users to control data sharing and provide consent.	Users may be unaware of or unable to manage data sharing, leading to involuntary exposure of personal information	Moderate
Social Engineering Attacks	Manipulation of individuals to disclose sensitive information	Unauthorized access to personal data, compromise of security credentials, and potential misuse of obtained information.	High

3.4. Location Privacy

Constant transmission of location information in VANETs can lead to the tracking and profiling of individual vehicles, compromising their location privacy. Unauthorized entities or malicious actors may exploit location data to monitor the movements of specific vehicles, raising privacy concerns for drivers and passengers [182]. Whenever a vehicle sends a message, no one but authorized entities should know their real identity and location of the vehicle. All the messages sent by the vehicle must be authenticated before processing, hence location privacy is an important design aspect to be considered in VANETs operations.

3.5. Identity Disclosure

The constant communication between vehicles and infrastructure components raises challenges related to protecting the identities of individuals involved in the network. VANETs often use persistent pseudonyms to protect the real identities of vehicles [183]. However, if not managed properly, these pseudonyms might become linkable to actual identities over time. The prolonged use of the same pseudonym could lead to the identification of specific vehicles and compromise the privacy of drivers.

3.6. Data Minimization

Data minimization is a privacy principle that advocates collecting only the minimum amount of data necessary for a specific purpose. In the context of Vehicular Ad Hoc Networks (VANETs), where vehicles continuously exchange information, data minimization is crucial to address privacy concerns [184]. VANETs involve the continuous exchange of data, including location, speed, and other information, to support various applications. The sheer volume of data exchanged raises challenges in determining what data is essential and ensuring that only necessary information is transmitted to preserve privacy.

Secondly, deciding on appropriate storage and retention policies for VANETs data presents challenges, particularly regarding how long data should be retained and for what purposes. Extended data retention periods may increase the risk of privacy breaches, especially if the stored data is not adequately protected. Obtaining user consent and providing individuals with control over the collection and sharing of their data is challenging in the dynamic and fast-paced environment of VANETs [185]. Lack of transparent consent mechanisms and user control may result in individuals unknowingly contributing to data exchange without clear understanding or approval.

3.7. User Consent and Control

Data privacy and protection require that people have control over their personal data and make informed choices regarding its usage. The consent model of privacy protection assumes that individuals control their personal information and are able to assess the risks associated with data sharing. User consent and control poses a challenge because of the dynamic nature [186] of VANETs; they have dynamic topology with vehicles entering and leaving the network frequently. Obtaining and managing user consent in such a dynamic environment is challenging. In result users may not have sufficient time to explicitly provide consent, leading to challenges in ensuring that their privacy preferences are respected.

3.8. Social Engineering Attacks

Social engineering is a form of manipulation used by attackers to deceive individuals or organizations into divulging confidential information, providing access to systems, or performing actions that may compromise security. These attacks exploit human psychology rather than relying on technical vulnerabilities. VANETs are primarily susceptible to technical security challenges, social engineering can play a role in manipulating individuals to compromise the security of the network [187]. Possible ways in which an attacker may perform social engineering attack include:

False Vehicle-to-Everything (V2X) communication: attackers send fake V2X messages to nearby vehicles, providing misleading information. Deceived vehicles may make unsafe decisions based on false information, leading to accidents or traffic disturbances.

Impersonation for access to secure zones: an attacker pretends to be an authorized entity (e.g., emergency vehicle) to gain access to secure zones within the VANETs, leading to unauthorized access can lead to security breaches, disruptions, or interference with emergency operations.

False traffic advisory: an attacker broadcasts false traffic advisories to vehicles, claiming accidents, road closures, or other incidents that didn't occur. This can cause panic, congestion, and lead to unauthorized route changes by deceived drivers.

3.9. VANETs security issues remedies

Addressing security issues in VANETs requires a multifaceted approach. To mitigate the risk of malicious attacks, robust cryptographic techniques, such as digital signatures and message authentication codes, should be employed to ensure the integrity and authenticity of exchanged information. Privacy concerns can be addressed through the implementation of pseudonym changing strategies, allowing vehicles to periodically change their identifiers to prevent long-term tracking. Intrusion detection and prevention systems play a crucial role in identifying and responding to security threats in real-time. Additionally, secure and efficient key management mechanisms are essential for protecting communication channels. Standardizing security protocols across the VANET ecosystem promotes interoperability and consistency in security measures. Ultimately, a combination of encryption, authentication, privacy-preserving techniques, and vigilant monitoring can contribute to a more resilient and secure VANET environment. Regular updates and collaboration within the research community are essential to staying ahead of emerging security challenges in the dynamic landscape of vehicular communications. In Table 3 below, it gives a summary of each security issues discussed and what mitigation strategies can be implemented.

Table 3 VANETs security issues mitigation strategies

Security Issue/Attack on VANETs	**Description**	**Mitigation Strategies**
Authentication & Authorization	Ensures the identity of communicating entities and grants appropriate access rights.	Use of strong cryptographic techniques for secure communication. Implementation of robust authentication protocols. Integration of access control mechanisms to restrict unauthorized access(RBAC, ABAC)
Sybil Attack	Creation of multiple fake identities to deceive the network.	Employ reputation-based systems to detect and isolate Sybil nodes. Collaborative approaches for detection involving neighboring vehicles. Use of secure positioning systems to mitigate identity spoofing.

Denial of Service Attack	Intentional disruption of network services or communication	Implementation of intrusion detection systems (IDS) to identify and filter malicious traffic. Traffic prioritization for critical safety messages. Utilization of cooperative defense mechanisms.
Location Spoofing	Manipulation of reported location information	Adoption of secure positioning systems. Time-synchronization mechanisms to detect replay attacks. Cooperative awareness for cross-verification of reported positions.
Eavesdropping	Unauthorized interception of wireless communications.	Implementation of end-to-end encryption for message confidentiality. Use of intrusion detection systems (IDS) to monitor for anomalous patterns. Continuous pseudonym changes to enhance privacy.

3.9.1. Authentication and Authorization

Authentication and authorization are critical components of security in Vehicular Ad Hoc Networks (VANETs) to ensure that only legitimate entities have access to the network and its resources. Utilizing digital certificates to authenticate the identities of vehicles and infrastructure components in the VANETs, which provides a strong mechanism for verifying the legitimacy of participants in the network. Authorization Solutions include the use of Role-Based Access Control (RBAC). It defines roles and assign permissions to vehicles based on their roles within the VANET (e.g., emergency vehicles, regular vehicles) [188]. Thus, simplifies authorization management and ensures that vehicles have appropriate access based on their roles. Secondly, Attribute-Based Access Control (ABAC), which uses the attributes (e.g., vehicle type, trust level) to make access control decisions, allowing for fine-grained control over permissions providing flexibility in defining access policies based on various attributes.

3.9.2. Sybil Attacks

VANETs have a highly dynamic topology with vehicles entering and leaving the network frequently, making it difficult to detect and prevent Sybil attacks. Reputation-based systems and collaborative approaches involving neighboring vehicles for detecting and isolating Sybil nodes. [189]. The absence of a centralized infrastructure in VANETs makes it challenging to establish a reliable and scalable authentication system, implementation of secure and tamper-resistant positioning systems, such as GPS, to mitigate identity spoofing.

3.9.3. Denial of Service Attacks

Deploy intrusion detection systems [190] to monitor network behavior and identify unusual patterns indicative of DoS attacks. The advantage is that early detection allows for a rapid response to mitigate the impact of the attack. Facilitating cooperation between vehicles through Vehicle-to-Everything (V2X) communication to collectively identify and isolate malicious entities. Thus enabling collaborative defense mechanisms, enhancing the network's resilience against DoS attacks.

3.9.4. Location Spoofing

Analyzing the strengths of communication signal between vehicles to assess the credibility of reporting a location [191]. Utilization of a strong authentication mechanisms, such as digital signatures, to verify the authenticity of location information reducing the risk of accepting spoofed location data from unauthorized sources, and adoption of time-synchronization mechanisms to detect replay attacks.

3.9.5. Eavesdropping Attacks

Implement a strong end-to-end encryption to secure the content of messages, preventing unauthorized access to sensitive information [192]. Deploy Intrusion Detection Systems to monitor network activities and detect anomalous patterns that may indicate eavesdropping attempts, and regularly change of the pseudonyms used for communication to enhance privacy and make it more challenging for eavesdroppers to track specific vehicles.

3.10. Privacy remedies

Privacy remedies in VANETs are essential to address concerns related to the continuous broadcasting of sensitive information by vehicles. Pseudonym changing mechanisms play a crucial role in enhancing privacy by allowing vehicles to periodically change their identifiers, making it more challenging for adversaries to track individual vehicles over time. Additionally, the implementation of group-based communication and anonymous authentication protocols can further

protect user identities and minimize the risk of profiling. A brief summary of the mitigation strategies proposed to compact Privacy challenges in VANETs is discussed in Table 4 below.

Table 4 Privacy issues in VANETs mitigation strategies

Security Issue/Attack on VANETs	**Description**	**Mitigation Strategies.**
Location Privacy	Risk of exposing the real-time location of a vehicle.	Use of pseudonyms to enhance user anonymity. Adoption of location cloaking techniques. Implementation of secure positioning systems.
Identity Disclosure	Unauthorized exposure of a user's real identity.	Adoption of pseudonyms for user identities. Implementation of end-to-end encryption. Secure key management practices.
Data Minimization	Inadequate efforts to limit the collection of unnecessary data.	Implementation of data anonymization techniques. Periodic purging of sensitive information. Use of minimal disclosure principles.
User Consent and Control	Lack of mechanisms for users to control data sharing and provide consent	Development of user-friendly interfaces for consent management. Implementation of granular access control mechanisms. User education and awareness.
Social Engineering Attacks	Manipulation of individuals to disclose sensitive information.	Conduct regular user awareness training on social engineering tactics. Implementation of two-factor authentication. Encourage skepticism and verification of requests.

Privacy-preserving data aggregation techniques enable the sharing of relevant information without disclosing specific details, contributing to a balance between communication efficiency and individual privacy. Standardizing privacy-enhancing measures across VANET deployments, along with user education and awareness programs, reinforces the overall privacy framework. These remedies collectively contribute to creating a more secure and privacy-aware environment within VANETs, fostering trust among users while leveraging the benefits of cooperative vehicular communication.

3.10.1. Location Privacy

A simple mixed group scheme establishes mixed areas in various parts of the town where vehicles can join it and quit. Vehicles change their pseudonyms at the same time as they enter the mixed zone, and their Identities change as they leave the same mixed zone. As a result, trackers cannot track vehicles entering the mixing zone under a given pseudonym and leaving under another pseudonym [193]. The application of Geo-Obfuscation techniques helps to blur or cloak the reported location of vehicles, making it more difficult to pinpoint the exact location of a vehicle, preserving privacy.

3.10.2. Identity Disclosure

Identity disclosure can lead to tracking and profiling of individual vehicles [194]. Some remedies suggested include, location cloaking which is a privacy mechanism that is used to satisfy specific privacy requirements by blurring users' exact locations into cloaked regions. Cloaking obscures the precise location, protecting against identity disclosure.

3.10.3. Data Minimization

In the context of VANETs where privacy concerns are significant, data minimization is crucial to protect user privacy. Mechanisms that can be deployed to ensure data minimization include, selective data transmission, allowing vehicles to selectively transmit only essential information, minimizing the amount of data shared with the network [195]. Moreover, reducing the risk of exposing sensitive information while maintaining communication efficiency. Implementing on-board filtering, anonymous data collection, and Data retention policies techniques whereby only relevant information is transmitted from one entity to another. Collecting and transmitting data in an anonymous or pseudonymous form, unlinking data from specific vehicle identities.

3.10.4. User Consent and Control

Implement explicit mechanisms that require users to provide consent before their data is collected or shared. This technique empowers users to make informed decisions about the usage of their data.

Dynamic Privacy Settings, allow users to dynamically adjust their privacy settings based on their preferences and the current context [196]. Enabling users to adapt their privacy preferences in real-time, providing greater control. Provision of revocable consent enabling users to revoke their consent at any time, stopping the collection or sharing of their data, and implement time windows for consent, allowing users to specify when their data can be collected or shared. Adding temporal control, giving users the ability to limit data sharing during specific periods.

3.10.5. Social Engineering Attacks

Basic solutions to be implemented in trying to reducing the attacks is educating users and creating awareness. Conducting regular training sessions to educate VANETs users about social engineering tactics and how to recognize and resist them. Multi-Factor Authentication (MFA) [197] is another mechanism that can be used, which adds an extra layer of security, requiring multiple forms of verification. Reducing the likelihood of unauthorized access, even if credentials are compromised.

4. Conclusion

The security of VANETs is a critical aspect that requires careful consideration and robust measures. VANETs present unique challenges due to their dynamic nature, high mobility, and the need for real-time communication. Addressing the privacy and security challenges in VANETs requires a holistic and collaborative approach involving industry stakeholders, researchers, policymakers, and users. Ongoing research and innovation are crucial to staying ahead of evolving threats and ensuring the continued development and deployment of secure and privacy-preserving VANETs systems. Striking the right balance between safety, functionality, and privacy is paramount to realizing the full potential of VANETs in creating intelligent, efficient, and secure transportation networks. The intertwining issues of security and privacy in modern technological landscapes, whether in VANETs or other domains, underscore the critical need for comprehensive and adaptive measures. Striking a delicate balance between ensuring the confidentiality, integrity, and availability of data, while respecting individual privacy rights, remains an ongoing challenge. Robust cryptographic techniques, secure communication protocols, and vigilant monitoring mechanisms are vital components of any effective security strategy. Similarly, privacy remedies such as pseudonym changing, anonymous authentication, and data aggregation contribute to safeguarding personal information in interconnected systems. As technology continues to evolve, a dynamic and collaborative approach, involving ongoing research, standardization efforts, and user awareness initiatives, is paramount to address emerging threats and challenges, fostering a secure and privacy-respecting digital environment for individuals and organizations alike.

Compliance with ethical standards

Acknowledgement

I appreciate the efforts of all people that helped me during the development of this work.

Disclosure of conflict of interest

The author has no any conflict of interest.

References

[1] Rashid K, Saeed Y, Ali A, Jamil F, Alkanhel R, Muthanna A. An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). Sensors. 2023 Feb 26;23(5):2594.

[2] Karabulut MA, Shah AS, Ilhan H, Pathan AS, Atiquzzaman M. Inspecting VANET with Various Critical Aspects–A Systematic Review. Ad Hoc Networks. 2023 Aug 14:103281.

[3] Al-Shareeda MA, Manickam S. A Systematic Literature Review on Security of Vehicular Ad-hoc Network (VANET) based on VEINS Framework. IEEE Access. 2023 May 10.

[4] Ning H, An Y, Wei Y, Wu N, Mu C, Cheng H, Zhu C. Modeling and analysis of traffic warning message dissemination system in VANETs. Vehicular Communications. 2023 Feb 1;39:100566.

[5] Desai D, El-Ocla H, Purohit S. Data Dissemination in VANETs Using Particle Swarm Optimization. Sensors. 2023 Feb 13;23(4):2124.

[6] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[7] Harish G, Shyamala Bharathi P. Energy-efficient QoS-compliant routing for dedicated short-range communications in smart transportation based on V–V and V–I approach. Soft Computing. 2023 Jul 12:1-1.

[8] Zhang T, Liu S, Xiang W, Xu L, Qin K, Yan X. A real-time channel prediction model based on neural networks for dedicated short-range communications. Sensors. 2019 Aug 13;19(16):3541.

[9] Min JH, Ham SW, Kim DK, Lee EH. Deep multimodal learning for traffic speed estimation combining dedicated short-range communication and vehicle detection system data. Transportation research record. 2023 May;2677(5):247-59.

[10] Kumar VD, Kumar VV, Kandar D. Data transmission between dedicated short range communication and WiMAX for efficient vehicular communication. Journal of Computational and Theoretical Nanoscience. 2018 Aug 1;15(8):2649-54.

[11] Kavitha Y, Satyanarayana P, Mirza SS. Sensor based traffic signal pre-emption for emergency vehicles using efficient short-range communication network. Measurement: Sensors. 2023 Jun 17:100830.

[12] Nyangaresi VO, Jasim HM, Mutlaq KA, Abduljabbar ZA, Ma J, Abduljaleel IQ, Honi DG. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. Electronics. 2023 Aug 31;12(17):3688.

[13] Rashid SA, Audah L, Hamdi MM. Intelligent Transportation Systems (ITSs) in VANET and MANET. InBiologically Inspired Techniques in Many Criteria Decision Making: Proceedings of BITMDM 2021 2022 Jun 4 (pp. 667-675). Singapore: Springer Nature Singapore.

[14] Thapliyal S, Wazid M, Singh DP, Das AK, Islam SH. Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system. Journal of Systems Architecture. 2023 Sep 1;142:102937.

[15] Jabbar R, Dhib E, Said AB, Krichen M, Fetais N, Zaidan E, Barkaoui K. Blockchain technology for intelligent transportation systems: A systematic literature review. IEEE Access. 2022 Feb 7;10:20995-1031.

[16] Panigrahy SK, Emany H. A survey and tutorial on network optimization for intelligent transport system using the internet of vehicles. Sensors. 2023 Jan 3;23(1):555.

[17] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[18] Rasheed A, Gillani S, Ajmal S, Qayyum A. Vehicular ad hoc network (VANET): A survey, challenges, and applications. InVehicular Ad-Hoc Networks for Smart Cities: Second International Workshop, 2016 2017 (pp. 39-51). Springer Singapore.

[19] Arif M, Wang G, Bhuiyan MZ, Wang T, Chen J. A survey on security attacks in VANETs: Communication, applications and challenges. Vehicular Communications. 2019 Oct 1;19:100179.

[20] Al-Heety OS, Zakaria Z, Ismail M, Shakir MM, Alani S, Alsariera H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. IEEE Access. 2020 May 6;8:91028-47.

[21] Hussain R, Hussain F, Zeadally S. Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems. 2019 Dec 1;101:843-64.

[22] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[23] Annoni M, Williams B. The history of vehicular networks. Vehicular ad hoc Networks: Standards, Solutions, and Research. 2015:3-21.

[24] Lee M, Atkison T. Vanet applications: Past, present, and future. Vehicular Communications. 2021 Apr 1;28:100310.

[25] SUPIAN AM, Yusof MH. Challenges in Data Communication and Networking in VANETs. Authorea Preprints. 2023 Oct 31.

[26] Bylykbashi K, Qafzezi E, Ampririt P, Ikeda M, Matsuo K, Barolli L. A Fuzzy-Based System for Determining Driver Stress in VANETs Considering Driving Experience and History. InInternational Conference on Advanced Information Networking and Applications 2022 Mar 31 (pp. 1-9). Cham: Springer International Publishing.

[27] Bowlin E, Khan MS, Bajracharya B, Appasani B, Bizon N. Challenges and Solutions for Vehicular Ad-Hoc Networks Based on Lightweight Blockchains. Vehicles. 2023 Aug 19;5(3):994-1012.

[28] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[29] Akhunzada A, Khan MK. Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues. IEEE Communications Magazine. 2017 Jul 14;55(7):110-8.

[30] Ahmad K, Khujamatov H, Lazarev A, Usmanova N, Alduailij M, Alduailij M. Internet of Things-Aided Intelligent Transport Systems in Smart Cities: Challenges, Opportunities, and Future. Wireless Communications and Mobile Computing. 2023 Apr 13;2023.

[31] Manimuthu A, Ngo T, Chattopadhyay A. Internet of Vehicles: Security and Research Roadmap. InMachine Learning and Optimization Techniques for Automotive Cyber-Physical Systems 2023 Mar 27 (pp. 257-287). Cham: Springer International Publishing.

[32] Arif M, Wang G, Geman O, Balas VE, Tao P, Brezulianu A, Chen J. Sdn-based vanets, security attacks, applications, and challenges. Applied Sciences. 2020 May 5;10(9):3217.

[33] Knight A. Hacking connected cars: Tactics, techniques, and procedures. John Wiley & Sons; 2020 Mar 17.

[34] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1;11(1):185-94.

[35] Upadhyaya AN, Shah JS. Attacks on vanet security. Int J Comp Eng Tech. 2018;9(1):8-19.

[36] Zhao T, Xie Y, Wang Y, Cheng J, Guo X, Hu B, Chen Y. A survey of deep learning on mobile devices: Applications, optimizations, challenges, and research opportunities. Proceedings of the IEEE. 2022 Mar 11;110(3):334-54.

[37] Chen S, Zong S, Chen T, Huang Z, Chen Y, Labi S. A taxonomy for autonomous vehicles considering ambient road infrastructure. Sustainability. 2023 Jul 19;15(14):11258.

[38] Xia Z, Wu J, Wu L, Chen Y, Yang J, Yu PS. A comprehensive survey of the key technologies and challenges surrounding vehicular ad hoc networks. ACM Transactions on Intelligent Systems and Technology (TIST). 2021 Jun 8;12(4):1-30.

[39] Leow D, O'Connor G, van Vulpen E. Operational deployment of semi-automated vehicle (level 2) and cooperative intelligent transport system on Eastlink. InAustralasian Transport Research Forum (ATRF), 41st, 2019, Canberra, ACT, Australia 2019 Oct.

[40] Agrawal R, Kumar A, Singh S. Vehicular Ad Hoc Network: Overview, characteristics, and applications. InAIP Conference Proceedings 2023 Jul 27 (Vol. 2721, No. 1). AIP Publishing.

[41] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[42] Kayasth BA, Patel RM. ITS Based OBU: A Fallback Mechanism in Vehicular Ad-Hoc Network. InInternational Conference on Computing Science, Communication and Security 2020 Mar 26 (pp. 196-209). Singapore: Springer Singapore.

[43] He Y, Wang D, Huang F, Zhang R, Gu X, Pan J. A V2I and V2V collaboration framework to support emergency communications in ABS-aided Internet of Vehicles. IEEE Transactions on Green Communications and Networking. 2023 Feb 15.

[44] Alrubaye JS, Ghahfarokhi BS. Geo-Based Resource Allocation for Joint Clustered V2I and V2V Communications in Cellular Networks. IEEE Access. 2023 Jul 31.

[45] Rahman AU, Ghosh A, Chandra A, Vychodil J, Blumenstein J, Mikulasek T, Prokes A. Time-variance of 60 GHz vehicular infrastructure-to-infrastructure (I2I) channel. Vehicular Communications. 2020 Dec 1;26:100288.

[46] Farsimadan E, Palmieri F, Moradi L, Conte D, Paternoster B. Vehicle-to-everything (V2X) communication scenarios for vehicular ad-hoc networking (VANET): An overview. InInternational Conference on Computational Science and Its Applications 2021 Sep 10 (pp. 15-30). Cham: Springer International Publishing.

[47] Santa J, Fernández PJ, Ortiz J, Sanchez-Iborra R, Skarmeta AF. SURROGATES: Virtual OBUs to foster 5G vehicular services. Electronics. 2019 Jan 22;8(2):117.

[48] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[49] Liu C, Huang H, Du H. Optimal RSUs deployment with delay bound along highways in VANET. Journal of Combinatorial Optimization. 2017 May;33:1168-82.

[50] Salari M, Kattan L, Gentili M. Optimal roadside units location for path flow reconstruction in a connected vehicle environment. Transportation Research Part C: Emerging Technologies. 2022 May 1;138:103625.

[51] Selvakumari P, Sheela D, Chinnasamy A. Chew's second Delaunay triangulation refinement scheme for optimal RSUs deployment to ensure maximum connectivity in vehicle to infrastructure communication. Wireless Personal Communications. 2022 Mar 1:1-31.

[52] Li J, Xu R, Liu X, Ma J, Chi Z, Ma J, Yu H. Learning for vehicle-to-vehicle cooperative perception under lossy communication. IEEE Transactions on Intelligent Vehicles. 2023 Mar 21.

[53] Pavithra GS, Pooja S, Rekha V, Mahendra HN, Sharmila N, Mallikarjunaswamy S. Comprehensive Analysis on Vehicle-to-Vehicle Communication Using Intelligent Transportation System. InInternational Conference on Soft Computing for Security Applications 2023 Apr 17 (pp. 893-906). Singapore: Springer Nature Singapore.

[54] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[55] Uzair M. Vehicular Wireless Communication Standards: Challenges and Comparison. International journal of electrical and computer engineering systems. 2022 Jul 15;13(5):379-97.

[56] Martínez VM, Ribeiro MR, Mota VF. Wi-Fi faces the new wireless ecosystem: a critical review. Annals of Telecommunications. 2023 Nov 9:1-7.

[57] Sarkar NI, Ahmed F, Gul S. Deploying a Low-Cost Wi-Fi-Based Vehicular Ad Hoc Network in a Shopping Mall Parking Lot: An Empirical Study. Electronics. 2023 Nov 16;12(22):4672.

[58] Ganeshkumar N, Kumar S. Obu (on-board unit) wireless devices in vanet (s) for effective communication—A review. Computational Methods and Data Engineering: Proceedings of ICMDE 2020, Volume 2. 2020 Nov 5:191-202.

[59] Farran H, Bokor L. A survey on efforts to apply IPv6 in V2X communication networks. Acta Technica Jaurinensis. 2023 May 31;16(2):42-61.

[60] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[61] Khan UA, Lee SS. Multi-layer problems and solutions in VANETs: A review. Electronics. 2019 Feb 11;8(2):204.

[62] Hussein NH, Yaw CT, Koh SP, Tiong SK, Chong KH. A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions. IEEE Access. 2022 Aug 16;10:86127-80.

[63] Gillani M, Niaz HA, Farooq MU, Ullah A. Data collection protocols for VANETs: a survey. Complex & Intelligent Systems. 2022 Jun;8(3):2593-622.

[64] Abbas AH, Ahmed AJ, Rashid SA. A cross-layer approach MAC/NET with updated-GA (MNUG-CLA)-based routing protocol for VANET network. World Electric Vehicle Journal. 2022 May 12;13(5):87.

[65] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[66] Poongodi M, Bourouis S, Ahmed AN, Vijayaragavan M, Venkatesan KG, Alhakami W, Hamdi M. A novel secured multi-access edge computing based vanet with neuro fuzzy systems based blockchain framework. Computer Communications. 2022 Aug 1;192:48-56.

[67] Shafi S, Ratnam DV. A trust based energy and mobility aware routing protocol to improve infotainment services in VANETs. Peer-to-Peer Networking and Applications. 2022 Jan 1:1-6.

[68] Shawky MA, Usman M, Imran MA, Abbasi QH, Ansari S, Taha A. Adaptive chaotic map-based key extraction for efficient cross-layer authentication in VANETs. Vehicular Communications. 2023 Feb 1;39:100547.

[69] Gnanajeyaraman R, Arul U, Michael G, Selvakumar A, Ramesh S, Manikandan T. VANET security enhancement in cloud navigation with Internet of Things-based trust model in deep learning architecture. Soft Computing. 2023 Apr 25:1-2.

[70] Al-Ani R, Baker T, Zhou B, Shi Q. Privacy and safety improvement of VANET data via a safety-related privacy scheme. International Journal of Information Security. 2023 Feb 6:1-21.

[71] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22;6(7):154.

[72] Karunathilake T, Förster A. A survey on mobile road side units in VANETs. Vehicles. 2022 May 20;4(2):482-500.

[73] Abbas G, Ullah S, Waqas M, Abbas ZH, Bilal M. A position-based reliable emergency message routing scheme for road safety in VANETs. Computer Networks. 2022 Aug 4;213:109097.

[74] Naskath J, Paramasivan B, Aldabbas H. A study on modeling vehicles mobility with MLC for enhancing vehicle-to-vehicle connectivity in VANET. Journal of Ambient Intelligence and Humanized Computing. 2021 Aug;12:8255-64.

[75] Tandon R, Gupta PK. A Hybrid Security Scheme for Inter-vehicle Communication in Content Centric Vehicular Networks. Wireless Personal Communications. 2023 Mar;129(2):1083-96.

[76] Nakazawa T, Tang S, Obana S. CCN-based inter-vehicle communication for efficient collection of road and traffic information. Electronics. 2020 Jan 7;9(1):112.

[77] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[78] Ullah S, Abbas G, Waqas M, Abbas ZH, Halim Z. Multi-hop emergency message dissemination through optimal cooperative forwarder in grid-based 5G-VANETs. Journal of Ambient Intelligence and Humanized Computing. 2023 Apr;14(4):4461-76.

[79] Mchergui A, Moulahi T, Ben Othman MT, Nasri S. Enhancing VANETs broadcasting performance with mobility prediction for smart road. Wireless Personal Communications. 2020 Jun;112:1629-41.

[80] Shankar A, Dayalan R, Chakraborty C, Dhasarathan C, Kumar M. A modified social spider algorithm for an efficient data dissemination in VANET. Environment, Development and Sustainability. 2022 Jan 6:1-44.

[81] Lin Z, Sun Y, Tang Y, Liu Z. An efficient message broadcasting MAC protocol for VANETs. Wireless Networks. 2020 Nov;26(8):6043-57.

[82] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[83] Shrestha R, Bajracharya R, Nam SY. Challenges of future VANET and cloud-based approaches. Wireless Communications and Mobile Computing. 2018 May 2;2018.

[84] Garg S, Singh A, Kaur K, Aujla GS, Batra S, Kumar N, Obaidat MS. Edge computing-based security framework for big data analytics in VANETs. IEEE Network. 2019 Mar 27;33(2):72-81.

[85] Khan S, Sharma I, Aslam M, Khan MZ, Khan S. Security challenges of location privacy in VANETs and state-of-the-art solutions: A survey. Future Internet. 2021 Apr 10;13(4):96.

[86] Malhi AK, Batra S, Pannu HS. Security of vehicular ad-hoc networks: A comprehensive survey. Computers & Security. 2020 Feb 1;89:101664.

[87] Rao BT, Patibandla RL, Narayana VL. Comparative study on security and privacy issues in VANETs. Cloud and IoT-Based Vehicular Ad Hoc Networks. 2021 Apr 22:145-62.

[88] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[89] Pratama RA, Rosselina L, Sulistyowati D, Sari RF, Harwahyu R. Performance evaluation on vanet routing protocols in the way road of central jakarta using ns-3 and sumo. In2020 International Seminar on Application for Technology of Information and Communication (iSemantic) 2020 Sep 19 (pp. 280-285). IEEE.

[90] Gupta L, Jain R, Vaszkun G. Survey of important issues in UAV communication networks. IEEE communications surveys & tutorials. 2015 Nov 3;18(2):1123-52.

[91] Al-Absi MA, Al-Absi AA, Sain M, Lee H. Moving ad hoc networks—A comparative study. Sustainability. 2021 May 31;13(11):6187.

[92] Azam F, Yadav SK, Priyadarshi N, Padmanaban S, Bansal RC. A comprehensive review of authentication schemes in vehicular ad-hoc network. IEEE access. 2021 Feb 18;9:31309-21.

[93] Zhang D, Zhang M, Ding F, Li SE, Li K. A stability-based clustering scheme for vehicular networks. In2020 IEEE 3rd International Conference on Electronics Technology (ICET) 2020 May 8 (pp. 809-813). IEEE.

[94] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[95] Ksouri C, Jemili I, Mosbah M, Belghith A. VANETs routing protocols survey: classifications, optimization methods and new trends. InDistributed Computing for Emerging Smart Networks: First International Workshop, DiCES-N 2019, Hammamet, Tunisia, October 30, 2019, Revised Selected Papers 1 2020 (pp. 3-22). Springer International Publishing.

[96] Lyu F, Zhu H, Zhou H, Qian L, Xu W, Li M, Shen X. MoMAC: Mobility-aware and collision-avoidance MAC for safety applications in VANETs. IEEE Transactions on Vehicular Technology. 2018 Aug 22;67(11):10590-602.

[97] Xu X, Liu K, Xiao K, Ren H, Feng L, Chen C. Design and implementation of a fog computing based collision warning system in VANETs. In2018 IEEE Symposium on Product Compliance Engineering-Asia (ISPCE-CN) 2018 Dec 5 (pp. 1-6). IEEE.

[98] Swain S, Senapati BR, Khilar PM. Evolution of vehicular ad hoc network and flying ad hoc network for real-life applications: Role of vanet and fanet. InModelling and Simulation of Fast-Moving Ad-Hoc Networks (FANETs and VANETs) 2023 (pp. 43-73). IGI Global.

[99] Hozouri A, Mirzaei A, RazaghZadeh S, Yousefi D. An overview of VANET vehicular networks. arXiv preprint arXiv:2309.06555. 2023 Sep 12.

[100] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[101] Bylykbashi K, Qafzezi E, Ampririt P, Ikeda M, Matsuo K, Barolli L. Performance evaluation of an integrated fuzzy-based driving-support system for real-time risk management in VANETs. Sensors. 2020 Nov 16; 20(22):6537.

[102] Ullah A, Yaqoob S, Imran M, Ning H. Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing. IEEE Access. 2018 Dec 16;7:1570-85.

[103] Nagpal S, Aggarwal A, Gaba S. Privacy and security issues in vehicular Ad Hoc networks with preventive mechanisms. InProceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021 2022 Jan 24 (pp. 317-329). Singapore: Springer Nature Singapore.

[104] Cahyadi EF, Su TW, Yang CC, Hwang MS. A certificateless aggregate signature scheme for security and privacy protection in VANET. International Journal of Distributed Sensor Networks. 2022 May;18(5):15501329221080658.

[105] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[106] Zhang S, Liu Y, Xiao Y, He R. A trust based adaptive privacy preserving authentication scheme for VANETs. Vehicular Communications. 2022 Oct 1;37:100516.

[107] Chaudhry SA. Comments on "A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs". IEEE Sensors Journal. 2022 Apr 18;22(13):13763-6.

[108] Yang Y, Zhang L, Zhao Y, Choo KK, Zhang Y. Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET. IEEE Transactions on Information Forensics and Security. 2022 Jan 6;17:317-31.

[109] Goudarzi S, Soleymani SA, Anisi MH, Azgomi MA, Movahedi Z, Kama N, Rusli HM, Khan MK. A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET. Ad Hoc Networks. 2022 Apr 1;128:102782.

[110] Nath HJ, Choudhury H. A privacy-preserving mutual authentication scheme for group communication in VANET. Computer Communications. 2022 Aug 1;192:357-72.

[111] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[112] Khan S, Luo F, Zhang Z, Rahim MA, Ahmad M, Wu K. Survey on issues and recent advances in vehicular public-key infrastructure (VPKI). IEEE Communications Surveys & Tutorials. 2022 May 26;24(3):1574-601.

[113] Viriyasitavat W, Xu LD, Sapsomboon A, Dhiman G, Hoonsopon D. Building trust of Blockchain-based Internet-of-Thing services using public key infrastructure. Enterprise Information Systems. 2022 Dec 2;16(12):2037162.

[114] Sucasas V, Aly A, Mantas G, Rodriguez J, Aaraj N. Secure multi-party computation-based privacy-preserving authentication for smart cities. IEEE Transactions on Cloud Computing. 2023 Jul 12.

[115] Sudarsono A, Yuliana M. An Anonymous Authentication With Received Signal Strength Based Pseudonymous Identities Generation for VANETs. IEEE Access. 2023 Feb 13;11:15637-54.

[116] Mohammed BA, Al-Shareeda MA, Manickam S, Al-Mekhlafi ZG, Alayba AM, Sallam AA. ANAA-Fog: A Novel Anonymous Authentication Scheme for 5G-Enabled Vehicular Fog Computing. Mathematics. 2023 Mar 16;11(6):1446.

[117] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep;33(9):e4528.

[118] Şahin MS, Akleylek S. A survey of quantum secure group signature schemes: Lattice-based approach. Journal of Information Security and Applications. 2023 Mar 1;73:103432.

[119] Abhilash MH, Amberker BB. Efficient group signature scheme using lattices. International Journal of Information Technology. 2022 Jun;14(4):1845-54.

[120] Tabassum T, Hossain SK, Rahman MA, Alhamid MF, Hossain MA. An efficient key management technique for the Internet of Things. Sensors. 2020 Jan;20(7):2049.

[121] Bettayeb S, Messai ML, Hemam SM. A robust and efficient vector-based key management scheme for IoT networks. Ad Hoc Networks. 2023 Oct 1;149:103250.

[122] Gowda NC, Manvi SS, Malakreddy B, Lorenz P. BSKM-FC: Blockchain-based secured key management in a fog computing environment. Future Generation Computer Systems. 2023 May 1;142:276-91.

[123] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[124] Katulić F, Sumina D, Groš S, Erceg I. Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes. IEEE Access. 2023 May 11.

[125] Kumar U, Venkaiah VC. A New Modified MD5-224 Bits Hash Function and an Efficient Message Authentication Code Based on Quasigroups. InCyber Security, Privacy and Networking: Proceedings of ICSPN 2021 2022 May 15 (pp. 1-12). Singapore: Springer Nature Singapore.

[126] Cini V, Ramacher S, Slamanig D, Striecks C, Tairi E. Updatable signatures and message authentication codes. InIACR International Conference on Public-Key Cryptography 2021 May 1 (pp. 691-723). Cham: Springer International Publishing.

[127] Alaa Y, Fanfakh A, Hadi E. A Survey of Parallel Message Authentication and Hashing Methods. Journal of University of Babylon for Pure and Applied Sciences. 2023 Apr 3:100-10.

[128] Wang S, Huang K, Ma K, Xu X, Hu X. A lightweight encryption and message authentication framework for wireless communication. IET Communications. 2023 Feb;17(3):265-78.

[129] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[130] Dong S, Su H, Xia Y, Zhu F, Hu X, Wang B. A Comprehensive Survey on Authentication and Attack Detection Schemes That Threaten It in Vehicular Ad-Hoc Networks. IEEE Transactions on Intelligent Transportation Systems. 2023 Aug 1.

[131] Hegde N, Manvi SS. Distributed integrity and non-repudiation scheme in the dynamic vehicular cloud environment. International Journal of Information and Computer Security. 2023;20(3-4):315-48.

[132] Elkhalil A, zhang J, Elhabob R, Eltayieb N. POOSC: Provably online/offline signcryption scheme for vehicular communication in VANETs. Computing. 2023 Nov;105(11):2539-61.

[133] Elkhalil A, Zhang J. Practical heterogeneous signcryption system for vehicular communication in VANETs. Computing. 2023 Jan;105(1):89-113.

[134] Kalmykov IA, Olenev AA, Kalmykova NI, Dukhovnyj DV. Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network. Information. 2022 Dec 31;14(1):27.

[135] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan;13(2):691.

[136] Poettering B, Rastikian S. Sequential digital signatures for cryptographic software-update authentication. InEuropean Symposium on Research in Computer Security 2022 Sep 22 (pp. 255-274). Cham: Springer Nature Switzerland.

[137] Meng L, Chen L. A Blockchain-Based Long-Term Time-Stamping Scheme. InEuropean Symposium on Research in Computer Security 2022 Sep 25 (pp. 3-24). Cham: Springer International Publishing.

[138] Weng Y, Zhang Y. A Survey of Secure Time Synchronization. Applied Sciences. 2023 Mar 20;13(6):3923.

[139] Guardiola-Múzquiz G, Soriano-Salvador E. SealFSv2: Combining storage-based and ratcheting for tamper-evident logging. International Journal of Information Security. 2023 Apr;22(2):447-66.

[140] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1; 23(4):145-62.

[141] Lima PM, Carvalho LK, Moreira MV. Ensuring confidentiality of cyber-physical systems using event-based cryptography. Information Sciences. 2023 Apr 1;621:119-35.

[142] Pei J, Shi Y, Feng Q, Shi R, Lan L, Yu S, Shi J, Ma Z. An efficient confidentiality protection solution for pub/sub system. Cybersecurity. 2023 Jul 4;6(1):34.

[143] Blechschmidt B, Stock B. Extended Hell (o): A Comprehensive Large-Scale Study on Email Confidentiality and Integrity Mechanisms in the Wild. InUSENIX Security Symposium 2023.

[144] Khan LS, Khan M, Hazzazi MM, Jamal SS. A novel combination of information confidentiality and data hiding mechanism. Multimedia Tools and Applications. 2023 Feb;82(5):6917-41.

[145] Yaseen M, Kamel MB, Ligeti P. Security Analysis and Deployment Measurement of Transport Layer Security Protocol. InRecent Innovations in Computing: Proceedings of ICRIC 2021, Volume 2 2022 Apr 16 (pp. 725-739). Singapore: Springer Singapore.

[146] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[147] Barati H. A hierarchical key management method for wireless sensor networks. Microprocessors and Microsystems. 2022 Apr 1;90:104489.

[148] Alimoradi P, Barati A, Barati H. A hierarchical key management and authentication method for wireless sensor networks. International journal of communication systems. 2022 Apr;35(6):e5076.

[149] Kalos V, Polyzos GC. Requirements and secure serialization for selective disclosure verifiable credentials. InIFIP International Conference on ICT Systems Security and Privacy Protection 2022 Jun 3 (pp. 231-247). Cham: Springer International Publishing.

[150] De Salve A, Lisi A, Mori P, Ricci L. Selective disclosure in self-sovereign identity based on hashed values. In2022 IEEE Symposium on Computers and Communications (ISCC) 2022 Jun 30 (pp. 1-8). IEEE.

[151] Parkinson S, Khan S. A survey on empirical security analysis of access-control systems: a real-world perspective. ACM Computing Surveys. 2022 Dec 7;55(6):1-28.

[152] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[153] Latif RM, Jamil M, He J, Farhan M. A Novel Authentication and Communication Protocol for Urban Traffic Monitoring in VANETs Based on Cluster Management. Systems. 2023 Jul;11(7):322.

[154] Gai K, She Y, Zhu L, Choo KK, Wan Z. A blockchain-based access control scheme for zero trust cross-organizational data sharing. ACM Transactions on Internet Technology. 2023 Aug 21;23(3):1-25.

[155] Liu G, Yan Z, Wang D, Wang H, Li T. Deptvm: Decentralized pseudonym and trust value management for integrated networks. IEEE Transactions on Dependable and Secure Computing. 2023 Feb 20.

[156] Rasslan M, Nasreldin MM, Aslan HK. An IoT Privacy-Oriented selective disclosure credential system. Journal of Cybersecurity. 2022 Jan 1;8(1):tyac013.

[157] Sharma P, Jindal R, Borah MD. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. the Journal of Supercomputing. 2022 Apr 1:1-29.

[158] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[159] Azam S, Bibi M, Riaz R, Rizvi SS, Kwon SJ. Collaborative learning based sybil attack detection in vehicular ad-hoc networks (vanets). Sensors. 2022 Sep 13;22(18):6934.

[160] Ahmed W, Di W, Mukathe D. Privacy-preserving blockchain-based authentication and trust management in VANETs. IET Networks. 2022 May;11(3-4):89-111.

[161] Su J, Ren R, Li Y, Lau RY, Shi Y. Trusted blockchain-based signcryption protocol and data management for authentication and authorization in VANETs. Wireless Communications and Mobile Computing. 2022 May 21;2022.

[162] Li X, Jing T, Li R, Li H, Wang X, Shen D. Bdra: Blockchain and decentralized identifiers assisted secure registration and authentication for vanets. IEEE Internet of Things Journal. 2022 Apr 1.

[163] Aghabagherloo A, Delavar M, Mohajeri J, Salmasizadeh M, Preneel B. An efficient and physically secure privacy-preserving authentication scheme for Vehicular Ad-hoc NETworks (VANETs). Ieee Access. 2022 Sep 1;10:93831-44.

[164] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[165] Hamdi MM, Dhafer M, Mustafa AS, Rashid SA, Ahmed AJ, Shantaf AM. Effect Sybil attack on security Authentication Service in VANET. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[166] Velayudhan NC, Anitha A, Madanan M. Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique. Wireless Personal Communications. 2022 Feb 1:1-29.

[167] Velayudhan NC, Anitha A, Madanan M. An optimisation driven deep residual network for Sybil attack detection with reputation and trust-based misbehaviour detection in VANET. Journal of Experimental & Theoretical Artificial Intelligence. 2022 Aug 18:1-24.

[168] Maleknasab Ardakani M, Tabarzad MA, Shayegan MA. Detecting sybil attacks in vehicular ad hoc networks using fuzzy logic and arithmetic optimization algorithm. The Journal of Supercomputing. 2022 Sep;78(14):16303-35.

[169] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[170] Jaya Krishna N, Prasanth N. An Insight View on Denial of Service Attacks in Vehicular Ad Hoc Networks. InAdvances in Computational Intelligence and Communication Technology: Proceedings of CICT 2021 2022 Apr 6 (pp. 273-285). Singapore: Springer Singapore.

[171] Sedar R, Kalalas C, Alonso-Zarate J, Vázquez-Gallego F. Multi-domain denial-of-service attacks in Internet-of-Vehicles: Vulnerability insights and detection performance. In2022 IEEE 8th International Conference on Network Softwarization (NetSoft) 2022 Jun 27 (pp. 438-443). IEEE.

[172] Shrestha R, Guerboukha H, Fang Z, Knightly E, Mittleman DM. Jamming a terahertz wireless link. Nature Communications. 2022 Jun 1;13(1):3045.

[173] Pietrantuono R, Ficco M, Palmieri F. Survivability analysis of IoT systems under resource exhausting attacks. IEEE Transactions on Information Forensics and Security. 2023 May 22.

[174] Oligeri G, Sciancalepore S, Ibrahim OA, Di Pietro R. GPS spoofing detection via crowd-sourced information for connected vehicles. Computer Networks. 2022 Oct 24;216:109230.

[175] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[176] Shayea GG, Mohammed DA, Abbas AH, Abdulsattar NF. Privacy-Aware Secure Routing through Elliptical Curve Cryptography with Optimal RSU Distribution in VANETs. Designs. 2022 Dec 1;6(6):121.

[177] Shen WY, Manickam S, Al-Shareeda MA. Review of advanced monitoring mechanisms in peer-to-peer (p2p) botnets. arXiv preprint arXiv:2207.12936. 2022 Jul 17.

[178] Jaiswal N, Pandey A, Yadav S, Purohit N. Intercept probability analysis of NOMA-enabled V2V communications over double-Rayleigh fading channels. In2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) 2022 Jun 6 (pp. 191-196). IEEE.

[179] Liang Y, Liu Y, Gupta BB. PPRP: preserving-privacy route planning scheme in VANETs. ACM Transactions on Internet Technology. 2022 Dec 12;22(4):1-8.

[180] AlMarshoud MS, Al-Bayatti AH, Kiraz MS. Location privacy in VANETs: Provably secure anonymous key exchange protocol based on self-blindable signatures. Vehicular Communications. 2022 Aug 1;36:100490.

[181] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[182] Bendiab G, Hameurlaine A, Germanos G, Kolokotronis N, Shiaeles S. Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. IEEE Transactions on Intelligent Transportation Systems. 2023 Jan 20.

[183] Hahn D, Munir A, Behzadan V. Security and privacy issues in intelligent transportation systems: Classification and challenges. IEEE Intelligent Transportation Systems Magazine. 2019 Apr 11;13(1):181-96.

[184] Malek MA. Bigger Is Always Not Better; less Is More, Sometimes: The Concept of Data Minimization in the Context of Big Data. Eur. J. Privacy L. & Tech.. 2021:212.

[185] Badole MH, Thakare AD. An optimized framework for VANET routing: A multi-objective hybrid model for data synchronization with digital twin. International Journal of Intelligent Networks. 2023 Jan 1;4:272-82.

[186] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[187] Raut RM, Asole S. A Survey on Security Threats in VANET and Its Solutions. InInternational Conference on Recent Trends in Artificial Intelligence and IoT 2023 Apr 4 (pp. 229-240). Cham: Springer Nature Switzerland.

[188] Sharmah D, Islam AU. Implementation of Role Based Access Control and Dynamic Load Balancing in Model Analysis and Auditing Services. Scandinavian Journal of Information Systems. 2023 Apr 10;35(1):910-22.

[189] Engoulou RG, Bellaiche M, Halabi T, Pierre S. A decentralized reputation management system for securing the internet of vehicles. In2019 International Conference on Computing, Networking and Communications (ICNC) 2019 Feb 18 (pp. 900-904). IEEE.

[190] Banafshehvaragh ST, Rahmani AM. Intrusion, anomaly, and attack detection in smart vehicles. Microprocessors and Microsystems. 2023 Feb 1;96:104726.

[191] Sharma A, Jaekel A. Machine learning approach for detecting location spoofing in vanet. In2021 International Conference on Computer Communications and Networks (ICCCN) 2021 Jul 19 (pp. 1-6). IEEE.

[192] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[193] Memon I, Chen L, Arain QA, Memon H, Chen G. Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks. International journal of communication systems. 2018 Jan 10;31(1):e3437.

[194] Asuquo P, Cruickshank H, Morley J, Ogah CP, Lei A, Hathal W, Bao S, Sun Z. Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures. IEEE Internet of Things Journal. 2018 Mar 27;5(6):4778-802.

[195] Palanca A, Evenchick E, Maggi F, Zanero S. A stealth, selective, link-layer denial-of-service attack against automotive networks. InDetection of Intrusions and Malware, and Vulnerability Assessment: 14th International Conference, DIMVA 2017, Bonn, Germany, July 6-7, 2017, Proceedings 14 2017 (pp. 185-206). Springer International Publishing.

[196] Cherubini M, Salehzadeh Niksirat K, Boldi MO, Keopraseuth H, Such JM, Huguenin K. When forcing collaboration is the most sensible choice: Desirability of precautionary and dissuasive mechanisms to manage multiparty privacy conflicts. Proceedings of the ACM on Human-Computer Interaction. 2021 Apr 22;5(CSCW1):1-36.

[197] Basha PH, Prathyusha G, Rao DN, Gopikrishna V, Peddi P, Saritha V. AI-Driven Multi-Factor Authentication and Dynamic Trust Management for Securing Massive Machine Type Communication in 6G Networks. International Journal of Intelligent Systems and Applications in Engineering. 2024;12(1s):361-74.