GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Check for updates

A review on security enhancements in vehicular sensor networks

Isaiah Awende Otieno *

Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo, Kenya.

GSC Advanced Research and Reviews, 2024, 21(03), 074–107

Publication history: Received on 14 October 2024; revised on 02 December 2024; accepted on 04 December 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.3.0457

Abstract

Vehicular Sensor Networks (VSNs) have emerged as a cornerstone in advancing intelligent transportation systems, enabling seamless communication between vehicles and infrastructure to enhance road safety, traffic management, and driving efficiency. However, the dynamic topology, high mobility, and stringent latency requirements of VSNs introduce unique challenges in ensuring robust security and optimal performance. This review paper provides a comprehensive analysis of recent advancements in security mechanisms and performance optimization techniques tailored for VSNs. It examines threats such as unauthorized access, data tampering, denial-of-service attacks, and privacy breaches while discussing state-of-the-art cryptographic methods, authentication protocols, and intrusion detection systems to mitigate these risks. Additionally, the paper explores performance-enhancing strategies, including efficient routing protocols, congestion control algorithms, and resource management frameworks. A critical evaluation of trade-offs between security and performance is also presented, highlighting the need for integrated solutions that balance these aspects in resource-constrained VSN environments. By synthesizing recent research findings and identifying current limitations, this review aims to guide future research toward developing resilient, efficient, and scalable vehicular sensor networks.

Keywords: VSNs; Vanets; Security; Privacy; Performance; Sensor networks

1. Introduction

The rapid advancement of intelligent transportation systems (ITS) has led to the widespread adoption of Vehicular Sensor Networks (VSNs), which enable seamless communication among vehicles, roadside infrastructure, and other network entities [1], [2]. A typical ITS is shown in Figure 1 below. By integrating sensors, communication technologies, and data analytics, VSNs have transformed modern transportation systems, enhancing road safety, traffic efficiency, and environmental sustainability [3]-[5]. These networks play a critical role in applications such as collision avoidance, traffic flow optimization, and autonomous driving, where real-time data sharing and processing are imperative. However, the unique characteristics of VSNs, including high mobility, dynamic topology, and heterogeneous communication protocols [6], introduce significant challenges in ensuring secure and high-performing network operations.

Security is a fundamental concern in VSNs due to the sensitivity of the data exchanged and the potential for malicious attacks, such as eavesdropping, data tampering, denial-of-service (DoS) attacks, and unauthorized access [7], [8]. Ensuring confidentiality, integrity, availability, and authenticity in such a dynamic environment requires robust cryptographic techniques, secure authentication protocols, and real-time intrusion detection mechanisms [9]-[11]. At the same time, the performance of VSNs is equally critical, as applications demand ultra-low latency, high throughput, and reliability to ensure seamless functioning in real-world scenarios [12], [13]. Achieving these performance metrics requires innovative solutions for efficient routing, congestion control, and resource management.

* Corresponding author: Isaiah Awende Otieno

The interplay between security and performance in VSNs adds complexity to designing effective solutions. Enhancing security mechanisms often comes at the cost of increased computational overhead, potentially degrading network performance [14]-[16]. Conversely, performance-optimized systems may introduce vulnerabilities by prioritizing speed over security [17]. As a result, there is a growing need for integrated approaches that balance these trade-offs and address the multifaceted requirements of VSNs.

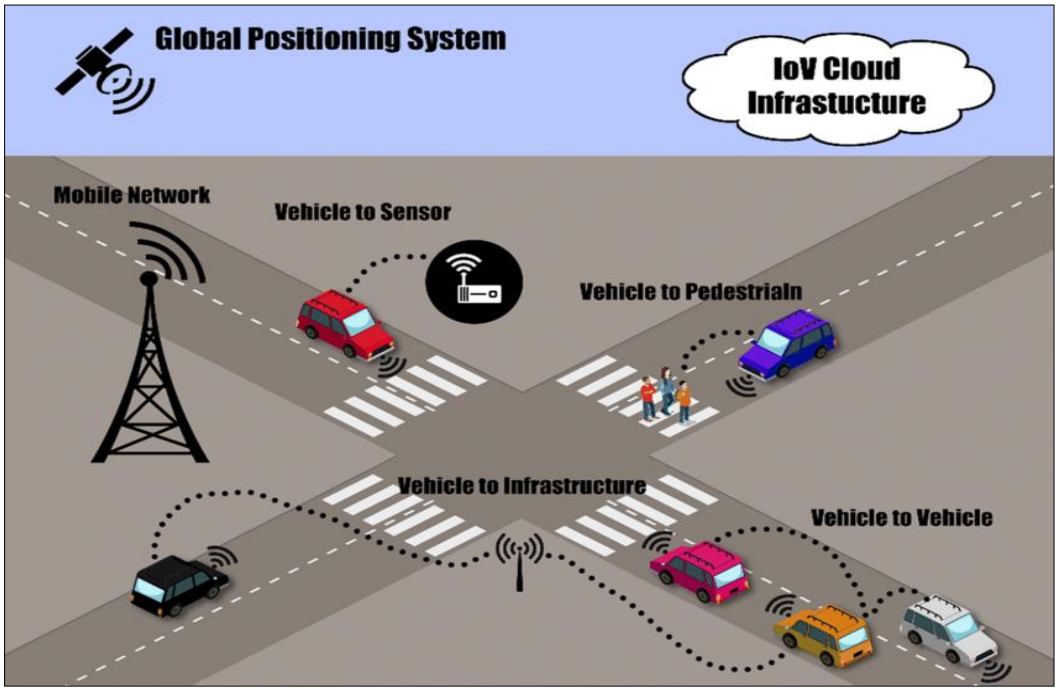

Figure 1 Intelligent transportation system

This review paper aims to provide a comprehensive analysis of the current advancements in security and performance enhancements for VSNs. By synthesizing existing research, this work identifies key challenges, evaluates state-of-the-art solutions, and highlights potential areas for future exploration. The paper is structured to discuss the primary security threats and mitigation strategies, followed by an examination of performance optimization techniques and their impact on VSN operations. Finally, a critical evaluation of the trade-offs between security and performance is presented to guide future research efforts toward building resilient and efficient VSNs.

2. Vehicular Sensor Network architecture

The architecture of a vehicular sensor network is a multilayered framework designed to support communication, sensing, and computation across diverse network components to enable intelligent transportation systems [18], [19]. As demonstrated in Figure 2, at its core, VSNs comprise three main entities: vehicles, roadside infrastructure, and backend servers, all interconnected through various communication technologies. Vehicles are equipped with sensors, on-board units (OBUs), and GPS devices that gather real-time data about the vehicle's speed, location, and surrounding environment [20]. These OBUs facilitate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, creating the foundation for cooperative driving and safety applications [21].

Roadside infrastructure, such as Roadside Units (RSUs), plays a pivotal role in extending the network's coverage and enhancing communication reliability [22]. RSUs act as intermediaries between vehicles and backend servers, enabling vehicle-to-roadside (V2R) and vehicle-to-cloud (V2C) interactions [23]. These units also facilitate access to critical services, including traffic signal management, dynamic traffic updates, and emergency response coordination [24]. Backend servers, typically hosted in data centers or cloud environments, aggregate and process the vast amount of data generated within the VSN [25]. They perform tasks such as advanced analytics, long-term storage, and decision-making to optimize overall system performance.

The communication framework within VSNs is often categorized into three layers: perception, network, and application. The perception layer is responsible for collecting data through on-board sensors and external sources, ensuring accurate and timely information flow. The network layer handles data transmission [26], employing various

communication protocols such as Dedicated Short-Range Communication (DSRC), cellular networks (e.g., 5G), and Wi-Fi [27], [28]. This layer also manages routing, mobility, and quality-of-service (QoS) requirements. The application layer hosts the intelligent transportation applications, including collision avoidance, autonomous driving, and real-time navigation [28], by utilizing the data processed from the lower layers.

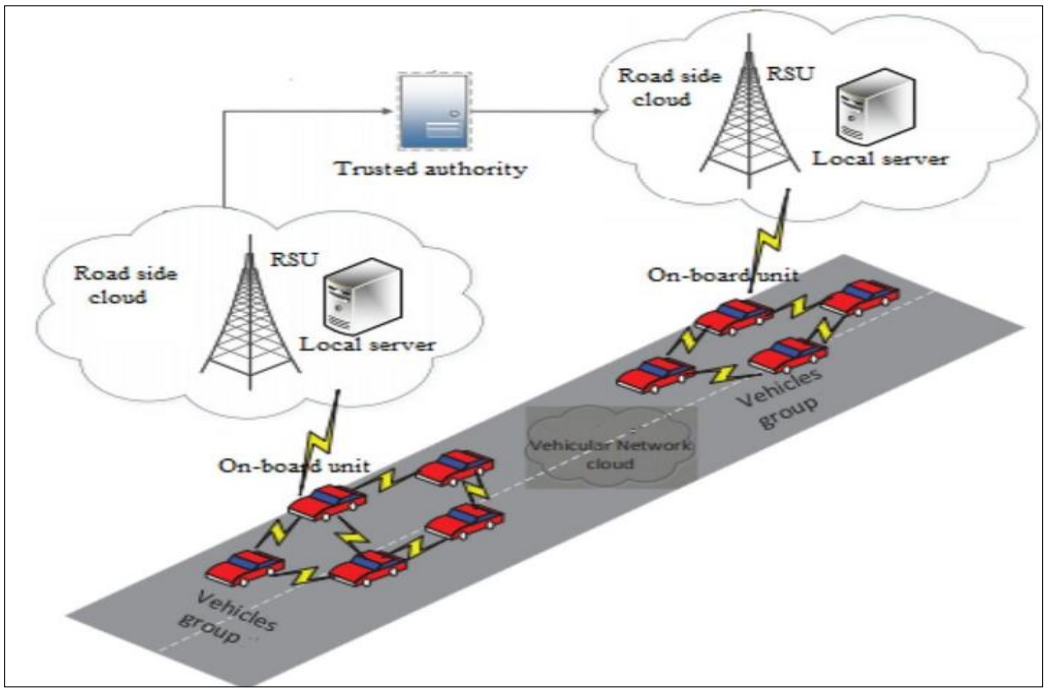

Figure 2 Vehicular Sensor Network architecture

A key feature of VSN architecture is its reliance on heterogeneous communication technologies [29] and protocols to meet the dynamic and diverse demands of vehicular environments. For instance, DSRC provides low-latency communication for safety-critical applications, while cellular networks offer higher bandwidth for infotainment and cloud-based services [30]. The architecture is also designed to support scalability and interoperability, ensuring seamless integration across different manufacturers, regions, and standards. The robustness and efficiency of the VSN architecture are critical for achieving the high levels of safety [31], performance, and reliability required in modern transportation systems.

3. Security issues in Vehicular Sensor Networks

Vehicular sensor networks face numerous security challenges due to their dynamic nature, high mobility, and reliance on wireless communication [32], [33]. The integrity, confidentiality, availability, and authenticity of data exchanged within these networks are critical to ensuring safe and reliable operations. However, various security vulnerabilities and threats can compromise these objectives, putting the effectiveness of VSNs at risk [34], [35]. Below is an extensive description of the major security issues encountered in VSNs:

3.1. Authentication and identity management

Authentication and identity management are critical components of vehicular sensor networks to ensure that only legitimate entities, such as vehicles, roadside units, and backend servers, participate in network activities [36], [37]. As shown in Figure 3, authentication verifies the identity of a communicating entity, preventing unauthorized access and protecting the network from impersonation attacks like identity spoofing. Identity management involves maintaining and verifying unique identifiers for each participant while ensuring scalability and efficiency in dynamic vehicular environments [38], [39]. Given the high mobility and real-time requirements of VSNs, traditional authentication mechanisms may not be suitable, necessitating lightweight and fast protocols [40], [41]. Additionally, privacy concerns must be addressed by incorporating techniques such as pseudonyms and anonymous authentication to protect user data while maintaining accountability [42]. Balancing security, performance, and privacy remains a significant challenge in designing robust authentication and identity management systems for VSNs.

Ensuring that only authorized entities can participate in the network is a fundamental requirement. In VSNs, vehicles and infrastructure need to authenticate themselves to each other to prevent unauthorized access [43].

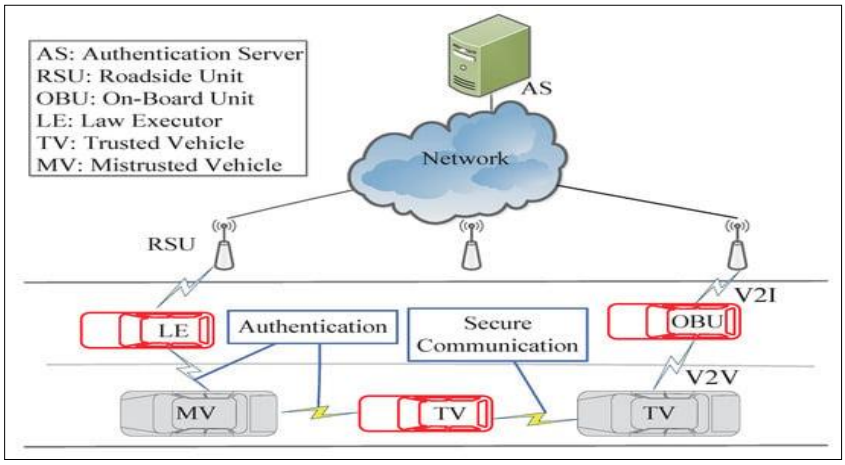

Figure 3 Authentication in VSNs

However, due to the high mobility of vehicles and the need for low-latency communication, achieving efficient and scalable authentication remains challenging [44]. Issues such as identity spoofing, where attackers impersonate legitimate entities, can lead to false data dissemination and compromise network trustworthiness.

3.2. Data confidentiality and privacy

Data confidentiality and privacy are fundamental to ensuring secure and trustworthy communication in vehicular sensor networks [45]. Confidentiality safeguards sensitive information, such as location, speed, and user identities, from being accessed or intercepted by unauthorized entities, typically through encryption techniques [46], [47]. Privacy focuses on protecting user-related data from exposure or misuse, ensuring that personal information cannot be traced back to individuals or misappropriated [48]. Figure 4 demonstrates a typical secure data sharing over VSNs. However, achieving these goals in VSNs is challenging due to the dynamic topology, real-time data exchange, and resource constraints of the network. Privacy-preserving mechanisms, such as pseudonym-based schemes and group signatures, are often used to anonymize data without compromising its utility [49]-[51]. Striking a balance between robust confidentiality measures and the computational efficiency required for high-speed vehicular communications is essential to maintaining secure and private VSN operations.

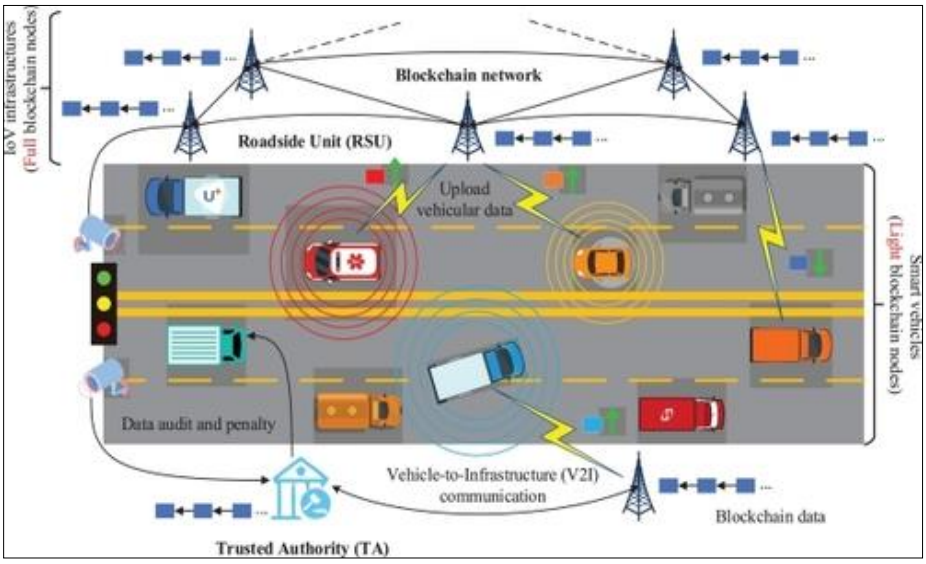

Figure 4 Secure data sharing over VSNs

The sensitive nature of vehicular data, such as location, driving behavior, and personal information, makes confidentiality and privacy paramount. Attackers can eavesdrop on communication channels to intercept private data, leading to breaches of user privacy [52], [53]. Ensuring data confidentiality often requires robust encryption techniques, but the computational overhead of these methods can strain resource-constrained devices in VSNs. Privacy-preserving schemes must also address issues such as anonymity and unlinkability without compromising functionality or security.

3.3. Data integrity and authenticity

Data integrity and authenticity are vital for the reliable operation of vehicular sensor networks, ensuring that the transmitted data is accurate, unaltered, and originates from a legitimate source [54]. As shown in Figure 5, integrity protects the data from unauthorized modifications during transmission, while authenticity verifies the identity of the sender, preventing malicious entities from injecting false information into the network [55],][56]. These aspects are crucial in scenarios like traffic management and collision avoidance, where incorrect or tampered data can lead to severe consequences. Techniques such as message authentication codes (MACs), digital signatures, and cryptographic hashing are commonly employed to uphold integrity and authenticity [57], [58]. However, these methods must be lightweight and efficient to meet the low-latency and high-speed requirements of VSNs. Balancing these measures with network performance is a critical challenge in designing secure vehicular communication systems.

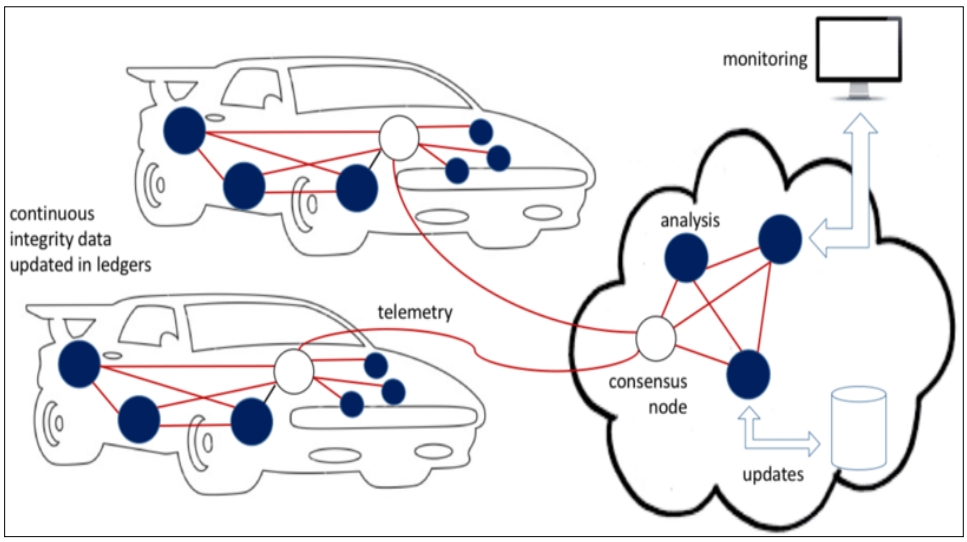

Figure 5 Data integrity and authenticity in VSNs

According to [59], data integrity ensures that information is not altered during transmission, while authenticity verifies that the source of the data is legitimate. In VSNs, attackers may tamper with transmitted data, such as altering traffic or location information, to mislead other vehicles or infrastructure [60]. This can result in traffic accidents, congestion, or denial of critical services. Message authentication codes and digital signatures are commonly employed to protect against these threats, but they must be lightweight to meet real-time requirements.

3.4. Denial-of-Service (DoS) attacks

DoS attacks aim to overwhelm the network or specific nodes, rendering them unavailable for legitimate use [61]. In VSNs, attackers can flood communication channels with excessive messages, jam wireless signals, or target specific components like roadside units [62]. This can disrupt critical services such as traffic management and emergency response, posing serious safety risks. The highly dynamic topology of VSNs exacerbates the challenge of detecting and mitigating DoS attacks effectively [63]. As demonstrated in Figure 6, Denial-of-service attacks in vehicular sensor networks aim to disrupt normal network operations by overwhelming resources, such as communication channels, roadside units, or onboard units, with excessive or malicious traffic [64]. These attacks can block critical safety messages, delay real-time data exchange [65], and render essential services like traffic management or emergency response unavailable, posing significant risks to road safety. DoS attacks can take various forms, including jamming wireless signals, flooding the network with bogus requests, or exploiting protocol vulnerabilities to cause resource exhaustion [66]. The dynamic and distributed nature of VSNs makes detecting and mitigating DoS attacks particularly challenging [67].

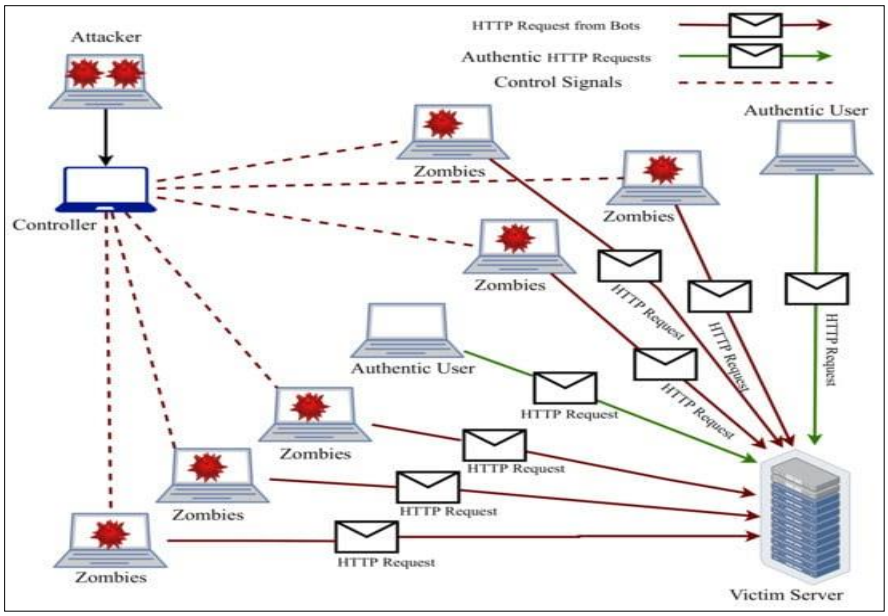

Figure 6 Denial-of-service attack

Effective countermeasures, such as intrusion detection systems, rate-limiting techniques, and adaptive resource allocation, are essential to ensure the network remains resilient and reliable under such threats.

3.5. Sybil attacks

In a Sybil attack, a malicious node generates multiple fake identities to manipulate the network [68]. In VSNs, this can lead to misleading decisions based on false traffic or safety information. For instance, an attacker might simulate a traffic jam to redirect vehicles to alternate routes, creating real congestion or enabling other malicious activities [69], [70]. Sybil attacks are particularly dangerous in VSNs because they undermine trust in the network and can cause widespread disruption [71]. As demonstrated in Figure 7, Sybil attacks in Vehicular Sensor Networks (VSNs) occur when a malicious entity creates multiple fake identities, or "Sybil nodes," to manipulate the network's operations.

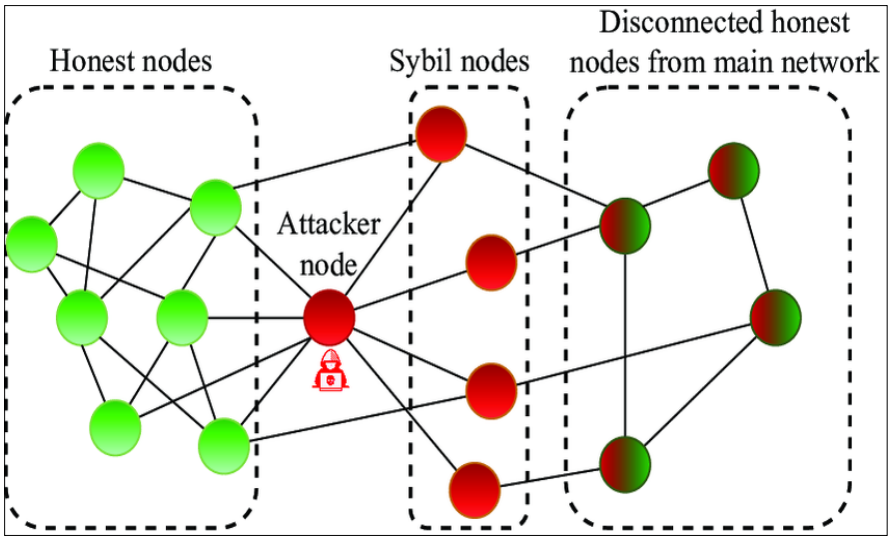

Figure 7 5. Sybil attack

These attacks can disrupt critical VSN functionalities, such as traffic management, route optimization, and collision avoidance, by disseminating false or misleading information. As explained in [72], Sybil attacks undermine trust in the network, as they exploit the assumption that each entity in the network corresponds to a single legitimate participant. Detecting and preventing these attacks is challenging due to the mobility and scalability of VSNs. Countermeasures, such

as identity verification, cryptographic techniques [73], and reputation-based systems, are employed to limit the effectiveness of Sybil attacks, ensuring the integrity and reliability of vehicular communications.

3.6. Location-based attacks

These exploit the reliance on accurate location information to disrupt network operations and mislead participants [74]. As shown in Figure 8, these attacks involve techniques such as location spoofing, where an attacker manipulates or falsifies location data to deceive other vehicles or infrastructure [75]. This can result in various harmful outcomes, such as traffic rerouting into unsafe areas, false accident reports, or interference with navigation systems. For example, an attacker could create a virtual traffic congestion scenario, prompting vehicles to avoid the area and overburden alternate routes [76]. The dynamic nature and high mobility of VSNs make it challenging to detect and mitigate these attacks effectively [77]. Countermeasures include cryptographic location verification, cross-referencing location data with trusted sources, and leveraging collaborative mechanisms among vehicles to identify inconsistencies and validate location accuracy [78].

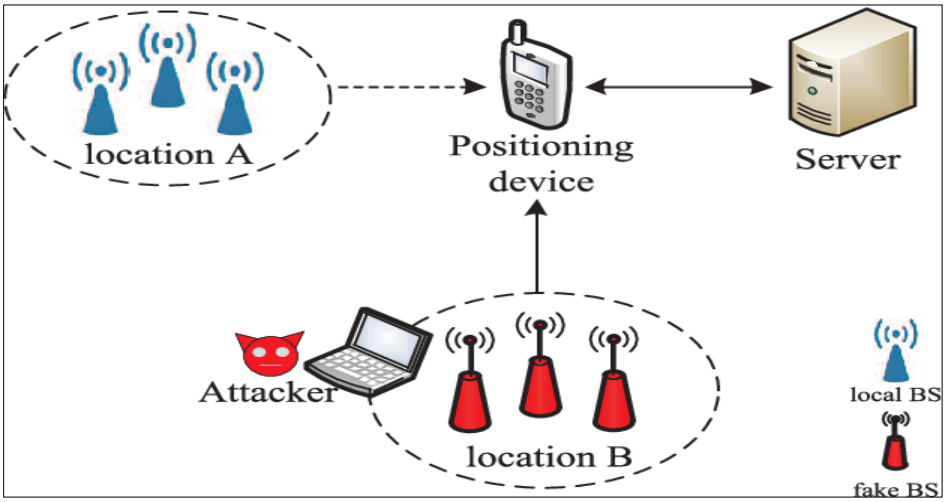

Figure 8 Location-based attack

As discussed in [79], VSNs rely heavily on accurate location information for functionalities such as navigation and collision avoidance. Attackers can exploit this dependency through location spoofing, where they send false location data to mislead other vehicles or infrastructure [80]. This can lead to accidents, incorrect traffic reports, or the rerouting of vehicles into dangerous areas. Detecting and mitigating location-based attacks require advanced verification mechanisms and context-aware systems.

3.7. Malware and software exploits

Malware and software exploits pose significant security threats in vehicular sensor networks, as they can compromise the functionality and safety of connected vehicles and infrastructure [81]. Malicious software, such as viruses, worms, or ransomware, can infect on-board units, roadside units, or backend servers, potentially gaining control over critical systems like vehicle control, navigation, or communication protocols [82]. Exploits target vulnerabilities in the software, firmware, or network protocols, allowing attackers to manipulate or hijack the system for malicious purposes, such as intercepting or altering data, disrupting communication, or even causing physical harm by overriding vehicle controls [83], [84]. Given the reliance of VSNs on complex, interconnected systems and real-time operations, detecting and preventing such attacks requires continuous monitoring, regular software updates, and the implementation of intrusion detection systems. Ensuring robust security measures, including secure booting, sandboxing, and patch management [85], is essential to defend against malware and software vulnerabilities in VSNs.

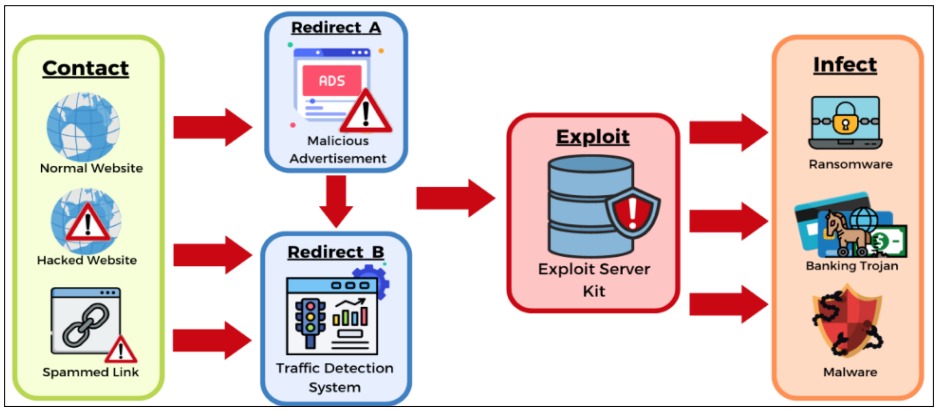

Figure 9 Malware and software exploits

As explained in [86], vehicles in a VSN often rely on embedded software and connected systems, making them susceptible to malware infections and software exploits. Attackers can exploit vulnerabilities in vehicle firmware or network protocols to gain unauthorized control over critical systems such as brakes, acceleration, or steering [87]. These attacks, often referred to as "vehicular hacking," pose severe safety threats to drivers and passengers.

3.8. Key management challenges

Key management in vehicular sensor networks presents several challenges due to the dynamic and resource-constrained nature of these networks [88]. Figure 9 gives a depiction of a key management scenario in VSNs. Secure communication in VSNs relies heavily on cryptographic keys for encryption, authentication, and data integrity [89], but managing these keys across a large number of highly mobile and frequently changing entities—such as vehicles, roadside units, and backend servers—becomes complex. Key distribution, storage, revocation, and renewal must be performed efficiently and securely to prevent unauthorized access or misuse [90].

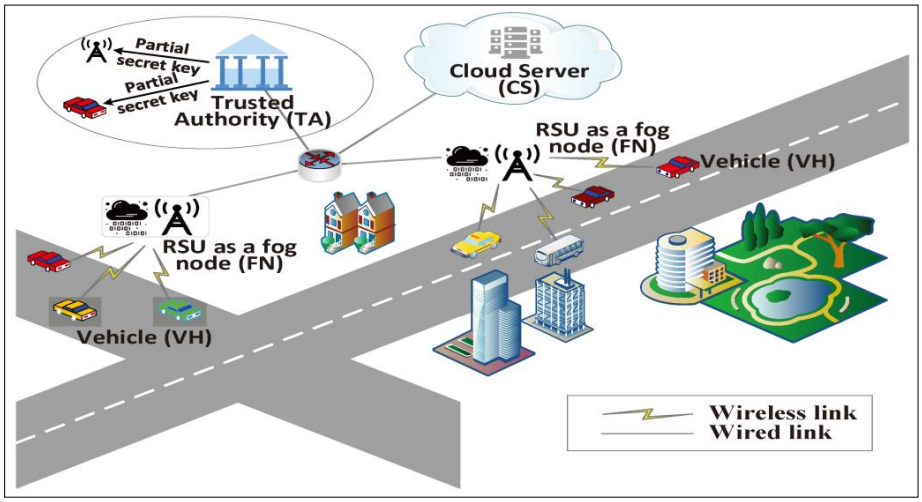

Figure 10 Key management in VSNs

Additionally, the ephemeral nature of vehicle connections and the potential for node churn (vehicles entering or leaving the network) further complicates key management. Balancing the need for robust security with the limited computational resources of the devices in VSNs requires lightweight, scalable, and adaptive key management protocols [91]. Moreover, the loss or compromise of cryptographic keys can lead to significant security vulnerabilities, making it crucial to implement mechanisms for key recovery and revocation without causing disruptions to network operations [92]. Secure communication in VSNs typically relies on cryptographic keys for encryption and authentication [93]. However, the dynamic and large-scale nature of VSNs complicates key distribution, storage, and revocation. Ensuring secure and efficient key management is challenging, particularly in scenarios where vehicles frequently join or leave the network. Additionally, the loss or compromise of cryptographic keys can severely impact network security.

3.9. Physical security threats

Physical security threats in vehicular sensor networks involve direct attacks on the hardware components of vehicles or roadside infrastructure, which can compromise the entire system's security [94]. These threats include tampering with on-board units, roadside units, or sensors to extract sensitive information, inject malicious code, or disrupt communications [95]. For example, an attacker with physical access to a vehicle's OBU could manipulate its data, such as location or speed, or install malware to gain unauthorized control over the vehicle's functions [96]. Similarly, physical attacks on RSUs could disable critical communication links or alter traffic management signals, leading to unsafe driving conditions [97]. Given that VSNs are often deployed in public or semi-public spaces, securing these physical components is essential to prevent unauthorized access [98] and ensure the overall integrity of the network. As shown in Figure 10, countermeasures, such as tamper-proof hardware, secure booting, and physical access controls, are necessary to protect against these vulnerabilities.

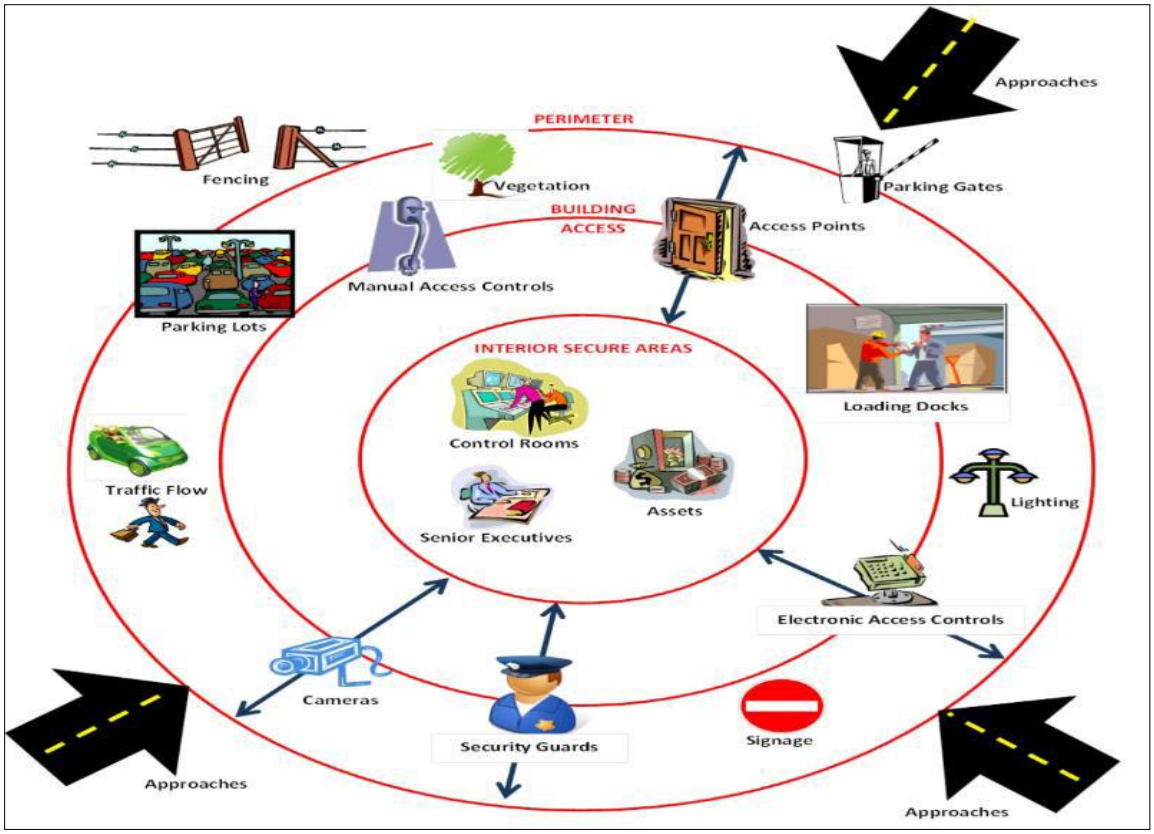

Figure 11 Remedies for physical security threats

According to [90], physical access to vehicles or roadside units can allow attackers to tamper with hardware, extract sensitive information, or inject malicious code. For instance, an attacker with physical access to an OBU or RSU could compromise the device and use it as a launch point for further attacks. Physical security measures, such as tamper-proof hardware and secure boot mechanisms, are necessary to counter these threats.

3.10. Insider attacks

These attacks occur when a trusted entity within the network, such as a legitimate vehicle, roadside unit (RSU), or network administrator, intentionally or unintentionally undermines the security of the system [100]. Insider attacks can be particularly dangerous because the insider already has authorized access to the network, making it difficult to detect malicious behavior [101]. As demonstrated in Figure 11, an insider may inject false information, manipulate data, or disrupt critical communication services, such as altering traffic flow data, providing inaccurate location information, or disabling key network components [102]. Since insiders can bypass certain security mechanisms, detecting and mitigating these attacks requires advanced monitoring systems, anomaly detection algorithms [103], and behavior-based security models that can identify deviations from normal operations. The challenge in defending against insider attacks lies in balancing trust while ensuring that the network remains secure from both external and internal threats.

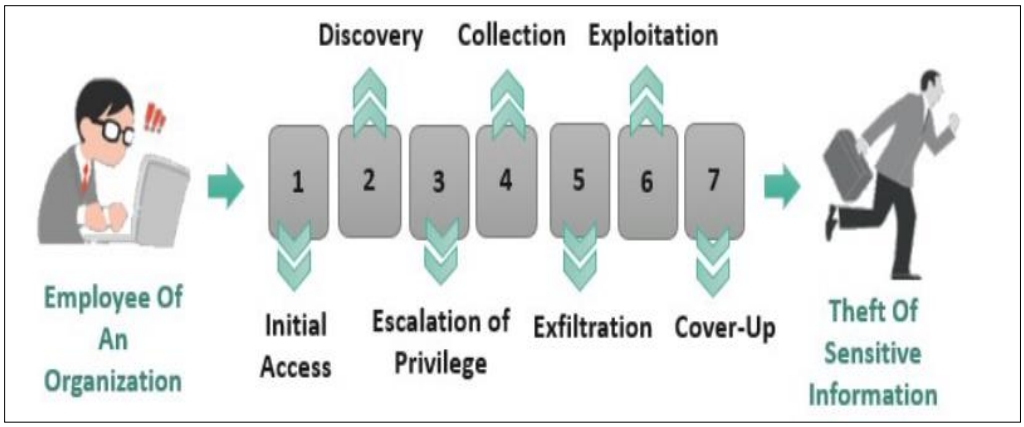

Figure 12 Insider threats

As explained in [104], insider attacks occur when a legitimate participant in the network behaves maliciously, either intentionally or due to compromise. For example, a vehicle may disseminate false information, or an RSU may be manipulated to favor specific entities [105]. Insider attacks are particularly difficult to detect and mitigate, as the malicious entity possesses valid credentials and may behave unpredictably.

3.11. Scalability and real-time constraints

Scalability and real-time constraints are critical challenges in vehicular sensor networks [106], as these networks must handle a large number of dynamic and mobile nodes while ensuring timely data exchange. VSNs are expected to support a growing number of vehicles and infrastructure elements across vast geographical areas, which demands scalable solutions for communication, data processing, and security [107]. As the network size increases, ensuring efficient resource management [108], routing, and data storage becomes more complex. At the same time, VSNs must meet stringent real-time requirements, such as low-latency communication for safety-critical applications like collision avoidance or traffic control [109]. Balancing the need for scalability with the imperative of real-time responsiveness often requires sophisticated algorithms and protocols that can adapt to fluctuating network conditions without sacrificing performance. Moreover, maintaining low overhead while scaling up to accommodate a large number of vehicles without compromising the timeliness of data delivery is a significant design challenge for VSNs [110]. The growing number of connected vehicles and devices in VSNs necessitates scalable security solutions [111]. Traditional methods may not scale effectively while maintaining real-time performance, especially under high mobility and dense traffic conditions. The need to balance security with performance adds complexity to designing effective countermeasures.

3.12. Trust management

Trust management in vehicular sensor networks deals with establishing and maintaining trust between network participants, such as vehicles, roadside units, and backend servers, to ensure secure and reliable communication [112], [113]. Given the decentralized and dynamic nature of VSNs, where vehicles frequently enter and exit the network, it becomes crucial to verify the reliability and authenticity of each entity to prevent malicious actors from manipulating network operations [114]. Figure 12 gives a depiction of how trust management can be upheld in VSNs. According to [115], trust management systems use reputation-based models, behavior analysis, and cryptographic techniques to evaluate the trustworthiness of participants based on their actions, such as adhering to communication protocols or providing accurate data.

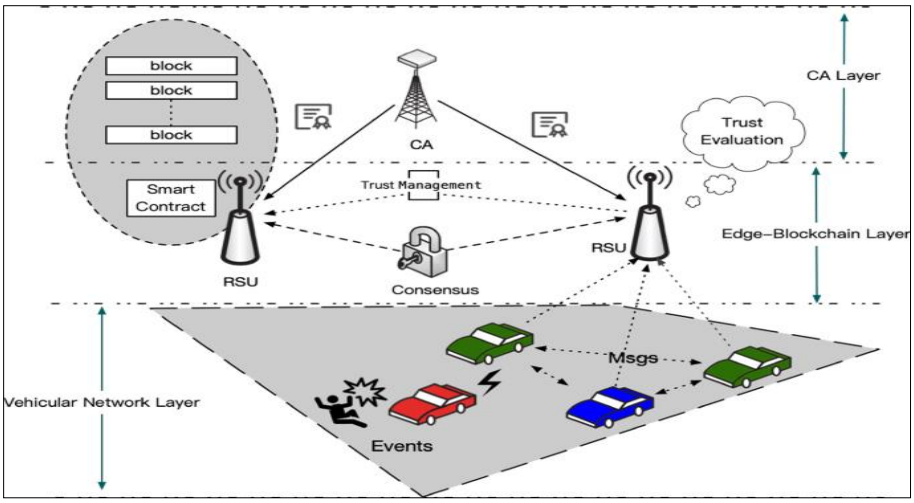

Figure 13 Trust management in vehicular sensor networks

These systems help detect and mitigate attacks like Sybil or insider threats, ensuring that only trusted nodes can influence network decisions. The challenge in trust management lies in balancing the need for robust security with the computational constraints of VSNs [116], while adapting to the high mobility and changing conditions of the vehicular environment.

4. Performance challenges in Vehicular Sensor Networks

Vehicular sensor networks are designed to enable communication and data exchange between vehicles, infrastructure, and other entities in intelligent transportation systems [117], [118]. While the potential benefits of VSNs are immense, there are numerous performance challenges that must be addressed to ensure their efficiency, reliability, and scalability in real-world applications [119]. These challenges stem from the unique characteristics of VSNs, including high mobility, dynamic topology, and diverse communication requirements, making it difficult to design systems that can meet stringent performance demands across a wide range of scenarios.

4.1. High mobility and dynamic topology

One of the most significant performance challenges in VSNs arises from the high mobility of vehicles and the resulting dynamic topology of the network [120]. Vehicles are constantly moving, which leads to frequent changes in network structure, link availability, and routing paths [121]. This can cause delays in data transmission, packet loss, and difficulties in maintaining stable connections [122]. Traditional routing algorithms, which are designed for static or low-mobility environments, often struggle to perform optimally in VSNs [123]. The network must adapt quickly to these changes while ensuring low-latency and high-throughput communication, particularly in critical safety applications such as collision avoidance and traffic management.

4.2. Real-time communication and low latency

Many applications in VSNs, such as safety-critical services (e.g., collision avoidance, emergency vehicle prioritization, and real-time traffic updates), require real-time communication with very low latency [124], [125]. This means that data must be transmitted and processed in near-instantaneous time to be actionable. Achieving this level of performance is challenging due to the limitations in available bandwidth, the unpredictability of wireless channels, and the need for fast decision-making. Furthermore, the varying communication distances between vehicles and roadside infrastructure, coupled with signal interference and congestion, can lead to delays in data transmission [126], which compromises the effectiveness of real-time services.

4.3. Scalability

As the number of connected vehicles and infrastructure elements increases, scalability becomes a critical concern for VSNs. A growing number of vehicles can lead to network congestion, where too many devices try to communicate over the same frequency channels or within limited bandwidth [127], resulting in delays, packet collisions, and network instability. Additionally, the sheer volume of data generated by VSNs (e.g., traffic information, sensor data, vehicle telemetry) can overwhelm existing processing and storage infrastructure if not handled efficiently [128], [129].

Scalability issues are further exacerbated by the need to support seamless communication between heterogeneous devices, including different vehicle models, road sensors, and infrastructure components, each with varying capabilities and communication protocols [130], [131]. Designing routing and data aggregation protocols that can handle a high density of vehicles while maintaining efficient resource utilization is a complex but necessary task.

4.4. Resource constraints

Vehicles and roadside units in VSNs are typically equipped with embedded systems with limited computational power, storage, and energy resources [132], [133]. This poses significant challenges in terms of performance optimization, as security mechanisms (such as encryption and authentication), routing protocols, and data processing techniques can be resource-intensive [134]. Optimizing these mechanisms to function within the resource constraints of these devices is critical to maintaining overall system performance. For instance, computationally expensive cryptographic operations can introduce delays, and inefficient routing algorithms can consume excessive power, reducing the operational lifespan of battery-powered devices [135]-[139]. As a result, VSNs need to leverage lightweight, efficient solutions that minimize resource consumption without compromising security or performance.

4.5. Communication reliability and interference

VSNs rely on wireless communication to transmit data between vehicles and infrastructure. However, the wireless medium is prone to a variety of interferences and issues that can affect communication reliability, such as signal attenuation, multipath fading, interference from other wireless devices, and congestion in dense traffic areas [140], as evidenced in Figure 13.

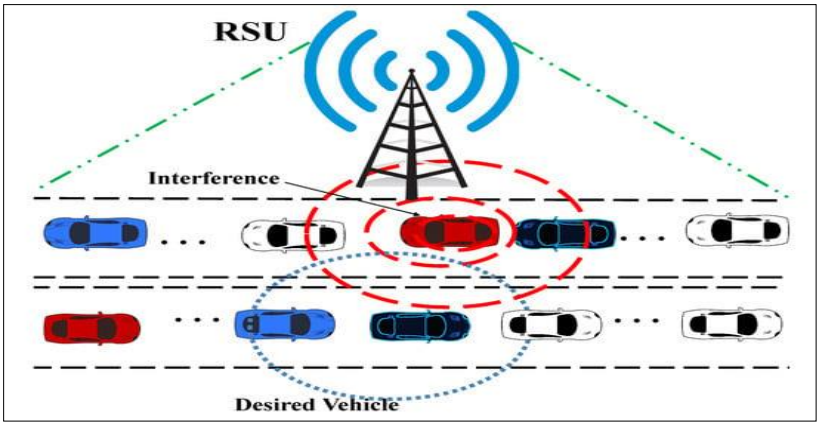

Figure 14 Interference in VSNs

These communication challenges can lead to packet loss, delays, and lower throughput, which are particularly problematic in applications requiring constant and reliable data exchange, such as autonomous driving and real-time traffic monitoring [141]-[143]. The need for robust communication protocols that can adapt to varying conditions and provide high reliability in different network topologies is crucial for the successful deployment of VSNs.

4.6. Quality of Service (QoS) and prioritization

Quality of Service (QoS) is another critical performance challenge in VSNs. Different applications within VSNs have varying requirements in terms of latency, bandwidth, and reliability [144], [145]. Safety-critical applications, such as collision avoidance, require low-latency communication and high reliability [146], whereas infotainment or navigation applications may tolerate higher latency but require higher bandwidth [147]. Ensuring that all applications meet their specific QoS requirements in a dynamic and high-density network is complex. Effective QoS management in VSNs involves prioritizing traffic based on application needs, dynamically adjusting resources, and using techniques such as traffic differentiation, bandwidth allocation, and load balancing.

4.7. Energy efficiency

Energy efficiency is a crucial concern in VSNs, particularly for battery-powered vehicles and roadside units [148]. The need for continuous communication, data processing, and sensor monitoring can lead to high energy consumption [149], which can reduce the lifespan of devices, especially in remote or mobile units that cannot be easily recharged. Efficient energy management strategies, such as adaptive transmission power control, energy-aware routing protocols,

and low-power sleep modes, are necessary to extend the operational time of these devices while maintaining network performance [150]-[154]. Balancing energy consumption with the demands for high performance, low latency, and reliability is one of the key trade-offs in VSN design.

4.8. Heterogeneity and interoperability

VSNs are composed of diverse devices, including vehicles from different manufacturers [155], various types of sensors, and different types of communication technologies (e.g., DSRC, 5G, Wi-Fi). Ensuring interoperability between these heterogeneous devices is a significant challenge for maintaining network performance [156]. The varying capabilities of devices, such as different processing powers, communication ranges, and energy capacities, require protocols and standards that can function seamlessly across these devices [157]. Achieving interoperability without introducing excessive overhead or compromising system performance is essential for the scalability and practical deployment of VSNs.

4.9. Security-performance trade-offs

Security mechanisms, such as encryption, authentication, and intrusion detection, are essential for protecting VSNs from malicious attacks [158]. However, these security measures can introduce additional overhead, which may degrade performance in terms of latency, throughput, and resource consumption. The challenge lies in finding an optimal balance between maintaining high security and ensuring that performance requirements, particularly for real-time and safety-critical applications, are met. Lightweight cryptographic techniques [159], efficient authentication protocols, and resource-aware security solutions are necessary to mitigate the impact of security measures on VSN performance.

In a nutshell, these performance challenges are multifaceted and interrelated, requiring a comprehensive approach to address issues such as high mobility, scalability, resource constraints, communication reliability, and security-performance trade-offs. Achieving optimal performance in VSNs is critical to their success in supporting intelligent transportation systems, autonomous driving, and real-time traffic management [160], [161]. To overcome these challenges, ongoing research and innovation in adaptive routing protocols, energy-efficient communication techniques, QoS management, and secure and lightweight data handling are essential for ensuring that VSNs can meet the demanding requirements of modern transportation networks.

5. Techniques for security enhancements in Vehicular Sensor Networks

Vehicular sensor networks are integral to intelligent transportation systems, enabling critical applications such as traffic management, autonomous driving, and safety communications [162]. However, the inherent vulnerabilities of these networks—due to their dynamic topology, high mobility, and reliance on wireless communication—make them susceptible to various security threats, including eavesdropping, data tampering, and DoS attacks [163], [164]. To address these challenges and ensure the integrity, privacy, and reliability of VSNs, several advanced security enhancement techniques have been developed. These techniques aim to protect against unauthorized access, maintain the confidentiality of communication, ensure data integrity, and defend against malicious attacks. Table 1 provides detailed description of these techniques.

Table 1 Techniques for security enhancements in VSNs

Technique	Examples	Explanation
Cryptographic		Cryptography plays a fundamental role in securing communication within VSNs [165]. Several cryptographic techniques are used to protect the confidentiality, integrity, and authenticity of data
	Public Key Infrastructure (PKI)	PKI is widely used in VSNs to manage digital certificates for encryption and authentication [166]. It ensures that only authorized vehicles and infrastructure can access the network and communicate securely.
	Lightweight encryption	Given the limited resources (such as processing power and battery life) of vehicular devices, lightweight encryption algorithms are developed to ensure secure communication without significant overhead [167], [168]. Examples include Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) with reduced key sizes [169], which provide strong security with low computational cost.

	Message Authentication Codes (MACs)	MACs are used to verify the authenticity and integrity of messages transmitted between vehicles and roadside units [170]. This prevents attackers from tampering with data during transmission [171]. A common technique involves the use of symmetric key cryptography [172], which enables verification of the sender's identity and message integrity.
Authentication and identity management		Authentication is critical for ensuring that only legitimate nodes can join and participate in the network [173]. Given the open nature of vehicular networks, there is a constant need to verify the identity of entities (vehicles, infrastructure) to prevent attacks like impersonation or Sybil attacks [174].
	Certificate-based	This technique uses digital certificates issued by a trusted authority to verify the identity of vehicles and RSUs [175]. The certificates contain public keys that are used for encryption and digital signature verification.
	Anonymous	Since privacy is a key concern in VSNs, vehicles are often assigned pseudonyms to avoid revealing their real identity [176]. Anonymous authentication protocols allow vehicles to prove their authenticity without exposing their actual identity [177], thereby protecting user privacy.
	Reputation-based	Reputation systems are used to evaluate the trustworthiness of nodes based on their past behavior [178]. Vehicles with a high reputation are more likely to be trusted for data exchange and routing, while nodes with low reputation may be ignored or flagged as malicious.
Secure routing protocols		Due to the highly dynamic nature of VSNs, traditional routing protocols are not well-suited for providing secure communication, as attackers can easily manipulate or disrupt communication paths [179], [180]. Secure routing protocols are essential to ensure data integrity and confidentiality during transmission.
	Geographic-based	Geographic routing protocols use the position of vehicles (obtained via GPS) to determine the best path for message delivery [181]. Secure geographic routing protocols employ encryption and authentication at each hop to ensure that only authorized nodes are involved in the routing process [182] and prevent malicious nodes from redirecting traffic or dropping packets.
	Trust-based	In these protocols, trustworthiness scores are assigned to nodes based on their past behaviors, such as forwarding packets correctly [183]. Nodes with high trust scores are more likely to be selected as part of the communication path [184]. This helps mitigate attacks by isolating untrustworthy or malicious nodes from the communication process.
	Secured Ad-hoc On-demand Distance Vector (AODV)	This protocol enhances the standard AODV routing protocol by adding cryptographic techniques [185] to ensure that routing information is authentic and unaltered. It uses digital signatures to authenticate the origin of route requests and prevents route poisoning attacks [186].
Intrusion Detection Systems (IDS)		Intrusion detection systems (IDS) are designed to monitor network traffic and identify suspicious activities that may indicate a security breach [187]. In VSNs, IDS can detect a wide range of malicious behaviors, such as DoS attacks, Sybil attacks, or malicious data injection.
	Signature-based	This method involves identifying known attack patterns by comparing incoming data with a database of signatures [188]. Signature-based IDS are effective for detecting well-defined attack types but are less adaptive to new, unknown attacks.
	Anomaly-based	Anomaly-based detection involves establishing a baseline of normal network behavior and identifying deviations from that baseline [189]. This approach can detect novel attacks by recognizing unusual patterns, such as an unusually high volume of traffic or irregular data packets [190]. In VSNs,

		this is particularly useful for detecting attacks like jamming or abnormal vehicle behavior.
	Collaborative	In a collaborative approach, vehicles and infrastructure share security information and work together to detect and mitigate security threats [191], [192]. This enhances detection accuracy and helps identify attacks that may not be visible from a single node's perspective.
Data integrity and authentication		Ensuring the integrity and authenticity of data is critical in VSNs to prevent malicious actors from injecting false information that could disrupt traffic flow, cause accidents, or hinder safety systems [193].
	Digital signatures	Digital signatures are used to verify the authenticity of data and ensure that the information has not been tampered with [194], [195]. Each vehicle or RSU uses its private key to sign data, and the recipient can verify the signature using the sender's public key.
	Hashing	Cryptographic hash functions are used to ensure that the data has not been altered during transmission [196], [197]. A hash value is computed for each message, and the recipient can compare it with the expected hash to verify data integrity.
Privacy-Preserving		Privacy is a significant concern in VSNs, as vehicles frequently exchange sensitive information such as location, speed, and driving behavior, which can be used to track individuals [198].
	Pseudonym-based	In VSNs, vehicles frequently change their identities by using pseudonyms instead of real identifiers to preserve privacy while still maintaining accountability [199], [200]. The pseudonyms are periodically updated to prevent tracking over time, ensuring the anonymity of the user.
	Mix networks	Mix networks involve routing messages through a series of intermediate nodes that shuffle and encrypt data to prevent the message's origin or destination from being easily traced [201], [202]. This technique can be used to enhance privacy while allowing for secure communication.
	Zero-knowledge proofs	Zero-knowledge proofs allow one entity to prove to another that it knows a piece of information (e.g., a password) without revealing the actual information [203], [204]. This is particularly useful for authentication in VSNs where privacy needs to be balanced with trust and security.
DoS mitigation		VSNs are vulnerable to various DoS attacks, such as jamming, flooding, and resource exhaustion [205].
	Rate limiting	This technique involves limiting the number of requests or messages a node can send within a certain time period to prevent flooding attacks [206].
	Traffic filtering	By analyzing incoming traffic for patterns typical of DoS attacks [207], malicious traffic can be identified and blocked, ensuring that only legitimate requests are processed.
	Anti-jamming	Anti-jamming strategies include frequency hopping and spread spectrum techniques [208] to avoid jamming and ensure uninterrupted communication.
Lightweight security		Considering the resource constraints of vehicles and RSUs, lightweight security protocols are necessary to ensure that security does not overly burden the network's performance [209], [210]. These mechanisms aim to provide strong security while minimizing overhead in terms of computation, storage, and communication.
	Lightweight encryption schemes	Enable secure communication without significantly degrading network performance [211].

	Efficient authentication protocols Compact signatures	

It is clear that the security challenges in vehicular sensor networks are multifaceted, requiring a combination of cryptographic, trust management, routing, and privacy-preserving techniques [212] to protect against a variety of attacks. The techniques mentioned above form a comprehensive approach to enhance the security, integrity, and privacy of VSNs, ensuring that they can operate safely and efficiently in dynamic and potentially adversarial environments. With ongoing advancements in security research, these techniques continue to evolve to address emerging threats and ensure the resilience of VSNs as they become an integral part of future intelligent transportation systems.

6. Methods for performance enhancements in Vehicular Sensor Networks

Vehicular sensor networks are an essential component of intelligent transportation systems, which leverage real-time data collection and communication to improve road safety, traffic management, and environmental monitoring. However, the dynamic and highly mobile nature of these networks introduces several performance challenges, including issues related to scalability, latency, energy efficiency, data integrity, and throughput [213], [214]. To optimize VSNs for these operational demands, several methods have been proposed to enhance the performance of the system across various levels, from network architecture to protocol design. This section explores these methods in detail, focusing on key aspects such as scalability, energy efficiency, real-time performance, and data management.

6.1. Scalable network architecture

One of the primary challenges in VSNs is ensuring scalability, as these networks must accommodate a large number of vehicles and infrastructure components [215]. As the number of connected vehicles increases, VSNs need to maintain stable communication and effective data management, which becomes more difficult due to the mobile and dynamic nature of the network. In a scalable VSN architecture, scalability concerns are addressed through hierarchical designs, efficient routing protocols, and distributed communication methods that allow for the network to grow without significant performance degradation [216]. The methods for enhancing scalability include:

Hierarchical routing protocols: Hierarchical architectures use multiple levels of communication, such as local clusters, regional groups, and global networks, to manage the traffic and reduce congestion [217]. Clustering nodes (vehicles and RSUs) into groups reduces the communication overhead [218] by aggregating data locally before transmitting it to the central server or base station.

Fog and edge computing: By introducing fog and edge computing into VSNs, data processing and storage are moved closer to the source of data generation, such as vehicles, reducing latency and network congestion [219], [220]. These decentralized computing models help in offloading computational tasks from centralized cloud servers, thereby improving the overall scalability of the network.

Content-Centric Networking (CCN): CCN approaches focus on the content rather than the end-to-end connection between nodes [221]. By enabling vehicles and RSUs to retrieve and cache relevant data locally, the need for direct communication with distant nodes is minimized, enhancing scalability.

6.2. Energy-efficient communication

Energy efficiency is a critical performance factor in VSNs due to the limited energy resources of vehicular sensors and mobile devices [222]. Given that these networks are typically deployed in resource-constrained environments, energy-efficient communication protocols are essential to prolong the lifespan of nodes and ensure the longevity of the entire network [223], [224]. The techniques for enhancing energy efficiency are as follows:

- *Low Power Wide Area Networks (LPWAN)*: LPWANs are designed to provide long-range connectivity while consuming minimal energy [225]. They are ideal for VSNs where large-scale sensor deployments are needed but energy resources are limited. Technologies such as LoRa (Long Range) and Sigfox offer solutions for energy-efficient communication.

- *Adaptive transmission power control*: In environments like VSNs, where the network topology frequently changes, adaptive transmission power control (TPC) can help manage the power used during data transmission [226]. By adjusting the transmission power based on the distance between nodes and the network conditions, vehicles can reduce energy consumption while maintaining a reliable communication link.
- *Duty cycling*: Duty cycling refers to the practice of turning off communication modules when they are not needed and waking them up periodically to send or receive data [227]. This approach significantly reduces the energy consumption of the network. Sleep modes and low-power listening mechanisms can help maintain low power consumption in vehicles, especially in low-traffic conditions.

6.3. Real-time communication and latency optimization

Real-time data exchange is a fundamental requirement for applications such as collision avoidance, traffic management, and environmental monitoring in VSNs [228]. Therefore, minimizing communication latency and ensuring timely delivery of messages is crucial for improving the performance of these networks. The various methods for reducing latency and optimizing real-time communication are described below:

- *Priority-based routing*: Real-time applications in VSNs often require prioritization of critical messages, such as warnings about road hazards or emergency vehicle alerts. Priority-based routing protocols assign higher priority to time-sensitive messages to reduce delay and ensure that urgent data is delivered without congestion or interference from less critical information [229].
- *Geographic routing*: Geographic or position-based routing protocols make use of the geographical locations of nodes (vehicles) and routing decisions based on proximity to the destination [230]. This minimizes the need for global topology information, reducing routing overhead and latency. Protocols like Greedy Perimeter Stateless Routing (GPSR) and Geocast-based routing are commonly used in VSNs to ensure fast delivery of messages in real-time applications.
- *Real-time traffic management*: Dynamic and adaptive traffic management protocols [231] can be used to adjust communication strategies in response to real-time traffic conditions. By considering traffic congestion, vehicle density, and network load, these protocols optimize routing decisions, reducing delays and ensuring that high-priority messages are transmitted quickly.

6.4. Data aggregation and compression

With the vast amount of data generated by vehicular sensors, raw data transmission can be inefficient and cause unnecessary congestion in the network [232]. Aggregating and compressing data before transmission can significantly reduce the volume of data sent over the network, leading to improved throughput and more efficient use of network resources. The techniques for data aggregation and compression are discussed below:

- *Data fusion*: In VSNs, data from multiple sources (e.g., vehicles, RSUs, and sensors) is often redundant. Data fusion techniques combine the data from various sources to reduce the volume of data that needs to be transmitted while preserving the important information [233]. Techniques like Kalman filters, Bayesian networks, and consensus algorithms are widely used for data fusion.
- *Compression algorithms*: Data compression techniques reduce the size of data packets before transmission, thereby reducing network congestion and improving overall throughput [234]. Advanced compression methods, such as lossless or lossy compression, can be tailored to the specific characteristics of vehicular data, such as video feeds or sensor measurements.

6.5. Efficient routing protocols

Routing protocols in VSNs are responsible for determining the most optimal path for data transmission, which is critical for improving network performance [235]. Given the high mobility of vehicles, traditional static routing protocols often fail to adapt to changes in the network topology, resulting in inefficient [236] data routing and increased delays. The methods for enhancing routing efficiency are described below:

Vehicular Ad Hoc Networks (VANETs) routing: VSNs are typically implemented using VANETs, which rely on vehicles as mobile nodes. Routing protocols such as Ad hoc On-demand Distance Vector (AODV), Optimized Link State Routing (OLSR), and Dynamic Source Routing (DSR) have been designed specifically for these types of networks [237]. These protocols are optimized for VSNs by adapting to vehicle mobility, topology changes, and dynamic traffic conditions.

Predictive routing: Predictive routing algorithms use historical mobility data, vehicle speed, and trajectory predictions to anticipate future network conditions and optimize the routing path accordingly [238]. These protocols aim to reduce the delay associated with topology changes by leveraging knowledge about vehicle movement patterns.

Multi-path routing: Multi-path routing protocols aim to send data through multiple routes to increase reliability and reduce the likelihood of network congestion or failure [239]. If one path becomes unavailable due to mobility or network issues, other paths can be used to maintain communication, ensuring higher reliability and lower latency.

6.6. Network coding for improved throughput

Network coding is a technique that can be applied to VSNs to increase throughput and reduce congestion by allowing data to be mixed (coded) at intermediate nodes rather than forwarded unchanged [240]. This allows for more efficient use of the available bandwidth, as data can be transmitted simultaneously along different paths. The techniques for enhancing throughput with network coding include:

- *Opportunistic network coding*: This approach uses network coding opportunistically at intermediate nodes to combine packets from different sources. By allowing nodes to combine and forward coded packets instead of relaying them individually, bandwidth utilization [241] is improved, and overall throughput is enhanced.
- *Cooperative communication*: In scenarios where vehicles can cooperate with each other, network coding can be used to enable vehicles to transmit coded messages [242], allowing for better use of the network resources and reducing redundancy in data transmission.

6.7. Data quality and reliability

Ensuring data quality and reliability is essential for the effectiveness of VSNs in safety-critical applications [243]. Data losses, corruption, and inconsistencies can significantly degrade the performance of VSN-based applications. Therefore, methods for ensuring high data reliability and quality must be implemented. The methods for enhancing data quality and reliability are described below:

- *Error detection and correction*: Techniques like cyclic redundancy check (CRC) and forward error correction (FEC) are used to detect and correct errors in transmitted data [244]. This ensures that data is delivered without loss or corruption, improving the reliability of the communication system.
- *Reputation-based mechanisms*: Reputation-based systems help ensure the reliability of data by assigning trust values to vehicles based on their past behavior [245]. If a vehicle is found to be transmitting faulty or malicious data, its reputation is degraded, encouraging honest data reporting and improving overall data quality.

7. Research gaps and future research directions

Vehicular sensor networks have been shown to be pivotal in enabling intelligent transportation systems, providing real-time communication between vehicles, infrastructure, and other entities to enhance road safety, traffic management, and environmental monitoring. However, VSNs face significant challenges related to security, privacy, scalability, and performance, especially as the number of connected vehicles continues to increase [246], [247]. Despite the progress made in securing VSNs, numerous research gaps remain, which require further exploration to ensure the robustness, reliability, and trustworthiness of these systems. This section outlines the key research gaps and future directions in enhancing the security of VSNs. Table 2 gives a summary of these research gaps and future research directions.

7.1. Scalability and resource constraints

One of the most critical challenges in VSN security is ensuring that security mechanisms are scalable to accommodate large and dynamic networks while operating efficiently on resource-constrained devices [248]. As the number of vehicles and roadside units (RSUs) grows, security protocols that are effective in small-scale networks may no longer be feasible in large-scale settings. Furthermore, vehicles and RSUs often have limited processing power, storage, and energy resources, which makes the implementation of security mechanisms such as encryption, authentication, and intrusion detection more difficult.

7.2. Privacy preservation and anonymity

Privacy and anonymity are critical concerns in VSNs, as vehicles constantly generate and exchange sensitive information such as location, speed, and route [249]. If compromised, this information can lead to privacy violations and pose risks

such as vehicle tracking and identity theft. Traditional authentication methods often trade off privacy for security, as they require vehicles to reveal their identities.

7.3. Resilience against insider attacks

Insider attacks are particularly dangerous in VSNs, as they involve legitimate entities within the network (e.g., vehicles or RSUs) that turn malicious. These attacks are difficult to detect because the malicious nodes are authorized to participate in the network [250]. Insider attacks can range from malicious data injection, route manipulation, selective forwarding, and unauthorized data access.

7.4. DoS and jamming attacks

DoS and jamming attacks are among the most common threats in VSNs. Malicious attackers can overwhelm the network with excessive traffic or intentionally jam communication channels, disrupting critical communications between vehicles and infrastructure [251. While traditional DoS mitigation strategies such as traffic filtering and rate-limiting can be effective, they may not always be sufficient to deal with sophisticated jamming attacks or coordinated DoS attacks that target specific network nodes.

7.5. Advanced Intrusion Detection Systems (IDS)

Intrusion detection systems are vital for identifying malicious activities within the network, but the existing IDS solutions for VSNs are often limited by the resource constraints of the devices and the dynamic nature of the network [252]. In traditional IDS models, a central server monitors traffic and behavior across the network, but in VSNs, this approach is difficult due to the lack of centralized control and the mobility of the nodes.

7.6. Secure data aggregation and sharing

VSNs rely on the collection and sharing of data from multiple sources, including vehicles, RSUs, and sensors. While this data is essential for applications such as traffic monitoring, hazard detection, and environmental surveillance, ensuring the security and privacy of this data [253] during aggregation and sharing is a challenge. Malicious nodes may attempt to inject false or corrupted data, leading to incorrect analysis or decisions.

7.7. Cross-layer security mechanisms

Cross-layer security mechanisms that span multiple layers of the VSN protocol stack (such as the physical layer, data link layer, and application layer) offer a promising approach for enhancing security in a holistic manner. Many existing security techniques are applied in isolation at individual layers, but they do not always work seamlessly together to address threats across the entire network [254].

7.8. Blockchain for VSN security

Blockchain technology has garnered significant attention for its potential in enhancing security and trust in decentralized networks [255]. The use of blockchain can provide tamper-proof logging of transactions, decentralized trust management, and secure communication, making it a promising candidate for securing VSNs.

Table 2 Research gaps and future research directions

Gap	Description
Scalability and resource constraints	*Research gap*: There is a need for lightweight, scalable, and efficient security solutions that can handle the large-scale, distributed nature of VSNs without imposing significant computational or energy overheads [256]. Many existing solutions do not scale well, and current cryptographic algorithms and protocols often require high computational costs, which are unsuitable for resource-constrained devices. *Future research directions*: Future research should focus on the development of lightweight cryptographic algorithms and security protocols specifically designed for large-scale VSNs. Research into energy-efficient cryptographic techniques, adaptive security models that can scale with the network size, and decentralized trust management systems would also be beneficial. Additionally, optimizing IDS mechanisms for scalability, such as distributed IDS or cloud-based IDS, can help improve detection capabilities in large networks.

Privacy preservation and anonymity	*Research gap*: While pseudonym-based approaches and anonymization techniques are used to protect user privacy, these methods often introduce trade-offs between security and privacy [257], [258]. Moreover, the frequent renewal of pseudonyms, as required by privacy-preserving protocols, may result in challenges for accountability and liability in case of malicious activities. *Future research directions*: There is a need for innovative privacy-preserving techniques that allow vehicles to maintain anonymity without compromising security or accountability. Research into zero-knowledge proofs for authentication, secure multi-party computation (SMC) protocols, and differential privacy can help achieve this balance. Furthermore, decentralized privacy-preserving schemes that do not rely on centralized trust authorities should be explored to enhance privacy while maintaining system resilience.
Resilience against insider attacks	*Research gap*: Existing intrusion detection and prevention systems (IDS/IPS) are often ineffective at detecting insider attacks [259], as they typically rely on external behaviors that may not be apparent when the attack comes from within the system. Current trust management models may also fail to identify malicious behavior if the attacker has previously established a good reputation within the network. *Future research directions*: Future research should focus on developing more robust trust management frameworks and anomaly detection techniques that can identify abnormal behavior originating from insider nodes. This includes behavior-based anomaly detection, collaborative trust models, and machine learning approaches that can identify patterns of insider threats. Furthermore, research into dynamic and evolving reputation systems, which can adapt to new attack strategies, is needed to mitigate the risk of insider attacks.
DoS and jamming attacks	*Research gap*: Existing DoS mitigation techniques are often ineffective against advanced jamming methods or distributed DoS (DDoS) attacks [260]. Many methods are reactive rather than proactive, making it difficult to predict and prevent such attacks before they occur. *Future research directions*: Research should focus on developing proactive defense mechanisms that can predict and prevent jamming or DoS attacks in real-time. Techniques such as frequency hopping, spatial diversity, and physical-layer security methods (e.g., using multiple antennas or cognitive radio techniques) can be investigated for their potential to mitigate jamming attacks. Additionally, distributed and collaborative DoS detection methods involving cooperation between vehicles and RSUs should be explored to better mitigate DDoS attacks.
IDS	*Research gap*: Current IDS systems in VSNs are often either too resource-intensive or lack the capability to detect new and sophisticated attack patterns [261]. Additionally, centralized IDS approaches do not scale well in highly dynamic networks with varying node mobility. *Future research directions*: Future research should focus on developing lightweight, decentralized IDS that can operate efficiently in VSNs. The integration of machine learning and artificial intelligence (AI) into IDS can significantly improve the detection of unknown or novel attack patterns. Machine learning-based approaches, such as deep learning, can be used to detect anomalies and predict potential security threats based on historical data. Moreover, collaborative IDS systems, where vehicles and infrastructure share intrusion-related information, can enhance detection accuracy and reduce false positives.
Secure data aggregation and sharing	*Research gap*: Existing data aggregation and sharing protocols do not fully address the risks of data manipulation and false data injection attacks [262], which can degrade the reliability of VSNs. Additionally, the aggregation of data from multiple sources while preserving privacy is not fully explored. *Future research directions*: Future work should focus on secure data aggregation techniques that prevent data tampering and ensure data integrity. Cryptographic methods like homomorphic encryption, which allows computations to be performed on encrypted data without revealing its content, can be used for privacy-preserving [263] data aggregation. Additionally, trust-based data fusion models and secure multi-party computation (SMC) techniques can be employed to ensure the reliability and confidentiality of aggregated data.
Cross-layer security mechanisms	*Research gap*: There is limited research on cross-layer security mechanisms in VSNs that can coordinate security functions at multiple layers to provide end-to-end protection [264], [265]. These mechanisms can provide more comprehensive defense strategies, but designing them in a way that is efficient and non-intrusive remains a challenge.

	Future research directions: Future research should focus on the design of integrated cross-layer security frameworks that coordinate the activities of different layers, such as cryptographic key management, secure routing, and IDS, to provide a more effective and unified defense against attacks. These frameworks should balance security with efficiency, especially in resource-constrained environments.
Blockchain for VSN security	*Research gap*: Blockchain-based solutions for VSNs are still in the early stages of research. Challenges remain in adapting blockchain to the high mobility and dynamic topology of VSNs, as well as ensuring scalability, latency, and energy efficiency [266]-[270]. *Future research directions*: Future research should focus on developing blockchain-based solutions for secure communication, decentralized authentication, and tamper-proof data sharing in VSNs. Research into lightweight blockchain protocols, such as permissioned blockchains, is needed to optimize these solutions for resource-constrained vehicles and RSUs. Furthermore, the integration of blockchain with other technologies, such as edge computing or fog computing, can enhance scalability and performance.

While substantial progress has been made in securing Vehicular Sensor Networks (VSNs), significant research gaps remain. Addressing challenges such as scalability, privacy, insider attacks, DoS mitigation, and cross-layer security will be crucial for the continued success of VSNs in real-world applications. The integration of emerging technologies like machine learning, blockchain, and edge computing holds great potential in enhancing the security, efficiency, and scalability of VSNs. As the field continues to evolve, interdisciplinary research that combines aspects of cryptography, network design, data privacy, and trust management will be essential to ensuring the robustness and resilience of VSNs in the face of emerging threats and demands.

8. Conclusion

Vehicular Sensor Networks (VSNs) are critical components of modern intelligent transportation systems, enabling real-time data exchange between vehicles, infrastructure, and other entities to improve road safety, traffic efficiency, and environmental monitoring. However, the decentralized, dynamic, and resource-constrained nature of VSNs exposes them to numerous security and performance challenges. In this review, key security issues faced by VSNs, including data confidentiality, privacy, integrity, authentication, and threats from malicious attacks such as DoS, Sybil, and insider attacks have been highlighted. This paper has also explored various techniques and methods for enhancing the security of VSNs, ranging from cryptographic solutions, intrusion detection systems, and secure routing protocols to privacy-preserving techniques, trust management, and authentication mechanisms. Moreover, performance enhancements in VSNs, such as scalability, energy efficiency, and real-time communication, are critical for maintaining the operational efficiency of the network as it grows and evolves. To this end, lightweight cryptographic methods, efficient routing protocols, and the development of adaptive security mechanisms have been identified as essential areas for further improvement. While significant progress has been made in both security and performance optimization, several research gaps persist, particularly in developing scalable, privacy-preserving, and resource-efficient solutions that can accommodate the increasing number of vehicles and infrastructure in VSNs. The future of VSNs lies in addressing these gaps through innovative and interdisciplinary approaches that integrate emerging technologies such as machine learning, blockchain, edge computing, and advanced cryptography. By focusing on improving the resilience of VSNs to security threats and enhancing their performance without compromising resource constraints, the next generation of VSNs can provide secure, reliable, and efficient communication for intelligent transportation systems.

References

[1] Hira S, Hira S. Smart energy management using vehicle-to-vehicle and vehicle-to-everything. InArtificial Intelligence-Empowered Modern Electric Vehicles in Smart Grid Systems 2024 Jan 1 (pp. 253-290). Elsevier.

[2] Gebali F, Elhadad MK. PUFGuard: Vehicle-to-Everything Authentication Protocol for Secure Multihop Mobile Communication. Computers. 2023 Nov 14;12(11):233.

[3] Prakash J, Murali L, Manikandan N, Nagaprasad N, Ramaswamy K. A vehicular network based intelligent transport system for smart cities using machine learning algorithms. Scientific reports. 2024;14.

[4] Zaheer T, Malik AW, Rahman AU, Zahir A, Fraz MM. A vehicular network–based intelligent transport system for smart cities. International Journal of Distributed Sensor Networks. 2019 Nov;15(11):1550147719888845.

[5] Rahman MA, Rahim MA, Rahman MM, Moustafa N, Razzak I, Ahmad T, Patwary MN. A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics. IEEE Transactions on Intelligent Transportation Systems. 2022 Jan 4;23(10):19727-42.

[6] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[7] Sheikh MS, Liang J, Wang W. A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets). Sensors. 2019 Aug 17;19(16):3589.

[8] Hamdare S, Kaiwartya O, Aljaidi M, Jugran M, Cao Y, Kumar S, Mahmud M, Brown D, Lloret J. Cybersecurity risk analysis of electric vehicles charging stations. Sensors. 2023 Jul 27;23(15):6716.

[9] Desai B, Patil K, Mehta I, Patil A. A Secure Communication Framework for Smart City Infrastructure Leveraging Encryption, Intrusion Detection, and Blockchain Technology. Advances in Computer Sciences. 2024 Jan 9;7(1).

[10] Sharma M. Enhancing Security and Privacy in Cyber-Physical Systems: Challenges and Solutions. In2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC) 2024 Jan 8 (pp. 0682-0686). IEEE.

[11] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[12] Teixeira PV, Raposo D, Lopes R, Sargento S. Software Defined Vehicles for Development of Deterministic Services. arXiv preprint arXiv:2407.17287. 2024 Jul 24.

[13] Alevizos L, Ta VT, Eiza MH. A novel efficient dynamic throttling strategy for blockchain-based intrusion detection systems in 6G-enabled VSNs. Sensors. 2023 Sep 21;23(18):8006.

[14] Abdulqader AF, Salih MM, Shaker NH, Sajid WA, Qasem W, Gajewska A, Khlaponin D. Optimizing IoT Performance Through Edge Computing: Reducing Latency, Enhancing Bandwidth Efficiency, and Strengthening Security for 2025 Applications. In2024 36th Conference of Open Innovations Association (FRUCT) 2024 Oct 30 (pp. 145-158). IEEE.

[15] Umoga UJ, Sodiya EO, Ugwuanyi ED, Jacks BS, Lottu OA, Daraojimba OD, Obaigbena A. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. Magna Scientia Advanced Research and Reviews. 2024;10(1):368-78.

[16] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[17] Mathur A, Barati M, Aujla GS, Rana O. Towards Scalable and Secure Blockchain in Internet of Things: A Preference-Driven Committee Member Auction Consensus Approach. Distributed Ledger Technologies: Research and Practice. 2024 Oct 16.

[18] Cheng X, Duan D, Gao S, Yang L. Integrated sensing and communications (ISAC) for vehicular communication networks (VCN). IEEE Internet of Things Journal. 2022 Jul 15;9(23):23441-51.

[19] Guo H, Zhou X, Liu J, Zhang Y. Vehicular intelligence in 6G: Networking, communications, and computing. Vehicular Communications. 2022 Jan 1;33:100399.

[20] Ameen HA, Mahamad AK, Saon S, Malik RQ, Kareem ZH, Bin Ahmadon MA, Yamaguchi S. Identification of driving safety profiles in vehicle to vehicle communication system based on vehicle OBD information. Information. 2021 Apr 29;12(5):194.

[21] Nyangaresi VO, Ghaib AA, Jasim HM, Abduljabbar ZA, Ma J, Al Sibahee MA, Aldarwish AJ, Ali AH, Neamah HA. Message Verification Protocol Based on Bilinear Pairings and Elliptic Curves for Enhanced Security in Vehicular Ad Hoc Networks. Computers, Materials and Continua. 2024 Oct 1;81(1):1029-57.

[22] Jooriah M, Datsenko D, Almeida J, Sousa A, Silva J, Ferreira J. A Co-Simulation Platform for V2X-Based Cooperative Driving Automation Systems. In2024 IEEE Vehicular Networking Conference (VNC) 2024 May 29 (pp. 227-230). IEEE.

[23] Arin J, Velez G, Bustamante P. A C-ITS Architecture for MEC and Cloud Native Back-end Services. IEEE Access. 2024 May 6.

[24] Ajaz F, Naseem M, Shabaz M, Khan MA. An architectural view of VANETs cloud: Its models, services, applications and challenges. International Journal of Web and Grid Services. 2024;20(3):292-341.

[25] Sharma A, Tokekar S, Varma S. A Comprehensive Survey on Network Resource Management in SDN Enabled Data Centre Network. 6G Enabled Fog Computing in IoT: Applications and Opportunities. 2023 Oct 2:333-53.

[26] Jawad M, Yassin AA, Al-Asadi HA, Abduljabbar ZA, Nyangaresi VO. IoHT System Authentication Through the Blockchain Technology: A Review. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2253-2258). IEEE

[27] 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.

[28] Zhou X, Ke R, Yang H, Liu C. When intelligent transportation systems sensing meets edge computing: Vision and challenges. Applied Sciences. 2021 Oct 17;11(20):9680.

[29] AbdlNabi MA, Hamza BJ, Abdulsadda AT. 6G optical-RF wireless integration: a review on heterogeneous cellular network channel modeling, measurements, and challenges. Telecommunication Systems. 2024 Sep 30:1-44.

[30] Clancy J, Mullins D, Deegan B, Horgan J, Ward E, Eising C, Denny P, Jones E, Glavin M. Wireless Access for V2X Communications: Research, Challenges and Opportunities. IEEE Communications Surveys & Tutorials. 2024 Apr 1.

[31] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[32] Venčkauskas A, Taparauskas M, Grigaliūnas Š, Brūzgienė R. Enhancing Communication Security an In-Vehicle Wireless Sensor Network. Electronics. 2024 Mar 7;13(6):1003.

[33] Muslam MM. Enhancing security in vehicle-to-vehicle communication: a comprehensive review of protocols and techniques. Vehicles. 2024 Feb 27;6(1):450-67.

[34] Alharb M, Alabdulatif A. Intelligent Transport Systems: Analysis of Applications, Security Challenges, and Robust Countermeasures. International Journal of Advanced Computer Science & Applications. 2024 Jun 1;15(6).

[35] Tu YJ, Piramuthu S. Security and privacy risks in drone-based last mile delivery. European Journal of Information Systems. 2024 Sep 2;33(5):617-30.

[36] Alshuraify A, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Blockchain-based Authentication Scheme in Oil and Gas Industry Data with Thermal CCTV Cameras Applications to Mitigate Sybil and 51% Cyber Attacks. International Journal of Intelligent Engineering & Systems. 2024 Nov 1;17(6).

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

[38] Ahmed MR, Islam AM, Shatabda S, Islam S. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access. 2022 Oct 25;10:113436-81.

[39] George SA, Jaekel A, Saini I. Secure identity management framework for vehicular ad-hoc network using blockchain. In2020 IEEE Symposium on Computers and Communications (ISCC) 2020 Jul 7 (pp. 1-6). IEEE.

[40] Mishra M, Reddy SR. Performance assessment and comparison of lightweight d2d-iot communication protocols over resource constraint environment. Multimedia Tools and Applications. 2024 Jan 26:1-30.

[41] 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.

[42] Sampaio S, Sousa PR, Martins C, Ferreira A, Antunes L, Cruz-Correia R. Collecting, processing and secondary using personal and (pseudo) anonymized data in smart cities. Applied Sciences. 2023 Mar 16;13(6):3830.

[43] Bagga P, Das AK, Wazid M, Rodrigues JJ, Park Y. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. Ieee Access. 2020 Mar 17;8:54314-44.

[44] Jiang K, Zhou H, Chen X, Zhang H. Mobile edge computing for ultra-reliable and low-latency communications. IEEE Communications Standards Magazine. 2021 Apr 23;5(2):68-75.

[45] Sheikh MS, Liang J, Wang W. Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey. Wireless Communications and Mobile Computing. 2020;2020(1):5129620.

[46] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).

[47] Hazra R, Chatterjee P, Singh Y, Podder G, Das T. Data Encryption and Secure Communication Protocols. InStrategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning 2024 (pp. 546-570). IGI Global.

[48] Yang Y, Yin Z. Resilient supply chains to improve the integrity of accounting data in financial institutions worldwide using blockchain technology. International Journal of Data Warehousing and Mining (IJDWM). 2023 Apr 1;19(4):1-20.

[49] Mundhe P, Verma S, Venkatesan SJ. A comprehensive survey on authentication and privacy-preserving schemes in VANETs. Computer Science Review. 2021 Aug 1;41:100411.

[50] Hasan O, Brunie L, Bertino E. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. ACM Computing Surveys (CSUR). 2022 Jan 18;55(2):1-37.

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

[52] Jagannath RO, Jain AK. Browser-in-the-middle attacks: A comprehensive analysis and countermeasures. Security and Privacy. 2024 Sep;7(5):e410.

[53] Rizvi S, Orr RJ, Cox A, Ashokkumar P, Rizvi MR. Identifying the attack surface for IoT network. Internet of Things. 2020 Mar 1;9:100162.

[54] Alam T. Data privacy and security in autonomous connected vehicles in smart city environment. Big Data and Cognitive Computing. 2024 Aug 23;8(9):95.

[55] Shah MS, Leau YB, Anbar M, Bin-Salem AA. Security and integrity attacks in named data networking: a survey. IEEE Access. 2023 Jan 23;11:7984-8004.

[56] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[57] 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.

[58] Shukla PK, Aljaedi A, Pareek PK, Alharbi AR, Jamal SS. AES based white box cryptography in digital signature verification. Sensors. 2022 Dec 2;22(23):9444.

[59] Wang H, Zhang J. Blockchain based data integrity verification for large-scale IoT data. IEEE Access. 2019 Nov 11;7:164996-5006.

[60] Karopoulos G, Kambourakis G, Chatzoglou E, Hernández-Ramos JL, Kouliaridis V. Demystifying in-vehicle intrusion detection systems: A survey of surveys and a meta-taxonomy. Electronics. 2022 Mar 29;11(7):1072.

[61] 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.

[62] Furqan HM, Solaija MS, Türkmen H, Arslan H. Wireless communication, sensing, and REM: A security perspective. IEEE Open Journal of the Communications Society. 2021 Jan 26;2:287-321.

[63] Kim S, Shrestha R, Kim S, Shrestha R. Internet of vehicles, vehicular social networks, and cybersecurity. Automotive cyber security: introduction, challenges, and standardization. 2020:149-81.

[64] Dibaei M, Zheng X, Jiang K, Abbas R, Liu S, Zhang Y, Xiang Y, Yu S. Attacks and defences on intelligent connected vehicles: A survey. Digital Communications and Networks. 2020 Nov 1;6(4):399-421.

[65] Morato A, Zunino C, Cheminod M, Vitturi S, Tramarin F. A TSN-based Technique for Real-Time Latency Evaluation in Communication Networks. In2024 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) 2024 May 20 (pp. 1-6). IEEE.

[66] Bukhowah R, Aljughaiman A, Rahman MH. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. Electronics. 2024 Mar 9;13(6):1031.

[67] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[68] Sharma S, Singh P, Kumar A. Fake Profile Detection on Social Networks—A Survey. InThe International Conference on Recent Innovations in Computing 2024 (pp. 403-416). Springer, Singapore.

[69] Stępień K, Poniszewska-Marańda A. Security measures with enhanced behavior processing and footprint algorithm against sybil and bogus attacks in vehicular Ad Hoc network. Sensors. 2021 May 19;21(10):3538.

[70] Nikitas A, Parkinson S, Vallati M. The deceitful connected and autonomous vehicle: defining the concept, contextualising its dimensions and proposing mitigation policies. Transport policy. 2022 Jun 1;122:1-0.

[71] Wang X, Ning Z, Zhou M, Hu X, Wang L, Zhang Y, Yu FR, Hu B. Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions. IEEE Communications Surveys & Tutorials. 2018 Nov 18;21(2):1314-45.

[72] Jethava G, Rao UP. Exploring security and trust mechanisms in online social networks: An extensive review. Computers & Security. 2024 Feb 28:103790.

[73] 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.

[74] Hemkumar D. Preserving location privacy against inference attacks in indoor positioning system. Peer-to-Peer Networking and Applications. 2024 Mar;17(2):784-99.

[75] Pettorru G, Pilloni V, Martalò M. Trustworthy Localization in IoT Networks: A Survey of Localization Techniques, Threats, and Mitigation. Sensors. 2024 Mar 29;24(7):2214.

[76] Usama M, Ullah U, Sajid A. Cyber Attacks Against Intelligent Transportation Systems. InCyber Security for Next-Generation Computing Technologies 2024 (pp. 190-230). CRC Press.

[77] Kumar R, Agrawal N. A survey on software-defined vehicular networks (SDVNs): a security perspective. The Journal of Supercomputing. 2023 May;79(8):8368-400.

[78] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[79] Al-Turjman F, Lemayian JP. Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. Computers & Electrical Engineering. 2020 Oct 1;87:106776.

[80] Khan SZ, Mohsin M, Iqbal W. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. PeerJ Computer Science. 2021 May 6;7:e507.

[81] Elkhail AA, Refat RU, Habre R, Hafeez A, Bacha A, Malik H. Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses. IEEE Access. 2021 Nov 23;9:162401-37.

[82] Zeddini B, Maachaoui M, Inedjaren Y. Security threats in intelligent transportation systems and their risk levels. Risks. 2022 Apr 21;10(5):91.

[83] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[84] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[85] Novković B, Golub M. Improving monolithic kernel security and robustness through intra-kernel sandboxing. Computers & security. 2023 Apr 1;127:103104.

[86] Sadaf M, Iqbal Z, Javed AR, Saba I, Krichen M, Majeed S, Raza A. Connected and automated vehicles: Infrastructure, applications, security, critical challenges, and future aspects. Technologies. 2023 Sep 4;11(5):117.

[87] Kim K, Kim JS, Jeong S, Park JH, Kim HK. Cybersecurity for autonomous vehicles: Review of attacks and defense. Computers & security. 2021 Apr 1;103:102150.

[88] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[89] Sun J, Xiong H, Zhang S, Liu X, Yuan J, Deng RH. A secure flexible and tampering-resistant data sharing system for vehicular social networks. IEEE Transactions on Vehicular Technology. 2020 Aug 11;69(11):12938-50.

[90] He Y, Zhou Z, Pan Y, Chong F, Wu B, Xiao K, Li H. Review of data security within energy blockchain: A comprehensive analysis of storage, management, and utilization. High-Confidence Computing. 2024 Apr 24:100233.

[91] Mohammed BA, Al-Shareeda MA, Alsadhan AA, Al-Mekhlafi ZG, Sallam AA, Al-Qatab BA, Alshammari MT, Alayba AM. Service based VEINS framework for vehicular Ad-hoc network (VANET): A systematic review of state-of-the-art. Peer-to-Peer Networking and Applications. 2024 May 3:1-23.

[92] Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023 Apr 19;23(8):4117.

[93] 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.

[94] El-Rewini Z, Sadatsharan K, Sugunaraj N, Selvaraj DF, Plathottam SJ, Ranganathan P. Cybersecurity attacks in vehicular sensors. IEEE Sensors Journal. 2020 Jun 22;20(22):13752-67.

[95] Dewangan KK, Panda V, Ojha S, Shahapure A, Jahagirdar SR. Cyber Threats and Its Mitigation to Intelligent Transportation System. SAE Technical Paper; 2024 Jan 16.

[96] Fakhfakh F, Tounsi M, Mosbah M. Cybersecurity attacks on CAN bus based vehicles: a review and open challenges. Library hi tech. 2022 Nov 22;40(5):1179-203.

[97] Altaf I, Kaul A. Vulnerable road user safety: A systematic review and mesh-networking based vehicle ad hoc system using hybrid of neuro-fuzzy and genetic algorithms. International Journal of Communication Systems. 2021 Sep 10;34(13):e4907.

[98] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781

[99] Chowdhury A, Karmakar G, Kamruzzaman J, Jolfaei A, Das R. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access. 2020 Nov 12;8:207308-42.

[100] 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.

[101] Liu L, De Vel O, Han QL, Zhang J, Xiang Y. Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys & Tutorials. 2018 Feb 1;20(2):1397-417.

[102] Ullah F, Edwards M, Ramdhany R, Chitchyan R, Babar MA, Rashid A. Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and Computer Applications. 2018 Jan 1;101:18-54.

[103] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[104] Khan N, J. Houghton R, Sharples S. Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. Cognition, Technology & Work. 2022 Aug;24(3):393-421.

[105] Silva R, Iqbal R. Ethical implications of social internet of vehicles systems. IEEE Internet of Things Journal. 2018 May 29;6(1):517-31.

[106] Adelantado F, Ammouriova M, Herrera E, Juan AA, Shinde SS, Tarchi D. Internet of Vehicles and real-time optimization algorithms: Concepts for vehicle networking in smart cities. vehicles. 2022 Nov 3;4(4):1223-45.

[107] Muratori M, Alexander M, Arent D, Bazilian M, Cazzola P, Dede EM, Farrell J, Gearhart C, Greene D, Jenn A, Keyser M. The rise of electric vehicles—2020 status and future expectations. Progress in Energy. 2021 Mar 25;3(2):022002.

[108] 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).

[109] Zekri A, Jia W. Heterogeneous vehicular communications: A comprehensive study. Ad Hoc Networks. 2018 Jun 1;75:52-79.

[110] Chekired DA, Togou MA, Khoukhi L. Hierarchical wireless vehicular fog architecture: A case study of scheduling electric vehicle energy demands. ieee vehicular technology magazine. 2018 Sep 18;13(4):116-26.

[111] Hildebrand B, Baza M, Salman T, Tabassum S, Konatham B, Amsaad F, Razaque A. A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions. Computer Science Review. 2023 May 1;48:100547.

[112] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[113] Hussain R, Lee J, Zeadally S. Trust in VANET: A survey of current solutions and future research opportunities. IEEE transactions on intelligent transportation systems. 2020 Mar 5;22(5):2553-71.

[114] 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.

[115] Alam S, Zardari S, Noor S, Ahmed S, Mouratidis H. Trust management in social internet of things (SIoT): a survey. IEEE Access. 2022 Oct 13;10:108924-54.

[116] Che H, Duan Y, Li C, Yu L. On trust management in vehicular ad hoc networks: A comprehensive review. Frontiers in the Internet of Things. 2022 Oct 31;1:995233.

[117] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[118] Rishiwal V, Agarwal U, Alotaibi A, Tanwar S, Yadav P, Yadav M. Exploring Secure V2X Communication Networks for Human-centric Security and Privacy in Smart Cities. IEEE Access. 2024 Sep 24.

[119] Khattak KS, Khan ZH. Evaluation and Challenges of IoT Simulators for Intelligent Transportation System Applications. Science, Engineering and Technology. 2024;4(1):94-111.

[120] Ahmed ZE, Hashim AA, Saeed RA, Saeed MM. Enhancing Smart City Mobility Using Software Defined Networks. In2024 9th International Conference on Mechatronics Engineering (ICOM) 2024 Aug 13 (pp. 299-303). IEEE.

[121] Dhanasekaran S, Ramalingam S, Baskaran K, Vivek Karthick P. Efficient distance and connectivity based traffic density stable routing protocol for vehicular Ad Hoc networks. IETE Journal of Research. 2024 Feb 1;70(2):1150-66.

[122] 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.

[123] Palladino A. Sharing, data and smart mobility: Towards innovative urban paradigms. Key Editore; 2024 Sep 15.

[124] Wang M, Mao J, Zhao W, Han X, Li M, Liao C, Sun H, Wang K. Smart City Transportation: A VANET Edge Computing Model to Minimize Latency and Delay Utilizing 5G Network. Journal of Grid Computing. 2024 Mar;22(1):25.

[125] Surutkar R, Jadhav C. VANET for Autonomous Vehicles. In2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS) 2024 Feb 24 (pp. 1-7). IEEE.

[126] Elassy M, Al-Hattab M, Takruri M, Badawi S. Intelligent transportation systems for sustainable smart cities. Transportation Engineering. 2024 Apr 14:100252.

[127] 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).

[128] 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.

[129] Sharma S, Kaul A, Ahmed S, Sharma S. A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions. International Journal of Communication Systems. 2021 Sep 25;34(14):e4905.

[130] Agbaje P, Anjum A, Mitra A, Oseghale E, Bloom G, Olufowobi H. Survey of interoperability challenges in the internet of vehicles. IEEE Transactions on Intelligent Transportation Systems. 2022 Aug 9;23(12):22838-61.

[131] Biswas A, Wang HC. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. Sensors. 2023 Feb 9;23(4):1963.

[132] 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.

[133] Hasan N, Aziz AA, Mahmud A, Alias YB, Besar RB, Hakim L, Bin Hamidi MA. Vehicle Sensing and Localization in Vehicular Networks. International Journal of Technology. 2024 Mar 1;15(3).

[134] Obi OC, Dawodu SO, Daraojimba AI, Onwusinkwue S, Akagha OV, Ahmad IA. Review of evolving cloud computing paradigms: security, efficiency, and innovations. Computer Science & IT Research Journal. 2024 Feb 2;5(2):270-92.

[135] Hussain MZ, Hanapi ZM. Efficient secure routing mechanisms for the low-powered IoT network: A literature review. Electronics. 2023 Jan 17;12(3):482.

[136] Aldin HN, Ghods MR, Nayebipour F, Torshiz MN. A comprehensive review of energy harvesting and routing strategies for IoT sensors sustainability and communication technology. Sensors International. 2023 Nov 27:100258.

[137] Khan SU, Khan ZU, Alkhowaiter M, Khan J, Ullah S. Energy-efficient routing protocols for UWSNs: A comprehensive review of taxonomy, challenges, opportunities, future research directions, and machine learning perspectives. Journal of King Saud University-Computer and Information Sciences. 2024 Jul 23:102128.

[138] Zhang Y, Zhao R, Mishra D, Ng DW. A Comprehensive Review of Energy-Efficient Techniques for UAV-Assisted Industrial Wireless Networks. Energies. 2024 Sep 23;17(18):4737.

[139] Nyangaresi VO, Abduljabbar ZA, Mutlaq KA, Bulbul SS, Ma J, Aldarwish AJ, Honi DG, Al Sibahee MA, Neamah HA. Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme. Scientific Reports. 2024 Jul 13;14(1):16223.

[140] Siddiqui MU, Qamar F, Ahmed F, Nguyen QN, Hassan R. Interference management in 5G and beyond network: Requirements, challenges and future directions. IEEE Access. 2021 Apr 15;9:68932-65.

[141] Wang J, Liu J, Kato N. Networking and communications in autonomous driving: A survey. IEEE Communications Surveys & Tutorials. 2018 Dec 20;21(2):1243-74.

[142] Ma Z, Xiao M, Xiao Y, Pang Z, Poor HV, Vucetic B. High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. IEEE Internet of Things Journal. 2019 Mar 25;6(5):7946-70.

[143] Ma Z, Xiao M, Xiao Y, Pang Z, Poor HV, Vucetic B. High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. IEEE Internet of Things Journal. 2019 Mar 25;6(5):7946-70.

[144] 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.

[145] Khan AA, Siddiqui S, Siddiqui MS. Delay management for heterogeneous traffic in vehicular sensor networks using packet fragmentation of low priority data. IET Communications. 2024.

[146] Moldovan C, Ulrich S, Köster V, Tiemann J, Lewandowski A. Advancing digital twin-based collision avoidance: a comprehensive analysis of Communication Networks for Safety-Critical Applications in Industry 4.0. Sensors. 2024 Feb 22;24(5):1405.

[147] Lim H. Toward Infotainment Services in Vehicular Named Data Networking: A Comprehensive Framework Design and Its Realization. IEEE Transactions on Intelligent Transportation Systems. 2024 Nov 13.

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

[149] 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.

[150] Mutar MS, Hamza ZA, Hammood DA, Hashem SA. A survey of sleep scheduling techniques in wireless sensor networks for maximizing energy efficiency. InAIP Conference Proceedings 2024 Oct 11 (Vol. 3232, No. 1). AIP Publishing.

[151] Dhabliya D, Soundararajan R, Selvarasu P, Balasubramaniam MS, Rajawat AS, Goyal SB, Raboaca MS, Mihaltan TC, Verma C, Suciu G. Energy-efficient network protocols and resilient data transmission schemes for wireless sensor Networks—An experimental survey. Energies. 2022 Nov 24;15(23):8883.

[152] Khan MN, Rahman HU, Almaiah MA, Khan MZ, Khan A, Raza M, Al-Zahrani M, Almomani O, Khan R. Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks. Ieee Access. 2020 Sep 25;8:176495-520.

[153] Maheswar R, Kathirvelu M, Mohanasundaram K. Energy Efficiency in Wireless Networks. Energies. 2024 Jan 15;17(2):417.

[154] 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).

[155] Mahi MJ, Chaki S, Ahmed S, Biswas M, Kaiser MS, Islam MS, Sookhak M, Barros A, Whaiduzzaman M. A review on VANET research: Perspective of recent emerging technologies. IEEE Access. 2022 Jun 16;10:65760-83.

[156] Rana B, Singh Y, Singh PK. A systematic survey on internet of things: Energy efficiency and interoperability perspective. Transactions on Emerging Telecommunications Technologies. 2021 Aug;32(8):e4166.

[157] Javed A, Malhi A, Kinnunen T, Främling K. Scalable IoT platform for heterogeneous devices in smart environments. IEEe Access. 2020 Nov 19;8:211973-85.

[158] Van Der Heijden RW, Dietzel S, Leinmüller T, Kargl F. Survey on misbehavior detection in cooperative intelligent transportation systems. IEEE Communications Surveys & Tutorials. 2018 Sep 30;21(1):779-811.

[159] 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.

[160] Kuru K, Khan W. A framework for the synergistic integration of fully autonomous ground vehicles with smart city. IEEE Access. 2020 Dec 23;9:923-48.

[161] Bakirci M. Enhancing vehicle detection in intelligent transportation systems via autonomous UAV platform and YOLOv8 integration. Applied Soft Computing. 2024 Oct 1;164:112015.

[162] Guerrero-Ibáñez J, Zeadally S, Contreras-Castillo J. Sensor technologies for intelligent transportation systems. Sensors. 2018 Apr 16;18(4):1212.

[163] Wang Z, Wang S, Bhuiyan MZ, Xu J, Hu Y. Cooperative location-sensing network based on vehicular communication security against attacks. IEEE Transactions on Intelligent Transportation Systems. 2022 Mar 28;24(1):942-52.

[164] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[165] El-Dalahmeh A, El-Dalahmeh M, Razzaque MA, Li J. Cryptographic methods for secured communication in SDN-based VANETs: A performance analysis. Security and Privacy. 2024:e446.

[166] Tesei A, Lattuca D, Luise M, Pagano P, Ferreira J, Bartolomeu PC. A transparent distributed ledger-based certificate revocation scheme for VANETs. Journal of Network and Computer Applications. 2023 Mar 1;212:103569.

[167] Khashan OA, Ahmad R, Khafajah NM. An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad Hoc Networks. 2021 Apr 15;115:102448.

[168] Amanlou S, Hasan MK, Bakar KA. Lightweight and secure authentication scheme for IoT network based on publish–subscribe fog computing model. Computer Networks. 2021 Nov 9;199:108465.

[169] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[170] Abhishek NV, Aman MN, Lim TJ, Sikdar B. Drive: Detecting malicious roadside units in the internet of vehicles with low latency data integrity. IEEE Internet of Things Journal. 2021 Jul 16;9(5):3270-81.

[171] Alshaeri A, Younis M. Efficient Distributed Authentication for Intelligent Transportation Systems Using Mobile Devices. IEEE Transactions on Intelligent Transportation Systems. 2024 Mar 27.

[172] Banoth R, Regar R. Asymmetric Key Cryptography. InClassical and Modern Cryptography for Beginners 2023 Jun 25 (pp. 109-165). Cham: Springer Nature Switzerland.

[173] BK S, Azam F. Ensuring Security and Privacy in VANET: A Comprehensive Survey of Authentication Approaches. Journal of Computer Networks and Communications. 2024;2024(1):1818079.

[174] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[175] Albouq SS. Certificate Revocation in Connected Vehicles. International journal of computer science and network security: IJCSNS. 2023 May;23(5):13-20.

[176] Khan S, Luo F, Zhang Z, Rahim MA, Khan S, Qadri SF, Wu K. A privacy-preserving and transparent identity management scheme for vehicular social networking. IEEE Transactions on Vehicular Technology. 2022 Jul 18;71(11):11555-70.

[177] 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.

[178] Alharthi A, Ni Q, Jiang R, Khan MA. A computational model for reputation and ensemble-based learning model for prediction of trustworthiness in vehicular ad hoc network. IEEE Internet of Things Journal. 2023 May 25;10(20):18248-58.

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

[180] Borkar GM, Mahajan AR. A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks. International Journal of Communication Networks and Distributed Systems. 2020;24(1):23-57.

[181] Sahoo A, Kumar Tripathy A. On routing algorithms in the internet of vehicles: a survey. Connection Science. 2023 Dec 31;35(1):2272583.

[182] Kumar R, Singh SK, Lobiyal DK, Kumar S, Jawla S. Security Metrics and Authentication-based RouTing (SMART) Protocol for Vehicular IoT Networks. SN Computer Science. 2024 Jan 27;5(2):236.

[183] Khalid NA, Bai Q, Al-Anbuky A. Adaptive trust-based routing protocol for large scale WSNs. IEEE Access. 2019 Sep 30;7:143539-49.

[184] Wang J, Yan Z, Wang H, Li T, Pedrycz W. A survey on trust models in heterogeneous networks. IEEE Communications Surveys & Tutorials. 2022 Jul 21;24(4):2127-62.

[185] 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.

[186] Boulaiche M. Survey of secure routing protocols for wireless ad hoc networks. Wireless Personal Communications. 2020 Sep;114(1):483-517.

[187] Sayyed T, Kodwani S, Dodake K, Adhayage M, Solanki RK, Bhaladhare PR. Intrusion Detection System. Int. J. of Aquatic Science. 2023 Jan 1;14(1):288-98.

[188] Otoum Y, Nayak A. As-ids: Anomaly and signature based ids for the internet of things. Journal of Network and Systems Management. 2021 Jul;29(3):23.

[189] Yang Z, Liu X, Li T, Wu D, Wang J, Zhao Y, Han H. A systematic literature review of methods and datasets for anomaly-based network intrusion detection. Computers & Security. 2022 May 1;116:102675.

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

[191] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[192] Li W, Meng W, Kwok LF. Surveying trust-based collaborative intrusion detection: state-of-the-art, challenges and future directions. IEEE Communications Surveys & Tutorials. 2021 Dec 28;24(1):280-305.

[193] Yoshizawa T, Singelée D, Muehlberg JT, Delbruel S, Taherkordi A, Hughes D, Preneel B. A survey of security and privacy issues in v2x communication systems. ACM Computing Surveys. 2023 Jan 13;55(9):1-36.

[194] Bralić V, Stančić H, Stengård M. A blockchain approach to digital archiving: digital signature certification chain preservation. Records Management Journal. 2020 Dec 4;30(3):345-62.

[195] Katuk N, Nordin N, Habbal A. Digital signature: Enabling trust and security in Industry 5.0 transactions. InThe Future of Human-Computer Integration (pp. 85-96). CRC Press.

[196] 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.

[197] Adeniyi EA, Falola PB, Maashi MS, Aljebreen M, Bharany S. Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. Information. 2022 Sep 20;13(10):442.

[198] Zavvos E, Gerding EH, Yazdanpanah V, Maple C, Stein S. Privacy and Trust in the Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems. 2021 Oct 27;23(8):10126-41.

[199] Babaghayou M, Labraoui N, Ari AA, Lagraa N, Ferrag MA. Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. Journal of Information Security and Applications. 2020 Dec 1;55:102618.

[200] Memon I, Shaikh RA, Shaikh H. Dynamic pseudonyms trust-based model to protect attack scenario for internet of vehicle ad-hoc networks. Multimedia Tools & Applications. 2024 Feb 11;83(5).

[201] Nyangaresi VO, Yenurkar GK. Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks. High-Confidence Computing. 2023 Nov 24:100178.

[202] Shirazi F, Simeonovski M, Asghar MR, Backes M, Diaz C. A survey on routing in anonymous communication protocols. ACM Computing Surveys (CSUR). 2018 Jun 12;51(3):1-39.

[203] Pathak A, Patil T, Pawar S, Raut P, Khairnar S. Secure authentication using zero knowledge proof. In2021 Asian Conference on Innovation in Technology (ASIANCON) 2021 Aug 27 (pp. 1-8). IEEE.

[204] Major W, Buchanan WJ, Ahmad J. An authentication protocol based on chaos and zero knowledge proof. Nonlinear Dynamics. 2020 Mar;99:3065-87.

[205] Simonjan J, Taurer S, Dieber B. A generalized threat model for visual sensor networks. Sensors. 2020 Jun 28;20(13):3629.

[206] Srinivas TA, Manivannan SS. Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm. Computer Communications. 2020 Nov 1;163:162-75.

[207] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[208] Wang X, Wang J, Xu Y, Chen J, Jia L, Liu X, Yang Y. Dynamic spectrum anti-jamming communications: Challenges and opportunities. IEEE Communications Magazine. 2020 Feb 14;58(2):79-85.

[209] Elahi MM, Rahman MM, Islam MM. An efficient authentication scheme for secured service provisioning in edge-enabled vehicular cloud networks towards sustainable smart cities. Sustainable Cities and Society. 2022 Jan 1;76:103384.

[210] Rawat GS, Singh K, Arshad NI, Hadidi K, Ahmadian A. A lightweight authentication scheme with privacy preservation for vehicular networks. Computers and Electrical Engineering. 2022 May 1;100:108016.

[211] Fan K, Bi Y, Yang Y, Zhang K, Li H. Secure and Efficient Lightweight Protocol for Emergency Vehicle Avoidance Based on Cloud. IEEE Network. 2023 Oct 24;37(4):314-22.

[212] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[213] 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.

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

[215] Ang LM, Seng KP, Ijemaru GK, Zungeru AM. Deployment of IoV for smart cities: Applications, architecture, and challenges. IEEE access. 2018 Dec 16;7:6473-92.

[216] Guleria K, Verma AK. Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks. Wireless Networks. 2019 Apr 15;25:1159-83.

[217] Chan L, Gomez Chavez K, Rudolph H, Hourani A. Hierarchical routing protocols for wireless sensor network: A compressive survey. Wireless Networks. 2020 Jul;26:3291-314.

[218] Zhang H, Ma J, Qiu Z, Yao J, Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Multi-GPU Parallel Pipeline Rendering with Splitting Frame. InComputer Graphics International Conference 2023 Aug 28 (pp. 223-235). Cham: Springer Nature Switzerland.

[219] Shaheen Q, Shiraz M, Hashmi MU, Mahmood D, Zhiyu Z, Akhtar R. A Lightweight Location-Aware Fog Framework (LAFF) for QoS in Internet of Things Paradigm. Mobile Information Systems. 2020;2020(1):8871976.

[220] Lucic MC, Wan X, Ghazzai H, Massoud Y. Leveraging intelligent transportation systems and smart vehicles using crowdsourcing: An overview. Smart Cities. 2020 May 8;3(2):341-61.

[221] Qiao X, Wang H, Tan W, Vasilakos AV, Chen J, Blake MB. A survey of applications research on content-centric networking. China Communications. 2019 Sep 27;16(9):122-40.

[222] Sachan S, Sharma R, Sehgal A. SINR based energy optimization schemes for 5G vehicular sensor networks. Wireless Personal Communications. 2022 Nov;127(2):1023-43.

[223] Mishra M, Gupta GS, Gui X. Network lifetime improvement through energy-efficient hybrid routing protocol for IoT applications. Sensors. 2021 Nov 9;21(22):7439.

[224] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[225] Chaudhari BS, Zennaro M, Borkar S. LPWAN technologies: Emerging application characteristics, requirements, and design considerations. Future Internet. 2020 Mar 6;12(3):46.

[226] Wang M, Chen T, Du F, Wang J, Yin G, Zhang Y. Research on adaptive beacon message transmission power in VANETs. Journal of Ambient Intelligence and Humanized Computing. 2022 Mar 1:1-3.

[227] Long J, Büyüköztürk O. Collaborative duty cycling strategies in energy harvesting sensor networks. Computer-Aided Civil and Infrastructure Engineering. 2020 Jun;35(6):534-48.

[228] Alanazi F. A systematic literature review of autonomous and connected vehicles in traffic management. Applied Sciences. 2023 Jan 30;13(3):1789.

[229] Ghaemi Y, El-Ocla H, Yadav NR, Madana MR, Raju DK, Dhanabal V, Sheshadri V. Intelligent transport system using time delay-based multipath routing protocol for vehicular ad hoc networks. Sensors. 2021 Nov 19;21(22):7706.

[230] Srivastava A, Prakash A, Tripathi R. Location based routing protocols in VANET: Issues and existing solutions. Vehicular Communications. 2020 Jun 1;23:100231.

[231] 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.

[232] Darwish TS, Bakar KA. Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues. IEEE Access. 2018 Mar 15;6:15679-701.

[233] Ding W, Jing X, Yan Z, Yang LT. A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion. Information Fusion. 2019 Nov 1;51:129-44.

[234] Ketshabetswe KL, Zungeru AM, Mtengi B, Lebekwe CK, Prabaharan SR. Data compression algorithms for wireless sensor networks: A review and comparison. IEEE Access. 2021 Sep 29;9:136872-91.

[235] Ali ZH, Ali HA. Energy-efficient routing protocol on public roads using real-time traffic information. Telecommunication Systems. 2023 Apr;82(4):465-86.

[236] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[237] Dafalla ME, Mokhtar RA, Saeed RA, Alhumyani H, Abdel-Khalek S, Khayyat M. An optimized link state routing protocol for real-time application over vehicular ad-hoc network. Alexandria Engineering Journal. 2022 Jun 1;61(6):4541-56.

[238] Van Thanh N, Linh TT. Real-time Trajectory Planning for Autonomous Vehicles in Dynamic Traffic Environments: A Survey of Modern Algorithms and Predictive Techniques. Journal of Intelligent Connectivity and Emerging Technologies. 2022 Dec 20;7(12):1-25.

[239] An H, Na Y, Lee H, Perrig A. Resilience evaluation of multi-path routing against network attacks and failures. Electronics. 2021 May 24;10(11):1240.

[240] Simpkin C, Taylor I, Harborne D, Bent G, Preece A, Ganti RK. Efficient orchestration of node-red iot workflows using a vector symbolic architecture. Future Generation Computer Systems. 2020 Oct 1;111:117-31.

[241] 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.

[242] Ali GM, Noor-A-Rahim M, Chong PH, Guan YL. Analysis and improvement of reliability through coding for safety message broadcasting in urban vehicular networks. IEEE Transactions on Vehicular Technology. 2018 Mar 28;67(8):6774-87.

[243] Sun P, Jia S, Liang D, Qu R. A Review on the Development of High-reliability Motor System for Safety-critical Applications-From Redundancy Design Prospective. IEEE Transactions on Transportation Electrification. 2023 Dec 7.

[244] Saleh AH, Mohammed MS. Enhancing Data Security through Hybrid Error Detection: Combining Cyclic Redundancy Check (CRC) and Checksum Techniques. International Journal of Electrical and Electronics Research. 2024 Jul 25;12(3):813-26.

[245] Kianersi D, Uppalapati S, Bansal A, Straub J. Evaluation of a reputation management technique for autonomous vehicles. Future Internet. 2022 Jan 19;14(2):31.

[246] Alladi T, Chamola V, Sahu N, Venkatesh V, Goyal A, Guizani M. A comprehensive survey on the applications of blockchain for securing vehicular networks. IEEE Communications Surveys & Tutorials. 2022 Mar 21;24(2):1212-39.

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

[248] Nilima SI, Bhuyan MK, Kamruzzaman M, Akter J, Hasan R, Johora FT. Optimizing Resource Management for IoT Devices in Constrained Environments. Journal of Computer and Communications. 2024 Aug 7;12(8):81-98.

[249] Zamani S, Tork Ladani B, Ashouri Talouki M. Privacy, reputation, and incentive provision for vehicular social networks. Journal of Reliable Intelligent Environments. 2023 Dec;9(4):447-61.

[250] Meng W, Li W, Wang Y, Au MH. Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. Future Generation Computer Systems. 2020 Jul 1;108:1258-66.

[251] Mallick MA, Nath R. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News. 2024;190(1):1-69.

[252] Begum K, Mozumder MA, Joo MI, Kim HC. BFLIDS: Blockchain-driven federated learning for intrusion detection in IoMT networks. Sensors. 2024 Jul 15;24(14):4591.

[253] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan;11(24):12040.

[254] Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEe Access. 2019 Jun 20;7:82721-43.

[255] Kumar R, Sharma R. Leveraging blockchain for ensuring trust in IoT: A survey. Journal of King Saud University-Computer and Information Sciences. 2022 Nov 1;34(10):8599-622.

[256] Ray S, Mishra KN, Dutta S. Big data security issues from the perspective of IoT and cloud computing: a review. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science). 2021 Oct 1;14(7):2057-78.

[257] Jiang H, Li J, Zhao P, Zeng F, Xiao Z, Iyengar A. Location privacy-preserving mechanisms in location-based services: A comprehensive survey. ACM Computing Surveys (CSUR). 2021 Jan 2;54(1):1-36.

[258] 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.

[259] Prajapati P, Bhatt B, Zalavadiya G, Ajwalia M, Shah P. A review on recent intrusion detection systems and intrusion prevention systems in IoT. In2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) 2021 Jan 28 (pp. 588-593). IEEE.

[260] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Apr 1;127:103096.

[261] Lampe B, Meng W. A survey of deep learning-based intrusion detection in automotive applications. Expert Systems with Applications. 2023 Jul 1;221:119771.

[262] Zhang Y, Zhao J, Zheng D, Deng K, Ren F, Zheng X, Shu J. Privacy-preserving data aggregation against false data injection attacks in fog computing. Sensors. 2018 Aug 13;18(8):2659.

[263] 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.

[264] Jaballah WB, Conti M, Lal C. Security and design requirements for software-defined VANETs. Computer Networks. 2020 Mar 14;169:107099.

[265] Chbib F, Zeadally S, Khatoun R, Khoukhi L, Fahs W, Haydar J. A secure cross-layer architecture for reactive routing in vehicle to vehicle (V2V) communications. Vehicular Communications. 2022 Dec 1;38:100541.

[266] Grover J. Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review. Vehicular Communications. 2022 Apr 1;34:100458.

[267] Saad M, Khan MK, Ahmad MB. Blockchain-enabled vehicular ad hoc networks: A systematic literature review. Sustainability. 2022 Mar 25;14(7):3919.

[268] Kudva S, Badsha S, Sengupta S, La H, Khalil I, Atiquzzaman M. A scalable blockchain based trust management in VANET routing protocol. Journal of Parallel and Distributed Computing. 2021 Jun 1;152:144-56.

[269] Juárez R, Bordel B. Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. Electronics. 2023 Nov 27;12(23):4794.

[270] Zheng X, Li M, Chen Y, Guo J, Alam M, Hu W. Blockchain-based secure computation offloading in vehicular networks. IEEE Transactions on Intelligent Transportation Systems. 2020 Sep 9;22(7):4073-87.