vehicles

MDPI

Review

Enhancing Security in Vehicle-to-Vehicle Communication: A Comprehensive Review of Protocols and Techniques

Muhana Magboul Ali Muslam

Department of Information Technology, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, P.O. Box 5701, Riyadh 11432, Saudi Arabia; mmmuslam@imamu.edu.sa

Abstract: Vehicle-to-vehicle (V2V) communication has played a pivotal role in modern intelligent transportation systems, enabling seamless information exchange among vehicles to enhance road safety, traffic efficiency, and overall driving experience. However, the secure transmission of sensitive data between vehicles remains a critical concern due to potential security threats and vulnerabilities. This research focused on investigating the security protocols that have been employed in vehicle-to-vehicle communication systems. A comprehensive review and analysis of relevant literature and research papers was conducted to gather information on existing V2V communication security protocols and techniques. The analysis encompassed key areas, including authentication mechanisms, encryption algorithms, key management protocols, and intrusion detection systems specifically applicable to V2V communication networks. Within the context of real-world V2V environments, this study delved into the challenges and limitations associated with implementing these protocols. The research aimed to provide a comprehensive understanding of the strengths and weaknesses of the current V2V communication security protocols. Furthermore, based on the findings, this paper proposes improvements and recommendations to enhance the security measures of the V2V communication protocol. Ultimately, this research contributes to the development of more secure and reliable V2V communication systems, propelling the advancement of intelligent transportation technology.

Keywords: communication protocols; efficiency in V2V communication; Internet of Things (IoT); Internet of Vehicle (IoV); intrusion detection systems; security protocols; safety and security; vehicle-to-vehicle (V2V) communication; vehicular ad hoc networks (VANETs)

Citation: Muslam, M.M.A. Enhancing Security in Vehicle-to-Vehicle Communication: A Comprehensive Review of Protocols and Techniques. *Vehicles* **2024**, *6*, 450–467. https://doi.org/10.3390/vehicles6010020

Academic Editor: Mohammed Chadli

Received: 27 December 2023
Revised: 15 February 2024
Accepted: 18 February 2024
Published: 27 February 2024

1. Introduction

The advent of vehicle-to-vehicle (V2V) communication has heralded significant advancements and opportunities in the automotive industry. The seamless exchange of information between vehicles holds the potential to revolutionize road safety, traffic management, and transportation efficiency. However, ensuring the secure transmission and protection of data in V2V communication networks is of paramount importance to guarantee the integrity, privacy, and reliability of the exchanged information. In the 1980s, the introduction of the internet led to a rapid growth in human communication. As technology continued to progress, the internet evolved into a global network facilitating communication between humans and devices. This technological evolution gave rise to concepts like "smart tech" and "Internet of Things" (IoT). Presently, IoT has become a widely discussed emerging topic globally, with numerous companies manufacturing and distributing IoT devices embedded with chips and sensors.

The increasing integration of vehicles with advanced communication technologies has enabled the development of smart transportation systems and connected vehicles. Vehicular communication systems, known as V2X (vehicle-to-everything) networks, facilitate real-time data exchange between vehicles, infrastructure, pedestrians, and other road users, enhancing road safety, traffic efficiency, and overall driving experience. However, as

these V2X systems become more prevalent, ensuring the security and privacy of the communication becomes a critical concern.

A proposal was put forth for a multi-protocol gateway solution aimed at facilitating efficient data exchange among entities originating from diverse technological backgrounds. This proposal systematically investigates the compatibility and real-time responsiveness attributes inherent in various Internet of Things (IoT) Ethernet-based communication technologies, specifically scalable service-oriented middleware over IP (SOME/IP), data distribution service (DDS), and enhanced communication abstraction layer (eCAL) middleware. The hardware architecture employed in the simulation is delineated, encompassing microprocessors equipped with native POSIX-based operating systems for the majority of nodes, along with a virtual Linux operating system on a general-purpose computer designed for simulated interactions with an IoT supervisor node. The transmitted data are organized in the format of a cyclic event resembling a heartbeat [1].

IoT operates in tandem with sensors, actuators, and microchips embedded in equipment, commonly known as smart devices. Sensors detect and gather data about environmental changes, while actuators are responsible for controlling IoT devices. Microchips ensure the functionality of the device by coordinating sensors and actuators, following instructions, and executing activities accordingly. The data collected by sensors are transmitted to other devices, where they are utilized for decision-making purposes. The advancements in vehicular communication have the potential to revolutionize the automotive industry and improve transportation efficiency. However, ensuring the security and privacy of V2X networks remains a paramount concern. Through an exploration of the latest research and developments, this paper aims to contribute to the understanding of the challenges and potential solutions in vehicular communication security. By addressing these challenges and implementing innovative security measures, the dream of a safe and connected future on the roads can be realized.

This paper explores the key challenges and cutting-edge solutions in the field of vehicular communication security. The aim is to identify the latest advancements, security protocols, and frameworks that address the vulnerabilities and risks associated with V2X networks.

This paper is organized as follows. Section 2 contains the literature review. Section 3 describes the methodology. Section 4 analyses the security protocols for vehicular communication. Section 5 provides conclusions and possible research directions.

This paper investigates the security protocols employed in vehicle-to-vehicle (V2V) communication systems, providing a comprehensive review and analysis of relevant literature and research papers to gather information on existing V2V communication security protocols and techniques by examining key areas such as authentication mechanisms, encryption algorithms, key management protocols, and intrusion detection systems specifically applicable to V2V communication networks. We identify the challenges and limitations associated with implementing these protocols in real-world V2V environments, and provide a comprehensive understanding of the strengths and weaknesses of current V2V communication security protocols. We also propose improvements and recommendations to enhance the security measures of the V2V communication protocol based on the research outcomes. This research contributes to the development of more secure and reliable V2V communication systems, advancing intelligent transportation technology.

2. Literature Review

The field of vehicular communication security has been the subject of significant research and development, leading to a vast array of scholarly articles and studies. Some notable contributions in this area are included in this section. While V2X communication systems offer numerous benefits, they also face several security challenges. One of the primary concerns is ensuring the confidentiality and integrity of data exchanged between vehicles and infrastructure. As the number of connected vehicles increases, so does the potential for cyberattacks and malicious activities.

The article proposes a solution for efficient data exchange between entities with different technological origins through a multi-protocol gateway. The author analyzes the compatibility and real-time responsiveness capabilities of various IoT Ethernet-based communication technologies, such as scalable service-oriented middleware over IP (SOME/IP), data distribution service (DDS), and enhanced communication abstraction layer (eCAL) middleware. Furthermore, the author explores the hardware architecture employed in their simulation, which comprises microprocessors equipped with native POSIX-based operating systems for most nodes, and a virtualized Linux OS on a general-purpose computer to simulate interaction with an IoT supervisor node. The transmitted data are organized in the form of a cyclic event known as a heartbeat [2].

The study presents a protocol for ensuring the security and privacy of V2X communications. This protocol is based on the principles of hash chain cryptography and offers a lightweight approach to message authentication. By incorporating a hash chain of secret keys for a message authentication code (MAC), the proposed protocol achieves highly secure message authentication at a significantly lower cost. To validate its effectiveness, the author has implemented the protocol using commercially available V2X devices. The results of experiments conducted on real networks demonstrate the superiority of the proposed protocol over both standard and non-standard protocols. Specifically, the proposed protocol reduces communication overhead by a factor of 6 and computation overhead by over 100 times when compared to the IEEE1609.2 (ieeexplore.ieee.org/document/7426684). Additionally, it reduces communication overhead by a factor of 4 and computation overhead by up to 100 times when compared to the non-standard security protocol—TESLA. Moreover, the proposed protocol significantly reduces the average end-to-end delay to 2.5 ms, representing a reduction of 24- and 28-fold compared to the IEEE1609.2 and TESLA protocols, respectively [3].

The article presents a proposal for a V2V data transmission protocol that is both efficient and secure. This protocol utilizes a one-way hash function to expedite the transmission of valuable information to the receiver. The proposed approach effectively defends against a range of security attacks, including modification, impersonation, replay, man-in-the-middle, stolen onboard unit, password guessing, and concatenation. The results of the study demonstrate that the suggested scheme outperforms existing V2V protocols in terms of execution time, storage cost, communication overhead, and energy consumption. The performance evaluation of the proposed method is conducted by considering various attributes such as energy consumption, communication overhead, computational time, and storage cost. It is concluded that the suggested protocol satisfies the authentication property under the assumption of a one-way hash function in the random oracle model [4].

On the performance evaluation of vehicular PKI protocol for V2X communications security, the study presents an in-depth performance evaluation of vehicular public key infrastructure (PKI) protocols used for securing V2X communications. The author evaluates the performance of PKI with respect to certificate reloading by comparing two communication profiles with and without V2X security, and shows that the end-to-end latency between a requesting vehicle and the PKI is not negligible [5].

The paper discusses the implementation of a 5G-MEC testbed for vehicle-to-everything (V2X) applications, which requires low latency and high computational capabilities at the network's edge. It also highlights the challenges researchers may face while replicating and deploying the testbeds. It offers a comprehensive overview of the implementation of a 5G-MEC testbed for V2X applications, scrutinizes several crucial testbeds and cutting-edge implementations, and deliberates on the potential obstacles that researchers may encounter while reproducing and deploying such testbeds. Moreover, it provides a summary of the instruments utilized to construct the testbeds and addresses unresolved concerns pertaining to their implementation [6].

The paper proposes a system for direct communication between two vehicles using a modulated tag and the wave emitted by an FMCW radar installed in the vehicle. The system allows for real-time signal detection and classification, adding redundancy to

computer video sensors without incorporating additional communication systems. The experiment proves the possibility of communication between the transponder and the radar. The experiment used real vehicles and a designed transponder and commercial radar. The radar has two transmitters, four receiver antennas, and is based on analogue device technology. The radar has a field of view of 120 degrees in azimuth and 15 degrees in elevation. Different modulation frequencies were used for classification purposes. A conventional algorithm suppressed clutter. The transponder had a detection rate of 97.42% and a small error in measured modulation frequency. The paper also discusses the limits of the radar's ability to resolve modulation frequency [7].

The paper discusses the benefits and deployment status of C-V2X (cellular vehicle-to-everything) technology, which is a wireless communication system used in autonomous driving and intelligent transportation systems. It also highlights the role of 5G NR (new radio) deployment in the evolution of C-V2X and its potential to change the future of transportation. The results of V2V tests show that PC5-based C-V2X devices have better performance in terms of latency compared to the Rel-14 standard ((https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/c-v2x_technology.pdf (accessed on 24 October 2023)) defined maximum latency for V2X applications. The paper also highlights that technical application layer specifications are not standardized in C-V2X, and regulations and insurance claims for ITS road accidents are yet to be defined [8].

In reference [9], an elaborate framework is proposed, encompassing network models, protocols, and architectures. The proposed solution delineates an architecture comprising a perception layer, coordination layer, application layer, artificial intelligence layer, and business layer. Sensors and actuators are housed in the perception layer, while the coordination layer integrates 4G and Wi-Fi. The application layer spans various applications, including web-based and multimedia applications. The business layer involves the development of business strategies based on application usage, and the artificial intelligence layer addresses cloud infrastructure.

The Internet of Vehicles incorporates diverse vehicular networks, for example, vehicle-to-mobile networks, vehicle-to-vehicle, vehicle-to-devices, vehicle-to-sensors, vehicle-to-human and vehicle-to-roadside infrastructure, as illustrated in Figure 1. Reference [10] introduces a communication protocol for the Internet of Connected Vehicles, emphasizing seamless and secure communication in vehicular ad hoc networks. Industry standards for IoV will be scrutinized, along with its associated benefits. The proposed architecture in [10] encompasses seven layers—data communication, acquisition, processing, data filtering, security, user–vehicle interface, and control layer—providing a comprehensive mechanism to safeguard IoV.

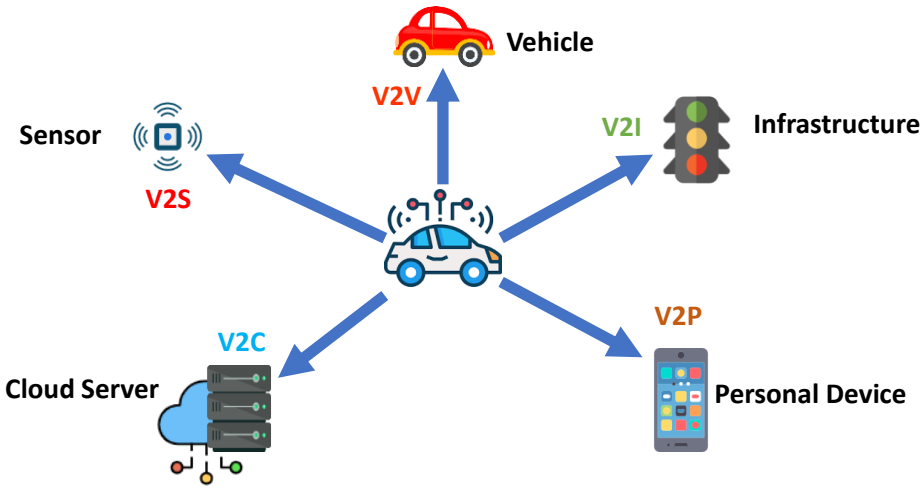

Figure 1. Internet of Vehicles communication.

In the context of connected vehicles, ref. [11] identifies various system exploits, for instance door locking, brake disabling and engine shutdowns categorized as threats within cyberattacks on autonomous connected vehicles. The structure of a connected vehicle includes components like onboard diagnostic ports (ODPs), a control area network (CAN), and an electronic control unit (ECU) rendering it susceptible to onboard diagnostic (OBD) attacks.

The framework proposed in [12] incorporates layered architecture, a network model, environmental model and interaction model, each contributing unique features. The network model addresses multi-network, multi-user, multi-technology, multi-device, and multi-communication methods. The interaction model elucidates the relationships among vehicles, networks, personal devices, sensors, roadside architecture, and humans. The environmental model pertains to vehicle communication beyond its perimeter.

To ensure the security of the Internet of Connected Vehicles, ref. [13] proposes an extended access control-oriented architecture (E-ACO) dependent on cloud computing functionalities. Access control models are introduced, preventing unauthorized access at different levels of E-ACO.

Through the implementation of an access control model within the Internet of Connected Vehicles (IoCV), the attainment of secure and privacy-enabled data communication becomes feasible. This access control framework is designed to grant permissions to security officials at various hierarchical levels, allowing them access to the communication integrated within the vehicles. The incorporation of security layers within this model serves to safeguard against the inadvertent disclosure of sensitive information from higher security echelons to lower security tiers. Derived from mathematical models, the "security and privacy-based access control model" assigns permissions and delineates roles for security officials navigating the IoCV landscape. This model facilitates secure communication channels utilizing both 4G and Wi-Fi technologies. Essential features of this model include mutually exclusive permissions and the dynamic separation of duties [14].

The research article by [15] introduces the attack-resistant trust (ART) management system. This system is conceived to fortify the security of ad hoc networks interlinked with the Internet of Vehicles. The primary objective of this mechanism is to identify and thwart malicious nodes within the network, thereby preventing disruptions to both the network itself and the associated connected vehicles. By subjecting the transferred data over the vehicular ad hoc network (VANET) and mobile network to rigorous evaluation and verification, this mechanism ensures the legitimacy of the transmitted information. The authors elucidate two pivotal models: the network model, which pertains to wireless networks featuring computational devices and sensors, and the adversary model, which scrutinizes diverse external attacks such as bad mouth attacks, simple attacks, and zig-zag attacks.

A dual authentication system, as outlined in [16], founded on a redesigned trusted platform module, emerges as a commendable solution for enhancing the security, privacy, and operational efficiency within the domain of the Internet of Vehicles. Conventional cryptographic, reputation-based, and hardware-based authentication mechanisms are deemed traditional and acknowledged to be inadequate due to inherent limitations. Upon the implementation of a privacy-preserving dual authentication system in the vehicle, the onboard unit (OBU) generates a temporary encrypted key, thereby facilitating the authentication of a session. Additionally, the vehicle undergoes verification by a trust authority, attesting to its legitimacy through a comprehensive examination of its reputation history. The successful completion of these two authentication phases culminates in the establishment of a communication session. Significantly, software defined networking (SDN) assumes a pivotal role by contributing a software layer to the Internet of Things (IoT), thereby simplifying and advancing network evolution.

In their scholarly contribution, ref. [17] introduced an innovative software-defined networking (SDN)-based model for securing data transfer within the realm of Internet of Things (IoT) vehicles. The deployment of SDNs within the IoT sector is orchestrated with the overarching goal of accomplishing diverse tasks within wireless networks. This

proposed model incorporates a middle box guard (MBG) as a fundamental component, designed to augment security through the implementation of policies derived from algorithms such as data flow abstraction and heuristic methodologies. To fortify the resilience of the middle box against potential security threats, an integer linear programming (LP) algorithm is employed, ensuring its robustness and mitigating its susceptibility to becoming a hotspot vulnerable to attacks. Furthermore, an additional algorithm is implemented to manage load balancing within the system.

Enhanced secure ad hoc on-demand distance vector (ES-AODV) routing, as presented by [18], constitutes a protocol devised for the identification of malicious nodes and the mitigation of potential attacks. This protocol serves to enhance network integrity by facilitating secure data transmission within vehicular ad hoc networks (VANETs). Central to its operation is an algorithm grounded in asymmetric key infrastructure, employing a public-private key mechanism in conjunction with elliptic curve cryptography (ECC). In this process, a key is generated through ECC and subsequently validated by a certificate authority to verify the legitimacy of the vehicle based on this key. It is imperative to note that ES-AODV routing represents a modification to the existing AODV protocol code.

The research article by [19] provides an examination of the opportunities and challenges inherent in security and forensics within the context of the Internet of Things (IoT). IoT devices, by virtue of their intrinsic attributes such as low power consumption and open connectivity, frequently become targets for malicious attacks. Considering that the primary purpose of IoT devices involves the collection of private and confidential data, safeguarding privacy emerges as a paramount concern. In response to these challenges, the article advocates for the development of a robust security architecture capable of identifying and preempting malicious attacks that might disrupt IoT networks. Consequently, the implementation of secure protocols is posited as an imperative measure to fortify the resilience of IoT ecosystems against potential threats.

Vehicular ad hoc networks (VANETs) are structured upon a layered architecture, delineated into the sensing layer, network layer, and application layer, as elucidated in [20].

Positioned at the foundational level of this architecture, the sensing layer is responsible for capturing information pertaining to environmental changes through the utilization of diverse sensors, including NFC, RFID, and wireless sensor networks. In parallel, the network layer assumes the central role of ensuring the integrity of communication channels among Internet of Things (IoT) entities. This is achieved through the application of various technologies, such as Bluetooth, 4G, and Wi-Fi, with an emphasis on maintaining secure communication. Simultaneously, the application layer is tasked with the transmission of data acquired from sensors, its subsequent processing, and the appropriate storage of the processed data.

The literature review provides a comprehensive overview of research in the field of vehicular communication security; however, there are several limitations and potential biases that warrant consideration. The review primarily concentrates on academic research articles, thereby overlooking valuable insights from industry reports, technical specifications, and governmental guidelines. The reviewed studies predominantly center on proposed solutions and advancements, although the review briefly touches upon challenges researchers may encounter in replicating and implementing testbeds. Furthermore, while the review outlines various methodologies proposed in the examined studies.

2.1. Challenges and Opportunities

In examining the literature review, several challenges and opportunities emerge within the realm of vehicular communication security.

2.1.1. Challenges

Cybersecurity Threats: Vehicular communication systems face a myriad of cybersecurity threats, including hacking, spoofing, jamming, and data breaches. Ensuring the

integrity, confidentiality, and availability of data exchanged between vehicles and infrastructure is paramount to safeguard against malicious attacks.

Privacy Concerns: The proliferation of connected vehicles raises significant privacy concerns regarding the collection, storage, and sharing of sensitive personal data. Balancing the benefits of data-driven services with the protection of individuals' privacy rights remains a complex challenge in vehicular communication systems.

Interoperability Issues: The interoperability of communication protocols and standards across diverse vehicular networks poses challenges for seamless data exchange and collaboration between vehicles, infrastructure, and other road users. Achieving interoperability requires addressing compatibility issues and establishing common standards to ensure effective communication among heterogeneous systems.

Scalability and Reliability: As the number of connected vehicles increases, scalability and reliability become critical considerations in vehicular communication systems. Ensuring the robustness and resilience of communication networks to accommodate growing traffic volumes and fluctuations in network conditions is essential for maintaining system performance and reliability.

Regulatory Compliance: Compliance with regulatory frameworks and industry standards presents challenges for stakeholders involved in the development and deployment of vehicular communication systems. Navigating complex regulatory landscapes and ensuring adherence to data protection, cybersecurity, and safety regulations require substantial resources and expertise.

2.1.2. Opportunities

Enhanced Safety and Efficiency: Vehicular communication technologies offer opportunities to enhance road safety and traffic efficiency by enabling real-time data exchange and collaborative decision-making among vehicles and infrastructure. Advanced driver assistance systems, traffic management solutions, and autonomous vehicle technologies can leverage vehicular communication to mitigate traffic congestion, reduce accidents, and improve overall transportation efficiency.

Innovation and Technological Advancements: The rapid advancement of communication technologies, such as 5G, edge computing, and IoT, presents opportunities for innovation and technological advancements in vehicular communication systems. Leveraging these technologies can enhance the capabilities of connected vehicles, enable new applications and services, and improve the overall user experience for drivers and passengers.

Data-Driven Insights: Vehicular communication systems generate vast amounts of data that can be leveraged to gain valuable insights into traffic patterns, road conditions, and driver behavior. Analyzing this data can inform the development of predictive analytics, traffic management strategies, and personalized mobility solutions to address the evolving needs of urban mobility and transportation planning.

Collaborative Ecosystems: Building collaborative ecosystems and partnerships between industry stakeholders, government agencies, academia, and research institutions can foster innovation and accelerate the development and deployment of vehicular communication systems. Collaborative initiatives can drive the co-creation of standards, protocols, and best practices, as well as facilitate knowledge sharing and technology transfer across different sectors.

Socioeconomic Benefits: Vehicular communication systems have the potential to generate significant socioeconomic benefits, including job creation, economic growth, and environmental sustainability. By enabling more efficient transportation systems, reducing traffic congestion, and minimizing emissions, connected vehicles can contribute to building smarter, greener, and more resilient cities for future generations.

3. Methodology

To investigate the security protocols implemented in vehicle-to-vehicle (V2V) communication systems, an extensive literature review and analysis was undertaken. The ensuing

methodology elucidates the systematic approach employed for acquiring pertinent information, delineating the criteria for selecting research papers, and conducting an analytical examination of the identified protocols.

3.1. Data Collection

3.1.1. Literature Search

A methodical exploration was executed across esteemed academic databases, namely, ACM Digital Library, Google Scholar and IEEE Xplore. Employing keywords such as "V2V communication security", "vehicular security protocols", and "IoT security in transportation", the search aimed to identify pertinent research articles, conference papers, and scholarly publications.

3.1.2. Source Selection

The collected papers were screened based on their relevance to the topic and their contribution to V2V communication security protocols. Only peer-reviewed articles, conference proceedings, and scholarly publications were included to ensure the accuracy and reliability of the information.

3.2. Data Analysis

3.2.1. Categorization

The chosen research papers underwent categorization predicated on discerned key areas expounded in their respective abstracts, key management protocols, encryption algorithms, intrusion detection systems and encompassing authentication mechanisms.

3.2.2. Thematic Analysis

The study utilized a thematic analysis methodology to extrapolate essential concepts, methodologies, and findings from each scholarly article. The analysis was particularly directed towards comprehending the design principles and functionalities inherent in security protocols, as well as evaluating their efficacy in addressing and mitigating security threats.

3.2.3. Comparison

Within each category, the security protocols were compared based on their features, strengths, and weaknesses. Comparative tables and charts were used to visually represent the similarities and differences between the protocols.

3.2.4. Real-World Relevance

The analysis extended to the examination of real-world scenarios and case studies presented in the selected papers. This involved evaluating the protocols' performance in practical V2V environments and identifying challenges faced during implementation.

3.2.5. Integration with IoT Protocols

To foster a deeper understanding, this study also explored communication protocols in the broader context of the IoT. A comparative analysis was performed to highlight the similarities and differences between IoT and V2V communication protocols, considering parameters such as message size, latency, energy consumption, and bandwidth consumption.

The methodology described above facilitated a structured and systematic approach to collecting, analyzing, and interpreting the relevant literature on V2V communication security protocols. The insights gained from this methodology form the basis for the subsequent analysis and discussions presented in this research paper.

4. Analysis of Vehicular Communication Security Protocols

Following the methodology, the next section presents the analysis of the collected data based on the previously presented themes and comparisons. The analysis of the literature

on vehicular communication security protocols reveals significant insights into their effectiveness in addressing key criteria including safety, security, efficiency, environmental protection, and commercialization (Table 1).

Table 1. Key findings and their implications for the advancement of V2V communication systems' security and highlights the contributions of research.

Technique	Objective	Results
A testing platform for V2X communication security [1]	Security	Investigates the security risks inherent in V2X communication, with the objective of establishing an information security testing and verification platform possessing independent intellectual property rights. This platform is designed to address diverse scenarios, including car-vehicle, car-person, car-road, car-cloud, among others.
Hash chain cryptography [2]	Security	Proposed a message authentication and privacy preservation protocol for vehicular-to-everything (V2X) communications, predicated on hash chain cryptography. This protocol manifests a discernible decrease in communication overhead by a factor of four and computational overhead by up to 100 times in contrast to a non-standard security protocol, TESLA.
Lightweight secure one-way hash function to send valuable information at the receiver side quickly [3]	Security	Introduces an efficient and secure V2V data transmission protocol utilizing a one-way hash function to expedite the processing of valuable information at the receiver side. The protocol demonstrates resilience against various security attacks, including modification, impersonation, replay, man-in-the-middle, stolen onboard unit, password guessing, and concatenation.
A vehicular public key infrastructure (PKI) protocol for V2X communications security [4]	Security	Evaluates the performance of a vehicular PKI-protocol tailored for V2X communications security, comparing communication profiles with and without V2X security. Findings indicate that for highly mobile networks, omitting security enhances performance, albeit still requiring at least half a second.
Quality of service (QoS) in a vehicle-to-everything (V2X) communication environment [5]	Safety, Environment Protection	Conducts an analysis demonstrating that turbo-based coding schemes satisfy all quality of service (QoS) parameters, exhibiting overall communication quality comparable to polar coding and superior to low-density parity-check (LDPC) coding. This suitability positions them favorably for small frame 5G V2X services.
5G-MEC testbed for Vehicle-to-Everything (V2X) applications [6]	Safety, Environment Protection	Provides an overview of the implementation of a 5G-MEC testbed for V2X applications, scrutinizes pertinent testbeds and cutting-edge implementations, and deliberates on the challenges researchers may encounter during testbed replication and deployment.
Direct communication between two vehicles using a modulated tag and the wave emitted by an FMCW radar installed in the vehicle [7]	Safety, Environment Protection	Reports a transponder detection rate of 97.42% and an average error in the measured modulation frequency of 0.5%.
The role of 5G NR (new radio) deployment in the evolution of C-V2X [8]	Efficiency, Security	Demonstrates that PC5-based C-V2X outperforms the Rel-14 standard's defined maximum latency of 100 ms for V2X applications.
Five layered architectures [9]	Safety, Efficiency, Commercialization	Better and secure IoV smart application development
Three protocols for secure communication in IoV [10]	Security	Advocates for improved and secure IoV smart application development, emphasizing the need for secure alternate routing if the current communication route is compromised.
In-vehicle network architecture in IoV [11]	Security	Additionally, underscores the importance of secure over-the-air updates for firmware upgrades, a security patches and software fixes in IoV, coupled with cloud-based secure storage.

Table 1. *Cont.*

Technique	Objective	Results
Seven layered model architecture [12]	Security	Addresses the imperative to enhance security, minimize device incompatibility, accommodate limited processing and storage capabilities.
Secure cloud-assisted connected cars authorization framework [13]	Security	Presents extended access control across diverse layers within the Internet of Vehicles (IoV), encompassing the application layer, object layer, cloud services layer, and virtual object layer, through the utilization of the vehicular cloud.
Security- and privacy-based access control model [14]	Security	Introduces the application of mutually exclusive permissions and dynamic separation of duties as a replacement for hierarchical positions, utilizing a tree-structured directory to store objects in IoCV.
Attack-resistant trust management scheme [15]	Safety, Environment Protection	Presents strategies to identify and counteract malicious threats while evaluating the trustworthiness of mobile nodes and data in vehicular ad hoc networks (VANETs).
Privacy-preserving dual authentication scheme [16]	Security	Integrates trust evaluation with the IoV authentication protocol, generating a temp encrypted key employing bilinear pair theory.
SDN-based data transfer security model [17]	Efficiency, Security	Addresses various kind of attacks including spoofing and flooding, through protocols based on tags and tunnels in the context of IoV.
Advanced secured routing algorithm [18]	Efficiency, Security	Elaborates on the identification of malicious codes, the prevention of blackhole attacks, and the provision of secure data transmission in VANET.
Security and forensics framework [19]	Security	Expounds on existing major security and forensics challenges within the Internet of Things (IoT) domain related to vehicles.
Vehicular communications expanded-layer architecture [20]	Security	Identifies intra- and inter-vehicle security threats, fostering a comprehensive understanding of security concerns within the vehicular context.

This section presents the findings and analysis of each criterion.

4.1. Safety and Security

Vehicular communication systems have the potential to greatly enhance road safety by enabling real-time information exchange between vehicles and infrastructure. The integration of secure authentication mechanisms and intrusion detection systems contributes to identifying malicious activities and potential threats. Protocols such as the enhanced secure ad hoc on-demand distance vector (ES-AODV) routing enhance data transmission security, ensuring the integrity of safety-critical information. However, challenges such as the timely detection of anomalies and the resilience against sophisticated attacks continue to be areas of research. Security remains a paramount concern in V2V communication systems due to the sensitive nature of exchanged data. The literature presents a variety of cryptographic approaches, including asymmetric key infrastructure and elliptic curve cryptography, to secure data transmission and authentication. The proposed dual authentication system and access control models contribute to the protection of data privacy. While these protocols exhibit promising security measures, the challenge lies in ensuring scalability and adaptability to evolving threats.

The impact of autonomous vehicle (AV) technologies on safety and security represents a transformative shift in the automotive industry and transportation landscape.

4.1.1. Safety Advancements

Autonomous vehicles have the potential to revolutionize road safety by significantly reducing the occurrence of accidents caused by human error. With advanced sensors, cameras, radar, lidar, and artificial intelligence (AI) algorithms, AVs can perceive their surroundings with a higher level of accuracy and respond to potential hazards more swiftly than human drivers. By eliminating factors such as distracted driving, speeding, and impaired driving, AVs aim to mitigate most traffic accidents. Studies suggest that

widespread adoption of AVs could prevent up to 90% of accidents, potentially saving thousands of lives annually.

4.1.2. Collision Avoidance Systems

AVs are equipped with sophisticated collision avoidance systems that can detect and respond to potential hazards in real time. These systems use data from sensors and communication with other vehicles (V2V) and infrastructure (V2I) to anticipate and avoid collisions. Through predictive analytics and machine learning algorithms, AVs can navigate complex traffic scenarios with greater precision and safety.

4.1.3. Cybersecurity Concerns

While AVs offer significant safety benefits, they also pose cybersecurity challenges. As AVs rely heavily on software and connectivity for their operation, they are vulnerable to cyberthreats such as hacking, malware, and unauthorized access. Cyberattacks on AVs could potentially compromise vehicle control systems, leading to accidents or malicious activities. Therefore, ensuring the cybersecurity of AVs is critical to maintaining road safety and protecting passengers' lives.

4.1.4. Data Privacy and Ethical Considerations

AV technologies generate and utilize vast amounts of data about vehicle operations, passengers' behaviors, and environmental conditions. Protecting the privacy of this data is essential to maintaining passenger trust and confidence in AVs. Moreover, ethical considerations arise regarding AV decision-making in critical situations, such as determining the lesser of two potential collision outcomes. Addressing these concerns requires the development of robust data privacy regulations and ethical guidelines for AV manufacturers and operators.

4.1.5. Regulatory Frameworks

To address safety and security concerns associated with AV technologies, governments and regulatory bodies are implementing comprehensive frameworks to govern their development, testing, and deployment. These frameworks include regulations and standards for cybersecurity, data privacy, safety certification, and ethical guidelines for AV operation. By establishing clear regulatory guidelines, policymakers aim to ensure the safe and responsible integration of AVs into public roadways while fostering innovation and technological advancement in the automotive industry.

In summary, the impact of autonomous vehicle technologies on safety and security represents a paradigm shift in transportation, offering the potential to drastically reduce traffic accidents and improve road safety. However, addressing cybersecurity challenges, protecting data privacy, and addressing ethical considerations are essential steps in realizing the full benefits of AV technologies while ensuring passenger safety and security.

4.2. Efficiency

Efficiency in V2V communication systems is measured by factors such as low latency, minimal energy consumption, and effective bandwidth utilization. Protocols like lightweight secure message broadcasting contribute to efficient data dissemination. The software-defined networking (SDN)-based data transfer security model aims to simplify network management, potentially improving efficiency. However, balancing security requirements with performance considerations is an ongoing challenge, particularly in high-traffic scenarios.

4.3. Environmental Protection

The integration of V2V communication systems can lead to reduced traffic congestion and optimized routing, ultimately contributing to environmental protection. The proposed architecture on the Internet of Connected Vehicles (IoCV) framework emphasizes envi-

ronmental considerations through its layers, such as perception and coordination layers. By enhancing traffic flow and minimizing unnecessary stops, these protocols indirectly promote reduced emissions and energy conservation.

4.4. Commercialization

The commercialization of V2V communication systems hinges on factors such as interoperability, adoption by manufacturers, and consumer acceptance. Industry standards and proposed architectures, such as the seven-layer IoCV architecture, aim to establish a comprehensive mechanism for secure and reliable communication. These standards, along with the ART management system and enhanced communication abstraction layer (eCAL) middleware, contribute to building a foundation for commercially viable systems. However, achieving widespread adoption and seamless integration across various manufacturers and models remains a challenge.

The analysis of the security protocols indicates that while significant progress has been made in addressing safety, security, efficiency, environmental protection, and commercialization criteria, challenges and trade-offs persist. The integration of cryptographic techniques, authentication mechanisms, and intrusion detection systems demonstrates a commitment to data integrity and privacy. However, the complex and dynamic nature of vehicular environments demands continuous innovation to combat emerging threats. Efforts to strike a balance between security and performance have led to the development of lightweight protocols, but optimization remains a challenge. As the field progresses, ensuring scalability, real-time responsiveness, and compatibility across heterogeneous vehicular networks will be crucial for the successful deployment of secure V2V communication systems.

The findings suggest that the development of secure V2V communication protocols requires a multidimensional approach that considers safety, security, efficiency, environmental protection, and commercialization (see Table 2). Ongoing research and collaboration among academia, industry, and policymakers will drive the evolution of these protocols to create a safer and more connected transportation landscape.

Table 2. Key findings and their implications for the advancement of V2V communication systems' security and highlights the contributions of research in the following categories. (Sa = safety, Ef = efficiency, Se = security, En = environmental protection, and Co = commercialization).

Article	Sa	Ef	Se	En	Co
Automotive IoT Ethernet-based communication technologies [1]	✓			✓	
Risks faced by V2X communication security [2]	✓		✓		✓
Experiments to evaluate the efficiency and effectiveness of V2X security protocols based on hash chain cryptography [3]		✓		✓	
A lightweight secure message broadcasting protocol specifically designed for V2V communication [4]		✓			✓
Performance evaluation of vehicular PKI protocol for V2X communications security [5]	✓				✓
Error correction coding for various propagation environments [6]	✓				✓
5G-MEC testbeds for V2X applications [7]		✓			✓
Car2Car communication using a modulated backscatter and automotive FMCW radar [8]		✓			✓
PC5-based cellular-V2X evolution and deployment [9]		✓		✓	
Five-layered architectures [10]	✓	✓			✓
Three protocols for secure communication in IoV [11]	✓		✓		
In-vehicle network architecture in IoV [12]			✓	✓	

Table 2. *Cont.*

Article	Sa	Ef	Se	En	Co
Seven-layered model architecture [13]	✓		✓		
Secure cloud-assisted connected cars authorization framework [14]	✓	✓	✓		
Security- and privacy-based access control model [15]		✓	✓		
Attack-resistant trust management scheme [16]	✓			✓	
Privacy-preserving dual authentication scheme [17]	✓		✓		
SDN-based data transfer security model [18]		✓	✓		
Advanced secured routing algorithm [19]		✓	✓		
Security and forensics framework [20]			✓		
Vehicular communications expanded-layer architecture [21]			✓		
Learning Internet of Things security "hands-on" [22]	✓	✓			
Cyberthreats facing autonomous and connected vehicles: future challenges [23]	✓	✓			✓
Internet of Things security and privacy, Internet of Things from hype to reality [24]	✓	✓			
The Internet of Automotive Things: vulnerabilities, risks and policy implications [25]	✓	✓			
Botnets and Internet of Things security [26]		✓	✓		
Security and privacy in vehicular communications: challenges and opportunities [27]	✓	✓			
Resource allocation for V2V communication [28].			✓		✓
Securing Internet of Things (IoT) using HoneyPots [29]	✓		✓		
A multilevel DDoS mitigation framework for the industrial Internet of Things [30]			✓	✓	
Automotive industry trends: IoT-connected smart cars and vehicles [31]				✓	
MQTT (MQ telemetry transport) [32]			✓		
Evaluation of publish–subscribe protocols for vehicle communications [33]				✓	
Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP [34]			✓	✓	
Internet of Things (IoT) with CoAP and HTTP protocol: a study on which protocol suits IoT in terms of performance [35]		✓		✓	
Performance evaluation of IoT protocols under a constrained wireless access network [36].		✓	✓	✓	✓
CoAP over SMS: performance evaluation for machine-to-machine communication [37].		✓			
Kaa IoT platform [38]			✓	✓	✓
A security analysis on standard IoT protocols [39]			✓	✓	
Towards efficient mobile M2M communications: survey and open challenges [40]	✓		✓		
Secure gateway—a concept for an in-vehicle IP network bridging the infotainment and the safety-critical domains [41]	✓	✓	✓		✓
A survey of in-vehicle communications: requirements, solutions, and opportunities in IoT [42]	✓		✓		
A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks [43]		✓	✓		✓
Publish–subscribe-enabled software-defined networking for efficient and scalable IoT communications [44]		✓	✓		
The potential security risks and issues of the drone transportation system (DTS) [45]	✓		✓		
Challenges faced in translating wearable data into valuable resources for medical application [46]	✓		✓		

References [21–46] evaluated in the above table, Table 2. Ref. [45] discusses the potential security risks and issues of the drone transportation system (DTS) in disrupting legacy aerial intelligent transport systems (AITSs) in smart cities, and evaluates the implementation of AI-based counter-invasive models for secure DTS smart city mobility. It also explores the alignment of emerging security architectures with DTS network technologies and the role of aviation policies in ensuring secure smart mobility through DTS. The paper provides research directions and recommendations for sustainable DTS in conjunction with AITS for trustworthy and secure airspace operations. The Ref. [46] reviews the performance of wearable devices in healthcare delivery and identifies key performance indicators (KPIs) in relation to evolving generation networks. It discusses the challenges faced in translating wearable data into valuable resources for medical application and provides insights on aligning these devices with the emerging B5G network.

The integration of 5G technology and edge computing has introduced significant advancements in the realm of vehicular communication security, particularly in the context of vehicle-to-vehicle (V2V) networks. The emergence of 5G networks offers enhanced connectivity, reduced latency, and increased bandwidth, thereby facilitating seamless and efficient communication among vehicles. Moreover, the deployment of edge computing infrastructure brings computation and data storage capabilities closer to the network edge, enabling faster processing of data and real-time decision-making. These developments have profound implications for V2V security by enabling more robust and responsive security protocols. With 5G's low-latency communication and edge computing's distributed architecture, V2V security mechanisms can be implemented closer to the source of data transmission, reducing vulnerabilities associated with data transfer delays and centralized processing. Additionally, the increased network capacity and bandwidth afforded by 5G networks allow for the implementation of more sophisticated encryption algorithms and intrusion detection systems, further bolstering V2V security. Overall, the integration of 5G and edge computing technologies represents a significant advancement in V2V security, offering enhanced protection against cyberthreats and vulnerabilities in vehicular communication networks.

The integration of vehicle-to-vehicle (V2V) communication protocols within larger Internet of Things (IoT) frameworks and protocols presents an opportunity for a more comprehensive understanding of vehicular communication systems. By aligning V2V protocols with broader IoT standards, such as those governing data transmission, security, and interoperability, a more cohesive and interoperable vehicular communication ecosystem can be established. Standardization efforts aimed at harmonizing V2V protocols with overarching IoT frameworks have been instrumental in promoting uniformity and compatibility across diverse vehicular networks. However, challenges related to interoperability persist, as varying proprietary protocols and technologies hinder seamless communication between different vehicular platforms. Addressing these interoperability issues requires concerted efforts from industry stakeholders and regulatory bodies to develop common standards and protocols that facilitate seamless integration and interoperability across V2V communication networks. Moreover, ongoing research and development initiatives focused on enhancing the compatibility and interoperability of V2V protocols within broader IoT frameworks are essential for realizing the full potential of connected and autonomous vehicles in modern transportation systems.

The existence of established or proposed standards plays a crucial role in shaping the adoption of secure vehicle-to-vehicle (V2V) communication systems. These standards provide a framework for interoperability, security, and overall system reliability, thereby influencing the development and deployment of V2V technologies. Existing standards, such as those defined by organizations like the Institute of Electrical and Electronics Engineers (IEEE) and the Society of Automotive Engineers (SAE), offer guidelines for V2V communication protocols, security mechanisms, and data formats. Adherence to these standards ensures compatibility and consistency across different V2V implementations, facilitating widespread adoption and interoperability among vehicles from various manufacturers.

Furthermore, proposed standards aimed at addressing emerging security challenges, such as those related to encryption, authentication, and intrusion detection, have significant implications for the future adoption of secure V2V communication systems. By establishing standardized protocols and practices for securing V2V communication, these initiatives pave the way for enhanced trust, reliability, and security in vehicular networks, ultimately accelerating the adoption of V2V technologies in real-world applications.

As shown in Figure 2, 38% of the articles surveyed deal with proposals for techniques and architectures, 15% with frameworks, and 8% with protocols.

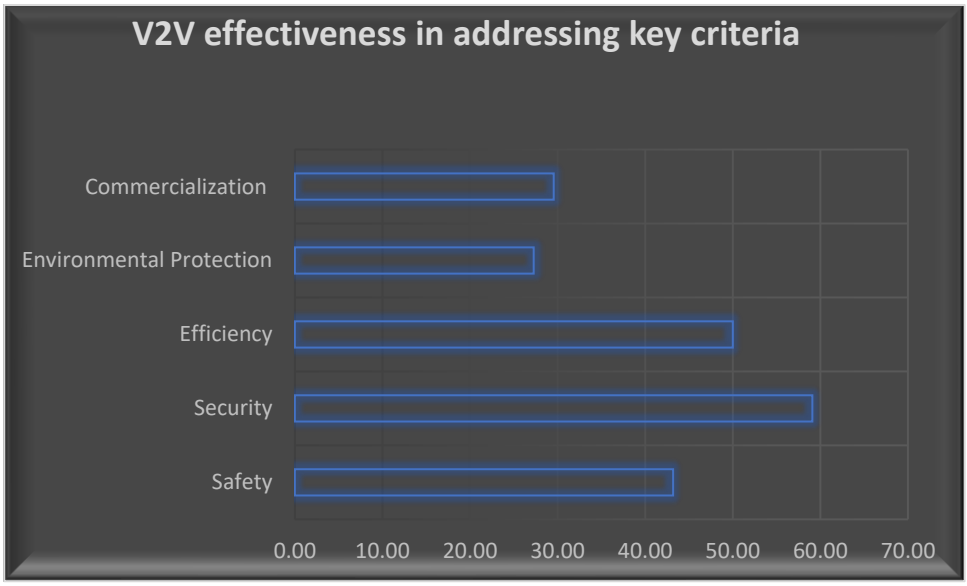

Figure 2. V2V communication based on the five basic criteria.

Moreover, Figure 3 shows the number of articles dealing with attacks related to the Internet of Vehicles, according to the data in Table 3.

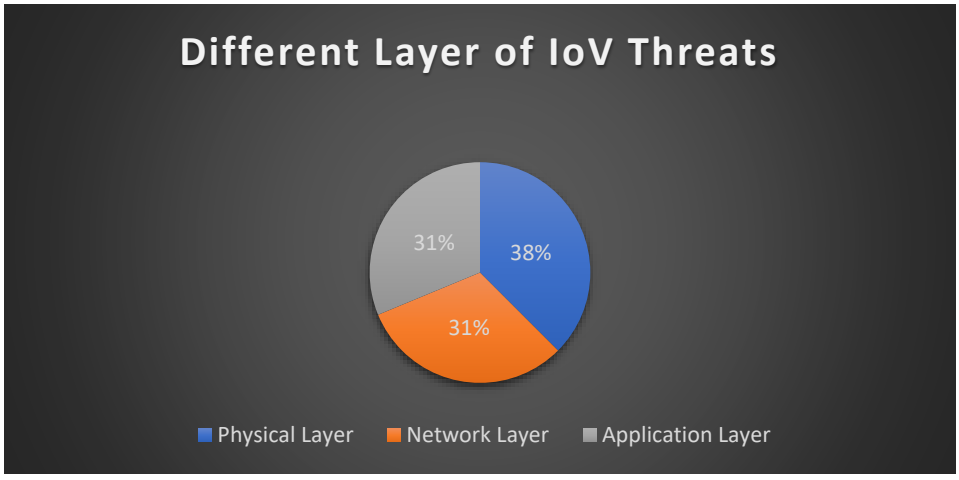

Figure 3. Papers that discuss attacks to IoV.

This study compares IoT and V2V communication protocols, highlighting similarities and differences, and performs a comparative analysis considering parameters such as message size, latency, energy consumption, and bandwidth consumption. The study aims to contribute to the development of more secure and reliable V2V communication systems, propelling the advancement of intelligent transportation technology. Table 1 summarizes the key findings and implications of the analysis of vehicular communication security

protocols. It provides insights into the effectiveness of these protocols in addressing criteria such as safety, security, efficiency, environmental protection, and commercialization. Table 1 presents objective results and highlights the contributions of research in investigating security risks inherent in V2X communication and developing information security testing and verification platforms. Table 2 emphasizes the multidimensional approach required for the development of secure V2V communication protocols. It considers factors such as safety, security, efficiency, environmental protection, and commercialization. The table likely presents a comparison or analysis of different protocols based on these dimensions, providing a comprehensive understanding of the requirements for creating a safer and more connected transportation landscape.

Table 3. Different kinds of threats and attacks related to IoV in different layers of communication protocol.

Article#	Threats/Attack	Physical Communication Layer	Network Communication Layer	Application Communication Layer
[A-1]	Sybil	Yes	Yes	Yes
[A-2]	Eavesdropping	Yes	No	No
[A-3]	Denial of service (DOS)	Yes	Yes	Yes
[A-4]	Node tampering	Yes	No	No
[A-5]	Malware	No	No	Yes
[A-6]	Jamming	Yes	No	No
[A-7]	Black holes	No	Yes	No
[A-8]	Replay	Yes	Yes	Yes
[A-9]	GPS spoofing	No	No	Yes
[A-10]	Wormhole	No	Yes	No

5. Conclusions

In conclusion, ensuring the secure transmission and protection of data in V2V communication networks is critical to ensuring the integrity, privacy, and reliability of the information exchanged. To understand the requirements for secure V2V communications, this paper examined the latest solutions for vehicular communications security and identified their key challenges. The latest advances, security protocols, and frameworks that address the vulnerabilities and risks associated with V2X networks were identified.

The security techniques that can be used in vehicle-to-vehicle (V2V) communications, including cryptographic approaches such as asymmetric key infrastructure and elliptic curve cryptography, play a critical role in secure vehicle-to-vehicle communications. These techniques provide a solid foundation for the secure, reliable and scalable exchange of data and information between vehicles. In addition, protocols such as enhanced secure ad hoc on-demand distance vector (ES-AODV) routing improve the security of data transmission and ensure the integrity of safety-critical information. In addition, a software-defined networking (SDN)-based security model for data transmission can further support secure and efficient V2V communication, while the proposed Internet of Connected Vehicles (IoCV) architecture promotes environmental protection.

Overall, there is a need for further research in areas such as (1) the impact of advances in autonomous vehicle technology on safety, (2) the safety of autonomous driving vehicles when operating on public roads, (3) the use of machine learning and artificial intelligence techniques to improve road safety and the security of autonomous vehicles and their communications, (4) real-time anomaly detection and resilience to sophisticated attacks, and (5) improving safe traffic flow and minimizing unnecessary stops.

In summary, the literature review has provided a comprehensive overview of research efforts and advances in the field of vehicular communication security. The main objectives of this review were to identify existing security protocols, analyze their strengths and weaknesses, investigate the integration of emerging technologies such as 5G and edge computing, examine the interface of V2V communication protocols with larger IoT frameworks,

and assess the impact of existing or proposed standards on the deployment of secure V2V communication systems. The approach included examining a variety of scientific articles, studies, and proposals to gain insight into the current state of V2V security protocols and potential opportunities for improvement. By synthesizing this information, the review aims to reinforce the importance of robust security measures in V2V communication systems and provide guidance for future research and development efforts to improve the security and reliability of vehicle networks.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares that there is no conflict of interest.

References

1. Ioana, A.; Korodi, A.; Silea, I. Automotive IoT Ethernet-Based Communication Technologies Applied in a V2X Context via a Multi-Protocol Gateway. *Sensors* **2022**, *22*, 6382. [CrossRef]
2. He, K.; Li, B. Automotive V2X Communication Security Key Technology and Test Method Research. In Proceedings of the 2022 7th International Conference on Cyber Security and Information Engineering (ICCSIE), Brisbane, QLD, Australia, 23–25 September 2022; IEEE: Piscataway, NJ, USA, 2022.
3. Hakeem, S.A.A.; El-Gawad, M.A.A.; Kim, H. Comparative Experiments of V2X Security Protocol Based on Hash Chain Cryptography. *Sensors* **2020**, *20*, 5719. [CrossRef]
4. Limbasiya, T.; Das, D. Lightweight Secure Message Broadcasting Protocol for Vehicle-to-Vehicle Communication. *IEEE Syst. J.* **2020**, *14*, 520–529. [CrossRef]
5. Haidar, F.; Kaiser, A.; Lonc, B. On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security. In Proceedings of the 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 24–27 September 2017; pp. 1–5. [CrossRef]
6. Wadatkar, P.V.; Garroppo, R.G.; Nencioni, G. 5G-MEC Testbeds for V2X Applications. *Future Internet* **2023**, *15*, 175. [CrossRef]
7. Lazaro, A.; Lazaro, M.; Villarino, R.; Girbau, D.; de Paco, P. Car2Car Communication Using a Modulated Backscatter and Automotive FMCW Radar. *Sensors* **2021**, *21*, 3656. [CrossRef] [PubMed]
8. Miao, L.; Virtusio, J.J.; Hua, K.-L. PC5-Based Cellular-V2X Evolution and Deployment. *Sensors* **2021**, *21*, 843. [CrossRef]
9. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.T.; Liu, X. Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects. Special Section on Future Networks: Architectures, Protocols, and Applications. *IEEE Access* **2016**, *4*, 5356–5373. [CrossRef]
10. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. *IEEE Internet Things J.* **2018**, *5*, 3701–3709. [CrossRef]
11. Eiza, M.H.; Ni, Q. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security. *IEEE Veh. Technol. Mag.* **2017**, *12*, 45–51. [CrossRef]
12. Contreras-Castillo, J.; Zeadally, S.; Guerrero Ibáñez, J.A. A seven-layered model architecture for Internet of Vehicles. *J. Inf. Telecommun.* **2017**, *1*, 4–22. [CrossRef]
13. Gupta, M.; Sandhu, R. Authorization Framework for Secure Cloud Assisted Connected Cars and Vehicular Internet of Things. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies (SACMAT '18), Indianapolis, IN, USA, 13–15 June 2018.
14. Habib, M.A.; Ahmad, M.; Jabbar, S.; Khalid, S.; Chaudhry, J.; Saleem, K.; Rodrigues, J.J.C.; Khalil, M.S. Security and privacy based access control model for internet of connected vehicles. *Future Gener. Comput. Syst.* **2019**, *97*, 687–696. [CrossRef]
15. Li, W.; Song, H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 960–969. [CrossRef]
16. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
17. Liu, Y.; Kuang, Y.; Xiao, Y.; Xu, G. SDN-Based Data Transfer Security for Internet of Things. *IEEE Internet Things* **2018**, *5*, 257–268. [CrossRef]
18. Tyagi, P.; Dembla, D. Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network. *Wirel. Pers. Commun.* **2018**, *102*, 41–60. [CrossRef]
19. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. *Future Gener. Comput. Syst.* **2019**, *78*, 544–546. [CrossRef]
20. Nanda, A.; Puthal, D.; Rodrigues, J.J.; Kozlov, S.A. Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions. *IEEE Wirel. Commun.* **2019**, *26*, 60–65. [CrossRef]

21. Ajakwe, S.O.; Nwakanma, C.I.; Kim, D.S.; Lee, J.M. Key Wearable Device Technologies Parameters for Innovative Healthcare Delivery in B5G Network: A Review. *IEEE Access* **2022**, *10*, 49956–49974. [CrossRef]
22. Voas, J.; Bojanova, I.; Kuhn, R.; Kolias, C.; Stavrou, A. Learning Internet of Things Security 'Hands-On'. *IEEE Secur. Priv.* **2016**, *14*, 37–46.
23. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
24. Dabbagh, M.; Rayes, A. Internet of Things Security and Privacy. *Internet Things Hype Real.* **2017**, 195–223. [CrossRef]
25. Bryans, J.W. The Internet of Automotive Things: Vulnerabilities, risks and policy implications. *J. Cyber Policy* **2017**, *2*, 185–194. [CrossRef]
26. Bertino, E.; Islam, N. Botnets and Internet of Things Security. *Computer* **2017**, *50*, 76–79. [CrossRef]
27. Bernardini, C.; Asghar, M.R.; Crispo, B. Security and privacy in vehicular communications: Challenges and opportunities. *Veh. Commun.* **2017**, *10*, 13–28. [CrossRef]
28. Xu, C.; Wang, S.; Song, P.; Li, K.; Song, T. Intelligent Resource Allocation for V2V Communication with Spectrum–Energy Efficiency Maximization. *Sensors* **2023**, *23*, 6796. [CrossRef]
29. Gadde, S.S.; Ganta, R.K.S.; Gopala Gupta Asalg, R.R.K.; Mohan Rao, K.R.R. Securing Internet of Things (IoT) Using HoneyPots. *Int. J. Eng. Technol.* **2018**, *7*, 820–824. [CrossRef]
30. Yan, Q.; Huang, W.; Luo, X.; Gong, Q.; Yu, F.R. A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things. *IEEE Commun. Mag.* **2018**, *56*, 30–36. [CrossRef]
31. Meola, A. Automotive Industry Trends: IoT Connected Smart Cars & Vehicles. *Bus. Insid.* **2016**.
32. Rouse, M.; MQTT (MQ Telemetry Transport). TechTarget. 16 March 2018. Available online: https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport (accessed on 24 October 2023).
33. Strihagen, K. Evaluation of Publish—Subscribe Protocols for Vehicle Communications. 21 June 2017. Available online: https://pdfs.semanticscholar.org/be4e/c6fe98b8c8a800fbd3f3b5af9e34daf39f64.pdf (accessed on 24 October 2023).
34. Naik, N. Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP. 30 October 2017. Available online: https://ieeexplore.ieee.org/document/8088251 (accessed on 24 October 2023).
35. Daud, M.A. Internet of Things (IoT) with CoAP and HTTP Protocol: A Study on Which Protocol Suits IoT in Terms of Performance. International Conference on Computational Intelligence in Information System. 21 October 2016. Available online: https://link.springer.com/chapter/10.1007/978-3-319-48517-1_15 (accessed on 24 October 2023).
36. Chang, Y.; Kunz, T. Performance Evaluation of IoT Protocols under a Constrained Wireless Access Network. In Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT), Cairo, Egypt, 11 April 2016; pp. 1–7. Available online: https://ieeexplore.ieee.org/document/7496622 (accessed on 24 October 2023).
37. Gligoric, N. CoAP over SMS: Performance Evaluation for Machine to Machine Communication. In Proceedings of the 2012 20th Telecommunications Forum (TELFOR), Belgrade, Serbia, 14 November 2012; pp. 1–4.
38. Technology, G. Kaa IoT Platform. 23 July 2016. Available online: https://www.kaaproject.org/automotive (accessed on 24 October 2023).
39. Zamfir, S.; Balan, T.; Iliescu, I.; Sandu, F. A security analysis on standard IoT protocols. In Proceedings of the 2016 International Conference on Applied and Theoretical Electricity (ICATE), Craiova, Romania, 6–8 October 2016; pp. 1–6. [CrossRef]
40. Pereira, C.; Aguiar, A. Towards Efficient Mobile M2M Communications: Survey and Open Challenges. *Sensors* **2014**, *14*, 19582–19608. [CrossRef] [PubMed]
41. Berg, J. Secure Gateway—A Concept for an in-Vehicle IP Network Bridging the Infotainment and the Safety Critical Domains. 2015. Available online: https://www.semanticscholar.org/paper/Secure-Gateway-%E2%80%93-A-concept-for-an-in-vehicle-IP-the-Berg-Pommer/485ff149d68d738505e11995e688752661dbcd0d (accessed on 24 October 2023).
42. Huo, Y.; Tu, W.; Sheng, Z.; Leung, V.C.M. A survey of in-vehicle communications: Requirements, solutions and opportunities in IoT. In Proceedings of the 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Italy, 14–16 December 2015; pp. 132–137. [CrossRef]
43. Luzuriaga, J.E.; Perez, M.; Boronat, P.; Cano, J.C.; Calafate, C.; Manzoni, P. A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks. In Proceedings of the 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015; pp. 931–936. [CrossRef]
44. Hakiri, A.; Berthou, P.; Gokhale, A.; Abdellatif, S. Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications. *IEEE Commun. Mag.* **2015**, *53*, 48–54. [CrossRef]
45. Chatzoulis, D.; Chaikalis, C.; Kosmanos, D.; Anagnostou, K.E.; Xenakis, A. 3GPP 5G V2X Error Correction Coding for Various Propagation Environments: A QoS Approach. *Electronics* **2023**, *12*, 2898. [CrossRef]
46. Ajakwe, S.O.; Kim, D.S.; Lee, J.M. Drone Transportation System: Systematic Review of Security Dynamics for Smart Mobility. *IEEE Internet Things J.* **2023**, *10*, 14462–14482. [CrossRef]