Article

Not peer-reviewed version

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

Muhana Magboul Ali Muslam *

Posted Date: 7 September 2023

doi: 10.20944/preprints202309.0430.v1

Keywords: Vehicle-to-Vehicle (V2V) Communication; Vehicular Ad-Hoc Networks (VANETs); Internet of Things (IoT); Internet of Vehicle (IoV); Communication Protocols; Security Protocols; Intrusion Detection Systems; Safety and Security; Efficiency in V2V Communication

Review

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

Muhana Magboul Ali Muslam

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

Abstract: Vehicle-to-Vehicle (V2V) communication plays 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 paper focuses on investigating the security protocols employed in Vehicle-to-Vehicle communication systems. A comprehensive review and analysis of relevant literature and research papers is conducted to gather information on existing V2V communication security protocols and techniques. The analysis encompasses 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 delves into the challenges and limitations associated with implementing these protocols. Moreover, to foster a deeper understanding, the paper investigates present communication protocols in the field of Internet of Things (IoT) that are tailored for V2V. Various parameters, such as bandwidth consumption, energy consumption, latency, and message size, are considered during the evaluation of these protocols to gauge their effectiveness. The research outcomes aim to provide a comprehensive understanding of the strengths and weaknesses of the current V2V communication security protocols. Furthermore, based on the findings, this paper will propose improvements and recommendations to enhance the security measures of the V2V communication protocol. Ultimately, this research will contribute to the development of more secure and reliable V2V communication systems, propelling the advancement of intelligent transportation technology.

Keywords: vehicle-to-vehicle (V2V) communication; vehicular Ad-Hoc networks (VANETs); internet of things (IoT); internet of vehicle (IoV); communication protocols; security protocols; intrusion detection systems; safety and security; efficiency in V2V communication

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. The introduction of the Internet in the 1980s 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). Currently, 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 paved the way for 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.

 doi:10.20944/preprints202309.0430.v1

A multi-protocol gateway solution was proposed for efficient data exchange between entities with different technological origins. It examines the compatibility and real-time responsiveness capabilities of various IoT Ethernet-based communication technologies, including Scalable Service-Oriented Middleware over IP (SOME/IP), Data Distribution Service (DDS), and enhanced Communication Abstraction Layer (eCAL) middleware. The hardware architecture used in their simulation is also discussed, which includes microprocessors with native POSIX-based operating systems for most nodes and a Linux OS (virtual) on a general-purpose computer for simulated interaction with an IoT supervisor node. The transmitted data are structured under the form of a heartbeat cyclic event. [27].

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 is transmitted to other devices, where it is 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.

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 include 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.

Investigates the development of secure key technologies and proposes test methodologies for assessing the security of V2X communication systems [1]. Conducted comparative experiments to evaluate the efficiency and effectiveness of V2X security protocols based on hash chain cryptography [2]. Introduces a lightweight secure message broadcasting protocol specifically designed for V2V communication [3]. 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 [4].

Internet of Vehicles consists of various vehicular networks such as vehicle to vehicle, vehicle to roadside infrastructure, vehicle to human, vehicle to devices, vehicle to sensors, and vehicle to mobile networks as shown in Figure 1. In [9] a detailed framework has proposed which includes network models, protocols, and architectures. This proposed solution has an architecture which consists of a perception layer, coordination layer, application layer, artificial intelligence layer, and business layer. Sensors and actuators are included in the perception layer while coordination layer has 4G and Wi-Fi. Application layer mentions about various applications such as web based, and multimedia applications. In business layer, business strategies are developed which is based on application usage. Artificial intelligence layer talks about cloud infrastructure.

[19] Presents the opportunities and challenges of security and forensics in relation to the Internet of Things (IoT). IoT devices are often targeted for attacks due to their inherent features such as low power consumption and open connectivity. This article addresses security challenges including authentication, access controls, authorization, privacy, and architecture. The absence of a key management and deployment system poses a challenge for authentication. Proper verification and privileges are necessary for authorization to function effectively. Given that the collection of private and confidential data is the purpose

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

of IoT objects, protecting privacy becomes a top priority. A security architecture must be developed to identify and prevent malicious attacks from disrupting IoT networks. Therefore, secure protocols must be implemented.

Vehicular Ad-Hoc Networks (VANETs) are based on a layered architecture that comprises the sensing layer, network layer, and application layer [20] The sensing layer, located at the bottom of the architecture, records information about environmental changes using sensors, including NFC, RFID, and wireless sensor networks. The network layer focuses on maintaining secure communication channels between IoT objects, utilizing technologies such as Bluetooth, 4G, and Wi-Fi. Meanwhile, the application layer transmits data received from sensors, processes it, and stores it accordingly.

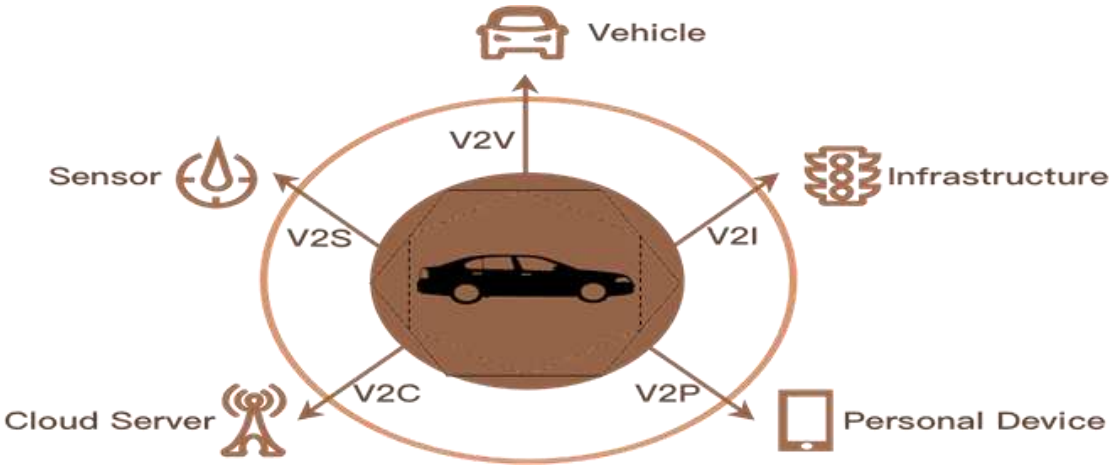

Figure 1. Internet of Vehicle Communication.

[10] have introduced a communication protocol for Internet of Connected Vehicles. Seamless and secure communication between vehicles is a mandatory requirement when it comes to vehicular ad-hoc networks. Industry standards that have been imposed for IoV will be analysed along with benefits of IoV. IoV facilitates intelligent transport systems where passengers and goods transport will be able to gain benefits. Authors have proposed a new architecture which will consist of 7 layers. Those layers are named as data communication layer, acquisition layer, processing layer, data filtering layer, security layer, user-vehicle interface layer, control layer. These layers will provide a comprehensive mechanism in protecting IoV. According to [11] connected vehicles are prone to various system exploits such as engine shutdowns, door locking and brake disabling. These are identified as threats and occur as a part of cyber-attacks focusing on autonomous connected vehicles. Analyses different types of cyber security threats aiming to malfunction vehicles. Some of the attacks identified are DDoS, malware, faults in onboard diagnostic units, and mobile application hacking. Structure of a connected vehicle is designed with components such as Electronic Control Unit (ECU), Control Area Network (CAN), Onboard Diagnostic Ports (ODP). As the vehicular networks are open to outside world, it's susceptible to OBD attacks where attacker tries to take control of the vehicle through injection of malicious codes into vehicle software.

This framework consists of layered architecture, interaction model, network model, and environmental model. Each model has its own features. Network model focuses on multi network, multi-user, multi-technology, multi device and multi communication methods, Interaction model explains about the relationship between vehicles, network, personal devices, sensors, roadside architecture, and humans. Environmental model is mainly about vehicle communication with other networks outside its perimeter [12] Proposed an architecture for authorization purposes to secure Internet of Connected Vehicles. This is called extended access control-oriented architecture. E-ACO is dependent on cloud computing functionalities. There are various access control model approaches introduced that can be deployed at different levels of E-ACO. Access controls prevent unauthorized access to a system. Clustered elements such as connected cars, traffic lights, devices with sensors can interact with other sensors in the same clustered elements or different elements. As explained, there are four layers in this architecture which are cloud services layer, object layer, application layer, and virtual object layer [13]. By deploying an access

 doi:10.20944/preprints202309.0430.v1

control mode into Internet of Connected Vehicles (IoCV), secure and privacy enabled data communication can be achieved. This access control model will provide permissions to security officials in different levels to access communication embedded in vehicles. These security layers will ensure that sensitive information is not disclosed from upper security levels to lower security levels. “Security and privacy-based access control model” which is derived from mathematical models will allocate permissions and roles to security officials who are traveling in IoCV. It will facilitate secure communication through 4G and Wi-Fi. Mutually exclusive permissions and dynamic separation of duties are key components of this model [14]. Attack resistant trust (ART) management system has been introduced by [15]. in their research article. This system will facilitate in protecting the ad-hoc network where the Internet of Vehicles are connected to. The objective of this mechanism is to detect malicious nodes connected in the network and prevent attacks from interrupting the network and connected vehicles. This mechanism will ensure that the data transferred over the VANET, and mobile network are legitimate after evaluating and verifying the data. There are two models namely, network model and adversary model are introduced by the authors. Network model refers to wireless networks with computational devices and sensors installed. Adversary model evaluates different types of attacks by external entities such as bad mouth attack, simple attack, and zig zag attacks.

A dual authentication system [16] that is based on a redesigned trusted platform module can be considered as a good solution for improving security, privacy, and efficiency of the Internet of Vehicles. Cryptography based, reputation evaluation based, and hardware-based authentications mechanisms are considered traditional and do not provide solutions completely due to inherent limitations. Once Privacy preserving dual authentication system is implemented in the vehicle, OBU will generate a temporary encrypted key which will authenticate a session. Also, vehicle will be verified by trust authority that it is legitimate using the reputation history. Once these two are achieved, communication session will be established. Software defined networks (SDN) plays a major role by providing a software layer into the IoT in order to simplify and evolve the networks [17]. have proposed an SDN based data transfer security model for securing the communication between IoT vehicles. SDNs are deployed in IoT sector with the aim of achieving various tasks in wireless networks. This model consists of a middle box guard (MBG) which will enhance the security by implementing policies based on algorithms like data flow abstraction and heuristic. An integer linear programming (LP) algorithm is used to ensure that middle box is well secure from being a hotspot and vulnerable to attacks. Also, another algorithm will handle the load balance.

Enhanced Secure Ad-hoc On-Demand Distance Vector (ES-AODV) Routing is a protocol introduced by [18] to detect malicious nodes and mitigate attacks. This helps the network by assisting in transmitting data securely in VANETs. This protocol uses an algorithm which is based on asymmetric key infrastructure (public-private key) combined with elliptic curve cryptography (ECC). A key will be generated by ECC, and certificate authority will verify the vehicle based on the key. It is a modification to the existing AODV protocol code.

3. Methodology

To investigate the security protocols employed in Vehicle-to-Vehicle (V2V) communication systems, a comprehensive literature review and analysis were conducted. The methodology outlined below describes the process used to gather relevant information, select research papers, and analyze the identified protocols.

3.1. Data Collection:

3.1.1. Literature Search:

A systematic search was performed across reputable academic databases, including IEEE Xplore, ACM Digital Library, and Google Scholar. Keywords such as "V2V communication security," "vehicular security protocols," and "IoT security in transportation" were used to identify relevant research articles, conference papers, and scholarly publications.

3.1.2. Source Selection:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

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 selected research papers were categorized based on the key areas identified in the abstract: authentication mechanisms, encryption algorithms, key management protocols, and intrusion detection systems.

3.2.2. Thematic Analysis:

A thematic analysis approach was employed to extract key concepts, methodologies, and findings from each paper. The analysis focused on understanding the security protocols' design principles, functionalities, and their effectiveness in 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 Internet of Things (IoT). A comparative analysis was performed to highlight the similarities and differences between IoT and V2V communication protocols, considering parameters such as bandwidth consumption, energy consumption, latency, and message size.

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.

Table 1. The table summarizes the 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 risks faced by V2X communication security, aims to build an information security testing and verification platform with independent property rights for car-vehicle, car-person, car-road, car-cloud, and other scenarios.
Hash chain cryptography [2]	Security	Proposes a light-weight message authentication and privacy preservation protocol for V2X communications based on hash chain cryptography. This protocol reduces the communication overhead by 4 times and the computation overhead by up to 100 times compared with a non-standard security protocol, TESLA.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

Technique	Objective	Results
Lightweight secure one-way hash function to send valuable information at the receiver side quickly [3]	Security	An efficient and secure V2V data transmission protocol using a one-way hash function to send valuable information at the receiver side quickly. It resists various security attacks, i.e., modification, impersonation, replay, man-in-the-middle, stolen on-board-unit, password guessing, and concatenation.
A vehicular Public Key Infrastructure (PKI) protocol for V2X communications security. [4]	Security	Evaluates the performance of a vehicular Public Key Infrastructure (PKI) protocol for V2X communications security by comparing two communication profiles with and without V2X security. The results show that skipping security provides better performance but still requires at least half a second, which is non-negligible in highly mobile networks.
Quality of Service (QoS) in a Vehicle-to-everything (V2X) communication environment [5]	Safety, Environment Protection	The analysis shows that turbo-based coding schemes satisfy all the QoS parameters and achieve overall communication quality comparable to polar and better than LDPC, making them suitable for small-frame 5G V2X services.
5G-MEC testbed for Vehicle-to-Everything (V2X) applications [6]	Safety, Environment Protection	Overview of implementing a 5G-MEC testbed for V2X applications, analyzes some important testbeds and state-of-the-art implementations, and discusses the challenges researchers may face while replicating and deploying the testbeds.
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	The detection rate of the transponder is 97.42%, and the average error in the measured modulation frequency is 0.5%.
The role of 5G NR (New Radio) deployment in the evolution of C-V2X [8]	Efficiency, Security	PC5-based C-V2X has better performance than the Rel-14 standard 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	Provide secure alternate routing if the IoV current communication route is compromised
In-Vehicle network architecture in IoV [11]	Security	Secure over the air update for software fixes, firmware upgrades, and security patches in IoV, cloud based secure storage for IoV
Seven layered model architecture [12]	Security	Increase security, reduce incompatibility among the devices, limited processing, and storage capabilities
Secure Cloud Assisted Connected Cars Authorization Framework [13]	Security	Provide extended access control to different layers in IoV (Application layer, Object layer, Cloud services layer, Virtual Object layer) with the use of vehicular cloud
Security and privacy-based access control model [14]	Security	Application of Mutually Exclusive Permissions and Dynamic Separation of Duties as a replacement for positions and storing the objects in a tree structured directory in IoCV

 doi:10.20944/preprints202309.0430.v1

Technique	Objective	Results
Attack-Resistant Trust Management Scheme [15]	Safety, Environment Protection	Identify and counterattack malicious threats and evaluating the trustworthiness of mobile nodes and data in VANETs
Privacy-Preserving Dual Authentication Scheme [16]	Security	Introduction of trust evaluation into IoV authentication protocol, a temporary encrypted key is generated utilizing bilinear pair theory
SDN-Based Data Transfer Security Model [17]	Efficiency, Security	Handle different attacks such as spoofing and flooding via protocols based on tags and tunnels
Advanced Secured Routing Algorithm [18]	Efficiency, Security	Identify malicious codes, preventing blackhole attacks and providing secured data transmission in VANET
Security and Forensics framework [19]	Security	Explanation of existing major security and forensics challenges within IoT domain relating to vehicles
Vehicular Communications Expanded Layer Architecture [20]	Security	Identification of intra and inter vehicle security threats

4. Analysis

Following the methodology, the next section would present the analysis of the collected data based on the thematic areas and comparisons you've outlined. 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 see table 1. This section presents the findings and analysis of each criterion:

4.1. Safety:

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.

4.2. Security:

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.

4.3. 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 Networks (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.

4.4. Environmental Protection:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

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 environmental 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.

4.5. 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. The table summarizes the 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
Risks faced by V2X communication security [1]	✓		✓		✓
Experiments to evaluate the efficiency and effectiveness of V2X security protocols based on hash chain cryptography [2]		✓		✓	
A lightweight secure message broadcasting protocol specifically designed for V2V communication [3]		✓			✓
Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security [4].	✓				✓
Error Correction Coding for Various Propagation Environments [5].	✓				✓
5G-MEC Testbeds for V2X Applications [6].		✓			✓
Car2Car Communication Using a Modulated Backscatter and Automotive FMCW Radar [7].		✓			✓
PC5-Based Cellular-V2X Evolution and Deployment [8].		✓		✓	
Five layered architectures [9]	✓	✓			✓
Three protocols for secure communication in IoV [10]	✓		✓		
In-Vehicle network architecture in IoV [11]			✓	✓	
Seven layered model architecture [12]	✓		✓		
Secure Cloud Assisted Connected Cars Authorization Framework [13]	✓	✓	✓		
Security and privacy-based access control model [14]		✓	✓		

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

Article	Sa	Ef	Se	En	Co
Attack-Resistant Trust Management Scheme [15]	✓			✓	
Privacy-Preserving Dual Authentication Scheme [16]	✓		✓		
SDN-Based Data Transfer Security Model [17]		✓	✓		
Advanced Secured Routing Algorithm [18]		✓	✓		
Security and Forensics framework [19]			✓		
Vehicular Communications Expanded Layer Architecture [20]			✓		
Learning Internet of Things Security 'Hands-On' [21]	✓	✓			
Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges [22]	✓	✓			✓
Internet of Things Security and Privacy, Internet of Things From Hype to Reality [23]	✓	✓			
The Internet of Automotive Things: vulnerabilities, risks and policy implications [24]	✓	✓			
Botnets and Internet of Things Security [25]		✓	✓		
Security and privacy in vehicular communications: Challenges and opportunities [26]	✓	✓			
Automotive IoT Ethernet-Based Communication Technologies [27]	✓			✓	
Resource Allocation for V2V Communication [28].			✓		✓
Securing Internet of Things (IoT) Using HoneyPots [29]	✓		✓		
A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things [30]			✓	✓	
Automotive Industry Trends: IoT Connected Smart Cars & 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]		✓	✓		

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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

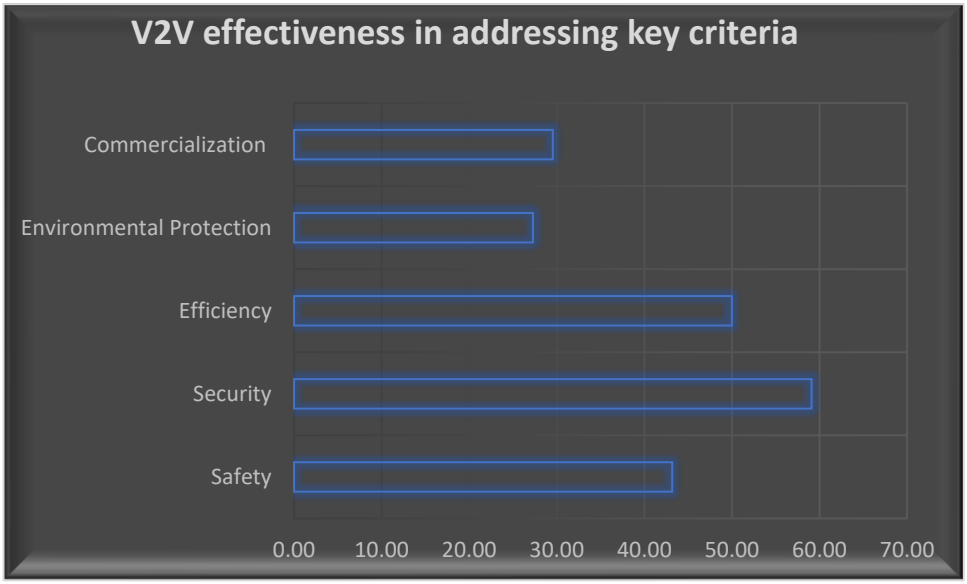

Figure 2. v2v communication based on the five basic criteria.

Moreover, Figure 3 shows the number of articles dealing with attacks on the Internet of Vehicles (IoV).

Table 3. Types of Attacks to IoV Layer wise.

Article	Attack	Physical Layer	Network Layer	Application Layer
1	Sybil Attack	✓	✓	✓
2	Eavesdropping Attack	✓		
3	Denial of service	✓	✓	✓
4	Node Tempering	✓		
5	Malware attack			✓
6	Jamming	✓		
7	Black holes		✓	
8	Replay attack	✓	✓	✓
9	GPS Spoofing			✓
10	Wormhole attack		✓	

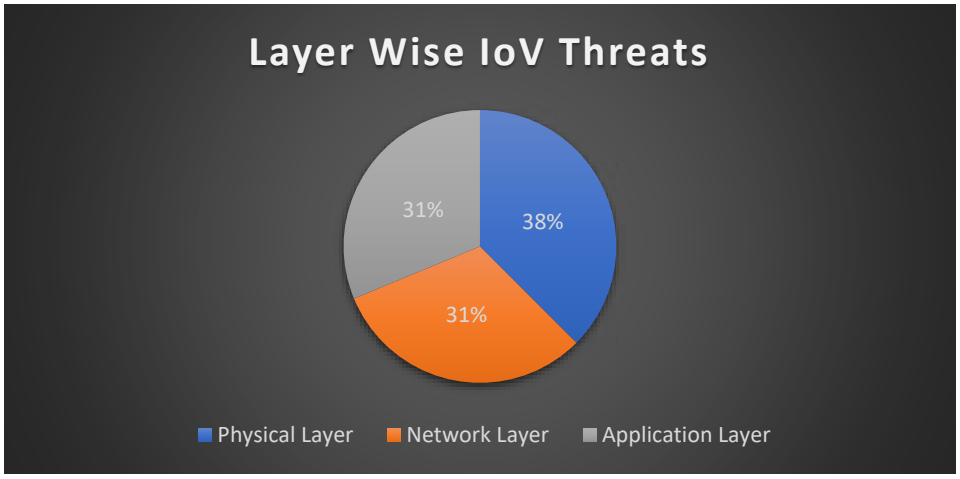

Figure 3. No. of Papers that discuss attacks to IoV.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

5. IoV Communication Protocol:

There are several lightweight protocols specifically designed for IoT (Internet of Things) applications. Here are some popular ones. This section focuses on highlighting the features of the protocols (MQTT, CoAP, AMQP, LwM2M and XMPP) see table-4. Basically, protocols for constrained devices are focused on this report but some protocols (HTTP) are included which as well is often regarded as the good IoT network protocol.:

MQTT (Message Queuing Telemetry Transport): MQTT is a lightweight publish-subscribe messaging protocol that is widely used in IoT applications. It operates on top of TCP/IP and is designed for constrained devices with low bandwidth and high-latency networks.

CoAP (Constrained Application Protocol): CoAP is a lightweight protocol designed for resource-constrained devices and networks. It is based on the RESTful architecture and operates over UDP or DTLS. CoAP is often used in IoT applications for resource-constrained environments.

AMQP (Advanced Message Queuing Protocol): AMQP is a messaging protocol that is often used in IoT applications for reliable message delivery. It provides a lightweight and efficient way to communicate between devices and back-end systems. AMQP supports both message queuing and publish-subscribe communication patterns.

LwM2M (Lightweight M2M): LwM2M is a protocol specifically designed for managing and monitoring IoT devices. It provides a lightweight and secure way to manage device configuration, firmware updates, and data reporting. LwM2M is built on top of CoAP and uses the OMA (Open Mobile Alliance) DM (Device Management) specification.

XMPP (Extensible Messaging and Presence Protocol): XMPP is an open standard protocol for real-time communication. While it was originally designed for instant messaging, it has been adapted for IoT applications. XMPP is often used for device-to-device communication in IoT systems.

5.1. Comparative Analysis Of Above IoV Communication Protocol:

Relative analysis of MQTT, CoAP, AMQP, LwM2M and XMPP includes the following features:

5.1.1. Message size and Message overhead:

MQTT: MQTT uses a lightweight protocol and has a relatively small message overhead compared to other protocols. The message size is typically small, consisting of a few bytes for the header, topic, and payload.

CoAP: CoAP also has a small message size and overhead. The protocol is designed to be efficient for constrained devices, resulting in lightweight messages. The message size is typically smaller than MQTT, with a similar structure including a header, options, and payload.

AMQP: AMQP supports larger messages and has a more extensive message structure compared to MQTT and CoAP. It provides a rich set of features, resulting in a higher message overhead. The message size can be larger, including properties, headers, and message body.

LwM2M: LwM2M uses CoAP as its underlying protocol, which means it shares similar characteristics in terms of message size and overhead. The message size is relatively small, and the overhead is lightweight, making it suitable for resource-constrained devices.

XMPP: XMPP has a larger message size and overhead compared to MQTT, CoAP, and LwM2M. The protocol includes XML-based message formats, resulting in larger message sizes. XMPP messages contain more metadata and are generally larger in size compared to the other protocols.

5.1.2. Bandwidth consumption and latency:

MQTT: MQTT is known for its efficient use of bandwidth due to its lightweight nature. It minimizes network traffic and reduces bandwidth consumption. MQTT's publish/subscribe model also helps reduce overall latency by enabling efficient message delivery.

CoAP: CoAP is designed to be bandwidth-efficient, similar to MQTT. It uses UDP or UDP-like transport protocols and includes features such as multicast and resource discovery, which help minimize

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

bandwidth consumption. CoAP's request/response model can introduce some latency compared to MQTT's publish/subscribe model.

AMQP: AMQP is more bandwidth-intensive compared to MQTT and CoAP due to its larger message sizes and more complex message structure. It requires more network resources for reliable message delivery, which can increase both bandwidth consumption and latency.

LwM2M: LwM2M, being based on CoAP, inherits its bandwidth efficiency characteristics. It focuses on constrained environments and reduces both bandwidth consumption and latency by keeping message sizes small and optimizing the protocol for resource-constrained devices.

XMPP: XMPP has a higher bandwidth consumption compared to MQTT, CoAP, and LwM2M due to its larger message sizes and the XML-based nature of its protocol. The overhead associated with XML can introduce additional latency and require more network resources.

5.1.3. Power consumption and Resource Requirement:

MQTT: MQTT is designed to be lightweight, making it suitable for devices with limited power and resources. It has low power consumption and can operate efficiently on constrained devices, making it a good choice for VoT applications.

CoAP: CoAP, like MQTT, is designed for constrained environments and has low power consumption. It is optimized for resource-constrained devices, enabling efficient communication with limited power and resources.

AMQP: AMQP is more resource-intensive compared to MQTT and CoAP. It requires more processing power and memory resources due to its complex message structure and additional features. Consequently, it may have higher power consumption and resource requirements.

LwM2M: LwM2M, based on CoAP, shares similar characteristics in terms of power consumption and resource requirements. It is designed to be lightweight and efficient on constrained devices, minimizing power usage and resource demands.

XMPP: XMPP can be more demanding in terms of power consumption and resource requirements compared to MQTT, CoAP, and LwM

5.1.4. Reliability and Interoperability:

MQTT: MQTT is known for its reliable message delivery. It provides quality of service (QoS) levels that allow for guaranteed message delivery, ensuring reliability even in unstable network conditions. MQTT is also highly interoperable, with support for multiple programming languages and a wide range of platforms.

CoAP: CoAP provides reliability through its Confirmable message type, which includes retransmission and acknowledgment mechanisms. It ensures reliable message delivery over unreliable networks. CoAP has good interoperability, with support for different platforms and programming languages, although it may not be as widely adopted as MQTT.

AMQP: AMQP is a highly reliable protocol that ensures message delivery and supports various reliability features such as acknowledgments, error handling, and transaction support. It is designed to be interoperable, enabling communication between different systems and messaging frameworks.

LwM2M: LwM2M, being based on CoAP, inherits the reliability features of CoAP, including Confirmable messages for reliable delivery. It provides mechanisms for handling network disruptions and supports interoperability between LwM2M-enabled devices and platforms.

XMPP: XMPP offers reliable message delivery through its acknowledgment mechanism, ensuring messages are successfully delivered. It supports a wide range of interoperable clients and servers, making it highly interoperable in the context of instant messaging and presence applications.

5.1.5. Security:

MQTT: MQTT supports security measures such as authentication, encryption (TLS/SSL), and access control mechanisms. It provides a lightweight security framework to protect the confidentiality and

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 7 September 2023 doi:10.20944/preprints202309.0430.v1

integrity of the messages being exchanged. However, the level of security implementation may vary across different MQTT brokers.

CoAP: CoAP provides security through Datagram Transport Layer Security (DTLS) protocol, which ensures secure communication over UDP. It offers authentication, encryption, and integrity protection. However, the security features in CoAP are more limited compared to MQTT.

AMQP: AMQP has robust security features, including authentication, access control, and end-to-end encryption. It supports different security protocols like TLS/SSL for secure communication. AMQP provides a comprehensive security framework to protect messages and ensure secure communication between systems.

LwM2M: LwM2M inherits the security features of CoAP, utilizing DTLS for secure communication. It provides authentication, encryption, and integrity protection to secure the exchange of data between devices and servers. However, the security features in LwM2M are more focused on device management rather than end-to-end application security.

XMPP: XMPP offers security features like TLS/SSL encryption for secure communication and authentication mechanisms. It provides options for end-to-end encryption and supports various authentication methods. XMPP has well-established security practices and extensions for securing instant messaging and presence applications.

In summary, when comparing MQTT, CoAP, AMQP, LwM2M, and XMPP. MQTT and CoAP are well-suited for resource-constrained devices and provide reliability and interoperability. AMQP offers advanced reliability features and strong interoperability but requires more resources. LwM2M, based on CoAP, is designed for device management with reliability and interoperability in constrained environments. XMPP focuses on instant messaging and presence applications, with good reliability, interoperability, and security features.

Table 4. The table below shows the COMPARATIVE ANALYSIS OF HIGHLIGHTED IOT COMMUNICATION PROTOCOL.

Criteria	MQTT	CoAP	AMQP	LwM2M	XMPP
Message size and overhead	Small (256MB)	small	larger	small	larger
Bandwidth consumption and latency	Efficient/lightweight	Efficient/lightweight	higher/complex	Efficient/lightweight	higher/complex
Power consumption and Resource Requirement	low power/limited	low power/limited	higher power and resources	low power/limited	higher power and resources
Reliability and Interoperability	Yes	Yes	Yes	Yes	Yes
Security	TLS/SSL	DTLS/ IPSec	TLS/SSL , SASL	TCP	TLS/SSL
Architecture	Client/Broker	Client/Server/Broker	Client/Server/Broker	Client/Server	Client/Server
Abstraction	Publish/Subscribe	Request/Response	Publisher/Subscribe	Request/ Response	Request/ Response
Header Size	2 Byte	4 Byte	8 Byte	Undefined	Undefined
Cache and Proxy Support	Partial	Yes	Yes	Yes	Yes
Quality of Service	QoS (0,1 & 2)	Confirmable/ Non-confirmable Message	Settle/Unsettle Format	Limited (via TCP)	QoS (0, 1, 2) & Error Handling
Transport Protocol	TCP	UDP, SCTP	TCP, SCTP	TCP	TCP/TLS/SSL

5. Conclusions

In conclusion, the integration of IoT in the automotive industry is paving the way for innovative advancements. The inclusion of various IoT devices within vehicles allows for activities such as fuel tracking, vehicle location tracking, and usage analytics. To facilitate the seamless transmission and retrieval of data, it is essential to connect these devices through appropriate protocols. This paper has provided an overview of four IoT protocols for in-vehicle communication. MQTT is a popular choice due to its persistent connection and bi-directional communication capabilities. CoAP, on the other hand, is preferred when IoT devices support UDP. For enhanced features like reliability and interoperability, AMQP is commonly employed. These protocols are open source in terms of licensing, providing flexibility and accessibility. Looking ahead, there is a need to explore and integrate additional protocols and gateways, while considering the incorporation of software-defined networks for improved communication. Furthermore, decentralized authentication emerges as a promising aspect to ensure a secure environment in the future. By continuing to explore these avenues, the automotive industry can further harness the potential of IoT for transformative advancements.

The v2v (vehicle-to-vehicle) communication protocols, including MQTT, CoAP, AMQP, LwM2M, and XMPP, play a crucial role in enabling efficient and seamless communication between vehicles. These protocols provide a framework for exchanging data and information in a secure, reliable, and scalable manner. MQTT (Message Queuing Telemetry Transport) offers lightweight publish-subscribe messaging, making it ideal for resource-constrained environments. Its efficient design and low overhead make it suitable for V2V communication, enabling real-time data exchange and event-driven interactions between vehicles. CoAP (Constrained Application Protocol) is another lightweight protocol designed for IoT environments. It operates over UDP and allows resource-constrained devices, such as vehicles, to communicate efficiently. CoAP's simplicity, low power consumption, and support for RESTful principles make it a viable option for V2V communication. AMQP (Advanced Message Queuing Protocol) is a versatile and robust messaging protocol that supports reliable communication over various networks. With its rich features, including message queuing, routing, and reliability mechanisms, AMQP offers a flexible solution for V2V communication, facilitating secure and scalable data exchange between vehicles. LwM2M (Lightweight Machine-to-Machine) is a protocol specifically designed for managing IoT devices. It provides a standardized way to monitor, control, and update devices, making it well-suited for V2V communication scenarios. LwM2M's efficiency, security, and device management capabilities contribute to establishing reliable connections between vehicles. Lastly, XMPP (Extensible Messaging and Presence Protocol) is an open standard for real-time communication. While traditionally used for instant messaging, XMPP can be adapted for V2V communication by enabling presence and messaging capabilities. Its extensibility and support for a wide range of features make XMPP a versatile choice for enabling vehicle-to-vehicle communication.

Overall, these v2v communication protocols, MQTT, CoAP, AMQP, LwM2M, and XMPP, offer diverse options for establishing efficient, secure, and scalable communication channels between vehicles. With the growing importance of connected and autonomous vehicles, the effective implementation of these protocols contributes to enhancing road safety, optimizing traffic management, and enabling innovative applications in the automotive industry.

References

1. K. He and B. Li, "Automotive V2X Communication Security Key Technology and Test Method Research," in 2022 7th International Conference on Cyber Security and Information Engineering (ICCSIE), IEEE, 2022.
2. S.A.A. Hakeem, M.A.A. El-Gawad, and H. Kim, "Comparative Experiments of V2X Security Protocol Based on Hash Chain Cryptography," Sensors, vol. 20, p. 5719, 2020, doi: 10.3390/s20195719.
3. T. Limbasiya and D. Das, "Lightweight Secure Message Broadcasting Protocol for Vehicle-to-Vehicle Communication," in IEEE Systems Journal, vol. 14, no. 1, pp. 520-529, March 2020, doi: 10.1109/JSYST.2019.2932807.
4. F. Haidar, A. Kaiser, and B. Lonc, "On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security," in 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, 2017, pp. 1-5, doi: 10.1109/VTCFall.2017.8288286.

5. D. Chatzoulis, C. Chaikalis, D. Kosmanos, K.E. Anagnostou, and A. Xenakis, "3GPP 5G V2X Error Correction Coding for Various Propagation Environments: A QoS Approach," Electronics, vol. 12, p. 2898, 2023, doi: 10.3390/electronics12132898.
6. P.V. Wadatkar, R.G. Garroppo, and G. Nencioni, "5G-MEC Testbeds for V2X Applications," Future Internet, vol. 15, p. 175, 2023, doi: 10.3390/fi15050175.
7. A. Lazaro, M. Lazaro, R. Villarino, D. Girbau, and P. de Paco, "Car2Car Communication Using a Modulated Backscatter and Automotive FMCW Radar," Sensors, vol. 21, p. 3656, 2021, doi: 10.3390/s21113656.
8. L. Miao, J.J. Virtusio, and K.-L. Hua, "PC5-Based Cellular-V2X Evolution and Deployment," Sensors, vol. 21, p. 843, 2021, doi: 10.3390/s21030843.
9. O. Kaiwartya, A.H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," Special Section On Future Networks: Architectures, Protocols, And Applications, 2016.
10. J.C. Castillo, J.A. Guerrero-Ibañez, and S. Zeadally, "Internet of Vehicles: Architecture, Protocols, and Security," IEEE Internet of Things, 2017.
11. M.H. Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cyber Security," IEEE Vehicular Technology Magazine, 2017.
12. J. Contreras-Castillo, S. Zeadally, and J.A.G. Ibáñez, "A seven-layered model architecture for Internet of Vehicles," Journal of Information and Telecommunication, 2017.
13. M. Gupta and R. Sandhu, "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, 2018.
14. M.A. Habib, M. Ahmad, S. Jabbar, S. Khalid, J. Chaudhry, K. Saleem, J.J.C. Rodrigues, and M.S. Khalil, "Security and privacy based access control model for internet of connected vehicles," Future Generation Computer Systems, pp. 687–696, 2019.
15. W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," IEEE Transactions On Intelligent Transportation Systems, 2016.
16. Y. Liu, Y. Wang, and G. Chang, "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm," IEEE Transactions On Intelligent Transportation Systems, 2017.
17. Y. Liu, Y. X. Yao Kuang, and G. Xu, "SDN-Based Data Transfer Security for Internet of Things," IEEE Internet of Things, 2018.
18. P. Tyagi and D. Dembla, "Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network," Wireless Personal Communications, pp. 41–60, 2018.
19. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," Future Generation Computer Systems, pp. 544–546, 2019.
20. A. Nanda, D. Puthal, J.J.P.C. Rodrigues, and S.A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," IEEE Wireless Communications, 2019.
21. J. Voas, I. Bojanova, R. Kuhn, C. Kolias, and A. Stavrou, "Learning Internet of Things Security 'Hands-On'," IEEE Security & Privacy, pp. 37-46, 2016.
22. S. Parkinson, P. Wardy, K. Wilsony, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," IEEE Transactions on Intelligent Transportation Systems, pp. 2898-2915, 2017.
23. M. Dabbagh and A. Rayes, "Internet of Things Security and Privacy," Internet of Things From Hype to Reality, 2017.
24. J.W. Bryans, "The Internet of Automotive Things: vulnerabilities, risks and policy implications," Journal of Cyber Policy, 2017.
25. E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, pp. 76-79, 2017.
26. C. Bernardinia, M. RizwanAsghar, and B. Crispoc, "Security and privacy in vehicular communications: Challenges and opportunities," Vehicular Communications, pp. 13-28, 2017.
27. 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. https://doi.org/10.3390/s22176382
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. https://doi.org/10.3390/s23156796.
29. S. S. Gadde, R. K. S. Ganta, A. G. Gupta, R. R. K, and K. M. Rao, "Securing Internet of Things (IoT) Using HoneyPots," International Journal of Engineering & Technology, 2018.
30. Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things," IEEE Communications Magazine, 2018.
31. A. Meola, "Automotive Industry Trends: IoT Connected Smart Cars & Vehicles," Dec. 20, 2016. [Online]. Available: *https://www.businessinsider.com/internet-of-things-connected-smart-cars-2016-10/?r=AU&IR=T*.

32. M. Rouse, "MQTT (MQ Telemetry Transport)," TechTarget, Mar. 16, 2018. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport. [Accessed Oct. 12, 2019].
33. K. STRIHAGEN, "Evaluation of publish – subscribe protocols for vehicle communications," Jun. 21, 2017. [Online]. Available: https://pdfs.semanticscholar.org/be4e/c6fe98b8c8a800fbd3f3b5af9e34daf39f64.pdf.
34. N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," Oct. 30, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/8088251.
35. M. A. Daud, "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, Oct. 21, 2016. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-48517-1_15. [Accessed Oct. 11, 2019].
36. Y. Chang and T. Kunz, "Performance evaluation of IoT protocols under a constrained wireless access network," Apr. 11, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7496622.
37. N. Gligoric, "CoAP over SMS: Performance evaluation for machine to machine communication," Nov. 14, 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6419577.
38. G. Technology, "Kaa IoT Platform," Jul. 23, 2016. [Online]. Available: https://www.kaaproject.org/automotive.
39. S. Zamfir, "A security analysis on standard IoT protocols," Oct. 08, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7754665.
40. C. Perira, "Towards Efficient Mobile M2M Communications: Survey and Open Challenges," May 10, 2014. [Online]. Available: https://www.mdpi.com/1424-8220/14/10/19582.
41. J. Berg, "Secure Gateway – A concept for an in-vehicle IP network bridging the infotainment and the safety critical domains," 2015. [Online]. Available: https://www.semanticscholar.org/paper/Secure-Gateway-%E2%80%93-A-concept-for-an-in-vehicle-IP-the-Berg-Pommer/485ff149d68d738505e11995e688752661dbcd0d.
42. Y. Huo and W. Tu, "A survey of in-vehicle communications: Requirements, solutions and opportunities in IoT," Dec. 15, 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7389040.
43. J. E. Luzuriaga and M. Perez, "A comparative evaluation of AMQP and MQTT protocols over unstable and mobile networks," Jan. 09, 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7158101.
44. T. Akram Hakiri ISSAT Mateur and P. Berthou, "Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications," Sep. 16, 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7263372."