CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Navigating the Challenges and Opportunities of Securing Internet of Autonomous Vehicles with Lightweight Authentication

Hazem Ali
Harrison Kurunathan*
Mohamed Hamdy Eldefrawy
Flavius Gruian
Magnys Jonsson

*CISTER Research Centre

CISTER-TR-250201

2025

Navigating the Challenges and Opportunities of Securing Internet of Autonomous Vehicles with Lightweight Authentication

Hazem Ali, Harrison Kurunathan*, MOHAMED HAMDY ELDEFRAWY, FLAVIUS GRUIAN, MAGNUS JONSSON

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: haali@isep.ipp.pt, jhk@isep.ipp.pt, mohamed.eldefrawy@hh.se, flavius.gruian@cs.lth.se, magnus.jonsson@hh.se

https://www.cister-labs.pt

Abstract

The Internet of Things (IoT) can be defined as the network of physical objects, or "things, 1d embedded with sensors and software for processing and exchanging data with other devices and ecosystems using the Internet as a medium. With its rapid growth over the past decade, it has permeated several application domains, including intelligent vehicular systems. The Internet of Autonomous Vehicles (IoAV) is a subset of IoT that envisions dynamic autonomous driving without human intervention. The dynamic nature of the environment in which autonomous vehicles operate introduces significant challenges, such as real-time communication and security vulnerabilities. These challenges cannot be directly addressed by standard cybersecurity solutions designed primarily for static IoT environments. In this work, we outline the various vulnerabilities of the IoAV systems, and we delve into the critical importance of adopting lightweight security protocols. These protocols are crucial to ensure robust protection while at the same time not jeopardizing the performance of the IoAV system. We also highlight the fast lightweight security protocols implemented on heterogeneous embedded, low-power, high-performance computing platforms as a viable solution to address these challenges.

© 2025 CISTER Research Center
www.cister-labs.pt

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 12 December 2024, accepted 26 January 2025, date of publication 3 February 2025, date of current version 7 February 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3537800

SURVEY

Navigating the Challenges and Opportunities of Securing Internet of Autonomous Vehicles With Lightweight Authentication

HAZEM ISMAIL ALI[1], HARRISON KURUNATHAN[2], MOHAMED HAMDY ELDEFRAWY[1], FLAVIUS GRUIAN[3], AND MAGNUS JONSSON[1], (Senior Member, IEEE)

[1]Department of Computing and Electronics for Real-Time and Embedded Systems (CERES), School of Information Technology (ITE), Halmstad University, 301 18 Halmstad, Sweden
[2]CISTER/ISEP, Polytechnic Institute of Porto, 4200-465 Porto, Portugal
[3]Department of Computer Science, Lund University, 221 00 Lund, Sweden

Corresponding author: Hazem Ismail Ali (hazem.ali@hh.se)

This work was supported in part by Halmstad University (Halmstad i Högskolan) Research Base Funding; in part by NordForsk 86220 through the Proposal HI2OT: Nordic University Hub on Industrial Internet of Things; in part by the Research Centre in Real-Time and Embedded Computing Systems (CISTER) Research Unit financed by National Funds through Fundacao para a Ciencia e a Tecnologia (FCT)/Ministry of Science, Technology and Higher Education (MCTES) (Portuguese Foundation for Science and Technology) under Grant UIDP/UIDB/04234/2020; and in part by the Project Route 25 funded by the EU/Next Generation within Call 02/C05-i01/2022 of the Recovery and Resilience Plan (RRP) and Hardware Abstraction Layer for a European Software Defined Vehicle Approach (HAL4SDV) Funding within the Chips Joint Undertaking (Chips JU)—The Public-Private Partnership for Research, Development and Innovation under Horizon Europe—and National Authorities under Grant TRB/2022/00061-C645463824-00000063 and Grant 101139789.

ABSTRACT The Internet of Things (IoT) can be defined as the network of physical objects, or ''things,'' embedded with sensors and software for processing and exchanging data with other devices and ecosystems using the Internet as a medium. With its rapid growth over the past decade, it has permeated several application domains, including intelligent vehicular systems. The Internet of Autonomous Vehicles (IoAV) is a subset of IoT that envisions dynamic autonomous driving without human intervention. The dynamic nature of the environment in which autonomous vehicles operate introduces significant challenges, such as real-time communication and security vulnerabilities. These challenges cannot be directly addressed by standard cybersecurity solutions designed primarily for static IoT environments. In this work, we outline the various vulnerabilities of the IoAV systems, and we delve into the critical importance of adopting lightweight security protocols. These protocols are crucial to ensure robust protection while at the same time not jeopardizing the performance of the IoAV system. We also highlight the fast lightweight security protocols implemented on heterogeneous embedded, low-power, high-performance computing platforms as a viable solution to address these challenges.

INDEX TERMS Lightweight authentication, Internet of Autonomous Vehicles (IoAV), embedded systems.

I. INTRODUCTION

The concept of autonomous vehicles was envisioned to become a reality by the late 20th century [1]. Human error, vehicle design and infrastructure were considered to be the main causes of accidents, fuelling the idea of machine-substitution of the human driver [2]. This led to technologies such as cruise control and eventually autonomous-driven vehicles enabled through the internet. The Internet of Autonomous Vehicles (IoAV) enables real-time communication between autonomous vehicles and their supporting infrastructures. This communication encompasses crucial information on the surroundings, traffic conditions, and security data that are vital to ensuring the safe and efficient functioning of autonomous vehicles.

As depicted in Figure 1, IoAV can be compartmentalized into three types of communication, namely vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C) communication [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

© 2025 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

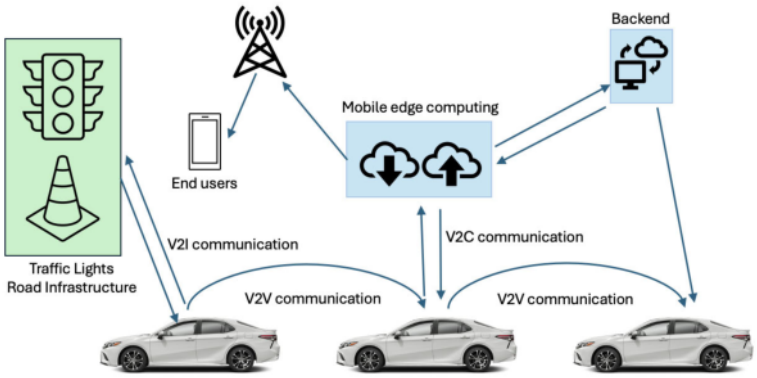

FIGURE 1. IoAV encompassing V2V, V2I and V2C real-time communications.

Vehicle-to-vehicle (V2V) communication enables autonomous vehicles to exchange critical data, such as real-time information on precise location, speed, intended path, and security data. This creates situational awareness among autonomous vehicles allowing them to adapt to dynamic traffic conditions. V2V communication enables multiple autonomous vehicle applications such as lane changes, braking manoeuvres, and speed adaptation based on road conditions. With coordinated communication, road congestion and bottlenecks at intersections can be avoided. Furthermore, V2V also facilitates driving methods such as platooning [4], which reduces aerodynamic drag and improves fuel efficiency.

Vehicle-to-Infrastructure (V2I) communication enables the vehicles to communicate with roadside units such as traffic lights and traffic management systems. Autonomous vehicles can use V2I to share real-time traffic data and coordinate with other vehicles connected to the infrastructure [5]. Through V2I communication, the vehicles can get an idea of traffic conditions such as road closures, traffic lights, construction zones, weather, and speed zones in advance to improve overall navigation and safety. Furthermore, this V2I can also reduce the bottlenecks at road intersections, enabling smoother traffic flow and reduced fuel consumption [6], [7].

Finally, *Vehicle-to-Cloud (V2C) communication* allows vehicles to constantly upload and access information on navigation data, sensors, and diagnostics [8], [9]. Akin to V2I communication, V2C can also aid in traffic data coordination. Connectivity through the cloud enables over-the-air software updates and remote diagnostics for autonomous vehicles. Combined with the scope of machine learning, V2C communication can enable predictive analysis of vehicular health monitoring for autonomous vehicles [10], [11].

In this work, we aim to explore lightweight authentication techniques employed in V2V and V2I communications, specifically focusing on minimizing computational load while maintaining adept security. We place a particular emphasis on authentication protocols which require fewer computational resources (i.e., *lightweight*) to execute without imposing a significant burden on the system's CPU or memory. In the context of V2V and V2I communications, we identify the security threats and offer insights into the suitability of these protocols for deployment in AVs.

An *Internet of Autonomous Vehicles (IoAV) system* is a networked ecosystem in which autonomous vehicles (AVs) are interconnected through the internet, enabling them to communicate with each other, with infrastructure, and with external networks. This connectivity enables data transfer, subsequently enhancing the operational efficiency, safety, and overall functionality of autonomous vehicles. With this interconnectivity, such an ecosystem is highly vulnerable to security threats [12]. In this work, we aim to survey the key cybersecurity threats impacting road traffic safety. *Authentication* is a critical process of IoAV as it is used for identity verification by coordinating communication between on-board vehicles, infrastructure, and remote servers.

Over the past decade, traditional [8], [13] and deep learning methodologies have been used for the detection of vehicles, pedestrians, and road lanes, and the field of autonomous vehicles has consistently evolved. Recently, machine learning and deep learning methods have been used extensively in authentication mechanisms within the IoAV ecosystem due to their ability to detect patterns, analyze complex data, and adapt to new threats. For example, researchers in [14] propose a novel federated learning collaborative authentication-based protocol to secure communication in IoAV vehicles. This protocol reduces the number of vehicle certifications for each dynamic Roadside Unit (RSU) while ensuring the safety of vehicle upload training parameters in the federated architecture. They also include an anonymous mutual authentication and key agreement. In another work [15], they used novel deep learning models that include algorithms like the Deep Sparse Stacked Autoencoder Network (DS2AN) algorithm to ensure the authentication and security of the vehicles. Furthermore, in [16], they developed trust management approaches for software-defined vehicles. This novel architecture works with a centralized software-defined network controller that serves as a learning agent and obtains

the optimal communication link policy using a deep learning approach. Therefore, with the ever-growing complexity and connectivity of these automotive systems, there is a mandate for robust authentication to ensure the integrity and security of data. lightweight authentication protocols are crucial to maintaining the performance of IoAV without burdening the limited computational resources.

Traditionally, intense cryptographic operations used in authentication mechanisms strain limited processing power and memory [17]. It is essential to look into methods such as hardware acceleration, protocol optimization, precomputed authentication, and dynamic resource allocation to reduce the computational strains due to intensive cryptographic operations. This survey aims to provide an in-depth analysis of security threats and their respective mitigation strategies. We identify the most critical security issues surrounding V2V and V2I communication in IoAV and explore state-of-the-art solutions to achieve efficient and reliable authentication protocols.

The contributions of this work are as follows:

- We outline the various vulnerabilities of the IoAV systems and discuss several cybersecurity attacks and their targeted regions of the IoAV networks.
- We stress the crucial importance of adopting lightweight security protocols by showcasing several real-life examples and discussing the concepts of lightweight protocols.
- We highlight fast lightweight security protocols implemented on heterogeneous embedded, low-power, high-performance computing platforms as a viable solution and present several research directions in line with system design, blockchain solutions and cryptographic functions.

The rest of this article is organized as follows: in Section II, we analyze some of the significant IoAV threats in the literature, then we discuss some real-life use cases of authentication-based threats in Section III. Protocols enabling vehicular communication and their key security issues are elaborated in Section IV. In Section V, we discuss some of the state-of-the-art lightweight authentication protocols, their advantages, their features and security issues. Then in Section VI, we discuss the challenges and provide the aspects of designing a secure authentication protocol in line with IoAV systems.

II. IoAV SECURITY THREATS

Security threats in IoAV are a significant risk to the safety, privacy, and functionality of the interconnected vehicles [18]. It is vital to understand these threats in order to design defence mechanisms that enhance the safety of vehicles. To mitigate the security risks introduced by the current growth in communication required for IoAV, a number of countermeasures have been proposed, including encryption, authentication, filtering and intrusion detection. In the following, we explore different security threats along with associated state-of-the-art defences. Table 1 presents some of the significant attack types, targeted vehicle parts, and their respective countermeasures.

A. DENIAL-OF-SERVICE (DoS) ATTACKS

Denial-of-Service (DoS) attacks target communication channels by overwhelming them with an excessive amount of traffic requests (Figure 2). These traffic requests lead to degradation and disruption of services. This deterioration results in significant operational risks for autonomous vehicles on the road [19].

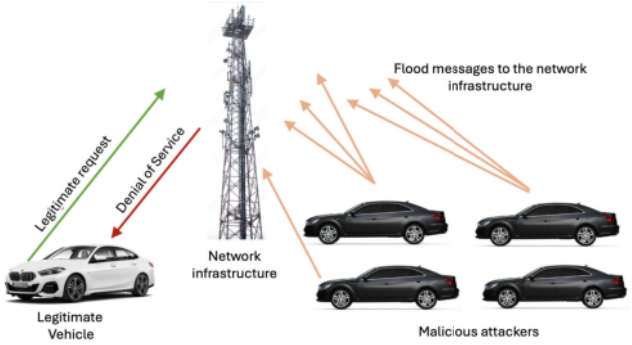

FIGURE 2. Denial-of-Service (DoS) attacks target communication channels and attempt to disrupt their functionality by overwhelming them with an excessive amount of traffic requests.

DoS attacks can occur through flooding V2X communication channels resulting in congestion that leads to excessive critical delay. This can result in catastrophic events such as the loss of critical messages, preventing vehicles from receiving essential safety information and coordination signals. Attackers can also specifically attack the crucial computing resources within IoAV components and vehicular internal networks. These targets encompass the onboard processing units of autonomous vehicles or the Controller Area Networks (CAN) responsible for internal communication.

The authors of [20] highlight a noteworthy example of such an attack. They present a selective DoS attack that specifically targets the CAN standard. This method is notable because it does not necessitate the exchange of complete frames for execution, rendering it undetectable via frame-level analysis. This stealthy nature of the attack makes it incredibly challenging to identify and counteract, exacerbating the potential risks and consequences for IoAV systems.

B. SYBIL ATTACKS

The Sybil attack (Figure 3) is a significant security concern in the IoAV context [3]. This attack derives its name from "Sybil," a book by Flora Rheta Schreiber [21], presenting a case study of a woman with dissociative identity disorder who exhibited multiple personalities. In the context of IoAV, a Sybil attack occurs when a malicious entity creates multiple fake identities (known as Sybil nodes) to deceive the

TABLE 1. Different attack types on IoAV and their respective countermeasures.

Attack Type	Description of the attack	Targeted Vehicle Parts	Countermeasures
Denial-of-Service	Malicious attacker floods the communication channel with false data and causes the vehicles unable to exchange critical information.	Communication Module, Processing Unit	Encryption and authentication of communication Rate limiting and traffic filtering Secure communication paths and protocols
Sybil Attack	Multiple fake identities (Sybil nodes) are created by the attacker to deceive the vehicles into accepting false information compromising trustworthiness	Identity Management System	Certificate-based authentication Reputation-based trust mechanisms Periodic validation of node identities
Replay Attack	An attacker eavesdrops legitimate messages in V2V and replays them to deceive other vehicles.	Communication Channel, Data Storage	Age of information Message integrity verification Nonces for replay prevention
Blackhole Attack	The attacker manipulates the data, causing disruption or interception of critical information.	Routing Infrastructure, Communication Channel	Secure routing protocols Reputation-based routing Intrusion detection systems (IDS)
Password Attack	The attacker gains unauthorized access in V2V by cracking the authentication credentials.	Authentication Module	Multi-factor authentication Intrusion detection systems (IDS)

IoAV system. These counterfeit identities, masquerading as legitimate vehicles or infrastructure, deceive the system into trusting them.

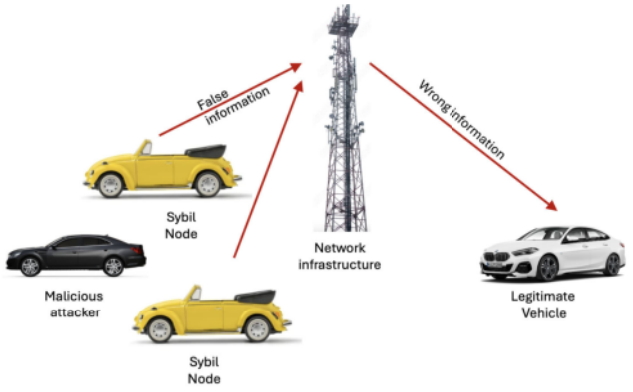

FIGURE 3. Sybil attack occurs when a malicious entity creates multiple fake identities (known as Sybil nodes) to deceive the IoAV system. These result in the legitimate vehicles taking wrong actions due to false information.

The Sybil nodes use these deceptive identities to gain control over the IoAV network, compromise its integrity, and manipulate its operations for malicious purposes. For example, Sybil nodes can inject false data into the IoAV network to misguide autonomous vehicles, leading to potentially dangerous decisions and movements on the road. Also, by generating many Sybil nodes, attackers can overwhelm the IoAV system resources, leading to DoS attacks.

Several defence mechanisms, such as solid authentication and digital signature methods, can mitigate Sybil attacks in IoAV [22]. Also, AI-based approaches, such as anomaly detection algorithms and behaviour analysis, can detect and separate suspicious activities associated with Sybil nodes. Furthermore, location-based detection using a directional antenna with beam-forming techniques can also be employed [22].

C. REPLAY ATTACKS

Replay attacks [3], [23] are a security concern in IoAV. The adversary copies legitimate data packets exchanged between autonomous vehicles or between vehicles and infrastructure components (Figure 4). Then, the adversary re-exchanges these copied packets, as they are or with tiny changes, back into the network. Replayed packets, which appear genuine to the IoAV system, can carry critical safety instructions or control commands in which autonomous vehicles may act in unsafe manoeuvres, leading to collisions on the road.

To mitigate replay attacks, IoAV can employ cryptographic primitives and security measures such as including timestamps and sequence numbers in data packets. Timestamps and sequence numbers can help detect and discard replayed packets with outdated or duplicate values. In the same context, moulding a time-to-live parameter for packets can limit their validity period, reducing the possibility window for such attacks [24], [25]. It can also be mitigated by using digital signatures or message authentication codes (MACs) that can verify the authenticity and integrity of data packets, making it harder for attackers to forge or replay them. Another security measure is the usage of cryptographic nonces or challenge-response methods that can ensure each communication session is unique, preventing attackers from reusing intercepted data.

D. BLACKHOLE ATTACKS

A Blackhole attack [3] is a security threat where malicious entities, called blackhole nodes, drop data packets instead of forwarding them. This can have dangerous consequences like missing traffic accident information. In such an attack, the malicious actor deceives other nodes in the network to transfer their network traffic data to blackhole nodes by falsely claiming that these nodes have certain advantages in the network, such as the shortest path to their final destinations. Blackhole attacks can have serious consequences, such as dropping all incoming communication packets, leading to a failure in communication and coordination within the IoAV components that increases the risk of accidents [26]. Blackhole attacks in IoAV can be prevented using [27]: (i) Intrusion Detection Systems (IDS) to detect abnormal traffic patterns and identify blackhole nodes based on their dropping behaviour. (ii) Secure and authenticated routing

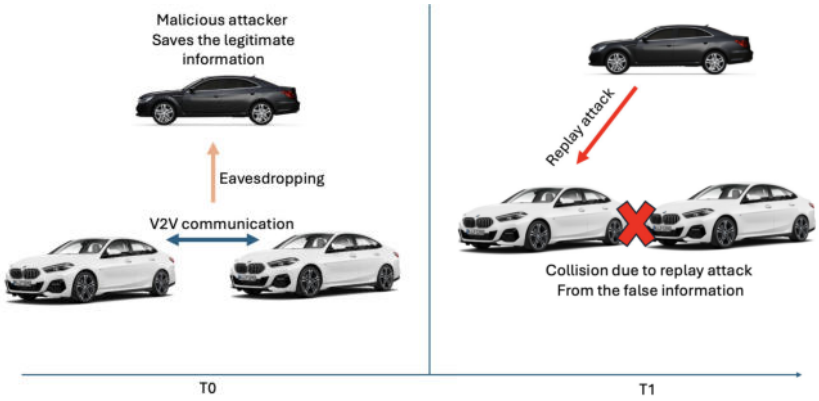

FIGURE 4. The adversary copies legitimate data packets exchanged between autonomous vehicles or between vehicles and infrastructure components. Then, the adversary re-exchanges these copied packets, resulting in catastrophes like collision.

protocols can be used to ensure that data packets are routed through authorized nodes, avoiding possible blackhole nodes. (iii) Implementing low-cost lightweight encryption and authentication protocols can protect data packets from being tampered with or read by blackhole nodes.

E. IMPERSONATION AND PASSWORD ATTACKS

In IoAV, impersonation attacks [27] involve malicious nodes pretending to be legitimate vehicles. These attacks utilize authentication violations to control weaknesses in the security mechanisms by forging the malicious node identity to achieve unauthorized access to manipulate the IoAV system. IoAV is susceptible to secret key disclosure attacks where the intruders focus on compromising the encryption keys to impersonate themselves as authorized nodes. Offline guessing attacks target authentication mechanisms and cryptographic keys to help attackers guess passwords, keys, or other sensitive information offline without interacting directly with the system [28]. Security measures like solid authentication methods, digital signatures, secure key management, public key infrastructure (PKI) with digital certificates, and secure Over-the-Air (OTA) [29] updates can help to stop or mitigate such attacks in IoAV.

III. VEHICLE CYBERSECURITY THREATS: REAL-LIFE CASE STUDIES

In this section, we explore some real-life instances of security vulnerabilities in vehicular networks due to weaknesses in authentication systems.

A. OAKLAND FOB MANIPULATION INCIDENT

Key fobs are wireless devices that allow vehicle owners to lock, unlock, start and even park their vehicles remotely. Fob manipulation refers to unauthorized control of vehicles using key fobs. A technical journalist purchased a car through a local car-sharing program that provides Toyota Prius and electric Chevrolet Bolt EVs with plans to spend the weekends in rural areas about 3 hours north of Oakland [30]. Unfortunately, when the telematics system of the vehicle lost its cell signal, the control unit of the car became inaccessible. In this instance, there is a possibility of a potential attacker manipulating the controls using the fob's shortened distance signal [31]. This is a possibility because the ''sender'' (the car) challenges the ''prover'' (the key fob), and then the ''sender'' can read how long it has taken to receive an answer since the initial challenge was sent. Lightweight authentication protocols, specifically *RFID-based Distance Bounding Protocols* [32], can effectively mitigate this threat. These protocols use cryptographic primitives to measure the time it takes for a signal to travel between the key fob and the car, ensuring that only devices within a specified distance can authenticate. This prevents relay attacks by ensuring that the authenticating device is physically close to the vehicle.

B. TESLA PHISHING VULNERABILITIES

A case study on credential theft done by [33] demonstrates the vulnerabilities in vehicular systems through infotainment systems in IoAV-enabled cars. Several companies, like Berla, offer sophisticated tools for data extraction from major vehicle brands, like Tesla. Such data extraction methods can be violated to perform credential theft of critical information from state-of-the-art vehicles with modern assistant systems like the Tesla autopilot.

Using phishing attacks in IoAV, client-level access can be stolen from the vehicle's business platform. This can even lead to the theft of the vehicle. Researchers from Mysk Inc [34]. demonstrated how connected autonomous vehicles could be susceptible to theft through a man-in-the-middle (MITM) phishing attack. This phishing attack, as depicted in Figure 5 can enable malicious actors to create and use new digital keys to unlock Tesla cars and access their systems.

The attack starts with the attacker issuing a counterfeit WiFi access point (e.g. ''Guest WiFi'') at a vulnerable location like a charging station. When the vehicle owner enters their real credentials on the spoof page, which resembles the real website, the credentials are immediately

FIGURE 5. Phishing attack in an IoAV-enabled network where user credentials are stolen using a fake guest WiFi terminal.

stolen. Then, the attacker sniffs and uses these credentials to access the genuine service. Multifactor authentication (MFA) security can also be circumvented by displaying a fake prompt that mimics the legitimate one, deceiving the victim into providing their one-time passcode (OTP). *Time-Locked One-Time Passwords* [35] with lightweight browser extension uses temporary passwords with fast expiry, thus making it harder to intercept credentials.

C. HIJACKING THROUGH VEHICLE CHARGING

In a connected IoAV network, malicious vehicles behave like legitimate vehicles by selectively dropping their packets. A session refers to the data exchange between the vehicles for a selective period. Unauthorized access to the IoAV ecosystem during a session is called a session hijacking attack. The case study in [36] shows a use case where the attacker can hijack the session wirelessly and prevent people from charging their vehicles. This use case further presents us with the possibility that these vehicles connected through an IoAV system could be victims of masquerading, man-in-the-middle attacks, and denial-of-service through session hijacking. *Mutual Certificate-Based Authentication* [37] with a minimal handshake process between vehicles and charging stations for authenticating each other with encrypted certificates can prevent hijacking at the charging sessions.

D. CHARLIE MILLER AND CHRIS VALASEK INCIDENT

The well-known incident [38] involving professional hackers Charlie Miller and Chris Valasek seizing control of a Jeep Cherokee in 2015 highlighted the genuine risk of connected car hijacking, bringing this threat to the forefront of public consciousness. When commencing their research, the investigators initially attempted to breach the multimedia system of the Jeep using a WiFi connection, which is provided as a subscription service by the vehicle manufacturer, Chrysler. They discovered that Chrysler's vehicles were generating their WiFi passwords before the actual setup of the time and date. These passwords were established using the default system time during the short span of seconds when the head unit initialized. In practical terms, for instance, January 01, 2013, 00:00 GMT translated to 00:00:32 GMT. The permutations for password combinations were minimal, making it relatively effortless for even amateur hackers to predict the appropriate password accurately. Their successful attack resulted in the recall of 1.4 million vehicles and underscored intelligent vehicle manufacturers' substantial challenge in securing their products. As we progress towards V2X (Vehicle-to-Everything) communication systems, where vehicles exchange data with each other and with surrounding infrastructure, similar concerns for cybersecurity exist. Analogous to the Jeep Cherokee case, where external access to a vehicle's systems enabled malicious control, V2X-connected cars face the challenge of safeguarding against unauthorized access and potential remote attacks. *Low-Latency Anonymous Authentication Protocol using elliptic curve cryptography (ECC)* [39] can ensure high security so that only trusted networks can communicate with the vehicle's system.

E. HEADLIGHT HACKING THROUGH BLACKTOOTH SPEAKER

In a recent incident [40], a smart vehicle (Toyota RAV4) fell victim to hacking and theft. A thorough analysis revealed that the attackers employed an innovative approach called "headlight hacking" to penetrate the car's interconnected systems through its headlight. The attackers exploited an apparent tool akin to a JBL Bluetooth speaker, which has been illicitly circulated on the dark web under the guise of an emergency ignition device for compatible smart vehicles. When interfaced with the vehicle's Controller Area Network (CAN), this device effectively bypasses all security protocols, granting direct entry to the vehicle's functionalities, including ignition, without necessitating the car's key. Data gathered from the car's telematics system indicate that the attackers accessed the CAN system by exploiting the Electronic Control Unit (ECU) within the headlight assembly. This vulnerability within the 2021 Toyota RAV4, classified as CVE-2023-29389, expands beyond the headlight entry method. It is one of several potential routes to access the car's CAN systems, enabling attackers to simulate the vehicle's key fob, unlocking and driving away with the car. Although that incident shows an attack on the in-vehicle network of the car (CAN) using a physical connection, the same effect may occur using a remote connection if the attacker utilizes the V2X communication vulnerabilities, which will be discussed in Section IV. *Proximity-based authentication with PUFs (Physical Unclonable Functions)* [41] connects devices using unique physical traits of the device that cannot be replicated, thus it secures access to the legitimate vehicle.

IV. VEHICULAR COMMUNICATION PROTOCOLS AND THEIR SECURITY ISSUES

Vehicular protocols are essential for enabling communication between vehicles and their various supporting infrastructures, as mentioned in Section I. These protocols enable a wide range of applications, from safety-critical systems to infotainment. However, extensive surveys, such as the one in [42], [43], [44], [45], and [46], point out a number of their challenges, including some related to security. Table 2 summarizes some of the prominent protocols and their security issues.

A. DEDICATED SHORT RANGE COMMUNICATION

Dedicated Short Range Communication (DSRC) is used for wirelessly connecting vehicles in short ranges. It operates at a band frequency of 5.9GHz. This protocol is based on the IEEE 802.11p standard that supports vehicular communication and is also supported by the European Telecommunications Standards Institute (ETSI). This protocol defines both V2V and V2I communication, with a range typically up to 1000 meters. DSRC is primarily used to enable applications such as collision detection and cruise control. Due to DSRC's ability to connect with road infrastructure, it can also reduce pollution and bottlenecks by relaying information on congestion levels, road conditions, and traffic signal status.

Some of the key security issues of the DSRC are as follows:

- **Lack of scalability:** Scalability refers to the system's ability to handle a growing workload or accommodate expansion. When the number of vehicles in the IoAV connected through DSRC increases, the management of cryptographic keys in the dynamic environment poses a major challenge.
- **Need for privacy:** The privacy refers to the protection of sensitive information about drivers, passengers, and vehicles from unauthorized access, collection, or misuse during data exchange between vehicles. This involves safeguarding location data, driving patterns, and personal identification to prevent tracking, profiling, or other privacy breaches. This short-range protocol is susceptible to attacks such as phishing and data interception, which puts the privacy of the clients using IoAV at a potential risk.
- **Communication vulnerabilities:** The communication is vulnerable to jamming DoS attacks where the attacker might try to disturb key functionality by using, for example, malicious interference on wireless communication systems, e.g., coordination and information regarding traffic safety and efficiency. [47].

B. CONTROLLER AREA NETWORK (CAN) BUS

The CAN bus is the most commonly used bus in the automotive industry [48]. It was first introduced in the BMW 850 in 1986. The motivation for this technology is to reduce vehicle wiring by 2 km. Eventually, this also reduced the vehicle's overall weight by at least 50kg. Despite the vehicle's systems and sensors being able to communicate at very high speeds (25Kbps–1Mbps), it lacked security measures to thwart attacks and abnormal communication conditions. As highlighted in [49], CAN communications face the following security issues:

- **Absence of Message Authentication for Nodes:** Since each Electronic Control Unit (ECU) transmits and receives all data on the same bus, there is the problem of points of failure due to lack of message authentication.
- **Lack of Encrypted Messages:** The CAN bus was not initially designed with cyber attack prevention in mind, lacking encryption. This exposes information, enabling unauthorized access, potential data alteration, and even data replacement, leading to operational errors.
- **Vulnerability to DoS Attacks and Replay Attacks:** CAN bus uses a message-oriented protocol, where all devices on the network receive all messages and it is not localized, but each device decides whether a message is relevant based on its identifier. This design makes it susceptible to DoS attacks and replay attacks, where an attacker could send high-priority frames to disrupt critical system functions.

C. FLEXRAY

FlexRay, introduced in the year 2000 and jointly developed by Daimler Chrysler, BMW, Freescale, and Phillips, is a high-bandwidth communication protocol designed for high-speed technology applications in automotive vehicles [49]. It was introduced to address the limitations of the CAN protocol in terms of speed, determinism, and reliability. It supports high data rates of up to 10Mbps and ensures determinism in communication through time-triggered events. It also supports network node synchronization, which is vital for novel ADAS-enabled IoAV vehicles. Some of the security limitations of FlexRay include:

- **Lack of built-in security mechanism:** FlexRay's absence of inherent security mechanisms makes it susceptible to spoofing and denial-of-service (DoS) attacks. The current features fail to ensure dependable communication in the presence of adversarial threats [50].
- **Lack of authentication mechanisms:** FlexRay communication is very susceptible to attacks like message spoofing, where the attackers can inject counterfeit messages, resulting in erroneous actions within the vehicle control systems. However, there are ongoing efforts to enhance its authentication and key management capabilities. For instance, the authors in [51] have introduced an authentication mechanism in the optional dual-channel mode to facilitate backward compatibility and have also proposed various techniques for cryptographic key management and authentication. Also, [52] presents protection schemes based on splitting authentication tags using independent channels to counter spoofing attacks.

TABLE 2. Vehicular protocols, their aspects and their security issues.

Protocol	Advantages	Covered Aspects	Security issues	Potential Solutions
DSRC	Low latency and high reliability Supports high data rate	Collision avoidance and ADAS Intersection management	Eavesdropping Message tampering Denial-of-service attacks	End-to-end encryption Block-chain authentication
LTE-V	Wide coverage Supports high-speed mobility Large-scale deployments	Multimedia services in vehicles Traffic and navigation assistance Telemetry	Middleman attacks GPS spoofing	Public Key Infrastructure Digital Signature
WiFi	Interoperability with WiFi and 5G Cost-effective	ADAS RSU integration	Replay attacks No pre-defined safety layers	One-time passwords Security/safety layers
C-V2X	Utilizes cellular infrastructure Supports cellular routing	V2X communications Congestion control	Jamming Infrastructure attacks	Frequency hopping Mutual authentication
CAN Bus	realtime data transfer Suitable for control data	V2V communication Cruise control	No in-built security layer Replay attacks	Intrusion detection systems Safety/Security layers
FlexRay	High bandwidth and deterministic Fault-tolerant network	Dependable communication Supports mobility	Spoofing Denial-of-service	Block-chain authentication Multi-factor authentication

D. AUTOMOTIVE ETHERNET

Automotive Ethernet (AE) emerged in 2013, drawing inspiration from audio-video Bridging (AVB) within the automotive sector. AVB itself is rooted in a series of IEEE standards governing Ethernet networks, dictating audio and video transmissions' transport, signaling, and synchronization. In Ethernet networks, a primary security concern involves the potential compromise of administrators, as adherence to security policies is crucial during new software installations, configuration adjustments, and the deployment of switches. These vulnerabilities open routes for attackers to assess the defences of the Ethernet network, probing until they identify susceptible points. Beyond this, attackers may exploit network access to gain insights into the network topology, understand traffic patterns for future attacks, and potentially seize control over switches and routers or manipulate information [49].

Despite Automotive Ethernet bringing high-speed communication, it also introduces key security challenges to the availability and confidentiality of vehicle systems:

- **Need for isolation:** Automotive Ethernet connects several critical systems, such as the ADAS and power train controls. However, there are not enough segmentation and isolation guidelines for these systems. Network segmentation techniques using virtual local area networks are used for the isolation of these critical systems from other critical systems [53].
- **Lack of Interoperability:** When different vehicles in real-time IoAV scenarios employ different communication protocols and generate different data types, there is a need to interoperate with different entities [54]. Improper integration of automotive Ethernet can lead to compatibility issues between different systems, resulting in the loss of integrity.

V. LIGHTWEIGHT AUTHENTICATION PROTOCOLS

Authentication protocols that decrease the computational strain on the system are needed to improve efficiency and resource utilization without compromising security. These lightweight protocols must be designed to take into account several factors, such as computational overhead, interoperability, and trade-offs involving security. They utilize techniques like streamlined cryptographic algorithms that require fewer computational resources to execute without imposing a significant burden on the system's CPU or memory. Moreover, these protocols should be able to work with smaller key sizes, contributing to lower memory usage and bandwidth requirements. However, they have to be designed by keeping in mind the trade-offs in the security of the system resulting from a smaller key size. There has also been research where the size of transmitted data packets has been minimized to reduce the strain on computational resources. In this section, we discuss some of the state-of-the-art lightweight authentication schemes that aid in securing IoAV systems.

A. PRE-SHARED KEY (PSK) AUTHENTICATION

Pre-shared key (PSK) authentication is a method in which a single symmetric key is distributed to all parties involved in a network, allowing them to authenticate and encrypt communications. This method can be utilized in a vehicular network to secure communication between access points (APs) and a trusted authority.

In [55], is presented a lightweight symmetric cryptography-based session key agreement scheme between each ECU and the manufacturer data center that uses a random nonce, concatenation operator, a simple hash function, and a keyed hash message authentication code. The security parameters for in-vehicle Ethernet-based communications are defined between the different ECUs. Pre-shared keys are used in this approach to secure the transmission between the internet protocol messages.

Mutual authentication techniques [56] have been used to enhance the security levels in the IoAV system. In this method, the session key is shared by the vehicles, and the random nonce is decided by both vehicles transmitting the messages. Based on their results, this method was able to mitigate unknown key share attacks, replay attacks, and key-compromised impersonation attacks.

The work in [57] generates and distributes a new session key between the vehicle virtual sensor and the selected physical sensor at every time interval. This ensures that access to sensor data is tightly controlled and restricted to authorized time periods. The session key is established using the ephemeral Elliptic Curve Diffie-Helman (ECDH) protocol [58]. This is done at the end of the authentication of the selected physical sensor and the vehicle virtual sensor using the PSK. This perfect forward secrecy strategy prevents the decryption of past or future transmissions with compromised keys.

B. SYMMETRIC KEY AUTHENTICATION

A symmetric key, also known as a private key, is a cryptographic key that is used for both encryption and decryption of data. In symmetric key cryptography, the same key is shared between communicating parties using methods such as PSK for key distribution. Symmetric key authentication verifies the identity of both vehicles, sending them to communicating parties using symmetric key cryptography. In this method, all the vehicles involved share a secret key, known only to them. When one vehicle wishes to authenticate itself to the other, it generates a message or a token and encrypts it using the shared secret key. The receiving vehicle decrypts the message using the same key and verifies its authenticity based on the decrypted content.

In symmetric key authentication, the integrity of the data must be verified using a pairwise symmetric key between two vehicles. Methods like RSA-based session key distribution or Diffie-Hellman key exchange can be used for symmetric key sharing. The method in [59] enables the pairwise symmetric key to be calculated based on its identification of the communication counterpart for a message m with a message authentication code, as shown in Figure 6.

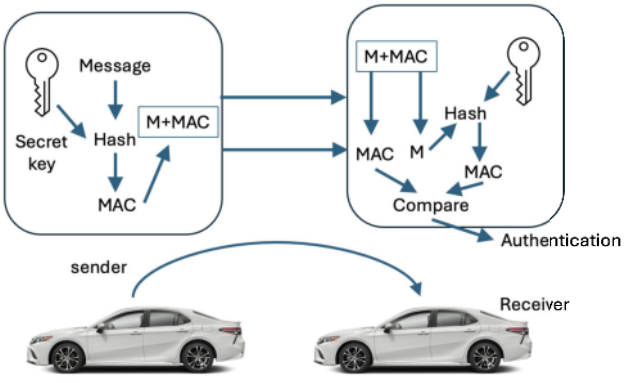

FIGURE 6. Pairwise symmetric key tobe calculated based on its identification of the communication counterpart.

Some prominent key disclosure security attacks include side-channel and leakage attacks, as side-channel attacks involve extracting sensitive information from the physical characteristics of a system, such as timing, power usage, or electromagnetic emissions. A novel MAC-based authentication scheme (NoMAS) proposed in [60] mitigates this leakage problem. The NoMAS scheme offers a solution for key disclosure issues by providing Hard Key and Soft Key Updates. The steps of NoMAS include the initialization, vehicle registration, authentication, message verification, password update, and key update stages, where symmetric keys are generated and shared across the connected vehicles. The work in [61] proposes a symmetric key for broadcasting basic safety messages in the same roadside unit group in a secured fashion. This group key is updated whenever a vehicle joins or leaves the network, making the system very secure by not even allowing the member leaving to access any current communication process. Through heuristic and Burrows-Abadi-Needham (BAN) [62] logic analysis which is used to verify the veracity of the security protocols, the authors verify the efficacy of this method.

The work in [63], proposed a quantum-key-based authentication and key agreement scheme that follows a role-based data access control Strategy. In this work, the vehicle privatization manages quantum session keys and the vehicles generate quantum session keys randomly. Secure agreement of the keys amongst vehicles is done through multilevel quantum keys such as the quantum prefilled key, the quantum protection key, and the quantum session key. Symmetric encryption algorithms and hash algorithms are used for authentication in this scheme to obtain better performance.

In [64], the authors present a quantum-resistant key management scheme tailored for Cellular-Vehicle-to-Everything (C-V2X) networks. Recognizing the vulnerabilities introduced by quantum computing to traditional cryptographic methods, the authors integrate blockchain technology with lattice-based cryptography to establish a decentralized system. The scheme ensures secure registration, key-agreement, periodic updates, and revocation processes. The results show a blockchain simulation validates its scalability under varying vehicle densities and transaction loads. Also, it provides a lightweight, efficient, and secure solution for key management in resource-constrained vehicular networks, addressing critical challenges such as single points of failure and the ever-growing threat of quantum computing.

C. ASYMMETRIC KEY AUTHENTICATION

Asymmetric key authentication is a cryptographic process that uses a pair of keys—a public key and a private key—to verify the identity of users. Contrary to symmetric encryption, asymmetric key authentication uses the public key to encrypt data and the private key to decrypt it, ensuring that only the intended recipient with the correct private key can access the information.

In [65], the authors propose a robust and scalable authentication scheme for vehicular networks based on Elliptic Curve Cryptography (ECC) to meet the diverse and growing service demands of autonomous vehicles. In this approach, vehicles register with a trusted authority (TA) once, enabling fast and efficient authentication with Cloud Service

Providers (CSPs). Any new CSP registered with the TA can participate in vehicular services seamlessly. A cloud broker, managed by the TA, connects all cloud services, simplifying user CSP selection. The security analysis shows that the scheme provides conditional privacy protection and meets the security needs of vehicular networks. Also, by utilizing ECC without complex bilinear pairings, the scheme is efficient and well-suited for vehicular network applications.

In [66], the authors propose a comprehensive security framework for vehicular networks featuring two main components: authentication and intrusion detection. The authentication module uses ECC to mutually authenticate the certificate authority, cluster heads, and vehicles, ensuring secure communications. The Intrusion Detection System (IDS) employs tensor-based dimensional reduction to reduce vehicular traffic data before analyzing it with Fuzzy C-Means (FCM) clustering combined with Multi-Objective Evolutionary Algorithm based on Decomposition (MOEA/D). However, the proposed framework uses a controller that can pose as a spoof. In addition, it does not protect against DoS or DDoS attacks, which are the biggest threat to availability.

Implementing lightweight authentication procedures is challenging while exchanging vehicle data in a vehicular cloud (VC). The study in [67] proposes a Dual Hashing-based Secure Hashing Algorithm-384 (DHS384) and Modified Elliptical Curve Cryptography (MECC). This method has an optimal resource allocation (RA) scheme to allocate resources optimally using the Improved Harris Hawks Optimization (IHHO) algorithm.

Researchers have found vulnerabilities in RSA public keys in recent years. For example, in 2020, in 75 million active RSA keys across the Internet, it was discovered that 1 in every 172 certificates using RSA keys is vulnerable to a practical attack known as 'factoring' [68]. In one of our recent works, we compare the algorithms ECC and RSA and compare the average time for digital signature formation. At the same security levels, we were able to conclude that ECC is 35.88% faster than RSA [9] (Figure 7). In order to obtain the same security level with a digital signature created by RSA with 3072 bits, ECC requires a 256-bit key, which leads to a less computationally expensive operation. These variations in the execution time have a dire impact on the underlying IoAV system. Researchers have compared the performance of ECC and RSA in line with key generation, encryption, and decryption time in [69]. RSA requires exponential calculation for encryption and decryption, on the other hand, the ECC algorithm (encryption and decryption) is faster and consistently displays better encryption (34%) and decryption speeds (35%).

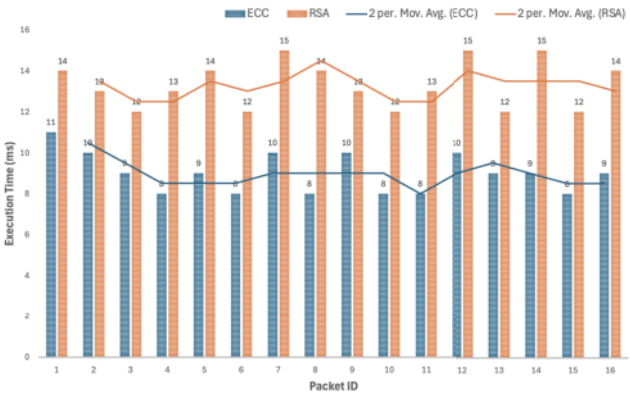

FIGURE 7. ECC is computationally less expensive and it is 35.88% faster than RSA while creating digital signatures [9].

D. CHALLENGE RESPONSE AUTHENTICATION

Challenge-response [17] is a lightweight authentication method used for verifying the identity of vehicles or their components by issuing a challenge to the connected vehicle. This challenge can be a random or specific request for authentication. The vehicle receiving the challenge generates a response, and if it is acceptable, a secret key is generated by the challenge-issuing Vehicle (as illustrated in Figure 8). The response is measured using hash functions or symmetric encryption schemes. The connected vehicles verify their authenticity using the same cryptographic algorithm and the shared secret key.

The security scheme in [70] proposes a challenge-response authentication protocol that uses upper-layer authentication to define the legitimacy of the corresponding terminal, and when verified, a location-dependent shared key is generated with minimal mismatched bits. Minimal mismatched bits between two vehicular entities improve the key agreement thus, enhancing the integrity of the exchanged messages critical for safe vehicular operations [71], [72], [73]. Based on the generated key, a PHY challenge-response algorithm for multi-carrier communication is generated for re-authentication. Simulation results of this proposed scheme show lower signal-to-noise ratios and are effective against active and passive attacks such as signatures forgery in the random oracle model.

The Wiggle protocol is a challenge-response scheme proposed in [74]. In this protocol, a challenge is issued to the candidate to be admitted into a platoon. This protocol is called wiggle because of the random longitudinal movements that the platoon is challenged to execute. This protocol prevents any attackers from joining the platoon and injecting fake vehicle control messages. They also utilize an adaptive cruise control (ACC) algorithm to execute the challenges and ensure the imperceptible changes to the vehicle's velocity while a Proof of Following (PoF) is executed.

The work in [75] proposes a lightweight and secure identity authentication protocol based on elliptic curve cryptography to furnish an effective and secure data transmission mechanism across a public communication channel for the Internet of Vehicles. The Physical Unclonable Function (PUF) is a hardware-based security technology that relies on the microscopic irregularities and physical characteristics of hardware devices to generate unique identifiers. PUF

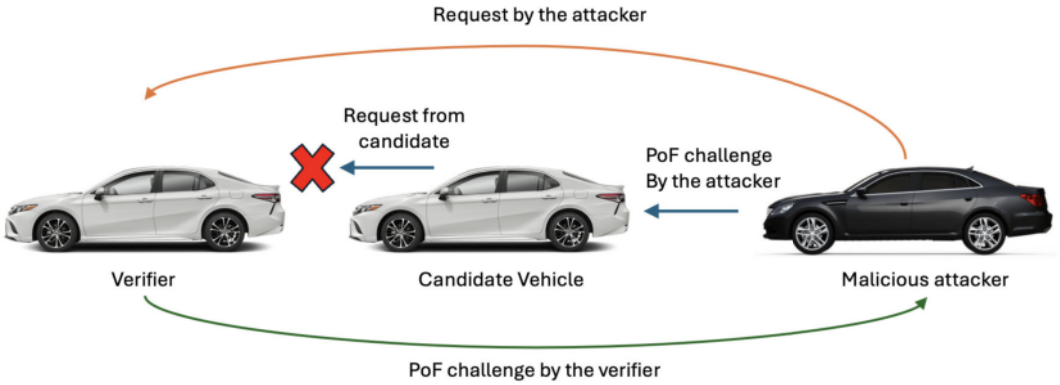

FIGURE 8. The malicious attacker prevents the platooning operation by intercepting the candidates' requests and replacing them with its own. The attacker masks itself as the verifier and issues a challenge.

generally functions using a challenge-response mechanism. When presented with a challenge, the PUF generates a distinct response based on its physical traits. This response serves as a unique identifier for the device. Due to the inherent irregularities in the hardware manufacturing process, even devices of the same model exhibit slight variations in their physical characteristics. This uniqueness makes PUF responses unclonable, meaning identical hardware models cannot generate the same response. As a result, the security of the system is enhanced.

E. LOW-RESOURCE AUTHENTICATION

With minimal computational resources in hand, the confidentiality and privacy of data transmitted between vehicles, roadside units (RSU), and control rooms is a critical issue that must be addressed effectively. Blockchain technology presents a potential solution for securing the IOVs because of its decentralization, stability, and transaction tracking capabilities. To overcome these issues, [76] introduces a blockchain-based lightweight authentication protocol for generating trustworthy IOV communication.

The work in [77] introduces an efficient and safe identity authentication scheme based on the Feige-Fiat-Shamir (FFS) zero-knowledge identification scheme [78] to resist guessing attacks. Unlike cryptographic schemes that require complex computations such as elliptic curves and large integer factorizations, the FFS scheme uses simpler number theory operations, thus effectively reducing the computational overhead.

A Certificate Authority (CA) is necessary for vehicles within communication range to establish authentication. However, as the vehicles move and the distance between them constantly varies, it is a challenge to make this happen. The work in [79] proposes a lightweight security protocol for authentication for V2X. This scheme employs a biometric device (BD) and a tamper-proof device (TPD), which together verify the driver and securely keep the keys. By decentralizing the CA's tasks by locally generating pseudo-identity and private keys for V2V authentication, the overall computational strain is reduced.

VI. CHALLENGES AND RESEARCH DIRECTIONS

Designing a secure authentication protocol for the IoAV involves multiple critical aspects to ensure the safety, integrity, and efficiency of vehicle communication. In the following, we give an outline of these aspects and their implementation considerations.

A. SECURE AND STRONG HASH FUNCTIONS

One research direction for IoAV is investigating the suitability of existing hash functions for developing a robust, lightweight authentication protocol. On the other hand, it is vital to tailor unique hash functions for IoAV applications to provide sufficient defense against differential and linear cryptanalysis. This line of research can explore modifications to the substitution box (S-box), a critical element in many symmetric cryptographic primitives, and assess the security implications of the enhanced S-box to provide sufficient defense against differential and linear cryptanalysis. Additionally, *it is crucial to explore cost-effective hardware implementation possibilities for deploying lightweight hash functions on resource-constrained devices with low power consumption* [80].

A solid cryptographic hash function must satisfy three criteria [81]:

- Preimage resistance: Retrieving the original message when the hash value is given should be challenging.
- Second Preimage Resistance (Weak Collision Resistance): It should be challenging to find a different message with the same hash value as a given message.
- Strong Collision Resistance: Finding two messages with the same hash value should be challenging.

A hash function takes an input of a fixed-size n-bit string and produces an m-bit string where $m < n$. The original hash function breaks the message into fixed-size blocks and produces a final message digest. These message digests can be of several types, such as MD2, MD4, and MD5,

which are used primarily for ensuring data integrity and verifying the authenticity of data [82], [83]. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST). Examples of the Secure Hash Algorithm include SHA-1, SHA-2, and SHA-3, with SHA-3 producing a message digest of 512 bits [81].

B. BLOCKCHAIN SOLUTIONS

Blockchain technology offers promising solutions for information security with its non-tampering, traceability, and collective maintenance features. It addresses challenges such as broadcast collision avoidance, resource scheduling, and privacy preservation in the IoAV context.

Blockchain is deployed in a decentralized fashion between entities such as vehicles, roadside units (RSUs), and other entities that act as nodes in the network. In line with IoAV's resource constraints and critical real-time requirements, a permissioned blockchain (e.g., Hyperledger Fabric [84]) is utilized. Permissioned blockchain restricts and can validate transactions, thus reducing computational overhead.

Cryptographic-based authentication methods such as Public Key Infrastructure (PKI), group signature, and identity-based schemes are adopted for IoAV. The PKI-based scheme aims to guarantee data integrity and privacy through PKI signatures. Nevertheless, due to the significant consumption of computing and communication resources, there is a need to enhance the efficiency of PKI-based authentication schemes. One method involves integrating PKI into decentralized blockchain systems to improve the security and integrity of the underlying networks. [85]. However, *it is crucial to carefully assess PKI-based and Blockchain schemes for their suitability in high vehicle density scenarios*, as they require substantial computing resources [86].

C. MINIMIZATION OF OVERHEAD COMMUNICATION

IoAV relies on low-latency and highly reliable communication. With heavy authentication and strong cryptographic techniques, there can be large overheads in IoAV systems. For instance, in one of our previous works, by integrating a lightweight hybrid cryptography scheme called TAKS [87] in a deterministic network protocol for intra-vehicle communication [88], we were able to witness an increase in delay between 20% and 60% based on the size of the keys of the cryptographic protocol. Also, the parameters governing the MAC layer of the protocol played a major role in determining the latency of the network and the incorporation of security into it. In one of our recent studies comparing various authentication schemes for cloud-enabled platooning [9], we arrived at the same conclusion: the authentication schemes, despite providing ample security, can also lead to large overheads and eventual breakdown of the system. With these studies in mind, *it is vital to define the tuning of several factors, such as network protocols, authentication schemes, and levels of security, for enabling good security in IoAV networks.*

D. SYSTEM DESIGN

In the realm of embedded IoT edge systems, including IoAV, computational resources are constrained, and tight timing constraints require a tradeoff between security and performance. Encompassing the entire system by modelling and analyzing end-to-end systems (hardware and software) is preferred over solely focusing on modeling security protocols like in [80], [85], and [86]. This is because it provides a holistic view of the system's security. This approach captures the complex interactions between components, identifies vulnerabilities that may arise from integration issues, and addresses systemic risks beyond protocol-specific flaws. It ensures that security measures are effectively balanced with performance, usability, and compliance requirements, enhancing overall resilience. By considering the full system, the possibility of developing accurate threat models, prioritizing risks, and future-proofing systems against emerging threats increases, resulting in a more robust and comprehensive security posture.

There exist a number of models of computation (MoC) and frameworks especially adapted for modeling, designing, and analyzing embedded systems. They usually focus on exposing parallelism, while providing tools for analyzing timing, memory use and communication bandwidth.

For instance, the dataflow MoC is regarded as a natural way of modeling stream processing in embedded applications, targeting both hardware and software implementations. For the automotive domain, [89] exposes a number of advantages of the dataflow MoC by introducing an approach transforming a Synchronous Dataflow (SDF) model into an automotive component. Some of these advantages come from the static analysis techniques, able to provide accurate information on throughput, latency, buffer sizes [90] and real-time behavior [91], [92]. Such insights help the designer to understand the system better and make informed decisions about the system architecture (hardware and software) and behavior. Toolchains based on dataflow MoCs, such as CAL/StreamBlocks [93], are becoming more mature and target both software and hardware implementations, starting with the same specification.

However, specific challenges persist: (i) targeted applications are distributed, spanning vehicles and road infrastructure rather than bound to a single computing platform [94]. This complexity requires intricate analyses and may call for unique communication channel models. Modern frameworks that are intended for distributed embedded applications, such as LinguaFranca [95], are still in their infancy and target mainly software implementations. In software-defined vehicles, optimizing dataflow and resource management is mandatory to achieve short response times, high throughput and predictability, which indirectly helps in ensuring the network's resilience under fluctuating conditions. Newer methods such as software-defined frameworks [96] refine the resource allocation and optimal resource distributions. Also, (ii) classic actor models (e.g., dataflow) inherently lack security considerations. For instance, incorporating

security layers into communication requires rethinking the framework and MoC components or adopting dedicated solutions specific to each application. Methods such as Concurrent Task Analysis (CoTA), System-Theoretic Process Analysis (STPA), and Fault Tree Analysis (FTA) have been used in the literature to mitigate operational safety hazards [97] but they do not incorporate security layers dedicated to hardware/software level. Solving the above challenges will allow more accurate analyses factoring in the overhead caused by security protocols and message encryption/decryption. In turn, these will yield more accurate estimates within realistic scenarios, which is crucial for illustrating how security measures impact timing and system resources.

VII. CONCLUSION

The Internet of Things (IoT) is a network of physical objects that are equipped with sensors, software, and other technologies to connect and exchange data over the Internet. Over the past decade, its rapid expansion has impacted various areas, including intelligent vehicular systems. The Internet of Autonomous Vehicles (IoAV), a subset of IoT, aims to enable autonomous driving without human intervention. However, the dynamic environments in which autonomous vehicles operate present significant challenges, such as real-time communication and security vulnerabilities. These challenges cannot be effectively addressed by traditional cybersecurity solutions designed for static IoT environments.

This survey article presents an overview of the current security issues related to the Internet of Autonomous Vehicles (IoAV) and their respective solutions. The survey highlights several crucial challenges when developing a lightweight authentication protocol within an IoAV ecosystem. It emphasizes the necessity of exploring cost-effective hardware implementations for deploying lightweight hash functions and evaluating PKI-based blockchain schemes for their suitability in high vehicle density scenarios. Additionally, it emphasizes the importance of defining network protocol parameters, system designs, and authentication schemes to enable secure IoAV systems without making compromises. Last but not least, enhancing the security and trustworthiness of an IoAV ecosystem through lightweight protocols deserves significant attention.

In the future, creating a secure and efficient authentication protocol for the Internet of Autonomous Vehicles (IoAV) is critical. This includes finding a balance between security and performance. Researchers must develop specific hash functions to protect against cryptanalysis and integrate Public Key Infrastructure (PKI) within decentralized blockchain systems to achieve this. Since PKI and blockchain can be computationally demanding in environments with a high density of vehicles, it is crucial to assess their performance carefully to prevent system delays. Additionally, it is essential to optimize network protocols and authentication schemes to maintain low latency in IoAV communication. To fully understand how security measures affect overall system performance, we should model the larger parts of the system using dataflow-based frameworks that are able to model both hardware and software. Overcoming challenges such as the distributed nature of IoAV and the lack of inherent security in traditional modeling frameworks is essential for an accurate and realistic analysis of security protocols in these networks.

REFERENCES

[1] P. A. Hancock, I. Nourbakhsh, and J. Stewart, "On the future of transportation in an era of automated and autonomous vehicles," *Proc. Nat. Acad. Sci. USA*, vol. 116, no. 16, pp. 7684–7691, Apr. 2019.

[2] M. L. Cunningham and M. Regan, "Autonomous vehicles: Human factors issues and future research," in *Proc. Australas. Road Saf. Conf.*, vol. 14, Oct. 2015, pp. 1–11.

[3] 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 Commun.*, vol. 26, no. 4, pp. 60–65, Aug. 2019.

[4] H. Kurunathan, J. Santos, D. Moreira, and P. M. Santos, "Towards safe cooperative autonomous platoon systems using COTS equipment," in *Proc. IEEE 24th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2023, pp. 464–469.

[5] J. Pereira, H. Kurunathan, E. Filho, and P. M. Santos, "Edge-aided V2X collision avoidance with platoons: Towards a hybrid evaluation toolset," in *Proc. 53rd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops (DSN-W)*, Jun. 2023, pp. 68–71.

[6] R. Reddy, L. Almeida, H. Kurunathan, M. G. Gaitán, P. M. Santos and E. Tovar, "Worst-case response time of mixed vehicles at complex intersections," *IEEE Open J. Intell. Transp. Syst.*, vol. 5, pp. 186–201, 2024, doi: 10.1109/OJITS.2024.3368797.

[7] R. Reddy, L. Almeida, M. Gaitan, H. Kurunathan, P. Santos, and E. Tovar, "Work-in-progress: Worst-case response time of intersection management protocols," in *Proc. IEEE Real-Time Syst. Symp. (RTSS)*, Dec. 2021, pp. 556–559.

[8] M. Araújo, J. Silva, P. M. Santos, H. Singh, D. Gunjal, J. Fonseca, P. Duarte, B. Mendes, R. Barbosa, P. Steenkiste, S. Sabamoniri, L. Lam, J. Pereira, and H. Kurunathan, "Demo: Object detection under 5G-edge mobility," in *Proc. IEEE 24th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2023, pp. 343–345.

[9] R. Rafael and E. T. Harrison Kurunathan, "An RT-cloud solution towards security in vehicular platooning systems," in *Proc. 35th Euromicro Conf. Real-Time Syst. Real-Time Cloud Workshop*, vol. 2, 2023, pp. 1–6.

[10] S. Vasavi, K. Aswarth, T. Sai Durga Pavan, and A. Anu Gokhale, "Predictive analytics as a service for vehicle health monitoring using edge computing and AK-NN algorithm," *Mater. Today, Proc.*, vol. 46, pp. 8645–8654, Aug. 2021.

[11] U. Shafi, A. Safi, A. R. Shahid, S. Ziauddin, and M. Q. Saleem, "Vehicle remote health monitoring and prognostic maintenance system," *J. Adv. Transp.*, vol. 2018, no. 1, pp. 1–10, 2018.

[12] E. Alalwany and I. Mahgoub, "Security and trust management in the Internet of Vehicles (IoV): Challenges and machine learning solutions," *Sensors*, vol. 24, no. 2, p. 368, Jan. 2024.

[13] N. U. A. Tahir, Z. Zhang, M. Asim, J. Chen, and M. Elaffendi, "Object detection in autonomous vehicles under adverse weather: A review of traditional and deep learning approaches," *Algorithms*, vol. 17, no. 3, p. 103, Feb. 2024.

[14] P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu, and H. Ma, "Federated learning-based collaborative authentication protocol for shared data in social IoV," *IEEE Sensors J.*, vol. 22, no. 7, pp. 7385–7398, Apr. 2022.

[15] H. Hemavathi, S. R. Akhila, Y. Alotaibi, O. I. Khalaf, and S. Alghamdi, "Authentication and resource allocation strategies during handoff for 5G IoVs using deep learning," *Energies*, vol. 15, no. 6, p. 2006, Mar. 2022.

[16] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, "Software-defined vehicular networks with trust management: A deep reinforcement learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1400–1414, Feb. 2022.

[17] M. A. Shawky, S. T. Shah, M. Abdrabou, M. Usman, Q. H. Abbasi, D. Flynn, M. A. Imran, S. Ansari, and A. Taha, "How secure are our roads? An in-depth review of authentication in vehicular communications," *Veh. Commun.*, vol. 47, Jun. 2024, Art. no. 100784.

[18] I. Pali, R. Amin, and M. Abdussami, "Autonomous vehicle security: Current survey and future research challenges," *Secur. PRIVACY*, vol. 7, no. 3, p. 367, May 2024.

[19] T. K. Mohd, S. Majumdar, A. Mathur, and A. Y. Javaid, "Simulation and analysis of DDoS attack on connected autonomous vehicular network using OMNET++," in *Proc. 9th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Nov. 2018, pp. 502–508.
[20] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Proc. 14th Int. Conf. Detection Intrusions Malware, Vulnerability Assessment (DIMVA)*, Bonn, Germany. Cham, Switzerland: Springer, Jan. 2017, pp. 185–206.
[21] F. R. Schreiber, *Sybil: The True Story of a Woman Possessed by Sixteen Separate Personalities*. Chicago, IL, USA: Regnery, 1973.
[22] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7298–7303.
[23] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog computing security challenges and future directions [energy and security]," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 92–96, May 2019.
[24] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, "Formal security analysis of LoRaWAN," *Comput. Netw.*, vol. 148, pp. 328–339, Jan. 2019.
[25] L. Pankaczi and M. Eldefrawy, "Enhancing the security of ISO/IEC 14443-3 and 4 RFID authentication protocols through formal analysis," in *Proc. IEEE Int. Conf. Omni-layer Intell. Syst. (COINS)*, Jul. 2023, pp. 1–6.
[26] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022.
[27] S. Sharma and B. Kaushik, "A survey on Internet of Vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100182.
[28] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment," *IEEE Access*, vol. 8, pp. 167875–167886, 2020.
[29] A. Ghosal, S. Halder, and M. Conti, "STRIDE: Scalable and secure over-the-air software update scheme for autonomous vehicles," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
[30] T. Roccia, "Today's connected cars vulnerable to hacking, malware," Mcafee, Tech. Rep., Mar. 2018. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/todays-connected-cars-vulnerable-hacking-malware/
[31] S. Rizvi, J. Willet, D. Perino, S. Marasco, and C. Condo, "A threat to vehicular cyber security and the urgency for correction," *Proc. Comput. Sci.*, vol. 114, pp. 100–105, Aug. 2017.
[32] G. Avoine, M. A. Bingöl, S. Karda , C. Lauradoux, and B. Martin, "A framework for analyzing RFID distance bounding protocols," *J. Comput. Secur.*, vol. 19, no. 2, pp. 289–317, Mar. 2011.
[33] D. Jacobs, K. R. Choo, M.-T. Kechadi, and N.-A. Le-Khac, "Volkswagen car entertainment system forensics," in *Proc. IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 699–705.
[34] *How a Credential Phishing Attack Could Lead to Tesla Car Theft and How to Mitigate It*. Accessed: May 3, 2024. [Online]. Available: https://vicone.com/blog/how-a-credential-phishing-attack-could-lead-to-tesla-car-theft-and-how-to-mitigate-it
[35] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, and W. Alasmary, "Security and privacy issues in autonomous vehicles: A layer-based survey," *IEEE Open J. Commun. Soc.*, vol. 3, pp. 811–829, 2022.
[36] G. Vailoces, A. Keith, A. Almehmadi, and K. El-Khatib, "Securing the electric vehicle charging infrastructure: An in-depth analysis of vulnerabilities and countermeasures," in *Proc. Int. ACM Symp. Design Anal. Intell. Veh. Netw. Appl.*, Oct. 2023, pp. 31–38.
[37] B. Vaidya and H. T. Mouftah, "Multimodal and multi-pass authentication mechanisms for electric vehicle charging networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 371–376.
[38] A. Drozhzhin, "Black hat USA 2015: The full story of how that jeep was hacked," Kaspersky Lab Daily, vol. 6, Aug. 2015. [Online]. Available: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/
[39] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, A. Khalil, M. A. Al-Shareeda, B. A. Mohammed, A. A. Alsadhan, A. M. Alayba, A. M. S. Saleh, H. A. Al-Reshidi, and K. Almekhlafi, "Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5G-assisted vehicular communications," *IEEE Access*, vol. 12, pp. 71232–71247, 2024.
[40] *Can Injection Attack—A New Tactic to Steal Smart Vehicles*. Accessed: Aug. 14, 2023. [Online]. Available: https://cyware.com/news/can-injection-attack-a-new-tactic-to-steal-smart-vehicles-1b1529f2
[41] J. Patel, M. L. Das, and S. Nandi, "On the security of remote key less entry for vehicles," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2018, pp. 1–6.
[42] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," *IEEE Access*, vol. 10, pp. 86127–86180, 2022.
[43] P. Bagga, A. Kumar Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in Internet of Vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.
[44] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, "Security and privacy in the industrial Internet of Things: Current standards and future challenges," *IEEE Access*, vol. 8, pp. 152351–152366, 2020.
[45] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 2985–2996, May 2021.
[46] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A survey on the usage of blockchain technology for cyber-threats in the context of Industry 4.0," *Sustainability*, vol. 12, no. 21, p. 9179, Nov. 2020.
[47] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 110–113, Jan. 2014.
[48] S. C. Hpl, "Introduction to the controller area network (CAN)," Appl. Rep. SLOA101, Aug. 2002, pp. 1–17.
[49] A. Martínez-Cruz, K. A. Ramírez-Gutiérrez, C. Feregrino-Uribe, and A. Morales-Reyes, "Security on in-vehicle communication protocols: Issues, challenges, and future research directions," *Comput. Commun.*, vol. 180, pp. 1–20, Dec. 2021.
[50] P.-S. Murvay and B. Groza, "Efficient physical layer key agreement for FlexRay networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9767–9780, Sep. 2020.
[51] D. Püllen, N. A. Anagnostopoulos, T. Arul, and S. Katzenbeisser, "Security and safety co-engineering of the FlexRay bus in vehicular networks," in *Proc. Int. Conf. Omni-Layer Intell. Syst.*, May 2019, pp. 31–37.
[52] D. Püllen, N. A. Anagnostopoulos, T. Arul, and S. Katzenbeisser, "Securing FlexRay-based in-vehicle networks," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103144.
[53] P. Hank, S. Müller, O. Vermesan, and J. Van Den Keybus, "Automotive Ethernet: In-vehicle networking and smart mobility," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2013, pp. 1735–1739.
[54] A. Ioana, A. Korodi, and I. Silea, "Automotive IoT Ethernet-based communication technologies applied in a V2X context via a multi-protocol gateway," *Sensors*, vol. 22, no. 17, p. 6382, Aug. 2022.
[55] H. Khemissa and P. Urien, "Towards a centralized security architecture for SOME/IP automotive services," in *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, Sep. 2023, pp. 977–978.
[56] P. M. Rao, "2PSLAF: Privacy-preserving secure lightweight authentication framework for vehicle-to-vehicle communications," *Res. Square*, Jan. 2024, doi: 10.21203/rs.3.rs-1298797/v3.
[57] S. Abbes and S. Rekhis, "Reinforcement learning for intelligent sensor virtualization and provisioning in Internet of Vehicles (IoV)," *IEEE Access*, vol. 12, pp. 54352–54370, 2024.
[58] J. Liu, S. Xu, R. Liu, Y. Tian, X. Zhu, and J. Xie, "LIA-V2X: A lightweight identity mutual and batch authentication protocol for V2X communication in Internet of Vehicles," 2024.
[59] J. Yoo and J. H. Yi, "Code-based authentication scheme for lightweight integrity checking of smart vehicles," *IEEE Access*, vol. 6, pp. 46731–46741, 2018.
[60] H. Sikarwar and D. Das, "A novel MAC-based authentication scheme (NoMAS) for Internet of Vehicles (IoV)," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 5, pp. 4904–4916, May 2023.
[61] Z. Zhou, X. Liu, C. Wang, and R. Lu, "Efficient and secure authentication scheme for Internet of Vehicles," in *Proc. Int. Conf. Intell. Inf. Process.* Cham, Switzerland: Springer, Jan. 2024, pp. 469–485.
[62] M. T. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.
[63] Q. Shi, Z. Yang, T. Cheng, C. Wang, Z. Wu, X. Zhang, and P. Xu, "QKBAKA: A quantum-key-based authentication and key agreement scheme for Internet of Vehicles," *IEEE Internet Things J.*, vol. 11, no. 7, pp. 12292–12306, Jul. 2023.

[64] Y. Gong and B.-J. Hu, "A quantum-resistant key management scheme using blockchain in C-V2X," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 11, pp. 16831–16844, Nov. 2024.

[65] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1654–1667, 2020.

[66] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8421–8434, Sep. 2019.

[67] J. Varalakshmi and S. Dhanasekaran, "A dual hashing-based authentication and secure data transmission scheme for vehicular cloud environment using MECC with optimal resource allocation mechanism," *Soft Comput.*, vol. 28, nos. 17–18, pp. 10423–10437, Sep. 2024.

[68] J. Kilgallin and R. Vasko, "Factoring RSA keys in the IoT era," in *Proc. 1st IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA)*, Dec. 2019, pp. 184–189.

[69] M. R. Khan, K. Upreti, M. I. Alam, H. Khan, S. T. Siddiqui, M. Haque, and J. Parashar, "Analysis of elliptic curve cryptography & RSA," *J. ICT Standardization*, vol. 11, no. 4, pp. 355–378, Nov. 2023.

[70] M. A. Shawky, M. Bottarelli, G. Epiphaniou, and P. Karadimas, "An efficient cross-layer authentication scheme for secure communication in vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 8738–8754, Jul. 2023.

[71] H. Kurunathan, K. Li, W. Ni, N. Li, E. Tovar, and M. Guizani, "Exploring LSTM-assisted A2C for physical layer security in vehicular cyber-physical systems," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2024, pp. 1177–1182.

[72] H. Kurunathan, K. Li, E. Tovar, A. Mario Jorge, W. Ni, and A. Jamalipour, "DRL-KeyAgree: An intelligent combinatorial deep reinforcement learning-based vehicular platooning secret key generation," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 11, pp. 16354–16369, Nov. 2024.

[73] K. Li, H. Kurunathan, R. Severino, and E. Tovar, "Cooperative key generation for data dissemination in cyber-physical systems," in *Proc. ACM/IEEE 9th Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2018, pp. 331–332.

[74] C. Dickey, C. Smith, Q. Johnson, J. Li, Z. Xu, L. Lazos, and M. Li, "Wiggle: Physical challenge-response verification of vehicle platooning," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2023, pp. 54–60.

[75] S. Wang, Z. Fan, Y. Su, B. Zheng, Z. Liu, and Y. Dai, "A lightweight, efficient, and physically secure key agreement authentication protocol for vehicular networks," *Electronics*, vol. 13, no. 8, p. 1418, Apr. 2024.

[76] A. Singh, P. Rani, J. V. N. Ramesh, S. V. Athawale, A. H. Alkhayyat, A. N. Aledaily, T. A. Prola, and R. Sharma, "Blockchain-based lightweight authentication protocol for next-generation trustworthy Internet of Vehicles communication," *IEEE Trans. Consum. Electron.*, vol. 70, no. 2, pp. 4898–4907, May 2024.

[77] M. Han, Z. Yin, P. Cheng, X. Zhang, and S. Ma, "Zero-knowledge identity authentication for Internet of Vehicles: Improvement and application," *PLoS ONE*, vol. 15, no. 9, Sep. 2020, Art. no. e0239043.

[78] J. M. Kizza, "Feige–Fiat–Shamir ZKP scheme revisited," *Int. J. Comput. ICT Res.*, vol. 4, no. 1, pp. 9–19, 2010.

[79] S. A. Abdel Hakeem, M. A. Abd El-Gawad, and H. Kim, "A decentralized lightweight authentication and privacy protocol for vehicular networks," *IEEE Access*, vol. 7, pp. 119689–119705, 2019.

[80] S. Windarta, S. Suryadi, K. Ramli, A. A. Lestari, W. Wildan, B. Pranggono, and R. W. Wardhani, "Two new lightweight cryptographic hash functions based on saturnin and beetle for the Internet of Things," *IEEE Access*, vol. 11, pp. 84074–84090, 2023.

[81] J. R. Vacca, *Cyber Security and IT Infrastructure Protection*. Rockland, MA, USA: Syngress, 2013.

[82] V. Fomichev, D. Bobrovskiy, A. Koreneva, T. Nabiev, and D. Zadorozhny, "Data integrity algorithm based on additive generators and hash function," *J. Comput. Virol. Hacking Techn.*, vol. 18, no. 1, pp. 31–41, Mar. 2022.

[83] C. Nist, "The digital signature standard," *Commun. ACM*, vol. 35, no. 7, pp. 36–40, Jul. 1992.

[84] J. Enare Abang, H. Takruri, R. Al-Zaidi, and M. Al-Khalidi, "Latency performance modelling in hyperledger fabric blockchain: Challenges and directions with an IoT perspective," *Internet Things*, vol. 26, Jul. 2024, Art. no. 101217.

[85] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and PKI system," *High-Confidence Comput.*, vol. 3, no. 1, Mar. 2023, Art. no. 100096.

[86] Z. Xu, X. Li, J. Xu, W. Liang, and K.-K.-R. Choo, "A secure and computationally efficient authentication and key agreement scheme for Internet of Vehicles," *Comput. Electr. Eng.*, vol. 95, Oct. 2021, Art. no. 107409.

[87] W. Tiberti, B. Vieira, H. Kurunathan, R. Severino, and E. Tovar, "Tightening up security in low power deterministic networks," in *Proc. 16th IEEE Int. Conf. Factory Commun. Syst. (WFCS)*, Apr. 2020, pp. 1–7.

[88] H. Kurunathan, R. Severino, Ê. Filho, and E. Tovar, "WiCAR—Simulating towards the wireless car," in *Proc. Comput. Saf., Rel., Secur. SAFECOMP Workshops*, Lisbon, Portugal. Cham, Switzerland: Springer, Sep. 15, 2020, pp. 136–147.

[89] M. O. Aybek, R. Jordão, J. Lundbäck, K.-L. Lundbäck, and M. Becker, "From the synchronous data flow model of computation to an automotive component model," in *Proc. 26th IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2021, pp. 1–8, doi: 10.1109/ETFA45728.2021.9613621.

[90] M. Boulasikis, F. Gruian, G. Callanan, and J. W. Janneck, "Analysing dataflow programs with causation traces," in *Proc. Int. Conf. Parallel Architectures Compilation Techn.*, Oct. 2022, pp. 534–535.

[91] H. I. Ali, B. Akesson, and L. M. Pinho, "Generalized extraction of real-time parameters for homogeneous synchronous dataflow graphs," in *Proc. 23rd Euromicro Int. Conf. Parallel, Distrib., Netw.-Based Process.*, Mar. 2015, pp. 701–710.

[92] H. I. Ali, B. Akesson, and L. M. Pinho, "Combining dataflow applications and real-time task sets on multi-core platforms," in *Proc. 20th Int. Workshop Softw. Compil. Embedded Syst.*, Jun. 2017, pp. 60–63.

[93] E. Bezati, M. Emami, J. Janneck, and J. Larus, "StreamBlocks: A compiler for heterogeneous dataflow computing (technical report)," 2021, *arXiv:2107.09333*.

[94] G. Callanan and F. Gruian, "Estimating stream application performance in early-stage system design," in *Proc. 56th Asilomar Conf. Signals, Syst., Comput.*, Oct. 2022, pp. 816–823.

[95] M. Lohstroh, C. Menard, S. Bateni, and E. A. Lee, "Toward a lingua franca for deterministic concurrent systems," *ACM Trans. Embedded Comput. Syst.*, vol. 20, no. 4, pp. 1–27, May 2021, doi: 10.1145/3448128.

[96] A. Nahar, K. K. Mondal, D. Das, and R. Buyya, "Clouds on the road: A software-defined fog computing framework for intelligent resource management in vehicular ad-hoc networks," *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 12778–12792, Dec. 2024.

[97] C. Correa-Jullian, M. Ramos, A. Mosleh, and J. Ma, "Operational safety hazard identification methodology for automated driving systems fleets," *Proc. Inst. Mech. Eng., O, J. Risk Rel.*, 2024, doi: 10.1177/1748006X241233863.

HAZEM ISMAIL ALI received the Ph.D. degree in electrical and computer engineering focused on real-time embedded systems from the Faculty of Engineering (FEUP), University of Porto, Portugal, in 2017. He is currently an Assistant Professor with the Department of Computing and Electronics for Real-Time and Embedded Systems (CERES), School of Information Technology (ITE), Halmstad University (HH), Sweden. His research interests include real-time embedded systems, high-performance computing, the Internet of Things (IoT), hardware/software acceleration, and embedded system design.

HARRISON KURUNATHAN received the bachelor's degree in electronics and communication engineering from SRM University, India, in 2012, the master's degree in very large-scale integration from the SSN College of Engineering, Anna University, India, in 2014, and the Ph.D. degree in electrical and computer engineering from the University of Porto, Portugal, in 2021. He is currently an Integrated Researcher with CISTER, Porto, Portugal. Before his current role, he was an Assistant Professor with the Department of Electronics and Communication Engineering, SRM University. His research interests include machine learning, wireless sensor networks, visible light communication (VLC), network protocols, network security, the Internet of Things (IoT), and cooperative cyber-physical systems (CPS).

MOHAMED HAMDY ELDEFRAWY received the Doctorate degree in electrical engineering from Alexandria University, Egypt, in 2014. He was a Senior Researcher with the Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia, and later as a Postdoctoral Researcher with the Department of Information Systems and Technology, Mid Sweden University, Sundsvall, Sweden. Currently, he holds an associate professor (senior lecturer) position with the School of Information Technology, Halmstad University, Sweden. With over 25 research articles published in esteemed journals and conferences, he is also the inventor of two U.S./PCT patents in cybersecurity. His research interests include network security, digital authentication, and information assurance. He was awarded the Bronze Medal at the 41st International Exhibition of Inventions in Geneva, Switzerland, in April 2013, and serves as a technical reviewer for numerous international journals and conferences.

FLAVIUS GRUIAN received the Diploma of Engineering degree in computer science from Politehnica University of Timisoara, Timisoara, Romania, in 1996, and the Ph.D. degree in computer science from Lund University, Sweden, in 2002. He is currently an Associate Professor in embedded systems with the Department of Computer Science, Lund University, Sweden. From 2005 to 2006 he was a Postdoctoral Fellow of the Department of Electrical and Computer Engineering, University of Auckland, New Zealand. His research interests include scheduling for real-time systems, low-power and low-energy systems, hardware/software co-design, the IoT, languages and tools for streaming applications, and compilation for ML hardware.

MAGNUS JONSSON (Senior Member, IEEE) received the B.S. and M.S. degrees in computer engineering from Halmstad University, Halmstad, Sweden, in 1993 and 1994, respectively, and the Licentiate of Technology and Ph.D. degrees in computer engineering from the Chalmers University of Technology, Gothenburg, Sweden, in 1997 and 1999, respectively. From March 1998 to March 2003, he was an Associate Professor in data communication with Halmstad University (acting between 1998 and 2000). Since 2003, he has been a Full Professor in real-time computer systems with Halmstad University, where he is currently the Deputy Program Director for the university-wide profile area smart cities and communities. Among previous assignments with Halmstad University are, e.g., the Department Manager, the Vice Dean, and the Director of Research. He has published over 135 scientific articles and book chapters, most of them in the areas of vehicular communication, real-time communication, industrial communication, wireless networking, real-time and embedded computer systems, optical networking, and optical interconnection architectures. He has served on the program committees of over 80 conferences and workshops and served as the International Liaison Co-Chair for the 28th International Conference on Distributed Computing Systems (ICDCS 2008), the General Co-Chair for the Fifth International Workshop on Multiple Access Communications (MACOM-2012) and MACOM 2016, and the TCP Co-Chair for Nets4cars-Nets4trains 2013, MACOM 2013, Nets4cars-Nets4trains 2014, and MACOM 2015. He has got five best paper awards.