

Automotive Ethernet architecture and security: challenges and technologies

Wael Toghuj¹, Nidal Turab²

¹Department of Computer Science, Al-Ahliyya Amman University, Amman, Jordan

²Department of Networks and Cybersecurity, Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received Sep 24, 2022

Revised Mar 7, 2023

Accepted Mar 9, 2023

Keywords:

Automotive ethernet

Autonomous vehicles

Intrusion detection system

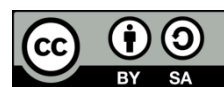
In-vehicle network

Time sensitive network

ABSTRACT

Vehicle infrastructure must address the challenges posed by today's advances toward connected and autonomous vehicles. To allow for more flexible architectures, high-bandwidth connections and scalability are needed to connect many sensors and electronic control units (ECUs). At the same time, deterministic and low latency is a critical and significant design requirement to support urgent real-time applications in autonomous vehicles. As a recent solution, the time-sensitive network (TSN) was introduced as Ethernet-based amendments in IEEE 802.1 TSN standards to meet those needs. However, it had hurdle to be overcome before it can be used effectively. This paper discusses the latest studies concerning the automotive Ethernet requirements, including transmission delay studies to improve worst-case end-to-end delay and end-to-end jitter. Also, the paper focuses on the securing Ethernet-based in-vehicle networks (IVNs) by reviewing new encryption and authentication methods and approaches.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Wael Toghuj

Department of Computer Science, Al-Ahliyya Amman University

Al-Saro, 19328, Amman, Jordan

Email: w.toghuj@ammanu.edu.jo

1. INTRODUCTION

Innovations in automotive design had led to an exponential growth in vehicle electronics. Modern vehicle design enhancements are due in huge amount to the usage of electronics to motorized systems. Vehicle tasks are divided into systems and sub-systems for the sake of passenger protection, reassurance and entertainment [1]. These systems must exchange data with one another over a complicated diverse in-vehicle network (IVN). IVN contain several communication protocols involving controller area network (CAN) [2], local interconnect network (LIN) [3], and FlexRay [4] protocols.

Currently, high-end cars like the BMW 7-Series with advanced technologies such as advanced driver-assistance systems (ADAS) may contain 150 or more electronic control units (ECUs), which are connected by IVN [5], [6]. Consequently, these architectures will require more bandwidth inside the vehicle, and functional safety will become more important [7]. Furthermore, the trend of autonomous driving will require hundreds of millions of lines of code in cars. For example, Tesla model 3 is equipped with eight surround cameras that provide 360° visibility around the vehicle at a range of up to 250 meters; twelve ultrasonic sensors comprise this vision system, automating such processes can require computations in the range of tera operations per second (TOPS) [8].

Another aspect of automotive networks is the vehicle to everything (V2X) is a vehicular communication system, where vehicle can communicate not only to other vehicles but also with traffic infrastructure, pedestrian and vehicle to another data network such as the cloud as illustrated in Figure 1 [9].

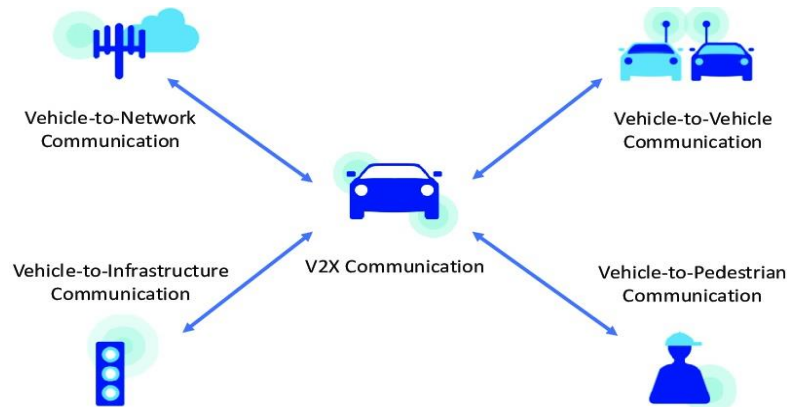


Figure 1. Vehicle to everything communication

Essential requirements for automotive networks are security and low-latency communication to comply with the strict performance constraints of such safety-critical vehicular purposes. However, the existing IVNs (LIN, CAN, and FlexRay) are not capable of providing sufficient bandwidth and have minimal flexibility and security. Thus, car manufacturers are preparing to take a giant step into IVN by deploying an Ethernet communication system between ECUs. As a result of adding several extensions to time-triggered (TT) Ethernet, the time-sensitive network (TSN) framework is defined in IEEE 802.1 TSN standards to manage and integrate safety-critical applications such as autonomous vehicles [10]. Therefore, today TSN has emerged as a front-runner and a competing technology to the well-established field-bus standard that have been the staple of industrial and automotive networking.

Still, the special characteristics of automotive networks bring a lot of hacking attacks, security gaps and other car network security problems that had serious effect on car driving safety and personal privacy, to improving trustworthy and effective algorithms and protocols. This paper discusses automotive TSN requirements including transmission delay studies to improve worst-case end-to-end delay (WCD) and end-to-end jitter. In addition to a survey of the security concerns related to automotive networks, we also focused on the need for the network security of automotive Ethernet. Moreover, this paper also provides insights into some countermeasures against cyber threats such as authentication, encryption, blockchain, and intrusion detection and prevention systems. In the next section we provide an overview of the latest studies regarding automotive TSN's functional and structural requirements.

2. REQUIREMENTS OF AUTOMOTIVE TSN

As noted in [11], the authors derived a list of requirements for future IVN processing platforms that must be met in order to satisfy the needs of the industry in the future. Two perspectives are used to analyze requirements: i) functional requirements, which define the functionalities or features the gateway (GW) controllers must support and ii) structural requirements, which describe the architectural and design aspects of the GW that are essential to its viability. A gap was detected in their analysis: no architecture exists yet that can satisfy all future automotive GW controller requirements. Furthermore, none of the solutions currently available addresses both structural and functional requirements simultaneously. Due to these constraints, GW chipsets for automotive networks cannot achieve all functionality and performance as well as flexibility and scalability.

Using the IEEE 802 automotive Ethernet architecture, TSN guarantees a keyframe transmission delay. Despite this, most studies on automotive TSN performance are based on a specific system and lacks a comprehensive and organized methodology. It is discussed in [6] how to design an optimal automotive TSN system and the methodology of designing automotive TSN systems from a global and holistic perspective. It is necessary to analyze the delay and jitter for each traffic to determine if the TSN design is successful. Therefore, the authors presented a complete and systematic automotive TSN simulation platform that used to study further scheduling algorithms and mechanisms, including either single or mixed scheduling algorithms. As an ultimate step, the authors examined the performance of a TSN network for autonomous driving, which was designed by a key motor company in Shanghai and contained traffic from a wide variety of domains.

An automotive Ethernet TSN profile has been implemented in [12] to increase real-time Ethernet functionality for the electrical and electronic (E/E) architecture. The authors evaluated multiple traffic shaping and scheduling mechanisms among automotive Ethernet systems. Each GW is equipped with TSN bridging. Around seventeen cyclic and periodic communication streams between different endpoints were created to

simulate a stable automotive network. Based on the OMNeT++ simulation framework, they implemented four sets of simulations, with different schedulers and shapers for parallel comparisons. Based on their obtained results, time-aware shaping ensures the shortest worst-case transmission latency for high-priority streams but gives a longer transmission latency for low-priority streams.

It is becoming increasingly important to integrate TSN with software-defined networking (SDN) to facilitate innovations in adaptability. According to [13], a per-class flow control scheme for TSN is proposed as part of software-defined in-vehicle systems. To facilitate per-class flow management, they introduced composability to WCD analysis of audio video bridging (AVB) flows. No matter what changes were made to other traffic classes, the composable WCD bound remained valid. Consequently, low-priority flows are not concerned about deadline violations when high-priority flows change. As a result, the analysis time is also reduced by up to 2.6x by simplifying the computation and enabling parallelization. When a similar amount of run-time was consumed, the proposed algorithm with hop-based weights could route roughly 1.6x more flows than existing solutions.

An analytical overview of the state-of-the-art of SDN-based security in automotive networks was presented in [14]; SDN with automotive Ethernet enabled more bandwidth, as a result, TSN real-time needs can be met. SDN provides centralized network intelligence using a network controller. Altogether, SDN opens new attack possibilities due to loss of control over all forwarding devices in case of controller failure or faulty network functions; stream rules can separate traffic. For example, crucial safety methods can be made difficult by the infotainment system. Security solutions like transport layer security (TLS), media access control security (MACsec), authentication, and anomaly detection systems (ADSs) could avoid unauthorized access to the network.

In autonomous vehicles, there were an increasing number of automotive ECUs as well as more advanced capabilities and features. Various automotive data types and formats must be transmitted and received by the ECU using heterogeneous automotive protocols and networks. Using a single link, whether it is an automotive Ethernet or a wireless medium, [15] proposed a new architecture and a data management method for a trailer ECU so that heterogeneous automotive networks can be communicated simultaneously. In addition, existing automotive networks can be integrated. Their experiment evaluated the performance of named data networking (NDN) as a communication protocol between ECUs, test results indicate that NDN is well suited for vehicular communication and has a high likelihood of meeting requirements.

Weiss and Steinhorst [16] proposed an approach that enables graceful degradation for real-time autonomous vehicle applications. It allows graceful degradation of the system while maintaining fail-operational requirements of critical applications, ensuring predictable end-to-end timing constraints, and ensuring graceful system degradation. This work focused on a distributed electronic system composed of multiple ECUs connected by switches and Ethernet. The main advantage was that resources in mixed critical systems could be utilized more efficiently if noncritical applications can accept reduced functionality after a failover. As well as providing a composable schedule for gracefully degrading systems, the authors provide a way to reserve service intervals for critical backup solutions that are distributed to non-critical ones. The failure scenario may result in a critical backup solution gaining control over the system's resources, leading to a degradation of the system. Compared to active redundancy, passive backup solution added almost no overhead in terms of computation power. The graceful degradation approach allowed multiple critical applications to be served on the same platform without compromising map success rate when compared with state-of-the-art approaches such as active redundancy. As a result of the experiments, the free-last strategy further enhanced the effect of graceful degradation by overlapping as many intervals of service as possible.

Covariance source mapper system was designed in [17], the authors implemented new mapper algorithm, which improves the accuracy and adaptability of the canvas source mapper. They evaluated the effectiveness of their tool on numerous testbeds, including emulators, manufacturing development bench, and testing vehicles of distinct brands, and confirmed that the tool achieved higher mapping accuracy than canvas. They further published the ground truth mapping of MessageIDs, ECUs, and vehicle models collected from real vehicles instead of database.

In safety-critical applications, such as autonomous vehicles, where unintended behavior is detrimental, asynchronous frameworks, like robot operating system (ROS), are increasingly being used. This problem was demonstrated by Bateni *et al.* [10] in the open-source full-stack autonomous vehicle software Autoware.Auto 1.0. Their alternative is the open-source framework Xronos, which uses a novel coordination strategy and predicts properties based on assumptions that are clearly stated. Moreover, it did not require TSN or other real-time networking services. A fault handler will be invoked by Xronos if these assumptions were violated. The authors demonstrated that Autoware.Auto could avoid the identified problems with manageable cost in end-to-end latency by porting it to Xronos. Additionally, they compared Xronos' maximum throughput with ROS using microbenchmarks under a variety of settings and find that it could match or exceed those frameworks in terms of throughput.

A developing 5G network and its ultra-reliable and low-latency communication integrated with TSN would provide an attractive solution for autonomous vehicles that need bandwidth, latency, and reliability. To

support such an integration, Satka *et al.* [18] proposed a technique to translate traffic between TSNs and 5Gs. According to the authors, an autonomous recycling site with several autonomous vehicles was chosen as a use case to evaluate the proposed technique and its proof-of-concept. Using TSN as the backbone communication system, each vehicle had its own onboard network. 5G was used to connect the vehicles and the remote-control center. Using the TSN simulator NeSTiNg, the simulation showed that the proposed method could be useful for network designers to evaluate TSN-5G heterogeneous networks.

Askariipoor *et al.* [19] described the evolution of car E/E architectures over the past few years and presented several major technologies for future vehicle architectures, including software architectures for high-performance computing units (HPVUs). Additionally, they underlined the importance of meeting IVN bandwidth needs using the automotive Ethernet that could provide higher bandwidth and higher security based on ISO 26262. As part of the HPVU presentation, they discussed challenges and technologies related to the integration and deployment of automotive software, including task mapping, software frameworks, and approaches for software configuration; a study of the current parameters of task mapping to boost task assignment quality was also conducted.

In [20], overlapping-based time-triggered (OTT) Ethernet algorithm is presented that predicts WCD for AVB traffic in autonomous vehicles. Preemption and non-preemption modes of the WCD form are provided separately. Based on a realistic vehicle scenario under light and heavy loading conditions, these models are evaluated using back-to-back and porosity configurations. WCDs are lower when the porosity style is used under light loading, but as the load increases, the back-to-back style begins to outperform it. Under all experimental settings, preemption also results in a lower WCD than non-preemption, especially when using the porosity style. Using back-to-back type and porosity under light and heavy loading scenarios, respectively, preemption mode reduces WCD by 4.92% and 4.48% on average with 20% overlapping ratio.

The integration of many applications under IVN and application dynamics presents even greater challenges to application and network management. Ernst *et al.* [21] provide a detailed description of the IVN reconfiguration process. Resources manager (RM) managed and configured the vehicle network independently of other sections of the network. They pointed out the continuous trend in automotive networks towards zonal architectures, which will dominate future vehicles, as opposed to heterogeneous federated systems. Figure 2 [21] shows a zone architecture, where all compute nodes are clustered into local zones that are interconnected with a switched network. In this case, automotive Ethernet would be a viable candidate. Each zone's controller integrates all critical and non-critical traffic. It is also noteworthy that a large part of the backbone traffic is safety-related, in contrast to the current vehicle networks. This is due to the rapid growth of high-resolution sensors required for automated driving. As driving automation continues to increase, that sensor traffic will become safety-critical, which means the integrating backbone will become more critical.

iDriving involves offloading perception and planning from the autonomous vehicle to roadside infrastructure, which drives the autonomous vehicle remotely at intersections. This requires iDriving to process huge volumes of sensor data at full frame rate with less than one hundred milliseconds tail latency without sacrificing accuracy. Several algorithms and optimizations are described in [22], which enable it to achieve this goal. The air traffic controller uses overlapping sensors to render accurate and lightweight perceptions, as well as a planner to jointly plan trajectories for multiple vehicles. Four ouster LiDARs comprise the testbed. As part of the testbed, AMD 5950x processors with sixteen cores run at 3.4 GHz and GeForce RTX 3080 GPUs run iDriving's planning and perception components. Through Ethernet cables and an Ethernet switch, LiDARs and edge computing units are connected. After collecting data for nearly 30 minutes, they measured and reported the end-to-end latency for each frame. A testbed at intersections demonstrated that iDriving allows greater safety and throughput than autonomous driving at intersections and is more efficient than using traffic lights.

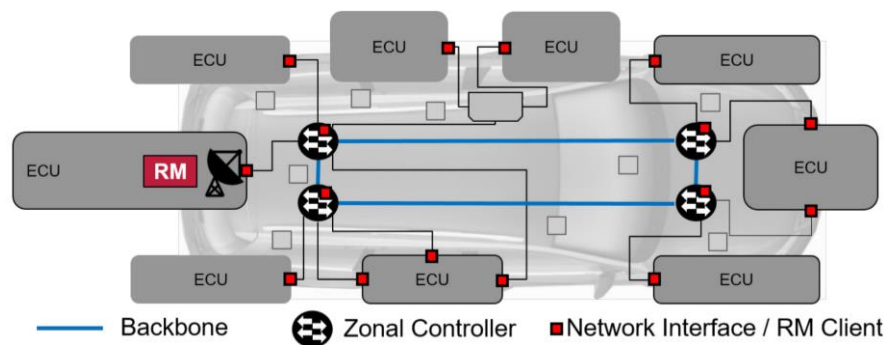


Figure 2. Ethernet backbone with zonal based architecture

3. SECURITY PROTOCOLS FOR IVN

The existing protocols for IVNs lack basic security measures. Furthermore, since IVNs rely heavily on sensors, autonomous vehicle faces many security threats due to the lack of authentication and encryption mechanisms. The following subsections provide an overview of the latest studies regarding protocols for enhancing the security of autonomous vehicles.

3.1. Cryptography: authentication and encryption algorithms

There is no common security protocol for automotive Ethernet, despite the benefits it can provide to IVN. According to [23], three security protocol candidates have been analyzed: MACsec, IPsec, and TLS. According to their assumptions, every connection in Figure 3 [23] was implemented with automotive Ethernet. The authors performed an in-depth analysis of existing security protocol candidates both in terms of security and performance, identifying source authentication and denial of service (DoS) protection as two key missing properties. An authentication protocol based on GWs is proposed, called Gatekeeper. With Gatekeeper, receivers can verify the sender's identity with the help of an on-path authenticator that co-locates with the into-vehicle GW or domain controller. Integrated with Gatekeeper, the time-lock puzzle slows down malicious traffic to stop DoS threats. In the performance evaluation, Gatekeeper is found to have a 0.03 ms latency overhead when transmitting CAN data and outperforms Tesla when transmitting LiDAR data, demonstrating its effectiveness and efficiency.

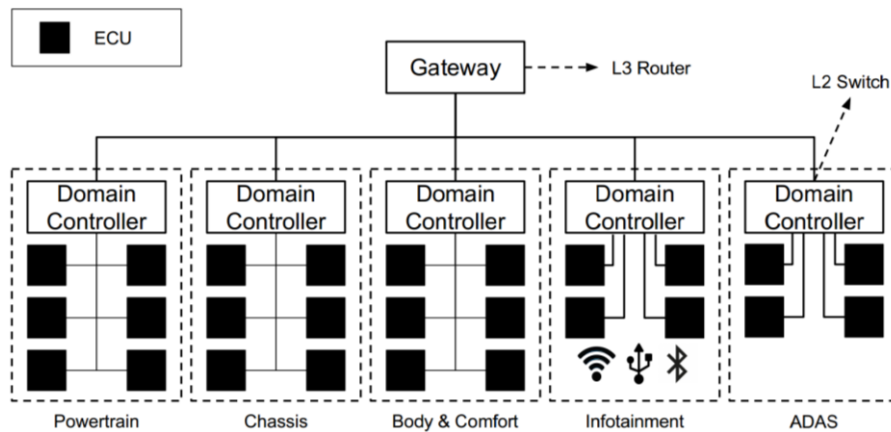


Figure 3. Ethernet-based IVN design

The cybersecurity issues of in-vehicle communication networks built on the security attributes of the components and the topology of the network that were evaluated in [24]. The undirected weighted graphs were used to represent the in-vehicle communication network topologies, the vulnerabilities were assessed based on the accurate attributes of the generated graph. Thirteen various vehicle models were examined to evaluate the exposure concentrations of the IVN using the Dijkstra's shortest route algorithm. From the database of the examined communication networks, the topologies were generated; then the security level of communication links was rated. After that, the analyzed networks were characterized by undirected weighted graphs and considering the protection level of the edges as resistance-like parameters.

According to the article [25], automotive Ethernet networks need secure networks, and there are problems with encryption and authentication algorithms. To improve the security of automotive Ethernet networks, the authors proposed improved AES encryption and MD5 authentication algorithms. In Figure 4 [25] the authors presented a network security flowchart based on the improved AES-128 encryption algorithm and the improved MD5 authentication algorithm. An experimental simulation of CANoe.Ethernet shows a 15% increase in the efficiency of AES-128 encryption algorithm, and a four times improvement in MD5 authentication algorithm. As a result, automotive Ethernet has further improved its active network security performance.

An efficient secure authentication scheme was proposed in [26], utilizing scalable service-oriented middleware over IP (SOME/IP) practice and a protected data exchange method altering the payload field of the original SOME/IP message. The security evaluation showed that the proposed authentication system can offer joint authentication and guarantee the secrecy of the released interim session key; and can avoid the common malicious incidents jointly. The performance tests established on inserted devices and the obtained results showed that there is minimal extra operating expense introduced by the secure system.

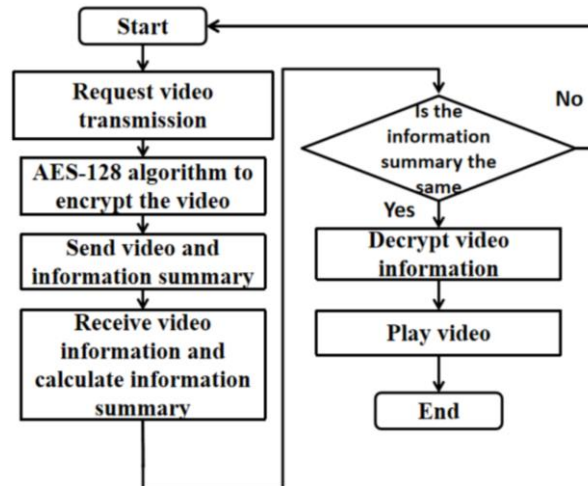


Figure 4. A proposed IVN flowchart

Internet of vehicles (IoV) composed of networked vehicles that supplied with sensors, software, and technologies to transfer messages over the internet under well-established standards and unmanned aerial vehicle (UAV) defined as an aircraft that controlled remotely and autonomously, (sometimes known as Drones) are new areas of study, but they lack efficient authentication method. One authentication method was proposed in [27] named authentication scheme for safety applications for internet of vehicles (EASSAIV) for authenticating messages. The suggested authentication method can collect, manage, and authenticate data delivered to roadside units, or between vehicles and authenticate the received data messages. They used automated validation of internet security protocols and applications (AVISPA) tool and modeled in SPAN using HLPS to verify the proposed authentication scheme. Simulation findings showed the performance of the suggested system is better than others.

A lightweight authentication architecture edge-based utilizing a deep learning (DL) algorithm for in vehicle communication networks was proposed in [28]. The Authors stated that their proposed authentication will enable distant vehicles to form a secure vehicular communication. Moreover, deep DL algorithms will be performed in an edge-based cloud data center for hacking detection. The authors held comprehensive simulations that demonstrated that the proposed algorithm improved the security level; it had F1-Score ranged 94.51 to 99.8%.

Quantum systems like NTRUEncrypt, are particularly important for securing in-vehicle communications. NTRUEncrypt was proposed in [29]. The elliptic curve Diffie–Hellman (ECDH), and Rivest–Shamir–Adleman (RSA) algorithms were used for session key arbitration. Their simulation results showed that, the NTRUEncrypt is faster by 66.06, 1530.98 times than ECDH, and RSA, respectively.

3.2. Cryptography: IVN using blockchain

The cross blockchain frameworks that accelerated the advent and utilization of a wide range of UAV networks-based applications was reviewed in [30]. The authors also presented latest advances in that domain; they introduced a variety of setup functionalities of four different blockchain ledgers that were combined to fulfill the purpose of a single UAV. They identified open issues and disputes related to the use of a cross-blockchain form for UAV networks.

The integration of edge computing (EC) with blockchain is incredibly effective for many practical UAV functions. Though, blockchain require powerful computations as blockchain demands tools to solve complex proof-of-work (PoW) problem to add up latest blocks to the blockchain. Computation requirements could be big matter for UAVs. Nilsen *et al.* [31] proposed a collaborative solution to deal with this problem based on many participating miners in a blockchain. Exclusively, they presented two innovative structures for mixing EC and the blockchain and to efficiently overwhelm various significant computation constraints.

UAVs had shattered in every sector of business industry, but UAV networks are susceptible to numerous attacks as they manage crucial data. Their utilization needs confidential and trustworthy UAV communications; therefore, it is important to make the UAV network dependable and resistant to security attacks. Sachdeva *et al.* [32] suggested a method based on blockchain to ensure UAV ad hoc network security. They used blockchain to provide data security and protecting the network from intrusions. It also allows the ground control stations (GCSs) and the UAV nodes to identify if interfering of data happens.

As a risk management issues of inappropriate maintenance of vehicle vulnerable components, uncontrolled steering, dangerous crash are crucial, Rahman *et al.* [33] proposed a theoretical outline for an essential vehicle health monitoring system (VHMS) manipulating IoT-driven multi-layer heterogeneous networks (HetNet) and ML practices to supervise vehicle parts status, and provide realtime notifications to the car owner/driver and store the data for more required deed with a safe and trustworthy information gathering and analytical scheme. The proposed security approaches for VHMS composed of three components: The first component is the access control-based security based on blockchain to record the attributes distribution between the vehicle devices. They also proposed the use of security and privacy policy-based access control (SPBAC) for car data exchange to defeat the isolation of responsibility difficulties to apply dynamic segregation duty (DSD); the second component was the authentication system for wireless sensor networks (WSN) based on anonymous access authentication (AAA-WSN) was created on the idea of a single key per authentication session (SKPAS); the third component was the encryption, the authors proposed the use of a lightweight attribute-based cryptography scheme system known as lightweight revocable hierarchical attribute-based encryption (LW-RHABE) or one time identity based authenticated asymmetric group key agreement (OTIBAAGKA).

3.3. Cryptography: other cryptography

The use of internet protocol security (IPSEC) to secure in-vehicle communication was proposed in [34], with the intention of low latency and minimum processing power and provides secure interchange of in-vehicle control messages. The proposed work focused on the extensive CAN. based on encapsulation of CAN frames into user datagram protocol (UDP) authenticity, integrity and confidentiality features of communication using IPsec protocol in transport mode. The authors evaluated their proposed solution in simulation environment with configuration based on real hardware. Their simulated results showed that proposed solution provided proper performance and security requirements for automotive networks.

As a means of improving the defense capabilities of automotive Ethernet, security protocol for automotive Ethernet was proposed by Wang *et al.* [35] by analyzing the security requirements and constraints of automotive Ethernet. Security modules of the protocol are key distribution (KD) and secure communication (SC); the GW ECU manages the distribution of keys to each legitimate ECU in a fixed order, whereas SC ensures the confidentiality and authenticity of the data. A hacker who does not possess the public key for the key distribution process cannot open the key distribution process as the GW ECU by disguised as a legitimate ECU. An automotive Ethernet platform using CANoe software and a MPC5646C microcontroller was constructed to evaluate the effectiveness and real-time performance of the system. This study proves that, on the assumption that real-time requirements are met, the proposed security protocol can enhance automotive Ethernet's defense capability.

Zelle *et al.* [36] the authors made two contributions for automotive security. In the first place, they presented man-in-the-middle (MITM) attacks on SOME/IP that can even occur if link layer security mechanisms are employed; an attacker can impersonate both the SOME/IP server and client of the vehicle to enable the attacker to communicate through the compromised ECU of the E/E system (either physically or remotely, as happened in the Jeep hack). Towards this end, they presented a formal analysis using the Tamarin tool for detecting MITM attacks, as well as a practical evaluation using the open-source reference SOME/IP implementation and the automotive development tool CANoe. In the second part, they propose two extensions to the SOME/IP protocol for securing SOME/IP service discovery and subsequent SOME/IP communications. For the first approach, certificates and digital signatures were used to obtain symmetric keys, which then allow SOME/IP communication to be secured. While the second approach relies exclusively on symmetric cryptography. By using these solutions, SOME/IP services can be authenticated and authorized.

Access system is necessary to provide a communication between CAN and Ethernet. CAN with flexible data rate (CANFD) to SOME/IP GW system was proposed in [37]. They implemented the security schemes in the routing procedure to provide truthfulness and secrecy. The security schemes were established on the MAC algorithm (AES128-CMAC, SHA256-HMAC) to provide truthfulness and the AEAD algorithm (AES256-GCM, Chacha20-poly1305) to offer truthfulness and privacy. They stated that the proposed system had reasonable performance.

Vehicle messages with the world were not secure by design; furthermore, the cars' internal devices are resource constrained to manage security processes. Yu *et al.* [38] proposed secure IVN that support data confidentiality, authentication, integrity, fine-grained access control, and certification. They used the concept of edge computing by introducing the security agent (SA), which manages cryptographic processes that require low resources. They stated that the performance of the proposed protocol execution time had low latency with acceptable security levels.

Automotive digital forensics is a new era for the automotive where most existing self-monitoring and diagnostic systems in vehicles only monitor safety-related incidents. Strandberg *et al.* [39] held a systematic literature review on the current IVN security research trends. They identified and assessed over three hundred

papers published in the period 2006 to 2021 and additionally mapped the relevant papers to distinct categories based on identified focus areas. Furthermore, they identified forensically important data from the literature, linked the data to categories, and mapped them to required security properties and stakeholders.

Messages sent to or from CAN could be vulnerable to different attacks, thus threaten the critical safety functions in ECUs, researchers around the world studied CAN fuzzing techniques. They found that present CAN fuzzing techniques, input values are randomly generated with no consideration CAN structure messages, causing non-trivial CAN fuzzing time. Moreover, current fuzzing systems do not have sufficient monitoring capabilities. Kim *et al.* [40] proposed a Structure-aware CAN fuzzing procedure, in the proposed structure of CAN messages were considered and fuzzing input values are methodically produced to detect exposed events in ECUs; the proposed fuzzing system takes a smaller amount of time to run than current systems.

Recent types of weaknesses and attacks against automotive vehicles are emerging every day, and the actual influence of the defined attacks remains ambiguous and need more studies. To deal with this dilemma, Solnør *et al.* [41] showed superior control attacks against an underactuated unmanned surface vehicle (USV) which leads to effective commandeering. Using innovative encryption, they showed that the data transmission can be secured to prevent commandeering challenges aggressively.

4. INTRUSIONS DETECTION SYSTEMS FOR IVN

The understanding of the prospects and challenges of intrusion detection systems (IDSs) in the automotive environment is crucial for engineers and manufacturers of vehicles. A good comparative study of IDSs presented in [42]. The authors outlined existing vehicular communication architectures and protocols; they addressed the probable attacks on in-vehicle communication networks. Subsequently, existing IDS conceptions were presented, while the general requirements on these systems from an automotive perspective were indicated and explained.

DL-based sequential prototype for detecting offline IDS on SOME/IP that enhances communication between several ECU components was proposed in [43]. The authors produced and identified a dataset with various groups as representative to evaluate their proposed intrusion detection system. Besides, they proposed a recurrent neural network (RNN), to represent occurrence of DL built on sequential model. Their obtained numerical results showed that RNN F1 Scores (the weighted average of both Precision and Recall) and Area under the curve (AUC) rates more than 0.8.

Another IDS graph-based gaussian naive bayes (GGNB) was proposed in [44]; the suggested IDS leveraging graph properties and page rank (PR) related features. The proposed GGNB is based on the PR analysis for identifying anomalies. PR (PR algorithm used by Google Search Engine to rank their websites). The proposed IDS used gaussian naive bayes (GNB) classifier. The GNB followed Gaussian normal distribution and support continuous data. Their simulated GGNB on the real raw CAN data set showed that the detection accuracy of DoS, fuzzy, spoofing, replay, mixed attacks were 99.61%, 99.83%, 96.79%, and 96.20% detection accuracy for, respectively.

The TSN per-stream filtering and policing (PSFP) can be utilized as a fundamental technology for detecting malicious traffic flows in vehicles, and in this manner provide network anomaly detectors services as explained by Meyer *et al.* [45]. They evaluated the detection systems based on backbone topology derived from a real vehicle and their traffic classification; their results showed that the detection accuracy depends on some factors such as: the corruption layer, the traffic type. the accuracy of the in-vehicle communication requirement, and the attack effect on the link layer. Most remarkably, the anomaly indicators TSN-PSFP approach remained free of false positive alarms.

TSN practice capable of accurately ensure the time conviction of the basic signals of automotive Ethernet; the TSN working group standardized the TNS based on automotive Ethernet. Yet, the protection system of the TSN protocol is seldom investigated. Luo *et al.* [46] analyzed the protection of the TSN automotive Ethernet as a pillar of E/E design; the authors utilized the Microsoft STRIDE threat model, and defenses for the protection of automotive TSNs were reviewed, the protection method PSFP defined in IEEE 802.1Qci was analyzed thoroughly, then they proposed anomaly detection system based on PSFP. After all, OMNeT++ was utilized to imitate a true TSN topology to assess the functioning of the suggested ADS.

To overwhelm the main challenges vehicle IDS exposed to in practice including low processing resources, inadequate real-time thoughtfulness, and low detection precision, Bi *et al.* [47] proposed a new ID system based on matrix of the message and time transfer. The proposed IDS is useful for ECU to attain real-time attack signal identification with high-level precision. They held experiments on real automobiles showed that their IDS detected many attacks with high accuracy while ingesting a lesser amount of computation resources.

A sequential convolutional network with worldwide concern to create ID model for IVN known as TCAN-IDS was proposed in [48]. The proposed TCAN-IDS constantly encrypts 19-bit characteristics containing of a negotiation bit and data field of the initial data into a data matrix equals to messages suggesting

previous instant. Subsequently, the characteristic removal prototype isolates its spatial-temporal characteristics. Remarkably, global interest based on channel and three-dimensional element measures, consequently, dispense with irrelevant byte variations. Irregular traffic is controlled by a two-class categorization module. Their simulated experiments showed that TCAN-IDS proved high recognition execution on widely common attack datasets.

An efficient model of lightweight IDS using a deep neural network (DNN) was developed in [49]. The proposed lightweight IDS aimed to detect anomalies on IoV system; the dataset used is IVN interaction procedure, the prototype categorizes diverse forms of incidents on vehicles under investigation, DoS, and fuzzing incidents. Testing revealed that the proposed model surpasses other classification models.

Anomaly detection in IVN protocols, particularly in automotive Ethernet became an expanding research field. The use of DL-based intrusion detection system competes a significant role in identifying unidentified attack forms in network traffic. Alkhatib *et al.* [50] compared the performance of diverse unsupervised deep and machine learning (ML) based anomaly detection systems, for real time recognition of irregularities on the audio video transport protocol ((AVTP) application layer protocol applied to the current Automotive Ethernet based IVN). The mathematical calculations, performed on the newly issued "Automotive Ethernet Intrusion Dataset" showed that DL patterns surpass other conventional IDSs in ML under distinct tentative situations.

ECUs are utilized to monitor different E/E systems in the automobile. Still, CANs are imposed to security weaknesses because they do not have cryptography and authentication techniques, lightweight algorithms for IDS are required for the in-vehicle network because of computation restrictions on CANs. Kim *et al.* [51] proposed a lightweight IDS algorithm for in-vehicle CAN based on the level of variation among consecutive data frames. Particularly, the suggested technique utilized compression algorithm of the CAN data frame built on exclusive-OR operations as means for estimating the difference amount.

The IVN protocols and security attacks were thoroughly investigated in [52], the authors illustrated the countermeasures to lessen attacks. They argued that despite there exist many IDSs, including CAN, FlexRay, and automotive Ethernet, those IDSs had their restrictions of recognition analysis, computational complication, recognition and learning times and toughness. They proposed the use of a hybrid blockchain, therefore data can be secure in a distributed approach. A hybrid blockchain merges the characteristics of both public and the private blockchains. A public blockchain (PuBC) is used for recording data issues and V2X functions, while a private blockchain (PvBC) is utilized to record logs of sensitive information and interactions.

An offline analysis of AVTP using a convolutional autoencoder (CAE) was done in [53]. In the CAE, convolutional neural networks (CNN) were used in both the encoder and decoder. To detect anomalies in the AVTP packet stream, which can cause the media streams to become interrupted, the reconstruction error of each sliding window of the media stream is measured. On the recently released automotive Ethernet intrusion dataset, the proposed approach is evaluated, as well as compared with other existing standard anomaly detection and signature-based prototypes in ML. According to the mathematical calculations, the suggested prototype is more accurate than the competing methods and outperforms them at expecting unidentified intrusions, with a precision of 0.94. Furthermore, the model provides low false alarm and lose recognition rates for diverse types of AVTP attacks.

5. RESULTS AND DISCUSSION

A network security issue has become increasingly prominent with the development of real-time critical systems such as autonomous vehicles. To ensure network security, TSN defines the 802.1Qci protocol to block malicious devices and attacks such as distributed denial of service (DDoS). Numerous ways can be applied to enhance the security of the IVN, including advanced encryption technologies, authentication methods, or intrusion detection tools. This paper is a comprehensive overview of recent studies on innovative IVN that described some key open challenges that represent encouraging opportunities for researchers to support with attaining security targets in upcoming autonomous vehicles. Some of the open challenges of autonomous vehicles are Data Protection and Privacy, Emerging Technologies such as Block chain, AI, DoS, and Hijacking. This paper highlights several research challenges of these open issues.

A substantial research attempts have been started to incorporate computing and communication knowledges into vehicles. This paper gave a brief survey of security-related concerns and possible proposed solutions in the IVN. We present the techniques that have been proposed so far to ensure security and privacy in such networks. Also, latest trends in security IVN networks and message transfer such as MAC sec, IPsec, and TLS we reviewed. Many security implementations and proposals for IVN for authentication and encryption, many papers proposed the use of authentication, IPSEC, blockchain and encryption. Yet still there is no such security standard for IVN that deals with all security challenges of IVN. One promising solution for the authentication and encryption problems with resource constrained vehicles is the use of authenticated encryption are forms of encryption which simultaneously assure the confidentiality and authenticity of data [54]–[56].

The paper also underlined the requirements of TSN and the need of implementing TSN with SDN. As an observed, the scheduling problem for TSN-based networks gained a tremendous interest last few years. This interest can be justified by the high complexity of the problem and the timeliness requirements that it can solve.

According to this review, automotive Ethernet still faces continuous major challenges such as:

a) Integration of Automotive Ethernet into autonomous vehicle architectures

Current solutions did not provide a comprehensive solution to the problem. This study discovered that no solution currently available is capable of meeting both functional and structural requirements simultaneously. It is essential to maintain a balance between functional and structural requirements in order to achieve a successful automotive IVN processing solution.

b) Meet real-time requirements for automotive Ethernet

These requirements can be met by SDN and TSN; as a result of its flexibility, SDN is ideally suited for orchestrating IVN configuration. Here, it should be noted that through SDN, network flows and devices can be controlled centrally. But consequently, it exposes all forwarding devices to attack in case of malicious network applications and controller failure.

c) Enhancing the security of IVN

This issue could be solved by implementing new encryption and authentication methods and approaches. Nevertheless, other factors must be taken into consideration in the TSN system, including bandwidth and configuration; security encryption can change the bandwidth requirements and also as part of the configuration of TSN streams, security considerations should also be taken into account. Considering the network architecture, DoS attacks remain the biggest hidden danger that needs to be highlighted. As shown in Figure 5, Automotive Ethernet attacks can be classified as following: DoS, frame injection, replay, spoofing, impersonation, ARP cache poisoning, and TCP hijacking. One possibility to detect these malicious purposes is the implementation IDSs, which might become worldwide mandatory regulations in the future. However, complete encryption, which ensures message authenticity and prevents eavesdropping, would consume a lot of resources and result in large latency values.

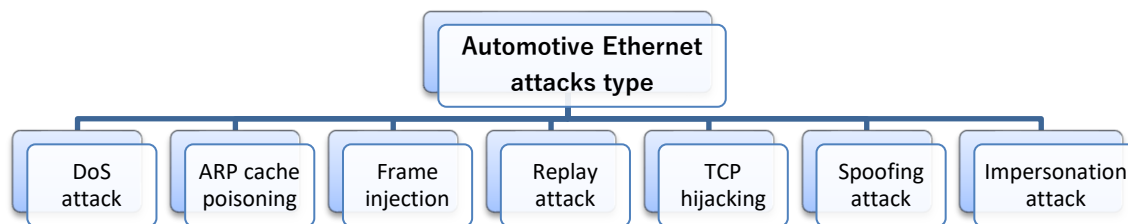


Figure 5. Automotive Ethernet attack patterns classification

d) Increasing the data transfer rate

Transmission of data at multiple gigabits in the near term, while aiming at a much higher transmission rate (over 100G) on a longer-term, including new innovations and extensions such as mechanisms for transmitting time-critical data. In addition, stringent timing requirements must be met: low latency, synchronization, and no noticeable jitter. Table 1 summarizes the numbers and types of sensors expected to be integrated into autonomous vehicle, and their bandwidth requirements [11].

Table 1. Expected future sensors needed for autonomous vehicle

Sensor	Quantity	Bandwidth
Lidar	1-10	< 100 Mbps
Radar	4-8	< 100 Mbps
Camera	2-16	1-5 Gbps
Ultrasonic	8-16	< 10 Mbps

In this paper, many studies on the security of TSNs were reviewed that aimed to enhance protocols, algorithms, and encryption mechanisms to ensure the security of IVNs, as well as architecture and integration issues. Table 2 summarizes the research papers in the IVN fields and their subjects. The IVN fields were categorized as follows: automotive TSN requirements, IVN security protocols, and intrusions detection systems for IVN.

Table 2. The IVN fields and their subjects in the reviewed works

Field	Paper(s)	Subjects	
Requirements of automotive TSN	[6], [11], [12]	List of requirements for future IVN processing platforms	
	[13], [14]	Integrate TSN with SDN with security	
	[15]	NDN	
	[16]	Graceful degradation for real-time autonomous vehicle applications	
	[17]	Improve the accuracy of the canvas	
	[10]	Reducing latency by porting it to Xronos	
	[18]	TSN-5G heterogeneous networks	
	[19]	HPVUs security	
	[20]	OTT Ethernet algorithm	
	[21]	Ethernet backbone with Zone based architecture	
	[22]	iDriving	
	[45], [46]	TSN PSFP, Protection of the TSN automotive Ethernet	
	Security protocols for IVN	[23], [24], [30], [35], [39]	Review of blockchain and security attributes of IVN
		[34]	IPSEC
[36]		Extensions to the SOME/IP protocol for securing SOME/IP service discovery	
[37]		CANFD	
[25]–[29], [33], [38]		Confidentiality, authentication, integrity	
[30]–[33]		Blockchain in IVN	
[40]		Structure-aware CAN Fuzzing procedure	
[41]		Mitigations against an underactuated USV	
Intrusions detection systems for IVN		[29], [42], [44], [47], [48], [53]	Intrusion Detection Systems
		[49], [51]	Lightweight Intrusion Detection Systems
	[50], [52], [53]	Review of diverse unsupervised DL and ML based anomaly detection systems	

6. CONCLUSION

Since the last few years, Ethernet-based IVN was one of the most emerging technologies, had been the focus of extensive research and considered as a potential solution, which fulfills the requirements of autonomous vehicle networking in terms of costs, cable harness weight, and bandwidth. In this respect, automotive Ethernet offers a homogeneous IVN with the appropriate flexibility and topology. Meanwhile, a more powerful and robust IVN is required to support challenging new requirements.

As a result, the integration of ethernet and communication techniques can improve driving safety, increase passenger's comfortability, and reduces traffic jam and latency. This work highlighted widely investigated essential properties of IVN and their applications for automotive. However, most studies on automotive TSN, security, IDS based on a single mechanism and lacks a comprehensive and systematic methodology. There is still a need for more studies about IVN confidentiality, reliability, and no hijacking.

In addition, even though many articles have been published about reducing transmission delay, there should be more research done to improve the security of the TSN automotive Ethernet backbone architecture, since this issue is considered today very crucial. Also, there are other issues that must be considered when building Ethernet-based IVNs, such as the scheduling problem for TSN, which plays an important role in achieving the necessary temporal isolation for jitter-sensitive flows.

REFERENCES




- [1] W. Zeng, M. A. S. Khalid, and S. Chowdhury, "In-vehicle networks outlook: Achievements and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1552–1571, 2016, doi: 10.1109/COMST.2016.2521642.
- [2] S. Corrigan, "Introduction to the controller area network (CAN)." Application Report SLOA101, pp. 1–17, 2002.
- [3] I. SC31, "ISO 17987-1:2016 road vehicles-local interconnect network (LIN)-part 1: General information and use case definition." ISO 17987-1:2016, 2016.
- [4] R. Makowitz and C. Temple, "Flexray - A communication network for automotive control systems," in *2006 IEEE International Workshop on Factory Communication Systems*, 2006, pp. 207–212, doi: 10.1109/WFCS.2006.1704153.
- [5] S. Pandey and B. Vermeulen, "Transient errors resiliency analysis technique for automotive safety critical applications," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014*, 2014, pp. 1–4, doi: 10.7873/DATE.2014.022.
- [6] F. Luo *et al.*, "Design methodology of automotive time-sensitive network system based on OMNeT++ simulation system," *Sensors*, vol. 22, no. 12, Jun. 2022, doi: 10.3390/s22124580.
- [7] L. van Dijk and G. Sporer, "Functional safety for automotive ethernet networks," *Journal of Traffic and Transportation Engineering*, vol. 6, no. 4, pp. 176–182, Aug. 2018, doi: 10.17265/2328-2142/2018.04.003.
- [8] R. Kemp, "Regulating the safety of autonomous vehicles using artificial intelligence," *Communications Law*, vol. 24, no. 1, pp. 24–33, 2019.
- [9] A. Mahmood, W. Zhang, and Q. Sheng, "Software-defined heterogeneous vehicular networking: The architectural design and open challenges," *Future Internet*, vol. 11, no. 3, Mar. 2019, doi: 10.3390/fi11030070.
- [10] S. Bateni *et al.*, "Xronos: Predictable coordination for safety-critical distributed embedded systems," *Prepr. arXiv.2207.09555*, Jul. 2022.
- [11] A. G. Marino, F. Fons, and J. M. M. Arostegui, "The future roadmap of in-vehicle network processing: A HW-centric (R-)evolution," *IEEE Access*, vol. 10, pp. 69223–69249, 2022, doi: 10.1109/ACCESS.2022.3186708.

- [12] Z. Zhou, J. Lee, M. S. Berger, S. Park, and Y. Yan, "Simulating TSN traffic scheduling and shaping for future automotive Ethernet," *Journal of Communications and Networks*, vol. 23, no. 1, pp. 53–62, Feb. 2021, doi: 10.23919/JCN.2021.000001.
- [13] W. Kong, M. Nabi, and K. Goossens, "Run-time per-class routing of AVB flows in in-vehicle TSN via composable delay analysis," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, Jun. 2022, pp. 1–7, doi: 10.1109/VTC2022-Spring54318.2022.9861007.
- [14] M. Cakir, "Security with software-defined networking in automotive networks," Hamburg University of Applied Sciences, 2020.
- [15] A. Elhadeedy and J. Daily, *ECU over named data networking (ECUoNDN): Data management and integration with heterogenous automotive networks*. TechRxiv IEEE, 2022.
- [16] P. Weiss and S. Steinhorst, "Predictable timing behavior of gracefully degrading automotive systems," *Springer Nature*, pp. 1–43, 2021.
- [17] F. Han, "A new mapping algorithm for vehicle CAN BUS mapping based on correlation method," University of Michigan Library, 2022.
- [18] Z. Satka *et al.*, "Developing a translation technique for converged TSN-5G communication," in *2022 IEEE 18th International Conference on Factory Communication Systems (WFCS)*, Apr. 2022, pp. 1–8, doi: 10.1109/WFCS53837.2022.9779191.
- [19] H. Askaripoor, M. Hashemi Farzaneh, and A. Knoll, "E/E architecture synthesis: Challenges and technologies," *Electronics*, vol. 11, no. 4, Feb. 2022, doi: 10.3390/electronics11040518.
- [20] K. M. Shalghum, N. K. Noordin, A. Sali, and F. Hashim, "Worst-case latency analysis for AVB traffic under overlapping-based time-triggered windows in time-sensitive networks," *IEEE Access*, vol. 10, pp. 43187–43208, 2022, doi: 10.1109/ACCESS.2022.3168136.
- [21] R. Ernst, D. Stöhrmann, A. Bendrick, and A. Kostrzewa, "Application-centric network management - addressing safety and real-time in V2X applications," *ACM Transactions on Embedded Computing Systems*, vol. 22, no. 2, pp. 1–25, Mar. 2023, doi: 10.1145/3528411.
- [22] F. Ahmad, C. Shin, W. Pang, J. Cashman, B. Leong, and R. Govindan, "iDriving: Toward safe and efficient infrastructure-directed autonomous driving," *Prepr. arXiv.2207.08930*, Jul. 2022.
- [23] S. Hu, Q. Zhang, A. Weimerskirch, and Z. M. Mao, "Gatekeeper: A gateway-based broadcast authentication protocol for the in-vehicle ethernet," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, May 2022, pp. 494–507, doi: 10.1145/3488932.3517396.
- [24] Z. Petho, I. Khan, and Á. Torok, "Analysis of security vulnerability levels of in-vehicle network topologies applying graph representations," *Journal of Electronic Testing*, vol. 37, no. 5–6, pp. 613–621, Dec. 2021, doi: 10.1007/s10836-021-05973-x.
- [25] J.-M. Li, S. Fu, Y.-J. Wu, and Y.-N. Xu, "High-efficiency encryption and authentication network security for automotive ethernet," *International Journal of Modeling and Optimization*, vol. 12, no. 2, pp. 36–43, May 2022, doi: 10.7763/IJMO.2022.V12.797.
- [26] B. Ma *et al.*, "An authentication and secure communication scheme for in-vehicle networks based on SOME/IP," *Sensors*, vol. 22, no. 2, Jan. 2022, doi: 10.3390/s22020647.
- [27] K. N. Qureshi, M. A. S. Sandila, I. T. Javed, T. Margaria, and L. Aslam, "Authentication scheme for unmanned aerial vehicles based internet of vehicles networks," *Egyptian Informatics Journal*, vol. 23, no. 1, pp. 83–93, Mar. 2022, doi: 10.1016/j.eij.2021.07.001.
- [28] H. Park, "Edge based lightweight authentication architecture using deep learning for vehicular networks," *Journal of Internet Technology*, vol. 23, no. 1, pp. 193–200, 2022.
- [29] Y. Zhu, Y. Liu, M. Wu, J. Li, S. Liu, and J. Zhao, "Research on secure communication on in-vehicle ethernet based on post-quantum algorithm NTRUencrypt," *Electronics*, vol. 11, no. 6, Mar. 2022, doi: 10.3390/electronics11060856.
- [30] R. Alkadi, N. Alnuaimi, C. Y. Yeun, and A. Shoufan, "Blockchain interoperability in unmanned aerial vehicles networks: State-of-the-art and open issues," *IEEE Access*, vol. 10, pp. 14463–14479, 2022, doi: 10.1109/ACCESS.2022.3145199.
- [31] J. M. Nilsen, J.-H. Park, S. Yun, J.-M. Kang, and H. Jung, "Competing miners: A synergetic solution for combining blockchain and edge computing in unmanned aerial vehicle networks," *Applied Sciences*, vol. 12, no. 5, Mar. 2022, doi: 10.3390/app12052581.
- [32] H. Sachdeva, S. Gupta, A. Misra, K. Chauhan, and M. Dave, "Improving privacy and security in unmanned aerial vehicles network using blockchain," *Prepr. arXiv.2201.06100*, Jan. 2022.
- [33] M. A. Rahman *et al.*, "A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19727–19742, Oct. 2022, doi: 10.1109/TITS.2021.3138255.
- [34] J. Lastinec and L. Hudec, "A study of securing in-vehicle communication using IPSEC protocol," *Journal of Electrical Engineering*, vol. 72, no. 2, pp. 89–98, Apr. 2021, doi: 10.2478/jee-2021-0012.
- [35] C.-T. Wang, G.-H. Qin, R. Zhao, and S.-M. Song, "An information security protocol for automotive ethernet," *Journal of Computers*, vol. 32, no. 1, pp. 39–52, 2021, doi: 10.3966/199115992021023201004.
- [36] D. Zelle, T. Lauser, D. Kern, and C. Krauß, "Analyzing and securing SOME/IP automotive services with formal and practical methods," in *The 16th International Conference on Availability, Reliability and Security*, Aug. 2021, pp. 1–20, doi: 10.1145/3465481.3465748.
- [37] Z. Zuo *et al.*, "Design of a CANFD to SOME/IP gateway considering security for in-vehicle networks," *Sensors*, vol. 21, no. 23, Nov. 2021, doi: 10.3390/s21237917.
- [38] D. Yu, R.-H. Hsu, J. Lee, and S. Lee, "EC-SVC: Secure CAN bus in-vehicle communications with fine-grained access control based on edge computing," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1388–1403, 2022, doi: 10.1109/TIFS.2022.3152405.
- [39] K. Strandberg, N. Nowdehi, and T. Olovsson, "A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 2, pp. 1350–1367, Feb. 2023, doi: 10.1109/TIV.2022.3188340.
- [40] H. Kim, Y. Jeong, W. Choi, D. H. Lee, and H. J. Jo, "Efficient ECU analysis technology through structure-aware CAN fuzzing," *IEEE Access*, vol. 10, pp. 23259–23271, 2022, doi: 10.1109/ACCESS.2022.3151358.
- [41] P. Solnør, Ø. Volden, K. Gryte, S. Petrovic, and T. I. Fossen, "Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field," *Journal of Field Robotics*, vol. 39, no. 5, pp. 631–649, Aug. 2022, doi: 10.1002/rob.22068.
- [42] O. Schell, J. P. Reinhard, M. Kneib, and M. Ring, "Assessment of current intrusion detection system concepts for intra-vehicle communication," *Informatik*, pp. 1–8, 2021.
- [43] N. Alkhatib, H. Ghauch, and J.-L. Danger, "SOME/IP intrusion detection using deep learning-based sequential models in automotive ethernet networks," in *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Oct. 2021, pp. 0954–0962, doi: 10.1109/IEMCON53756.2021.9623129.
- [44] R. Islam, M. K. Devnath, M. D. Samad, and S. M. Jaffrey Al Kadry, "GGNB: Graph-based gaussian naive Bayes intrusion detection system for CAN bus," *Vehicular Communications*, vol. 33, Jan. 2022, doi: 10.1016/j.vehcom.2021.100442.




- [45] P. Meyer, T. Häckel, S. Reider, F. Korf, and T. C. Schmidt, "Network anomaly detection in cars: A case for time-sensitive stream filtering and policing," *Prepr. arXiv.2112.11109*, Dec. 2021.
- [46] F. Luo, B. Wang, Z. Fang, Z. Yang, and Y. Jiang, "Security analysis of the TSN backbone architecture and anomaly detection system design based on IEEE 802.1Qci," *Security and Communication Networks*, vol. 2021, pp. 1–17, Sep. 2021, doi: 10.1155/2021/6902138.
- [47] Z. Bi, G. Xu, G. Xu, M. Tian, R. Jiang, and S. Zhang, "Intrusion detection method for in-vehicle CAN bus based on message and time transfer matrix," *Security and Communication Networks*, vol. 2022, pp. 1–19, Mar. 2022, doi: 10.1155/2022/2554280.
- [48] P. Cheng, K. Xu, S. Li, and M. Han, "TCAN-IDS: Intrusion detection system for internet of vehicle using temporal convolutional attention network," *Symmetry*, vol. 14, no. 2, Feb. 2022, doi: 10.3390/sym14020310.
- [49] D. Basavaraj and S. Tayeb, "Towards a lightweight intrusion detection framework for in-vehicle networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, Jan. 2022, doi: 10.3390/jsan11010006.
- [50] N. Alkhatib, M. Mushtaq, H. Ghauch, and J.-L. Danger, "Unsupervised network intrusion detection system for AVTP in automotive ethernet networks," in *2022 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2022, pp. 1731–1738, doi: 10.1109/IV51971.2022.9827285.
- [51] W. Kim, J. Lee, Y. Lee, Y. Kim, J. Chung, and S. Woo, "Vehicular multilevel data arrangement-based intrusion detection system for in-vehicle CAN," *Security and Communication Networks*, vol. 2022, pp. 1–11, Jan. 2022, doi: 10.1155/2022/4322148.
- [52] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, vol. 10, no. 8, Apr. 2021, doi: 10.3390/electronics10080893.
- [53] N. Alkhatib, M. Mushtaq, H. Ghauch, and J.-L. Danger, "AVTNet: convolutional autoencoder for AVTP anomaly detection in automotive ethernet networks," *Prepr. arXiv.2202.00045*, 2022.
- [54] M. A. Jimale *et al.*, "Authenticated encryption schemes: A systematic review," *IEEE Access*, vol. 10, pp. 14739–14766, 2022, doi: 10.1109/ACCESS.2022.3147201.
- [55] N. Turab and Q. Kharna, "Secure medical internet of things framework based on parkerian hexad model," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 6, 2019, doi: 10.14569/IJACSA.2019.0100608.
- [56] M. Abu-Alhaija, N. M. Turab, and A. Hamza, "Extensive study of cloud computing technologies, threats and solutions prospective," *Computer Systems Science and Engineering*, vol. 41, no. 1, pp. 225–240, 2022, doi: 10.32604/csse.2022.019547.

BIOGRAPHIES OF AUTHORS



Wael Toghuj    received the B.Sc. and M.Sc. degrees in Computer Engineering from Kabardino-Balkarian State University, Nalchik, Russian Federation, in 1997. He received Ph.D. in Computer Science from Stavropol State University (North-Caucasus Federal University), Stavropol, Russian Federation, in 2009. Currently, he is an Assistant Professor at the Department of Computer Science, Al-Ahliyya Amman University, Jordan. His research interests include data reliability and security, fault-tolerant systems, multi-errors correcting codes, human-computer interaction, simulations and multimedia systems. He can be contacted by this email: w.toghuj@ammanu.edu.jo.



Nidal Turab    Ph.D. in computer science Professor at the Networks and Cyber Security Department, Al-Ahliyya Amman University, Jordan. His research interests include WLAN security, computer networks security and cloud computing security, eLearning and internet of things. He can be contacted by this email: N.turab@ammanu.edu.jo.