International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 2.102

Detecting Intrusion in an Ethernet based Vehicular Network

S Shrinidhi Rao[1], Subir Kumar Roy[2]

[1]International Institute of Information Technology, Bangalore, India
Email: *shrinidhi.r[at]iiitb.ac.in*
[2]International Institute of Information Technology, Bangalore, India
subir[at]iiitb.ac.in

Abstract: ***The automobile Intra-Vehicular Network (IVN) is made up of numerous bus systems such as Controller Area Network (CAN), FlexRay, Media Oriented Systems Protocol (MOST), and Local Interconnect network (LIN) that are interconnected via Gateways. With the advent of connected cars and enhanced processing capabilities of modern automobiles, cybersecurity concerns of automobiles are increasing and CAN and FlexRay are not equipped to deal with these requirements. There is also a shift towards usage of Ethernet as the primary backbone of the automotive bus since it has established itself as a reliable mode of fast communication across various ap-plication domains. Automobile bus systems are vulnerable to cyberattacks owing to weak access mechanisms, and security measures and form the internal attack surface of the system. Along with firewalls, honeypots and other protection mechanisms, Intrusion Detection systems play a crucial role in keeping the communication safe by detecting attacks in real time. In this paper we investigate various methods of Intrusion Detection, keeping in mind the current trend towards Automotive Ethernet as the primary communication backbone.***

Keywords: IVN, Automotive Ethernet, Intrusion Detection

1. Introduction

Modern automobiles rely heavily on electronic components to aid mechanical components. Drive-by-wire systems, elec-tronic stabilization, brake force distribution, seat belt pre-tensioners and airbag systems have become an industry stan-dard. These systems are controlled by multiple electronic control units which are spread across the automobile, com-municating between themselves, various sensors and actuators, exchanging huge amount of data while providing sophisticated functionalities. Majority of these applications need high speed reliable communication. A wide variety of vehicle commu-nication bus systems are used including but not limited to CAN, LIN, MOST and FlexRay depending on the bandwidth requirement.

a) The move towards Automotive Ethernet

Conventional automobiles have a distributed architecture where all Electronic Control Units (ECUs) are connected to a central bus via gateways and other network devices. Current trend is that the cars have a domain-centric architecture, where the automotive electronics are divided into multiple domains according to their functionality [1]. Each domain would have all its ECUs connected to the same bus system and each of the domains are then interconnected via gateways. There is a shift in the industry towards Zonal architecture, where a central zone controller will manage all its ECUs and traffic within the zone [1]. Each of the zones are then interconnected by the bus backbone. This would eventually lead to significantly higher computing capabilities and more reliability on software. This is driven by CASE megatrend, which refers to Connected, Autonomous, Shared and Electric domains which are driving the new era of automobiles, and would make a car "Server On Wheels" within the next decade [2].

Increasing number of sensors, actuators, interfaces and increased computing capabilities of automotive ECUs also demand a high-speed, reliable communication channel. Different domains in the car need to communicate with each other faster than ever. Modern cars rely heavily on software functionalities and could run a few million lines of code [48]. The complexity, cost, and weight of wiring harnesses has increased such that the wiring harness is the third costliest and third heaviest component in a car [38]. Today, multiple different proprietary standards for communication are used, with each component typically using a dedicated wire/cable. By moving to a single standard, all the communications from all the different components can coexist on the same network, with a single pair going to each location in the car from a central switch. Given that Ethernet has already addressed most of the above concerns, it is very clear that Ethernet is the right way forward [3]. Traditional Ethernet is plagued by noise susceptibility, lack of control of bandwidth allocation, lack of synchronisation between devices [49]. It is also limited by energy and weight constraints in an automotive setup. IEEE has set up various task forces, that are working on these issues to make Ethernet a viable option for the Automotive Industry [4].

b) Vulnerabilities of Automotive Bus Systems

Miller and Valasek took the world by storm when they halted a Jeep Cherokee on the highway in a remote manner, while the driver was sitting inside and had full control of the car [5]. They were able to gain access to the system due to the weak authentication mechanism of the Multimedia system. This led to Fiat Chrysler to recall about 14 lakh vehicles

[53]. Kosher et al. attempted to provide a concrete framework for carrying out cybersecurity analyses of automobiles. They were generally being analyzed in an abstract manner till this framework was described. At first, they focused on what an attacker would be able to do if he had access to the car's internal network. They identified multiple weakness in the CAN Protocol stack, and exploited vulnerabilities in the system to gain access to various

components of the car, including stopping the engine and brakes, proving that any bad agent with access to the CAN bus can easily gain access to any other ECUs in the system. This is generally referred to as the internal attack surface of the automobile. Building upon this work, they established the set of messages that allow them to control various components like the lights, brakes, locks and engine, and about how to inject code into key ECUs to insert persistent capabilities [6].

They further explored the possibility of external attack surfaces via which an attacker can gain access to the system [7]. Through reverse engineering of the source code, use of a dis-assembler to map control flow, identify potential vulnerabilities and logging options to understand normal operation of the ECU, they were able to identify vulnerabilities and break into the ECUs. This opened up a promising research area and security of automobile networks started gaining importance. Researchers were able to mount variety of attacks including Denial of Service, Spoofing and eavesdropping attacks, Bus-Off attacks, Port Scanning, Tapping etc onto various bus systems like the CAN, FlexRay, LIN and MOST. Study of these attacks are out of scope for this paper, and thus we refer the reader to references [8]- [11], which capture some of the unique attacks on the communication bus, sensors and actuators.

c) Securing the Automotive Bus System

Firewalls monitor traffic and filters out unwanted traffic based on configured security rules. Firewalls have been studied in an automotive setup, while considering the resource constraints in an automobile [12] [13]. Honeypots are devices that represent itself as a potential target of high value, diverting the attacker to it [14]. Honeypots have to be realistic and separated so that attacker is drawn to it and at the same time, it will not affect normal functions or give out actual information. Honeypots extract information on the attack, deflects and reports the attack to the user. Primary value of the Honeypot lies in the fact that it exposes known or unknown vulnerabilities deliberately and represents itself as a high value target. Another class of security enforcers are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). While IDS are designed to observe the network and detect anomalies and report them, IPS are designed to respond to these attacks. IDS and IPS are generally placed after Firewall, so that the packets filtered by the firewall (based on set rules) are further scrutinized for malicious content. IDS and IPS algorithms are generally complex and analyse data packets in depth to detect an attack [15] [16].

Security issues of Ethernet have been studied for a long time in the context of industry and networking [17]. Automotive Ethernet could pose additional security issues owing to the design being limited by resource constraints. Seonghoon Jeong Et al. [26] studied the Automotive Ethernet, audited security as defined by open source security testing methodology, identified weak points and suggested improvements that can be done on the network. The paper concludes that Automotive Ethernet is being standardized and developed with security in mind, but there is scope for further improvement. Researchers in [18]- [20] study Automotive Ethernet security vulnerabilities in depth and established the need for security in such networks.

Firewalls, Honeypots, IDS, IPS play an important role in securing communication channels. The aim of this paper is to explore Intrusion detection Mechanisms, that is deployable in an Automotive Ethernet Setup. We have studied over hundred papers in the literature on Intrusion Detection Systems to identify some of the most effective intrusion detection methods for Automotive Ethernet. We observed that, majority of the study have been carried out with respect to CAN and FlexRay, or from a system perspective.To the best of our knowledge very few research reports or publications are available in the literature on IDS for Automotive Ethernet. This is the first paper to survey IDS methods in the context of Automotive Ethernet serving as an effective reference for those who are interested in developing IDS systems for Automotive Ethernet.

In the following sections, we discuss about various Intrusion Detection systems that were studied for Automotive Ethernet. We also look into IDS designed for other transport systems like the Avionics, Train and Ship systems, due to similarities in the cyber-security challenges faced and constraints in resources available and technological limitations. We then extend the study to IDS systems for Internet of Things since they are designed keeping in mind the power limitations of such systems, which could well be translated to power limitations in an automotive system, especially in electric cars. We further explore methods of IDS systems established on CAN or FlexRay, that could very well be translated to the Automotive Ethernet protocol.

2. Intrusion Detection Systems

Intrusion Detection Systems monitor activities in the network or directly on the host and raises an alarm if any unexpected events occur in the system. Vast number of authors have surveyed IDS in a CAN Bus system environment. Papers

[21] - [24] proved to be a good reference for our study since they have studied and well established the taxonomy of IDS methods, their classification and drawbacks. IDS can be classified and grouped in multiple ways, depending on deployment strategy, detecting approach, attacking techniques, layering methods, reaction type, data source and analysis frequency. These can be further classified based on fine grain classifiers. Interested readers can refer to the above papers on the same.

Popular classification methods are based on detection approach (Signature, Anomaly and Specification) and deployment strategies (Host and Network).

- Host based IDS are deployed on the ECU, which monitors the internal activities occurring in the system. These systems monitor the software and identify unauthorised, malicious code executing during run time.
- Network based IDS, which are deployed on the Gateways and Bus system, monitor the traffic for malicious traffic patterns. These systems identify attack patterns on the bus.

- In a Specification based IDS, the system monitors the traffic based on a set of thresholds and rules that describe the well-known behaviour of the system components. Any deviation would be flagged as an attack. Interested researchers can refer [39] as they have explored the use of Specification based IDS for IPv6 enabled, re-source constrained wireless sensor networks, which can be well translated to an automotive network. One could further study the research reported in [41] and [42], where the researchers have explored the applicability of a specification-based approach to detect cyber attacks within the vehiclular network.
- In a Signature based IDS, the system monitors the traffic based on a set of thresholds and rules that describe the attack pattern of well known attacks. Any traffic pattern that matches the set rules would be flagged as an attack. Studies [40] and [43] are good references to signature based Intrusion Detection methodologies.
- Anomaly Based methods try to detect anomaly in the system. Various detection methods like physical fingerprinting, statistical analysis, Machine learning based methods, network characteristics like frequency are used. The research reported in references [44] and

[45] illustrate the aspects for an adaptation of Statistical-based attack detection to the automotive domain and evaluate the anomaly detectors.

Multiple IDS methods can be used together to form a hybrid system improving accuracy of detection. Hybrid IDS are also being extensively studied, allowing drawbacks of one method to be complemented and overcome by the other. Similarly, IDS can be distributed across the network and the host to improve accuracy of detection and reliability.

a) Intrusion detection systems for Automotive Ethernet

Researchers in [25] developed an IDS algorithm for Automotive Ethernet, based on rule matching. It is designed such that when the MCU starts, the IDS mechanism boots, downloads the rule set from memory, acquires network data and scans them against the rules set. If there is a match, the event is recorded, else is is discarded. This IDS mechanism belongs to Specification based IDS class. The authors claim that the IDS conforms to the Automotive Open System Architecture (AUTOSAR) standards [54] and is integrated in the Complex Device Driver of the architecture. They have defined a comprehensive evaluation model for the IDS and compared it with the well established Suricata method [58], proving that this model works better.

Researchers in [26] present an IDS for detecting AVTP (Audio Video Transport Protocol) stream injection attacks in an Automotive Ethernet network. The proposed IDS is based on a deep learning model, involving the feature generation process and a two dimensional convolutional neural network model. The detection model distinguishes whether AVTP packets transmitted over automotive Ethernet are benign or injected on a packet-by-packet basis. Experimental results showed that the model exhibited good performance and can classify almost all the streams correctly. The methods could not be evaluated in real-time on Raspberry Pi3 raising concerns of real-time performance on a constrained hardware setup.

Researchers in [27] compared performances of different unsupervised deep and machine learning based anomaly detection algorithms, for real-time detection of anomalies on the Audio Video Transport Protocol. Compared methods included Deep learning based IDS such as Convolution based Autoencoder and Long Short Term Memory based Autoencoders, Machine Learning Based IDS such as One-Class SVM, Local Outlier Factor and Isolation Forest based IDS. The research was conducted on an Automotive Ethernet Intrusion Dataset and showed that deep learning methods outperform other state of the art machine learning methods.

Researchers in [33] studied the traffic characteristics of Ethernet traffic, considering an Audio-Video Bridge System in ADAS (expand on an acronymn when first presented), and chose parameters for classification such as Duration, Protocol Type, Source and Destination bytes etc. They further propose Decision Tree, Random Forest, SVM (expand on an acronymn when first presented) and ANN (expand on an acronymn when first presented) as four likely methods of feature extraction algorithm. Although their paper does not provide any experimental results, they plan to implement the system on Raspberry Pi, to account for limitations of system resources.

Researchers in [28] proposed a concept for a host based IDS for the ISO 15118 specification, that describes the protocol for managing Vehicle-to-Grid charging sessions. They used the concepts of specification based IDS to focus on deviation from the protocol specific behaviour. Then they further used statistical based approach to detect anomalous behaviour which evaluated packet parameters of frequency, payload length and time lapsed between a message request and response. The proposed system would be classifiable as a hybrid IDS, and it performed very well for the five attack scenarios that were deployed, promising a good security solution for Automotive Ethernet. The results show that the anomaly based approach complemented the specification based approach thus giving a wholesome IDS.

SOME/IP or the Scalable service-Oriented Middleware over IP protocol specifies a middleware for remote procedure calls on top of the TCP/IP protocol stack. It is an automotive middleware solution that can be used for control messages. It was designed from the very beginning to fit on devices of different sizes and different operating systems perfectly. This includes small devices like cameras, AUTOSAR devices, and up to head units or telematics devices. It was also made sure that SOME/IP supports features of the Infotainment domain as well as that of other domains in the vehicle, allowing SOME/IP to be used for MOST replacement scenarios as well as more traditional CAN scenarios. [47] The AUTOSAR has standardised SOME/IP and was designed for embedded devices in the automotive domain. The protocol standard does not specify any security measures and devices on the network have no easy way of determining the authenticating and verifying the integrity of the messages. This situation facilitates an attacker to compromise a valid device and execute attacks from inside the network, for example by plugging compromised hardware into entertainment systems.

Researchers in [29] worked on a Deep learning based sequential model for offline intrusion detection. Target layer was SOME/IP application layer Protocol in Automotive Ethernet Networks. Due to absence of such publicly available data sets they generated and labeled a data set with several classes representing realistic intrusions, and a normal class to assess the IDS. The training data set comprises around 274 attacks and contains 2807 packets; while the testing data set had about 300 attacks and is composed of 2771 packets. By running a three fold cross-validation with early stopping, they ensured statistical confidence in the model's prediction performance. Results showed that model performed well, with acceptable F1 score and no significant difference in performance metrics across the three cross-validations.

Residual Neural Network (ResNet) nad Efficient Net (EfficientNet) models are Convolutional Neural Network architectures which are designed to efficiently process and classify data using multiple layers of the neural network

[56]. Wavelet transform is the decomposition of a signal into set of time and frequency components. It is used in digital image processing and compression to improve image quality. Researchers in [55] proposed a method for detecting and identifying abnormalities in Automotive Ethernet based on wavelet transform and deep convolutional neural network. By defining attack scenarios and extracting normal and abnormal data corresponding to these scenarios, pre-processing this data by fixing the packet size and normalizing the network image data, they have conducted extensive evaluations of the proposed method's performance, considering the size of network image data and multi-resolution levels. The results demonstrate that the proposed method can effectively detect an abnormality. In the experimental setup, Automotive Ethernet was used as communication backbone for other networks such as CAN, FlexRay and LIN. Furthermore, the results suggest that the method is more effective in terms of time-cost compared to default ResNet and EfficientNet methods.

Researchers in [37] present an anomaly detection system for SOME/IP based on Rule Based Approach. The system named Esper, a Complex Event Processing engine, applies a domain-specific rule set to a stream of SOME/IP packets. They considered specific type of anomalies including malformed packets, protocol violations, timing issues and system specific violations. Implementation of the IDS was written in JAVA, which accepts rules written in Event Processing Language

[52]. The User Datagram Packets (UDP) are acquired, parsed, de-serialised, and packets with only one SOME/IP packets were considered. Checks for compliant header fields, changing addresses, the frequency of notifications, and missing responses were implemented showing the flexibility and ease of-use of the approach. Performance measurements show that the implemented system can only run a sub-set of rules for the aircraft cabin network at line rate.

Researchers in [30] propose a novel dynamic temporal convolutional network-based IDS that focuses on highly time-correlated properties of the Communication Ethernet used in Train Networks. The proposed IDS has two main components - first is a feature engineering component which creates a suitable data environment for the detection method and second is a detection method which essentially is a classification method and is used to detect temporal network intrusions. The experimental results indicated that the proposed DyTCN-IDS is not only computationally efficient, but also yields a superior result in terms of macro false alarm rate (0.09%), macro F-score (99.39%), and accuracy (99.40%).

Researchers in [31] propose a hybrid intrusion detection method to defend network attacks against the train ECN, in particular IP Scan, Port Scan, Denial of Service (DoS) and Man in the Middle (MITM). Thirty-four features of different protocol contents were extracted from the raw data generated from the ECN testbed to form a specific data set. They designed six base classifiers based on several typical convolutional neural networks and recurrent neural networks, which were then integrated using dynamic weight matrix voting method. The experiment results show that the method has an outstanding ability to aggregate advantages of all the base classifiers and achieves a superior detection performance with the accuracy of 0.975.

b) Researchers in [32] propose an IDS, based on Support

Vector machines to build an anomaly detection engine. The Particle Swarm Optimization-Support Vector Machines (PSO-SVM) and Genetic Algorithm-Support Vector Machines (GA-SVM) optimization algorithms were used to optimize the kernel function parameters of SVM. They built two attack classification models based on random forest: the iterative dichotomiser3 (ID3) and classification and regression tree (CART). The built intrusion detection and attack classification model was tested using the KDD-99 data-set and the data-set from the simulation of train real-time Ethernet. PSO-SVM improves the intrusion detection accuracy from 90.3% to 95.75%, GA-SVM improves the detection accuracy from

90.3% to 95.85%. The experimental results show that the intrusion detection system of train real-time Ethernet can use the GA-SVM model for detection of abnormal data and the CART model can be used to distinguish between the types of attacks to better complete subsequent responses and operations.

Portscan attack is a technique where the attackers scan network and identify weak points in the network. Bad agent scans all the ports on a network and identifies those without active firewalls or anti-viruses in place, or with weak security mechanisms. Once these weak points are identified, hackers can figure out if these ports are used to send and receive data and then use these to infiltrate into the network.

Researchers in [34] presented an IDS framework where the system monitored and acquired network traffic data in real time, from an Ethernet based avionics communication system. The proposed anomaly based IDS worked in four

stages: Network monitoring and Data acquisition, Traffic Classification and Feature Extraction, Data Pre-processing and Training, Anomaly detection. Portscan attack, Distributed Denial of Service (DDoS) attack, and Portscan attack followed by DDoS were simulated to check the performance of the system. Network was monitored using Wireshark tool on the maintenance port. Packet based features were extracted using Wireshark [50] and Flow-based features were extracted using CICFlowmeter [51] and fed into a ML algorithm to extract and classify data. Support Vector Machines, Logistic Regression, Random Forests and Artificial Neural Networks were used for data classification. Using Forest of Trees and Mean Decrease in Impurity methods, feature space was reduced, aiding in improved resource management. The performance results demonstrated that the flow features performed better than packet-based in predicting the attack.

Sinkhole attacks can be carried out by either compromising a network node or inserting a phony node into the system. The malicious node attempts to direct traffic from other nodes towards itself by advertising itself as the fastest way to the base node. This attracts all of the nodes towards itself and results in traffic flowing through it. The data can then be easily altered by the sinkhole node, jeopardizing the network's security.

6LoWPAN is one of Internet of Things standard, which allows IPv6 over the low-rate wireless personal area networks. Researchers in [35] proposed an IDS to identify sinkhole attacks on the routing services in IoT. The method aims to mitigate adverse effects found in IDS that disturb its performance, like false positive and negative, as well as the high resource cost. The system combines watchdog, reputation and trust strategies for detection of attackers by analyzing the behavior of devices. Simulation results show that the IDS achieves a sinkhole detection rate up to 92% on fixed scenario and 75% in mobile scenario. Researchers in

[36] proposed a lightweight intrusion detection model based on analysis of nodes consumed in 6LowPAN. The sensor nodes with irregular energy consumption are identified as malicious attackers. Simulation results show the proposed intrusion detection system provides the method to accurately and effectively recognize malicious attacks.

Researchers in [46] describe an implementation of an intrusion detection system (IDS) on an FPGA for 10 Gigabit Ethernet. Although this is not developed for automotive segment, this paper proves to be a good starting point for researchers trying to explore hardware based Intrusion Detection Systems. The developed hardware includes an exact string matching circuit for 1,225 Snort rules on a single device for the 10Gigabit Ethernet. The proposed circuit also provides packet filtering for an intrusion protection system. Using the FPGA and the IDS circuit generator, the proposed system is able to update the matching rules corresponding to new intrusions and attacks. It has been optimised for low power consumption.

A replay attack allows an intruder to enter commands on the network. To carry out such an attack, the intruder needs to first pre-capture packets. By repeating these packets on the network, the attacker can confuse vehicle systems and even cause them to execute instructions based on erroneous data. XGBoost is a scalable and extremely accurate gradient boosting solution that pushes the limits of computing power for boosted tree algorithms. It was designed primarily to enhance the performance and computational speed of machine learning models. Researchers in [57] devised a low cost IDS method for Automotive Ethernet and tested it on Raspberry-Pi along with three other GPUs, proving its lightweight, inexpensive, real-time intrusion detection. The work involved an IDS based on the XGBoost machine learning classifier and is proposed to identify replay attacks in automotive ethernet networks deployed on the AVTP protocol.

The paper [59] proposes a novel Intrusion Detection System (IDS) for hybrid automotive in-vehicle networks using a Swin Transformer-based approach to achieve zero false positive rates. The authors conducted experiments on benchmark datasets containing attacks on automotive communication protocols, such as CAN and Ethernet.

The model's hierarchical design leverages self-attention mechanisms to extract spatial-temporal features efficiently. Experimental results demonstrate that the system achieves high accuracy and zero false positives, outperforming traditional machine learning methods. This advancement underscores the potential of transformer-based architectures for secure automotive communication.

Finally, the paper [60] explores several strategies for de-tecting intrusions in Ethernet-based automobile systems. It utilizes ideas from the Automotive Open System Architecture (AUTOSAR) specification to create novel Intrusion Detection System (IDS) designs. These models try to detect and prevent vulnerabilities to AUTOSAR diagnostics. The IDS ensures real-time identification and neutralization of cyber threats by utilizing signature-based, anomaly-based, and machine-learning detection methods, hence improving automotive ar-chitectural security.

3. Summary and Conclusion

During the course of this literature survey, we realised that there is a lack of reported literature on Intrusion Detection Systems tailored for Automotive Ethernet. Researchers are focusing on CAN and FlexRay as primary bus systems and abundance of research work in the literature are focused on these two bus systems. Much of the work on Automotive Ethernet deal with SOME/IP protocol and AVTP protocols. The following comments summarise our survey.

- Attack signature- based IDS detect well known attacks by analysing traffic patterns against known attack signatures. There are no major research which focused on this type of IDS for Automotive Ethernet. These systems guarantee that the known attacks would be detected in the network and would be cost effective compared to other methods.
- Specification based IDS use rule-based matching algo-rithms to analyse traffic behaviour and classify abnor-mal packets, detecting attacks. Advantage here is that the method can identify attacks which exploit zero day

vulnerabilities. Systems like Suricata and Snort could be very well used to deploy such IDS on the automotive network. There are few researchers who have taken this approach and proved good detection results.

- Anomaly detection engines could use more complex algorithms including but not limited to ML, DL and ANN networks to detect anomalies in the network. These sys-tems can be good at detecting both known and unknown attacks if the underlying system is modelled and trained effectively. This field is being pursued by researchers extensively and could possibly detect zero day attacks.
- Hybrid systems combine multiple types of IDS to form a much more exhaustive system. Hybrid system comprising of Signature based and Specification based systems would complete each other and prove more effective in detecting threats. Combining various ANN and ML engines to extract the best information also have been studied.
- There is a scope for hardware based IDS, where an MCU closely tied with the Network or Gateway monitors traffic and tries to detect abnormal traffic. In general, Hardware IDS tend to perform better that their software counterparts since they are specifically tailored for the system they are deployed in.

References

[1] I. Nadav, "The evolutionary path to Zonal E/E Architecture", in Guard Knox, 16th February, 2021.
[2] A. Lock, N. Tracey, D. Zerfowski, "Entering New Worlds", in Real Times, Issue 2019-2020, ETAS.
[3] J. Bush, "The evolution of gateway processors in the auto market", in Electronic Specifier, 3rd October 2017.
[4] "Automotive Ethernet: An Overview", AXIA, 915-3510-01 Rev A, May-2014.
[5] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," in Wired, Security, 21st July, 2015.
[6] K. Koscher et al., "Experimental Security Analysis of a Modern Au-tomobile," 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447-462, doi: 10.1109/SP.2010.34.
[7] Stephen Checkoway, 2011. "Comprehensive experimental analyses of automotive attack surfaces", In Proceedings of the 20th USENIX con-ference on Security (SEC'11). USENIX Association, USA, 6.
[8] Wolf, Marko, Andre´ Weimerskirch and Christof Paar. "Security in Automotive Bus Systems." (2004).
[9] Z. El-Rewini et al., Cybersecurity Attacks in Vehicular Sensors, IEEE Sensors Journal, April 2020
[10] Z. El-Rewini et al., Cybersecurity challenges in vehicular communica-tions, Vehicular Communications, Volume 23, 2020
[11] Paul Carsten, Todd R. Andel, Mark Yampolskiy, and Jeffrey T. McDon-ald. 2015. "In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions." In Proceedings of the 10th Annual Cyber and Information Security Research Conference (CISR '15). Association for Computing Machinery, New York, NY, USA, Article 1, 1–8.
[12] Pese,´ M., Schmidt, K., and Zweck, H., "Hardware/Software Co-Design of an Automotive Embedded Firewall," SAE Technical Paper 2017-01-1659, 2017, https://doi.org/10.4271/2017-01-1659.
[13] B. Elend, T. Adamson, "Cyber security enhancing CAN transceivers", NXP Semiconductors, iCC 2017
[14] V. Verendel, D. K. Nilsson, U. E. Larson and E. Jonsson, "An Approach to using Honeypots in In-Vehicle Networks," 2008 IEEE 68th Vehicular Technology Conference, 2008, pp. 1-5, doi: 10.1109/VETECF.2008.260.
[15] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby and A. Mouzakitis, "Intrusion Detection Systems for Intra-Vehicle Networks: A Review," in IEEE Access, vol. 7, pp. 21266-21289, 2019, doi: 10.1109/AC-CESS.2019.2894183
[16] A. Borkar, A. Donode and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," 2017 International Conference on Inventive Computing and In-formatics (ICICI), 2017, pp. 949-953, doi: 10.1109/ICICI.2017.8365277.
[17] T. Kiravuo, M. Sarela-and J. Manner, "A-Survey-of Ether-net LAN Security," in IEEE Communications-Surveys-&-Tutorials, vol. 15, no. 3, pp. 1477-1491, Third-Quarter 2013, doi: 10.1109/SURV.2012.121112.00190.
[18] A. Talic, "Security Analysis of Ethernet in Cars," Dissertation, 2017.
[19] H. Ju, B. Jeon, D. Kim, B. Jung and K. Jung, "Security Considerations for In-Vehicle Secure Communication," 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 1404-1406, doi: 10.1109/ICTC46691.2019.8939742.
[20] Z. El-Rewini, K. Sadatsharan, D. Selvaraj, S. Plathottam, P. Ran-ganathan, "Cybersecurity challenges in vehicular communications", Ve-hicular Communications, Volume 23,2020,100214.
[21] Lokman, SF., Othman, Abu-Bakar, "Intrusion detection system for automotive Controller Area Network bus system: a review.", J Wireless Com Network, 2019, 184. https://doi.org/10.1186/s13638-019-1484-3
[22] C. Young, J. Zambreno, H. Olufowobi and G. Bloom, "Survey of Automotive Controller Area Network Intrusion Detection Systems," in IEEE Design & Test, vol. 36, no. 6, pp. 48-55, Dec. 2019, doi: 10.1109/MDAT.2019.2899062.
[23] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernandez´-Ramos, and V. Kouliaridis, "Demystifying In-Vehicle Intrusion Detec-tion Systems: A Survey of Surveys and a Meta-Taxonomy," Electronics, vol. 11, no. 7, p. 1072, Mar. 2022, doi: 10.3390/electronics1107107
[24] W. Wu et al., "A Survey of Intrusion Detection for In-Vehicle Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 3, pp. 919-933, March 2020, doi: 10.1109/TITS.2019.2908074.
[25] Z. Zihan, C. Lirong, Z. Haitao and Z. Fan, "Research on Intrusion Detection Technology Based on Embedded Ethernet," 2021 18th In-ternational

Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2021, pp. 587-600, doi: 10.1109/ICCWAMTIP53232.2021.9674069.
[26] Seonghoon Jeong, Boosun Jeon, Boheung Chung, Huy Kang Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks", Vehicular Com-munications, Volume 29, 2021, 100338, ISSN 2214-2096
[27] Alkhatib, Natasha, Maria Mushtaq, Hadi G. Ghauch and Jean-Luc Danger. "Unsupervised Network Intrusion Detection System for AVTP in Automotive Ethernet Networks." (2022).
[28] Lindwall, Hanna and Ovhagen, Pontus, "A Concept for an Intrusion Detection System over Automotive Ethernet", Masters Thesis, Lund University, 2020
[29] N. Alkhatib, H. Ghauch and J. -L. Danger, "SOME/IP Intrusion De-tection using Deep Learning-based Sequential Models in Automotive Ethernet Networks," 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2021
[30] C. Yue, L. Wang, D. Wang, R. Duo, H. Yan, "Detecting Temporal Attacks: An Intrusion Detection System for Train Communication Ethernet Based on Dynamic Temporal Convolutional Network", Security and Communication Networks, vol. 2021, Article ID 3913515, 21 pages, 2021.
[31] C. Yue, L. Wang, D. Wang, R. Duo and X. Nie, "An Ensemble Intrusion Detection Method for Train Ethernet Consist Network Based on CNN and RNN," in IEEE Access, vol. 9, pp. 59527-59539, 2021, doi: 10.1109/ACCESS.2021.3073413.
[32] R. Duo, X. Nie, N. Yang, C. Yue and Y. Wang, "Anomaly Detection and Attack Classification for Train Real-Time Ethernet," in IEEE Access, vol. 9, pp. 22528-22541, 2021, doi: 10.1109/ACCESS.2021.3055209.
[33] B. Jeon, H. Ju, B. Jung, K. Kim and D. Lee, "A Study on Traffic Characteristics for Anomaly Detection of Ethernet-based IVN," 2019 International Conference on Information and Communication Technol-ogy Convergence (ICTC), 2019, pp. 951-953
[34] M. H. Naeem, I. H. Abbasi and M. Mohsin, "An Autonomous Intrusion Detection System for Ethernet-Based Avionics Communication Bus," 2021 International Conference on Engineering and Emerging Technolo-gies (ICEET), 2021
[35] C. Cervantes, D. Poplade, M. Nogueira and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015
[36] Lee, TH., Wen, CH., Chang, LH., Chiang, HS., Hsieh, MC. (2014). "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN." In: Huang, YM., Chao, HC., Deng, DJ., Park, J. (eds) Advanced Technologies, Embedded and Multimedia for Human-centric Computing. Lecture Notes in Electrical Engineering, vol 260. Springer, Dordrecht
[37] N. Herold, S. Posselt, O. Hanka and G. Carle, "Anomaly detection for SOME/IP using complex event processing," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 1221-1226, doi: 10.1109/NOMS.2016.7502991.https://www.ieee802.org/802 tutorials/2017-07/tutorial-Automotive-Ethernet-0717-v02.pdf
[38] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han and L. Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks," 2014 IEEE International Conference on Communications (ICC), 2014, pp. 1796-1801, doi: 10.1109/ICC.2014.6883583.
[39] K. Atefi, S. Yahya, A. Rezaei and S. H. Binti Mohd Hashim, "Anomaly detection based on profile signature in network using machine learning technique," 2016 IEEE Region 10 Symposium (TENSYMP), 2016, pp. 71-76, doi: 10.1109/TENCONSpring.2016.7519380.
[40] U. E. Larson, D. K. Nilsson and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," 2008 IEEE Intelligent Vehicles Symposium, 2008, pp. 220-225, doi: 10.1109/IVS.2008.4621263.
[41] M. Muter, A. Groll and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," 2010 Sixth International Conference on Information Assurance and Security, 2010, pp. 92-98, doi: 10.1109/ISIAS.2010.5604050.
[42] K. A. Taher, B. Mohammed Yasin Jisan and M. M. Rahman, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection," 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 2019, pp. 643-646, doi: 10.1109/ICREST.2019.8644161.
[43] M. Muter¨ and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," 2011 IEEE Intelligent Vehicles Symposium (IV), 2011, pp.1110-1115, doi: 10.1109/IVS.2011.5940552.
[44] M. Marchetti, D. Stabili, A. Guido and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), 2016, pp. 1-6, doi: 10.1109/RTSI.2016.7740627.
[45] Katashita, Toshihiro, Yoshinori Yamaguchi, Atusi Maeda and Kenji Toda. "FPGA-Based Intrusion Detection System for 10 Gigabit Eth-ernet." IEICE Trans. Inf. Syst. 90-D (2007): 1923-1931. https://some-ip.com/
[46] A Modern Car Runs on 100 Million Lines of Code — but Who Will Write Them in the Future? Porscha AG, December 2021
[47] Automotive Ethernet Changes the Automotive Industry, AutoPi, 2021
[48] https://www.wireshark.org/
[49] https://github.com/ahlashkari/CICFlowMeter
[50] https://docs.oracle.com/cd/E13213 01/wlevs/docs20/epl guide/overview.html

[51] Fiat Chrysler recalls 1.4 million cars after Jeep hack, BBC news, 2015
[52] https://www.autosar.org/
[53] M. L. Han, B. I. Kwak and H. K. Kim, ”TOW-IDS: Intrusion Detection System Based on Three Overlapped Wavelets for Automotive Ethernet,” in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 411-422, 2023, doi: 10.1109/TIFS.2022.3221893.
[54] https://medium.com/@enrico.randellini/image-classification-resnet-vs-efficientnet-vs-efficientnet-v2-vs-compact-convolutional-c205838bbf49
[55] Pedro et al.,”Machine Learning-Based Intrusion Detection System for Automotive Ethernet: Detecting Cyber-Attacks with a Low-Cost Plat-form”,
[56] Suricata, https://suricata.io/documentation/ , accessed on 02-12-2023
[57] Y Qin, X. Luo, Y. He, and J. Xie, ”A Zero False Positive Rate of IDS Based on Swin Transformer for Hybrid Automotive In-Vehicle Networks,” Electronics, vol. 13, no. 7, p. 1317, Apr. 2023. https://doi.org/10.3390/electronics13071317
[58] V. Appajosyula, ”Advanced Intrusion Detection Systems for Ethernet-Based Automotive Architectures,” in SAE Technical Paper 2024-28-0121, 11th SAEINDIA International Mobility Conference (SIIMC 2024), 2024, pp. 1–10. doi: 10.4271/2024-28-0121.