In-Vehicle Intrusion Detection Systems

Subjects: Computer Science, Information Systems

Contributor: Georgios Karopoulos , Georgios Kambourakis , Efstratios Chatzoglou , José Luis Hernández Ramos ,

Breaches in the cyberspace due to cyber-physical attacks can harm the physical space, and any type of vehicle is an alluring target for wrongdoers for an assortment of reasons. Especially, as the automobiles are becoming increasingly interconnected within the Cooperative Intelligent Transport System (C-ITS) realm and their level of automation elevates, the risk for cyberattacks augments along with the attack surface, thus inexorably rendering the risk of complacency and inaction sizable. Next to other defensive measures, intrusion detection systems (IDS) already comprise an inextricable component of modern automobiles in charge of detecting intrusions in the system while in operation.

vehicle intrusion detection system intra-vehicle network CAN bus

1. Introduction

In recent years, the technological development of the automotive industry is promoting the manufacturing of increasingly connected vehicles, allowing interaction with other vehicles and components on the road, the so-called vehicle-to-everything (V2X) communications [1]. A key aspect in this trend is the incorporation and integration of a large number of electronic components, including sensors, actuators, and electronic control units (ECUs), to provide specific functions within the vehicle, such as power train, chassis, and body systems. These components are grouped forming subnets, which communicate through gateways using different protocols composing an in-vehicle dense network. While an increasing number of electronic components in vehicles—modern vehicles are composed of 70 to 100 ECU connecting to the in-vehicle network (IVN)—is essential for the development of future autonomous vehicles, this trend also brings along a much larger attack surface that could ultimately affect passengers' safety.

Among the different intra-vehicular network protocols, including FlexRay [2], Local Interconnect Network (LIN) [3], or Media Oriented Systems Transport (MOST) [4]), currently the Controller Area Network (CAN) protocol represents the prevailing standard due to its low cost and fault tolerance properties [5]. However, as often pinpointed in the literature [6][7][8], CAN suffers from the lack of basic security services, including authentication and data encryption, and presents a vulnerable arbitration mechanism. These security shortages have motivated the need to develop security techniques to identify potential attacks as well as to mitigate their impact.

Particularly, the development and deployment of intrusion detection systems (IDS) in the vehicular context have aroused a significant interest in recent years [9]. IDS approaches are widely used in information communication technologies (ICT) to monitor and analyze network traffic and/or local activity, so that attacks or misuse can be

detected. This analysis identifies anomalous patterns when potentially suspicious activity occurs, revealing violations of the established security policy (such as the transmission of unusually large amounts of data). However, the use of IDS for IVN must consider any requirement applicable to the particular context, including the real-time reaction times and resource constraints. On the other hand, a vehicular IDS (VIDS) can detect assaults by just monitoring the IVN traffic, and this is a significant plus, vis-à-vis other defense approaches such as ECU authentication [10] and hardware-enforced isolation [11]. Simply stated, opposite to other types of defenses, a VIDS does not alter the existing IVN architecture, does not produce extra IVN traffic, and does not mandate any changes to the underlying bus protocol. Thus far, several works have analyzed the use of VIDS, proposing diverse categories to classify these approaches [6][12][13]. Nevertheless, the lack of a unified, plain taxonomy hinders the analysis of existing VIDS proposals, as well as the identification of new research opportunities addressing cybersecurity issues in IVN. Moreover, none of the existing surveys on the topic cover the large volume of related wok in the last couple of years, whereas information on datasets and simulators to support IVN IDS research is rather scattered.

2. In-Vehicle Intrusion Detection Systems

Recently, the research of in-vehicle security has seen increased attention. The following content will introduce recent surveys on VIDS. Specifically, these contents provide a summary of twelve recent surveys on intra-vehicle IDS and filter out key points per work, such as categorization of VIDS approaches, feature extraction, employed datasets, attack types, performance and evaluation, and research gaps. To ease comparison, **Table 1** offers an overview of the surveyed works and their contribution.

Table 1. Summary of previous survey works on the field of IVN IDS sorted by year in descending order. ✓: provided, ✗: not provided.

Survey	Year	No of Works	Intra-Vehicle Protocol	Categorization of Works	Performance Comparison	Research Gaps
[14]	2021	30	CAN	✓	✗	✓
[8]	2021	23	CAN	✓	✗	✓
[15]	2020	5	CAN	✓	✓	✗
[13]	2020	20	CAN	✓	✓	✓
[5]	2019	42	LIN, CAN, FlexRay, Ethernet, MOST	✓	✓	✓
[6]	2019	15	CAN	✓	✗	✗
[7]	2019	25	CAN	✓	✗	✓
[16]	2019	24	CAN	✓	✗	✗

Survey	Year	No of Works	Intra-Vehicle Protocol	Categorization of Works	Performance Comparison	Research Gaps
[17]	2019	6	CAN	✓	✗	✗
[18]	2018	19	CAN	✓	✓	✓
[9]	2018	9	CAN	✓	✓	✓
[19]	2018	[14] 17	CAN	✓	✗	✓

er gives a brief analysis of the main communication protocols (CAN, LIN, and FlexRay), but basically focuses on CAN only. To this end, the authors provide an overview of vulnerabilities, potential entry points for data injection, and attacks against the CAN bus. The countermeasures are categorized into cryptographic and IDS solutions. Regarding the latter, 30 VIDS approaches were surveyed from 2008 to 2020. Furthermore, the research challenges associated with IDS-based approaches are identified and summarized.

The work in [8] provides a survey of cybersecurity of in-vehicle networks. It analyzes vulnerabilities and security requirements in CAN-based IVNs, as well as protection mechanisms. Vulnerabilities pertaining to confidentiality, authenticity, availability, integrity, and non-repudiation are analyzed; IDS systems are referenced as an availability protection measure. The authors review 23 state-of-the-art works on CAN-based VIDS systems and classify them into four categories: physical characteristics-based, timing interval-based, entropy-based, and artificial learning-based.

Hafeez et al. [15] classify in-vehicle IDS in four categories: message parameter-based, information theory-based, machine learning-based, and fingerprinting-based. The first detection method works on the MAC layer and was identified in 11 of the surveyed works. An information theory-based VIDS, discussed in three of the included works, exploits entropy. On the other hand, machine learning and fingerprinting-based approaches were identified in seven and five works, respectively. The authors focused on the latter approach, which operates on the physical layer, and provided a survey of such methods. All the considered fingerprinting-based VIDS approaches were attached to CAN and ECU units and followed physical layer detection techniques, such as variations in clock and energy. It was noted that four out of the five fingerprinting-based IDS approaches achieved high accuracy (>96%). While different advantages and disadvantages of each approach are presented, it has to be noted that three of them require the presence of an additional ECU.

The work in [13] surveys intrusion detection solutions in CAN-based IVN. The authors classify generic IVN countermeasures as follows: (a) encryption- and authentication-based, (b) firewall implementations, and (c) IVN IDSs. Out of these, encryption- and authentication-based solutions are not appropriate due to the resource constraints of IVNs, that is, cost, computational power, bandwidth, and storage capacity. The implementation of firewalls is not a realistic solution as vehicles tend to have a long lifecycle and IVNs a wide attack surface. The authors argue that an IDS applied to IVN is a viable countermeasure that can be applied to such a resource-constrained environment while being backward-compatible. Furthermore, the paper provides a classification of attacks to IVNs based on the network layer model into (a) physical layer, (b) data-link layer, and (c) application layer attacks. They survey 8 works and identify 15 different attacks in total for all categories. Regarding intrusion

detection, a taxonomy is proposed from the technology implementation perspective. The authors survey 20 papers and categorize them as (a) fingerprint-based, (b) parameter monitoring-based, (c) information theory-based, and (d) machine learning-based. The comparison of the aforementioned IDS systems led to the following observations. First, there is no single IVN IDS that can detect attacks from different layers; thus, different IDS solutions should be used to cover all layers. Second, while machine learning methods have the advantage of detecting unknown attacks, they require more resources and do not fit well with the automotive environment; to this end, a cloud-based solution has been proposed. Third, most existing VIDS methods show high accuracy, but this accuracy is measured against attacks on a single layer only. This means that these VIDS use features associated with a single layer only; a single VIDS solution covering all layers would benefit from features associated with more than one layers. The paper also provides a discussion of future trends and challenges in the IVN IDS domain.

Al-Jarrah et al. [5] contributed a review of the state-of-the-art intra-vehicle IDS. First, the paper presented an overview of each intra-vehicle network, that is, LIN, CAN, FlexRay, Ethernet, and MOST. The authors compared the aforementioned networks in terms of system cost, bandwidth, protocol efficiency, fault tolerance, MAC mechanism, topology, and security threats. They also categorized the reviewed intra-vehicle IDSs into flow-based, payload-based, and hybrid IDSs, with 19, 17, and 6 works in each category, respectively. Regarding datasets used to evaluate VIDSs, 21 works out of 42 works used real data, 11 out of 42 works used simulated data, and 10 out of 42 did not provide information on the data used. Furthermore, features used by intra-vehicle IDSs were categorized into two types, i.e., physical and cyber features. As such, 2 out of 42 works used physical features to detect attacks, 4 out of 42 works used a combination of cyber and physical features, and 2 out of 42 works did not provide any description of the features used. Regarding attack types, the authors considered the following cyberattacks against intra-vehicle networks: denial of service (DoS), message injection and replay, message manipulation, masquerade, and malware attack. The authors compared each work using various metrics, that is, confusion matrix, detection accuracy, detection rate, false positive, false negative, F-measure, and ROC curve. In addition, the authors took under consideration the following benchmark models for each work: decision trees, ANNs and deep learning, SVM and OCSVM, and random forest. The research challenges presented can be summarized in the following topics: importance of intra-vehicle IDS placement, missing standard benchmark detection model for performance comparison, defining and selecting important features, lack of benchmark datasets, conclusive evaluation metrics, and developing a context-aware IDS.

Young et al. [6] provided an overview of the vulnerabilities and threats in the automotive ecosystem, identified known attacks in CAN, compared VIDS approaches, and discussed advantages and disadvantages of each surveyed work. The authors first explained three major vulnerabilities in CAN, namely, lack of message authentication, unsegmented network, and unencrypted messages. Regarding threats and attacks, the authors detailed known attacks by using either the onboard diagnostics (OBD) port to scan the CAN bus network or remote exploitation techniques. These attacks may allow the attacker to acquire complete control of several functions of the vehicle, such as disabling the brakes or stopping the engine. Additionally, they provided a categorization of IDSs based on detection features, namely, message frequency, message interval, signatures, cyber-physical, entropy, CAN fields, sensor data, and deep neural network. Finally, they compared 15 works in terms of features used, types of detected attacks, and dataset used.

Also focused on IDS approaches for the CAN bus, [7] offered a detailed description of vulnerabilities and potential attacks that can be launched against CAN-based IVN. They propose a taxonomy to categorize VIDS approaches for a CAN bus network considering deployment strategies, detection approaches, attack techniques, and technical challenges. In particular, they analyze 25 approaches and describe a set of challenges derived from the proposed analysis for the definition of VIDS approaches for CAN bus networks. Moreover, 24 IDS approaches for the CAN bus are analyzed by [16] based on the information they extract from the network and the way they build their model. Additionally in the same direction, [17] proposes five criteria to classify CAN-based VIDS approaches: data source, detection method, data analysis location, analysis frequency, and behavior after detection. Besides describing some of the main CAN vulnerabilities, the authors analyze six papers considering such classification.

Loukas et al. [18] presented a classification and survey of in-vehicle IDS. Specifically, they classified the surveyed works based on the target vehicle category, i.e., aircraft, land vehicle, and watercraft, and compared works in the literature for each of these categories. Regarding CAN-based VIDS approaches, the authors compared 19 works in the literature, dated from 2008 to 2017. They used various characteristics to collate the surveyed works, such as the employed architecture, deployment, features, technologies, and evaluation. A similar comparison is also presented for 23 works for VANET. The authors also summarized IVN threats and attacks used for the evaluation of each VIDS approach. Finally, they discussed open issues and presented their conclusions.

The survey in [9] examined 24 relevant works, 9 out of which are directly identified as in-vehicle IDSs; in **Table 1** it consider only those intended for IVN networks. The authors approached the topic through three major axes: attacks, VIDS taxonomy, and challenges in IDS deployment. Attacks are classified into insider or outsider, active or passive, and attacks on confidentiality, integrity, authentication, or availability. Regarding a possible taxonomy, the authors classify VIDSs based on reaction type, detection methodology, validation strategy, and deployment location. One of the main challenges in the deployment of IDS is the absence of real-world deployment and testing, which may affect the actual performance and applicability of these VIDSs. Additionally, most of the proposed VIDSs in the literature were utilized in few attacks, not covering a large portion of the attack surface, and these works did not elaborate on the pros and cons of their proposed scheme. Other key factors are related to (a) the absence of publicly available datasets to run experiments, and (b) the deployment location of the VIDS, because it can greatly affect its energy consumption and overall detection effectiveness. The authors concluded that the so-far proposed IDS schemes are unable to identify zero-days and mitigate threats beforehand.

The work in [19] surveyed proposals in the CAN intrusion detection area and considered their adoption implications. The authors gave an overview of CAN protocol and presented the challenges associated with intrusion detection in CAN-based vehicles. They reviewed 17 VIDS solutions from 2012 to 2018 and classified them into signature- and anomaly-based, further dividing the latter into statistical, knowledge-based, and machine learning.

The following are additional review works on IVN security that, although not exclusively IDS-oriented, partially cover the IVN IDS domain and are cited here for the sake of completeness; note that these are not included in **Table 1**. In [12], security in intelligent connected vehicles is reviewed, covering attacks and defenses on vehicles and vehicular communication networks (both in-vehicle and inter-vehicle). The paper provides a classification of

attacks; the categories pertaining to in-vehicle networks are replay, Sybil, and impersonation assaults. There is also a classification of defenses; the categories of defenses related to the in-vehicle attacks listed above are cryptography and network security (IDS) solutions. In [20], the authors provide an overview of IVN security by summarizing IVN vulnerabilities and attacking methodologies; furthermore, they present a generic attack procedure that outlines the different phases of attacking IVNs. The countermeasures that have been proposed to tackle existing attacks are reviewed and classified into three distinct categories: (a) encryption- and authentication-based, (b) anomaly-detection-based IDSs, and (c) separating the IVN from input interfaces, such as the OBD port. Finally, challenges and future directions are discussed.

A summary of the main characteristics of the related work in IVN IDS is presented in **Table 1**. Overall, the identified surveys are recent, that is, between 2018 and 2021, with their majority published in 2019 (5 out of 12 works); regarding the surveyed works that each paper includes, the oldest ones are dated back to 2008. However, each survey covers only part of the topic and there is no complete, up-to-date comparison of the related work in IVN IDSs. The vast majority of surveys focuses on CAN as intra-vehicle protocol, whereas all of them offer some kind of taxonomy, although very different to each other. Interestingly, all the surveys recapitulated in **Table 1** refer to possible attacks and some additionally provide a taxonomy for attacks, but none rely on some generally accepted threat model such as STRIDE, even though the idea of such an analysis already exists [21]. Moreover, no work elaborates on the currently publicly available datasets that can be used for evaluating the proposed solution, whereas recent standardization efforts are not included and discussed in detail.

References

1. Ghosal, A.; Conti, M. Security issues and challenges in V2X: A survey. Comput. Netw. 2020, 169, 107093.
2. Makowitz, R.; Temple, C. Flexray-a communication network for automotive control systems. In Proceedings of the 2006 IEEE International Workshop on Factory Communication Systems, Turin, Italy, 28–30 June 2006; pp. 207–212.
3. Ruff, M. Evolution of local interconnect network (LIN) solutions. In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484), Orlando, FL, USA, 6–9 October 2003; Volume 5, pp. 3382–3389.
4. Cooperation, M. MOST-Media Oriented Systems Transport. MOST Specif. Rev. 2005, 3, E2.
5. Al-Jarrah Y., O.; Maple, C.; Dianati, M.; Oxtoby, D.; Mouzakitis, A. Intrusion Detection Systems for Intra-Vehicle Networks: A Review. IEEE Access 2019, 7, 21266–21289.
6. Young, C.; Zambreno, J.; Olufowobi, H.; Bloom, G. Survey of Automotive Controller Area Network Intrusion Detection Systems. IEEE Des. Test 2019, 36, 48–55.

7. Lokman, S.F.; Othman, A.; Husaini, M. Intrusion detection system for automotive Controller Area Network (CAN) bus system: A review. EURASIP J. Wirel. Commun. Netw. 2019, 2019, 184.
8. Xie, Y.; Zhou, Y.; Xu, J.; Zhou, J.; Chen, X.; Xiao, F. Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges. Softw. Pract. Exp. 2021, 51, 2108–2127.
9. Sharma, S.; Kaul, A. A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud. Veh. Commun. 2018, 12, 138–164.
10. Palaniswamy, B.; Camtepe, S.; Foo, E.; Pieprzyk, J. An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network. IEEE Trans. Inf. Forensics Secur. 2020, 15, 3107–3122.
11. Hu, S.; Chen, Q.A.; Joung, J.; Carlak, C.; Feng, Y.; Mao, Z.M.; Liu, H.X. CVShield: Guarding Sensor Data in Connected Vehicle with Trusted Execution Environment. In Proceedings of the ’20: Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security, New Orleans, LA, USA, 18 March 2020; Chen, Q.A., Zhao, Z., Ahn, G., Eds.; ACM: New York, NY, USA, 2020; pp. 1–4.
12. Dibaei, M.; Zheng, X.; Jiang, K.; Abbas, R.; Liu, S.; Zhang, Y.; Xiang, Y.; Yu, S. Attacks and defences on intelligent connected vehicles: A survey. Digit. Commun. Netw. 2020, 6, 399–421.
13. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A Survey of Intrusion Detection for In-Vehicle Networks. IEEE Trans. Intell. Transp. Syst. 2020, 21, 919–933.
14. Aliwa, E.; Rana, O.; Perera, C.; Burnap, P. Cyberattacks and countermeasures for in-vehicle networks. ACM Comput. Surv. 2021, 54, 1–37.
15. Hafeez, A.; Rehman, K.; Malik, H. State of the Art Survey on Comparison of Physical Fingerprinting-Based Intrusion Detection Techniques for In-Vehicle Security. SAE Int. 2020, 7.
16. Dupont, G.; den Hartog, J.; Etalle, S.; Lekidis, A. A survey of network intrusion detection systems for controller area network. In Proceedings of the 2019 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Cairo, Egypt, 4–6 September 2019; pp. 1–6.
17. Gmiden, M.; Gmiden, M.H.; Trabelsi, H. Cryptographic and Intrusion Detection System for automotive CAN bus: Survey and contributions. In Proceedings of the 2019 16th International Multi-Conference on Systems, Signals Devices (SSD), Istanbul, Turkey, 21–24 March 2019; pp. 158–163.
18. Loukas, G.; Karapistoli, E.D.; Panaousis, E.A.; Sarigiannidis, P.G.; Bezemskij, A.; Vuong, T. A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Netw. 2019, 84, 124–147.
19. Tomlinson, A.; Bryans, J.; Shaikh, S.A. Towards viable intrusion detection methods for the automotive controller area network. In Proceedings of the 2nd ACM Computer Science in Cars

Symposium, Munich, Germany, 13–14 September 2018; pp. 1–9.

20. Liu, J.; Zhang, S.; Sun, W.; Shi, Y. In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. IEEE Netw. 2017, 31, 50–58.
21. Islam, M.; Sandberg, C.; Bokesand, A.; Olovsson, T.; Kleberger, P.; Lautenbach, A.; Söderberg-Rivkin, A.; Kadhirvelan, S.P.; Hansson, A.; Broberg, H. Deliverable D2: Security Models (Version 2.0), Vinnova/FFI (Fordonsutveckling/Vehicle Development). 2016. Available online: https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf (accessed on 3 March 2022).