Intrusion detection system in intelligent connected vehicles based on two-step algorithm

Tianyu Liu[a], Yongpei Jian[b*], Tonghong Chong[c], Xu Lu[d], Pingyi Liu[e], Xianfeng Jia[f]

CATARC Intelligent and Connected Technology Co., LTd, Tianjin 300000, China

E-mail: [a]liutianyu@catarc.ac.cn, [b*]jianyongpei@catarc.ac.cn, [c]chongtonghong@catarc.ac.cn, [d]luxu@catarc.ac.cn, [e]liupingyi@catarc.ac.cn, [f]jiaxianfeng@catarc.ac.cn.

Abstract. Intelligent connected vehicles are an inseparable object in the Internet of Things. The automotive industry is facing enormous challenges when it comes to ensuring the safety and reliability of vehicles. In this case, intelligent connected vehicle suppliers are committed to providing secure systems to ensure users' driving safety and protect them from possible cyberattacks. This article proposes an intrusion detection system based on an embedded environment suitable for intelligent connected vehicles. The two-step algorithm is used to detect possible attacks. To evaluate the performance of the system, this paper conducts experimental tests, calculates classic accuracy evaluation parameters, and compares them with simulated cyberattack data sets. The results show that this method has superior detection performance for common cyberattacks. When testing this method under a Free State attack, performance was degraded.

Keywords: Intrusion Detection System; Intelligent Connected Vehicles; Bayesian Network; Cybersecurity.

1 Introduction

Modern cars are regarded as intelligent objects in the Internet of Things ecosystem [1]. Intelligent connected vehicles (ICVs) have complex architectures because they integrate multiple automatic driving functions and communication interfaces [2,3]. Attacks from external networks can harm these functions, posing risks to the security of drivers and impacting the company's functioning, passengers' confidentiality, and finances. Consequently, the enhancement of car networking amplifies the inherent possibility of network assaults [4,5]. After analyzing the existing problems, the ISO 21434 standard was introduced to integrate the network security process into the current security process and ensure that all major participants in the automotive industry, whether automobile manufacturers (OEMs) or parts suppliers (TIERs), can realize the importance of network security in product development, and ensure "design security" [6].

C. Chen et al. (eds.), *Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023)*, Atlantis Highlights in Computer Sciences 17,
https://doi.org/10.2991/978-94-6463-304-7_60

With the emergence of sophisticated technologies, the automotive industry is gradually integrating novel features into vehicles, which were inconceivable just a few years back. In the forthcoming years, there will be a gradual enhancement in the level of automobile connectivity and autonomous driving. Currently, many ICVs exchange data via wireless means, such as Wi Fi. Nevertheless, every fresh communication channel introduces fresh vulnerabilities, particularly for the fundamental internal network serving as the backbone of vehicle functionalities [7,8]. Indeed, the availability of internet connectivity exposes vehicles to heightened perils of cyber assaults and escalates the susceptibilities of the entire system. Cybersecurity attacks can have different sources and causes. For example, attackers can smuggle personal information, monitor individual actions, and even remotely control vehicles. The contemporary automobile's internal network, known as the controller area network (CAN) bus, encompasses approximately 70 nodes. The nodes correspond to different electronic control units (ECUs) maneuvering distinct vehicle features like windows, air conditioning, or the engine [9,10]. Should a malevolent individual obtain access to these nodes, the vehicles' cybersecurity will be violated [11]. CAN bus security problems have been exposed for a long time and solved by various means. These methods have some effect, but they are not efficient in performance. Traditional CAN bus intrusion detection methods target physical features to identify attack patterns, introducing concepts such as information rate analysis [12] and temporal feature analysis [13].VoltageIDS, proposed by Choi et al. [14], achieves a lighter-weight intrusion detection system (IDS) with a smaller demand for computing power. However, none of these traditional IDSs can detect unknown attacks on the CAN bus. Therefore, machine learning-based IDSs capable of detecting novel attacks have become the mainstream research direction, such as DNN [15] and LSTM [16]. Overall, the existing research on CAN bus IDS still has a lot of room for improvement in detection performance, and there are still many controversies in the selection of methods [17,18].

In this research, we present a kind of intrusion detection system (IDS), which can analyse the flow of the CAN bus and find out if the information sent over it is harmful. Based on the analysis of one sub-system of the automobile network, the emphasis was put on the ECU, which was essential for the regular running of the car, to make a preliminary analysis of its potential use in ICVs.

2 Methods

2.1 Parameters

Firstly, it is necessary to perform a domain analysis to know the parameters and associated ECUs. These parameters should be taken into account, as well as their associated ECUs, in the process of mapping a vehicle and any potential network hazards that may arise in relation to them. To get the real circumstances of a car being attacked, it is necessary to determine the circumstances that might cause a particular attack, particularly the parameters that can recognize the possible attack. The application field has to be defined using an ontology. For identifying the frame of

reference and the parameters, we refer to a variety of ontologies to identify the application domain. The Automotive Ontology Community Group, the W3C Task Force, and the Salerno University Expert Group were used. The following parameters were selected as the parameters of interest: revolutions per minute (RPM), throttle, brake, steering, gear, speedometer, radiator, laser radar, and lines. The following parameters can be obtained based on the above parameters of interest: engine temperature, acceleration, speed, swerve, and obstacles.

2.2 System architecture

The system architecture is shown in Fig. 1. The application of the system on chip (SoC) coupled through a transmitter and receiver to an OBD II interface enables an embedded IDS to analyse the traffic stream in a car and check if there is a network attack. A two-step algorithm is adopted for spatiotemporal analysis and then makes probability analysis on the data set. This framework offers potential for further follow-up analysis via a link module that will enable vehicles to interact with external clouds.

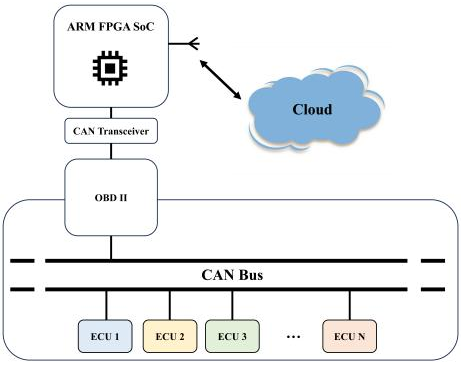

Fig. 1. System architecture.

2.3 Two-step algorithm

To detect potential attacks, a two-step classification algorithm is proposed in this paper. The working principle is as follows:

The first step is preprocessing, analyzing 20 status frames (each includes the accurate values for every vehicle parameter of interest). A unique timestamp is used for each status frame, and it occurs at intervals of 5 ms.

In the second step, based on a Bayesian network, it is determined whether the vehicle is under attack or not based on the parameter values in each frame and information for further analysis.

As noted above, it is necessary to record all the values of each ECU considered frame by frame. Take 20 frames (N) as a group each time and average the values of each parameter, excluding maximum and minimum values in the calculation. Each

parameter will get an average vector, which constitutes the state of the system within a 100-millisecond period.

To determine if there is any possibility of attack, we can send the data of those parameters to the Bayesian network to see if there is any attack. The Bayesian network is created by using a predefined data set, which has all the parameters. The connection relationship of the Bayesian network can also be obtained according to the existing automobile classification [19,20]. The complete Bayesian network is shown in Fig. 2. The data layer, including all essential parameters of interest like RPM, represents the original data. The information layer, including parameters derived from basic parameters like speed, represents the processed information. The knowledge layer refers to the knowledge obtained from the information, decoding whether there is an attack. The validity of the proposed approach can be assessed by the pre-neural training and subsequent inference.

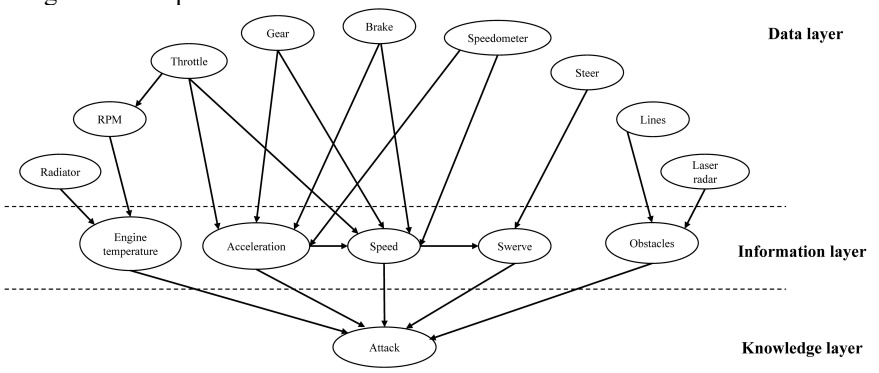

Fig. 2. Bayesian network.

3 Results and discussion

In order to verify our method, we define the types of attacks that can be used in the experiment, including the following four types: DoS attack, Fuzzy attack, Impersonation attack, and Free State attack.

This research adopts CARLA [21], which can simulate the actual car and the environmental interaction. It is an open-source software for the study of ICV experiments and autonomous driving. Besides the simulation, the structure also comprises the steering wheel and the pedal, which enables vehicles connected to the CAN bus to be controlled through the simulation of the CAN bus, the simulation of the outside environment, and the realization of the IDS based on SoC. In order to conduct the experiments, four datasets were crafted, each representing a distinct type of attack. These datasets encompass approximately 8158 frames of data wherein the vehicle was consistently subjected to around 1000 malevolent messages. We conducted simulations in CARLA to replicate the driving conditions of cars in an urban environment. The simulations included instances of simulated vehicle attacks based on real cases. We made the assumption that the communication channel is flawless, thus no data loss, and we only take into account the CAN frame's ID and

data frame. In this case, when a frame is marked as an attack, the attacking node can be uniquely identified. Once the data set is obtained, Bayesian networks can be used. Simple estimation is used for calculating prior probability and conditional probability tables.

In order to evaluate the system performance, precision, recall, and F1 score were calculated and compared with the KIA SOUL data set (Fig. 3) [22]. Our method has high precision, recall, and F1 score in DoS, Fuzzy, and Impersonation attacks (Fig. 3a-c) but lower performance in Free State attack (Fig. 3d). It is more objective because the last attack type is more challenging to identify. After all, it is easily marked as a fault or other situation. It is worth mentioning that, compared with the simulated data set, our system has a better response to the real data set (Fig. 3a-d), which indicates that the system will have the opportunity to conduct a real simulation environment or vehicle test in the future.

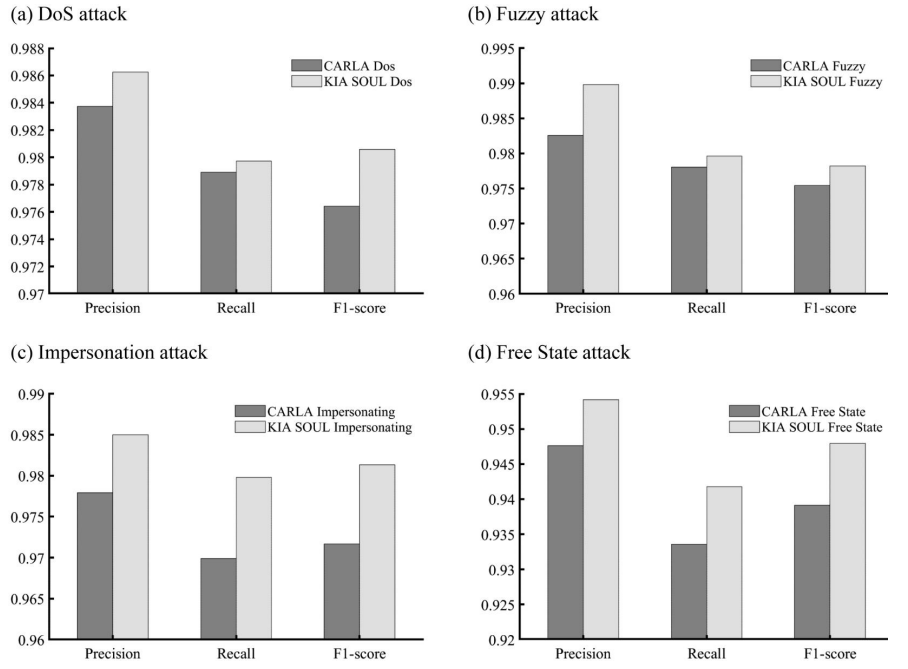

Fig. 3. Precision, recall, and F1 score results of the experiment. (a) DoS attack. (b) Fuzzy attack. (c) Impersonation attack. (d) Free State attack.

4 Conclusion

We propose an embedded intrusion detection system in this research, which can verify whether there is a network attack in ICVs. In practice, possible attacks CAN be identified by probability analysis of data transmitted in ECU subsystems interconnected by CAN protocol. This research aims to examine the inherent weaknesses of ICVs and seek remedies for minimizing the susceptibilities of

contemporary vehicle networks. To appraise the efficiency of this approach, it is juxtaposed against diverse data sets presented in the literature. The results obtained from the practical implementation of this system are gratifying; however, additional studies are required to determine its efficacy in actual scenarios.

References

1. Lombardi, M., Pascale, F., Santaniello, D. (2021) Internet of things: A general overview between architectures, protocols and applications. Information, 12(2): 87. https://doi.org/10.3390/info12020087.
2. Lu, Y., Da Xu, L. (2018) Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2): 2103-2115. https://doi.org/10.1109/JIOT.2018.2869847.
3. Marilisa, B., Luigi, P., Nicola, B. G. (2018) C-ITS communication: an insight on the current research activities in the European Union. International Journal of Transportation Systems, 3: 52-63. https://www.iaras.org/iaras/filedownloads/ijts/2018/019-0007(2018).pdf.
4. Zhao, H., Guo, J., Wu, Z., Liu, T. (2021) Cyber security risk analysis and evaluation for intelligent vehicle gateway. In: International Conference on Smart Transportation and City Engineering 2021. Chongqing. pp. 662-670. https://doi.org/10.1117/12.2613656.
5. Liu, J., Yao, Y., Wang, H., Jia, W., Wu, Y., Liu, X., Zhang, Q. (2021) Research on management methods of automotive cybersecurity tools. In: 2021 2nd International Conference on Information Science and Education (ICISE-IE). Chongqing. pp. 100-103. https://doi.org/10.1109/ICISE-IE53922.2021.00029.
6. Buczak, A. L., Guven, E. (2015) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2): 1153-1176. https://doi.org/10.1109/COMST.2015.2494502.
7. Lin, C. W., Sangiovanni-Vincentelli, A. (2012) Cyber-security for the controller area network (CAN) communication protocol. In: 2012 International Conference on Cyber Security. New York. pp. 1-7. https://doi.org/10.1109/CyberSecurity.2012.7.
8. Fowler, D. S., Cheah, M., Shaikh, S. A., Bryans, J. (2017) Towards a testbed for automotive cybersecurity. In: 2017 IEEE International Conference on Software Testing, Verification and Validation (ICST). Tokyo. pp. 540-541. https://doi.org/10.1109/ICST.2017.62.
9. Hoppe, T., Kiltz, S., Dittmann, J. (2011) Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. Reliability Engineering & System Safety, 96(1): 11-25. https://doi.org/10.1016/j.ress.2010.06.026.
10. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., Savage, S. (2010) Experimental security analysis of a modern automobile. In: 2010 IEEE symposium on security and privacy. Berkeley. pp. 447-462. https://doi.org/10.1109/SP.2010.34.
11. Onishi, H. (2012) Paradigm change of vehicle cyber security. In: 2012 4th International Conference on Cyber Conflict (CYCON 2012). Tallinn. pp. 1-11. https://ieeexplore.ieee.org/abstract/document/6243987.
12. Miller, C., Valasek, C. (2013) Adventures in automotive networks and control units. Def Con, 21(260-264), 15-31. http://iotsecuritylab.com/wp-content/uploads/2014/08/Adventures-in-Automotive-Networks-and-Control-Units.pdf.
13. Gmiden, M., Gmiden, M. H., Trabelsi, H. (2016) An intrusion detection method for securing in-vehicle CAN bus. In: 2016 17th International Conference on Sciences and

Techniques of Automatic Control and Computer Engineering (STA). Sfax. pp. 176-180. https://doi.org/10.1109/STA.2016.7952095.
14. Choi, W., Joo, K., Jo, H. J., Park, M. C., Lee, D. H. (2018) VoltageIDS: Low-level communication characteristics for automotive intrusion detection system. IEEE Transactions on Information Forensics and Security, 13(8), 2114-2129. https://doi.org/10.1109/TIFS.2018.2812149.
15. Kang, M. J., Kang, J. W. (2016) Intrusion detection system using deep neural network for in-vehicle network security. PloS one, 11(6), e0155781. https://doi.org/10.1371/journal.pone.0155781.
16. Hossain, M. D., Inoue, H., Ochiai, H., Fall, D., Kadobayashi, Y. (2020) LSTM-based intrusion detection system for in-vehicle can bus communications. IEEE Access, 8, 185489-185502. https://doi.org/10.1109/ACCESS.2020.3029307.
17. Chen, L., Zheng, M., Liu, Z., Lv, M., Zhao, L., Wang, Z. (2021) SDAE+ Bi-LSTM-Based situation awareness algorithm for the CAN bus of intelligent connected vehicles. Electronics, 11(1), 110. https://doi.org/10.3390/electronics11010110.
18. Tariq, S., Lee, S., Woo, S. S. (2020) CANTransfer: Transfer learning based intrusion detection on a controller area network using convolutional LSTM network. In: Proceedings of the 35th annual ACM symposium on applied computing. New York. pp. 1048-1055. https://doi.org/10.1145/3341105.3373868.
19. Colace, F., De Santo, M., Vento, M. (2010) A multiexpert approach for Bayesian network structural learning. In: 2010 43rd Hawaii International Conference on System Sciences. Koloa. pp. 1-11. https://doi.org/10.1109/HICSS.2010.23.
20. Casillo, M., Coppola, S., De Santo, M., Pascale, F., Santonicola, E. (2019). Embedded intrusion detection system for detecting attacks over CAN-BUS. In: 2019 4th International Conference on System Reliability and Safety (ICSRS). Rome. pp. 136-141. https://doi.org/10.1109/ICSRS48664.2019.8987605.
21. Dosovitskiy, A., Ros, G., Codevilla, F., Lopez, A., Koltun, V. (2017) CARLA: An open urban driving simulator. In: Conference on robot learning. Mountain View. pp. 1-16. https://proceedings.mlr.press/v78/dosovitskiy17a.html.
22. Lee, H., Jeong, S. H., Kim, H. K. (2017) OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST). Calgary. pp. 57-5709. https://doi.org/10.1109/PST.2017.00017.