Denial of Service (DoS) attacks on CAN Bus and Countermeasures: A review

Narayan Khatri
Department of Information and Communication Engineering
Yeungnam University
Gyeongsan, South Korea
narayankhatrig@gmail.com

Seung Yeob Nam
Department of Information and Communication Engineering
Yeungnam University
Gyeongsan, South Korea
synam@ynu.ac.kr

***Abstract*—In-vehicle automotive network is vulnerable to various cyber-attacks because of its poor design of the safety and security functions of the vehicle. Controller Area Network (CAN) is widely used protocol for in-vehicle communication in the automotive domain. However, CAN was not designed with security in mind and can be easily attacked. Hackers can launch Denial of Service (DoS) attack to the vehicle through external devices like OBD-II diagnostics port, infotainment systems, etc., and can endanger the lives of drivers and passengers. Thus, Intrusion Detection System (IDS) in in-vehicle network is investigated intensively recently. This paper particularly reviews Intrusion Detection Systems for mitigating DoS attack in in-vehicle CAN networks.**

Keywords—in-vehicle networks, controller area network (CAN), intrusion detection system (IDS), security, denial of service (DoS) attack

I. Introduction and Background

Today automobiles provide flexible driving experience for passengers. The evolution of Connected Vehicles and Intelligent Transportation System (ITS) have made the transportation system and its managers well informed and take safer and smarter use of the transportation facility. With connected car, it is possible to share internet access and information with other devices either inside or outside the vehicle. Hundreds of Electronic Control UnitS (ECUs) are installed in modern vehicles for making them smart and providing safety to passengers. It is estimated that 75% of vehicles will have access to internet by 2020 [2]. The external interfaces connected in the vehicle like the on-board diagnostics (OBD)-II port and infotainment systems provide adversaries a way to access and hack the in-vehicle network. Moreover, modern vehicles can use wireless mediums like Wi-Fi, Bluetooth and wired medium like USB to communicate with the devices inside or outside the vehicles. Miller and Valasek [12] have demonstrated practical attacks on the vehicle and were able to disable critical functioning of the vehicle like brake and accelerometer remotely. Thus, vehicles are vulnerable to cyber-attacks, and security should be handled with a high priority for ensuring the safety of driver and passengers.

The Controller Area Network (CAN) Bus protocol is widely used in in-vehicle communication for controlling and providing various functionalities to the vehicle system. It helps critical real-time communication such as engine management, brake control, airbags, body systems control, etc. The CAN protocol helps smooth transmission of CAN packets between various ECUs and other inter-connected buses inside the vehicle network. Initially CAN was used in automobiles due to its simplicity, deterministic contention resolution mechanism, and reduced network complexity and wiring costs. However, it was not designed with security in mind. CAN is based on broadcast communication, i.e., every ECUs connected in the bus can send/receive message transmitted in the bus. There is no authentication mechanism for messages and lacks encryption of messages. Furthermore, ID based priority mechanism for arbitration process makes CAN vulnerable to attacks. In this paper, we explore the vulnerabilities in CAN network and review Intrusion detection systems that are developed for preventing Denial of Service attacks on CAN bus. The rest of the paper is organized as follows. In Section II, we explore CAN bus and its vulnerabilities. In Section III, we discuss the machine learning based IDS system to detect DoS attacks on CAN bus. In Section IV, we give discussion and summary. Section V concludes the paper.

II. CAN Protocol Vulnerabilities

There are two formats of CAN bus frame, one with 11-bit of identifier and other with 29-bit identifier frame. Fig. 1 shows the CAN standard frame format. It consists of seven fields: Start of Frame (SOF), arbitration, control, data, cyclical redundancy check (CRC), acknowledge (ACK), and end of frame (EOF).

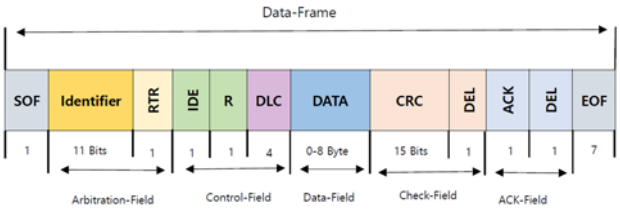

Fig. 1 CAN base frame format

Data frame is used for actual data transmission. The Identifier field represents the message priority. The priority of the message would be higher if it has lower ID value [1]. In addition, actual data field is in the range of 0-64 bits. When two or more than two nodes are transmitting data simultaneously, arbitration mechanism is used for contention resolution. If any node is transmitting a dominant (0) bit in the bus, all other nodes in the bus will read this dominant bit

	Start Bit	ID Bits										The rest of the Frame
		10	9	8	7	5	4	3	2	1	0	
Node 15	0	0	0	0	0	0	0	1	1	1	1	
Node 16	0	0	0	0	0	0	1	Stopped Transmitting				
CAN Data	0	0	0	0	0	0	0	1	1	1	1	

Fig. 2. CAN Bus arbitration mechanism [14]

regardless the bit they have transmitted. If the nodes see high priority messages in the bus, it stops transmission [11].

Fig. 2 depicts the arbitration mechanism in CAN Bus. As shown in fig. 2, Node 16 (binary representation: 00000010000) stopped transmission after it sees dominant bit in the bus transmitted by Node 15 (binary representation: 00000001111) at the seventh ID bit. Thus, node 15 continues its transmission winning the arbitration and has the highest priority. The CAN bus has various vulnerabilities like broadcast communication, no authentication of messages, no encryption of CAN frames, ID-based priority scheme, etc. [11]. Due to broadcast communication, attackers can read the messages transmitted in the bus if they are able to control one node. Due to lack of authentication of messages, receiver cannot distinguish whether the message is valid or fake. Thus, an attacker can send fake messages with valid IDs by taking control of malicious node. The ID based priority scheme makes CAN bus vulnerable to DoS attack [11]. When the malicious node transmits smaller ID frames at high rate then all other nodes in the bus will stop transmitting its frames due to arbitration mechanism of CAN bus. Thus, vehicle might malfunction or can be completely out of control thereby risking the life of passengers.

TABLE I. COMPARISON OF VARIOUS MACHINE LEARNING BASED IDS FOR DOS ATTACK DETECTION

Articles	Attack Methodology	Approach Used	Performance Metric (in %)						Performance Evaluation
			Accuracy	Precision	Recall	False positive rate (FPR)	Error rate (ER)	Detection rate	
Song et al. [3]	DoS attack	Machine learning (DCNN)	×	1.0	0.9989	×	0.03	×	High detection rate , Computationally expensive, Cannot detect unknown attacks
Seo et al. [4]	DoS attack	Machine learning (GAN)	0.979	0.968	×	×	×	0.996	High Detection rate, High memory and computation time
Alshammari et al. [5]	DoS attack	Machine learning (KNN)	0.975	1.00	0.971	×	×	×	High accuracy, Long training time
Nazakat et al. [6]	DoS attack	Machine learning (MLP)	1.0	×	×	×	×	×	Cannot detect unknown attacks
Song et al. [7]	DoS attack	Message Interval	×	×	×	×	×	1.0	High detection rate for injection attack, detection rate decreases as messages have irregular patterns
Kang et al. [8]	Injection attack	Deep Neural Network	0.978	×	×	0.016	×	0.99	Computational complexity, high training and testing time
Taylor et al. [9]	Timing-based	Machine learning	×	×	×	×	×	×	Low false alarm rate, lacks information about OCSVM training time for non-linear data
Taylor et al. [10]	Message synthesizing	Machine learning (LSTM)	×	×	×	×	×	×	Anomaly detection with low false alarm

III. MACHINE LEARNING BASED INTRUSION DETECTION SYSTEM TO DETECT **DOS** ATTACKS ON CAN BUS

In this section, we describe various machine learning based IDS system for detecting DoS attacks on CAN bus. Table I compares various machine learning algorithm's performance results along with attack methodology and intrusion detection approaches. Various intrusion detection strategies have been proposed in the literature such as anomaly based, message frequency based, timing based, signature-based detection, etc. Anomaly-based Intrusion detection is flexible for in-vehicle network due to their memory, power and communication constraints. Fig. 3 shows the general framework for anomaly-based intrusion detection system to detect DoS attack in in-vehicle CAN networks using machine-learning algorithms. The framework consists of training and testing phase. Machine learning based IDS system requires training data, which is pre-processed and suitable features are extracted. The data is trained through the machine-learning algorithm and the model is developed. During the testing phase, real CAN packets are collected and passed through the machine-learning based IDS model. The IDS model will classify those packets as attack packets or normal packets. There are several algorithms that were developed for DoS attack detection in CAN bus. This section briefly explain those algorithms.

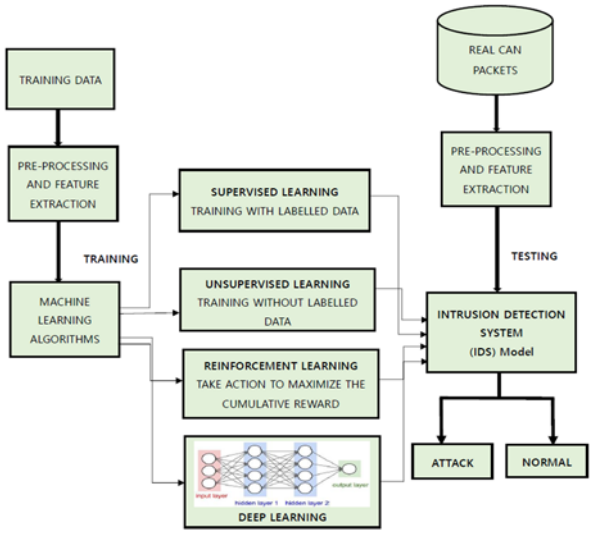

Fig. 3. General framework for anomaly-based Intrusion Detection System to detect DoS attack in In-vehicle CAN Networks using Machine Learning Algorithms

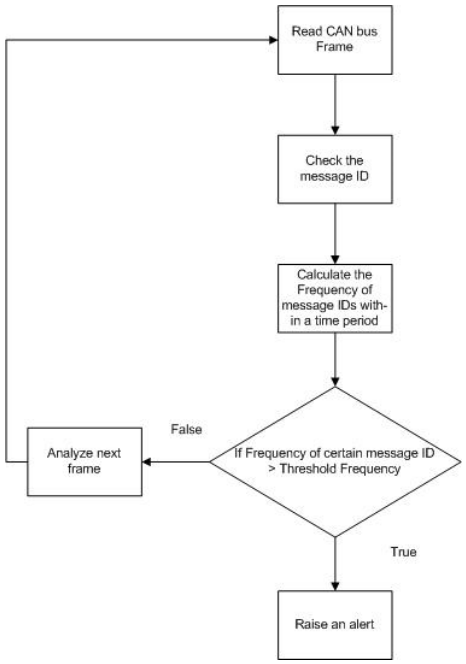

Fig. 4. Flowchart for DoS attack detection algorithm

Previous literature's assume that attacker can launch DoS attack by injecting high priority messages within a short interval of time i.e., rate of messages would be very high during DoS attack compared to normal case CAN bus messages. Thus, IDS systems were developed based on frequency analysis or timing analysis of messages [13]. Fig. 4 shows the flow chart for DoS attack detection system based on frequency analysis of CAN bus messages. The system read CAN bus frame and calculates the frequency of message IDs in the bus within a certain time period. If frequency of message IDs is greater than the threshold frequency previously set, the system will raise an alert.

Song et al. [3] proposed the Deep Convolutional Neural Network (DCNN) model for intrusion detection on CAN bus. The performance evaluation results show that they have very low error rate and high detection rate with precision of 100%. The fundamental drawback of the model is that the training and testing phases are performed offline to reduce time-consumption. However, in real-time scenarios, IDS system should detect intrusion within a short amount of time. The intrusion detection system assumes that the computing power is high, which is not feasible for computationally deprived in-vehicle networks. Furthermore, the model cannot detect the attacks not present in training dataset because it is based on supervised learning algorithm. The authors of the paper have developed the labelled dataset with normal and attack CAN traffic. For DoS attack, they have injected messages with ID '0x000' every 0.3 milliseconds in the CAN traffic recorded for 30 to 40 minutes. The unavailability of public datasets with variety of attack types and frame format in in-vehicle CAN is another hurdle for security research. Seo et al. [4] proposed a novel intrusion detection system based on GAN (Generative Adversarial Network) called as GIDS (GAN based Intrusion Detection System) which is a deep learning algorithm. The model can detect unknown attacks using normal data only for training purpose. The model obtained the detection rate of 99.6% for DoS attack, which is very high. GIDS takes 0.18 seconds to detect about 1954 CAN messages, which is very suitable for practical application. The drawback of the model is that, it might misclassify the anomalous behavior caused due to internal malfunctioning of ECUs as anomalous behavior caused by the external intruder thereby increasing the false alarms. Alshammari et al. [5] proposed KNN (K-nearest neighbor) algorithm for DoS attack detection and obtained the accuracy of 97.5%. They performed training and testing on the dataset provided by authors in [3]. The training time for the KNN model took more than half an hour. Nazakat et al. [6] proposed MLP (Multi-layer Perceptron) algorithm for detecting DoS attack on in-vehicle CAN networks. The results shows that the model with 120 number of hidden layers and learning rate of 0.01 run for 50 Epochs provided accuracy of 100%. Although the model performance is higher, the authors did not give clear explanation of how the attack is launched and how the proposed IDS system works to mitigate those attacks. As the model is based on supervised learning, the fundamental problem of detecting unknown attacks is of great concern. Song et al. [7] proposed an IDS system based on time-interval analysis of the message IDs. The normal messages in CAN bus have uniformity of occurrence. The injected messages can be distinguished from normal ones if the message IDs have short interval of occurrence. The result shows that the lightweight model can detect attack with 100% detection accuracy. However, this model is very simple and is only able to detect attacks which injects huge amount of messages in the CAN bus. The model may be inefficient if the attack type changes like message tampering or the attacks that includes changes in the message semantics. In addition, the model cannot detect messages with irregular occurrences. Kang et al [8] proposed IDS based on deep neural network (DNN). The statistical features of CAN data were captured using unsupervised deep-belief network and classify them as anomalous or not. The experiment results shows model can detect 3900 frames within 7 to 8 milliseconds, and obtained 99% detection rate while keeping false positives under 1%-2%. The drawback of this IDS system is that the computational complexity, training and testing time will increase as the number of layers in DNN model increases. The authors of the paper do not address these issues. Taylor et al. [9] proposed supervised one-class support vector machine (OCSVM) to detect intrusions that deviates from normal frequencies of the CAN frame. The proposed algorithm compares average inter-packet timing of current and historical packets. If the current average inter-packet timing deviates from average historical inter-packet timing, anomaly is detected. However, authors do not present in details about the kernel functions used in their OCSVM algorithm. In [10], authors proposed long short-term memory (LSTM) recurrent neural network for intrusion detection in CAN bus. The proposed neural network is trained in a way to predict the next packet's payload. Anomaly is detected if the frames deviate from those predicted values from neural network.

IV. Discussion and Summary

In Section III, we discussed the machine learning based approaches for DoS attack detection in CAN bus. Those algorithms showed high detection rates for injection attacks.

However, there is no evaluation result for the case where the attack types were changed like message modification attack or the message patterns were irregular. Most of the work assumes that attacker launch DoS attack by injecting high priority messages at short time-interval. However, this attack scenario is very simple. The future research should dive deeper to investigate more sophisticated DoS attack scenarios and variety of attack patterns. The previous IDS systems will fail to detect attacks if the attacker acts smartly through the manipulation of CAN payloads. For machine learning models, obtaining labelled datasets for training and testing purpose is another issue since the CAN frames are not open by automobile manufacturers. As the advancement in vehicle technology is rising and vehicles are more prone to attacks, there is a need for co-ordination between vehicle manufacturers and automotive security researcher's in-order to secure the in-vehicle CAN networks. Since the ECUs have low computational power, machine-learning models requiring small memory and low computational time should be developed for in-vehicle networks. The problem of high training and testing time should be addressed since real-time intrusion detection should be fast and effective. Furthermore, unsupervised machine learning algorithms should be taken into more consideration for the development of future in-vehicle network intrusion detection systems.

V. Conclusion and Future Works

Thus, in this paper we discussed Denial of Service attack detection schemes for in-vehicle CAN networks. We highlighted the merits and demerits of those approaches. As the vehicle technology gets advanced, the vehicles tend to be the target of hackers. The future attacks can be threatening and security of vehicles should be handled with a high priority. Machine learning based IDSs might be a good solution to detect new and unknown attack types, and thus, more research is needed in this field.

In the future, we will investigate the lightweight machine learning algorithms to detect DoS attacks in CAN bus. Unsupervised learning algorithms like isolation forest, local outlier factor, and k-nearest neighbor should be investigated in more detail for future research works.

Acknowledgment

This research was supported in part by Basic Science Research Program through National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2020R1A2C1010366, 2015R1D1A1A01058595). This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) Support Program (IITP-2019-2016-0-00313) supervised by the IITP (Institute for Information communications Technology Promotion).

References

[1] S. F. Lokman, A. T. Othman, and M. Abu-Bakar, "Intrusion detection system for automotive controller area network (CAN) bus system: a review," EURASIP Journal on Wireless Communications and Networking, Article number: 184 (2019).

[2] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," IEEE Transactions on Intelligent Transportation Systems, volume 21, issue: 3, March 2020.

[3] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," Vehicular Communications, volume-21, January 2020, 100198.

[4] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, UK.

[5] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," Wireless Engineering and Technology, vol. 9, pp. 79-94, October 2018.

[6] I. Nazakat and K. Khurshid, "Intrusion detection system for in-vehicular communication," 2019 15th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan.

[7] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia.

[8] M. Kang and J. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," PLos ONE 11(6): e0155781, 2016.

[9] A. Taylor, N. Japkowicz, and S. Leblanc, "Frequency-based anomaly detection for the automotive CAN bus," 2015 World Congress on Industrial Control Systems Security (WCICSS), London, UK.

[10] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), Montreal, Canada.

[11] O. Avatefipour and H. Malik, "State-of-the-art survey on in-vehicle network communication (can-bus) security and vulnerabilities," Available : https://arxiv.org/abs/1802.01725 , 2018.

[12] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, 2015.

[13] M. Gmiden, M. H. Gmiden, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," 2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Sousse, Tunisia.

[14] https://en.wikipedia.org/wiki/CAN_bus