Proceedings of the International Conference on Applied CyberSecurity (ACS) 2021

Intrusion Detection for CAN Using Deep Learning Techniques

Rawan Suwwan, Seba Alkafri, Lotf Elsadek, Khaled Afifi
Imran Zualkernan Fadi Aloul

Department of Computer Science & Engineering
American University of Sharjah, UAE
{g00075916, g00073279, b00075151, b00073944
izualkernan, faloul}@aus.edu

Abstract. With the advent of Internet of Vehicles (IoV), cars and commercial vehicles represent a convenient attack surface for cyber attacks. Many automobiles use the Controller Area Network (CAN) bus for internal communication. CAN is known to be susceptible to various types of cyber attacks. One constraint on intrusion detection systems (IDS) for CAN is that they need to be efficient due to lack of resources and the high traffic on a typical CAN network. This paper presents an implementation of simple 1D Convolutional Neural Network (CNN), Long Short Term (LSTM) and Gated Recurrent Units (GRU) networks on a recent attack data set for CAN. All models thus developed outperformed the existing state-of-art and achieve an almost perfect F1-Score of 1.0.

Keywords—CAN Attacks, Cybersecurity, Deep Learning, GRU, LSTM, CNN

1 Introduction

As modern automobiles are increasingly digital, cyber attacks on board networks like the Controller Area Network (CAN) bus pose potentially fatal consequences. With the advent of 5G, the Internet of Vehicles (IoV) is fast becoming a reality [1]. Therefore, connected cars will be at an increasing risk of being attacked for malicious purposes. This paper explores the implementation of an intrusion detection system (IDS) that detects CAN attacks. An IDS is a software or hardware security tool that detects attacks that cannot be prevented by other security mechanisms and responds to mitigate the effects of the attack. CAN is a standardized message-based protocol widely used in vehicles for communication. CAN is a network bus that connects all the different components or ECUs (Engine Control Unit) in the car. In an automotive CAN bus system, ECUs may include the engine control unit, airbags, audio system or other components. A modern car can have up to 70 ECUs, where each of them transmits information that needs to be shared with other parts of the network [2]. CAN is currently the standard in today's vehicles as per the CAN FD standards (ISO 11898-1 and ISO 11898-2). Fig. 1 shows the standard components of a CAN data frame. CAN data can be vulnerable to malicious monitoring as they are transmitted via broadcast. Furthermore, encryption is not used which can lead to the sniffing and hacking of the data.

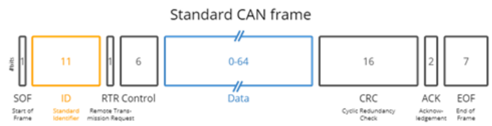

Fig. 1. A standard CAN frame.

2 Previous Work

Table I shows a summary of previous work in intrusion detection for CAN networks. As Table I shows, three common data sets (i.e., [2], [3], [4]) in addition to a number of custom data set have been used. This makes it difficult to compare results across studies. Data from a variety of vehicles including Kia, Hyundai, Honda, Dodge, Suzuki, etc. has been used. As Table I shows, a variety of techniques including signature based (e.g., [5], [6]), traditional machine learning (e.g., [7], [8], [9], [10]), deep learning (e.g., [11], [12], [13]), and unsupervised learning (e.g., [14], [15]) have been explored. The generally considered attacks include Denial of Service (DoS), Impersonation, Fuzzing, and Spoofing of Gear or RPM packets. In addition, other attacks like Replay, Injection, Camouflage have also been explored. Finally, as Table I shows, most techniques have yielded impressive results. In this paper we explore the most recent commonly used data set [4] because it is publicly available and hence allows for direct comparison to other work.

TABLE I. SUMMARY OF PREVIOUS WORK

Ref.	**Attacks**	**Dataset**	**Vehicle**	**Techniques**	**Results**
Lee et al. [5] (2017)	DoS, Imp., Fuzzy	[2]	Kia Soul	Signature based	Could detect attacks based on time
Moulahi et al. [7] (2021)	DoS, Imp., Fuzzy	[2]	Kia Soul	RF, DT, SVM, DTD	Accuracy 98.1%-98.5%
Javed et al. [11] (2021)	DoS, Imp., Fuzzy	[2]	Kia Soul	CNN+Attention-GRU	F1-Score 93.9-94.38
Seol et al. [16] (2018)	DoS, Fuzzy, Gear, RPM	[3]	Hyundai's YF Sonata	GAN	Accuracy 99.6% - 99.9%
Song et al. [12] (2020)	Gear, RPM	[3]	Hyundai's YF Sonata	RESNET+LSTM	Accuracy 91%
Amato et al. [13] (2021)	Dos, Fuzzy, Gear, RPM	[3]	Hyundai's YF Sonata	DNN	Accuracy 98%-100%
Mehedi et al [17] (2021)	Dos, Fuzzy, Gear, RPM	[4]	Hyundai Avante CN7	1D CNN	Accuracy 97.8-98.1%

					F1-Score 0.92-0.95
Hanselmann et al. [15] (2020)	Plateau, change, Playback, Flooding, Suppress	[18]	Unknown	LSTM+Auto Enco,	Accuracy 99.1-99.2%
Omid et al. [8] (2019)	DoS, Fuzzy	Cus-tom	Dodge RAM Pickup	OCSVM-MBA	Accuracy 95.5%-97%
Zhou et al. [19] (2019)	Abnormal	Cus-tom	Unknown	Siamese Tri-plet DNN	Accuracy 83%
Qin et al. [20] (2021)	Replay, Temper	Cus-tom	Unknown	LSTM	F1-Score 85%
Delwar et al.[21] (2021)	DoS, Fuzzy, Spoofing	Cus-tom	Toyota, Sub-aru, Suzuki	1D CNN	Accuracy 99.8%
Xun et al. [22] (2021)	Abnormal	Cus-tom	Luxgen U5, Buick Regal	Deep SVDD	Accuracy 98.5%
Li et al. [9] (2021)	Abnormal	Cus-tom	Luxgen U5	M-SVDD, G-SVDD	Accuracy 98.37%-99.53%
He et al. [10] (2021)	Injection, Camou-flage, Suspension, Tempering,	Cus-tom	Jeep and Un-known	LightGBM	F1-Score 90.49-100.
Jin et al. [6] (2021)	Drop, Re-play, Tempering	Cus-tom	Unknown	Signature-based	Accuracy: 66%-100%
Leslie [14] (2021)	Abnormal	Cus-tom	Unknown	Ensemble Clustering	F1-Score 100

3 Dataset and Feature Engineering

Table II shows a breakdown of the classes in the dataset [4]. This dataset was also collected for different states for the car (stationary vs. driving). This paper used the data from the driving round, which comprised of 2,000,733 data points. Each data point includes a Timestamp (logging time), Arbitration_ID (CAN identifier), DLC (data length code), Data (CAN data field), Class (Normal or Attack), and SubClass (attack type) of each CAN message. For example, one datapoint may look like `16.05236,130,8,14 80 10 80 00 00 0A 73`. The ID (e.g., `130`) and the DLC (e.g., `8`) were discarded. The Data field contains the actual packet data (e.g., `14 80 10 80 00 00 0A 73)` from the CAN frame. Since data length was arbitrary, the ending bits were padded with 00 in case the data length was shorter than 8 bytes. The data was scaled and since the data was unbalanced, Synthetic Minority Oversampling Technique (SMOTE) was used to balance the data. Each of the datapoints was labelled with one of the Sub-class attack types as shown in Table II. This resulted in a multi-class classification problem.

TABLE II. CLASS BREAKDOWN OF DATASET

Sub-Class	Description	
	Definition	***Type***
Normal	Normal traffic in CAN bus	Normal
Flooding (DoS)	Flooding attack aims to fill the CAN bus segment with a massive number of traffic messages so that the network bus is congested and hence prevents the targeted service traffic to come through	Attack
Spoofing	CAN messages are injected to control certain desired functions as the source destination is spoofed.	Attack
Replay	Replay attack is to extract normal traffic at a specific time and replay (inject) it into the CAN bus.	Attack
Fuzzing	Random messages are injected to cause unexpected behavior of the vehicle	Attack

4 Neural Network Architectures

As Table I shows, Mehedi et al. [17] used a 1DCNN to achieve a an F1-Score of 0.92 to 0.95 on this data set. However, as Table I shows, LSTMs (e.g., [12], [15], [20]) and GRUs (e.g., [11]) have been used successful for ID as well. In addition, time difference between the blocks arriving seems to be a useful feature for intrusion detection (e.g., [5], [6]). Therefore, we considered the time difference as well as the padded data as inputs to 1DCNN, LSTM, Bidirectional LSTM and a GRU model. The LSTM, Bidirectional LSTM, and GRU used a Dense()-Dropout(0.35)-Dense(4) network using the SGD optimizer, learning rate of 0.1, and cross-entropy loss. The 1DCNN used a Conv1D(8)-Dropout(0.25)-MaxPooling1D-Flatten-Dense(ReLU)-Dense(4) network. Each of the above model was trained using a 60/20/20 training/validation/testing split for a total of 30 epochs each. No overfitting was observed based on the loss curves for any of the models.

5 Results

Fig 2. shows the performance metrics for the best models of each type. As the Figure shows, all four models were able to achieve high F1-scores of at least 0.99 or more and hence outperforming Mehedi et al. [17]. This can clearly be attributed to the inclusion of the time difference data in addition to the packet data.

	Precision	Recall	F1-Score	Support
Normal	0.99	0.99	0.99	13384
Flooding	1.00	1.00	1.00	11337
Fuzzing	1.00	1.00	1.00	11618
Replay	0.99	0.99	0.99	11670
Spoofing	1.00	1.00	1.00	11959
Accuracy			1.00	59968
Macro Average	1.00	1.00	1.00	59968
Weighted Average	1.00	1.00	1.00	59968

(a) LSTM

	Precision	Recall	F1-Score	Support
Normal	1.00	1.00	1.00	13384
Flooding	1.00	1.00	1.00	11337
Fuzzing	1.00	1.00	1.00	11618
Replay	1.00	1.00	1.00	11670
Spoofing	1.00	1.00	1.00	11959
Accuracy			1.00	59968
Macro Average	1.00	1.00	1.00	59968
Weighted Average	1.00	1.00	1.00	59968

(b) GRU

	Precision	Recall	F1-Score	Support
Normal	1.00	1.00	1.00	13384
Flooding	1.00	1.00	1.00	11337
Fuzzing	1.00	1.00	1.00	11618
Replay	1.00	1.00	1.00	11670
Spoofing	1.00	1.00	1.00	11959
Accuracy			1.00	59968
Macro Average	1.00	1.00	1.00	59968
Weighted Average	1.00	1.00	1.00	59968

(c) 1D CNN

	Precision	Recall	F1-Score	Support
Normal	0.98	1.00	0.99	13384
Flooding	1.00	1.00	1.00	11337
Fuzzing	1.00	1.00	1.00	11618
Replay	0.99	0.98	0.99	11670
Spoofing	1.00	1.00	1.00	11959
Accuracy			0.99	59968
Macro Average	0.99	0.99	0.99	59968
Weighted Average	0.99	0.99	0.99	59968

(d) BiDirectional LSTM

Fig. 2. Performance metrics for the best models

Table III summarizes the results of K-fold testing confirming that the 1DCNN had the best mean macro F1-Score of 0.9997 with a very small standard deviation of 9.2223e-5 showing that this is a robust model in addition to being accurate. Fig. 3 shows the results of 10-fold testing showing that 1DCNN seemed to have performed the best overall with the greatest number of high F1-Score models.

TABLE III. K-FOLD TESTING RESULTS (K=10)

Method	***Mean Macro F1-Score***	***Standard Deviation***
LSTM	0.9944	0.00230
GRU	0.9993	0.00035
1DCNN	0.9997	9.2223e-5
BiDirectional LSTM	0.9944	0.002304

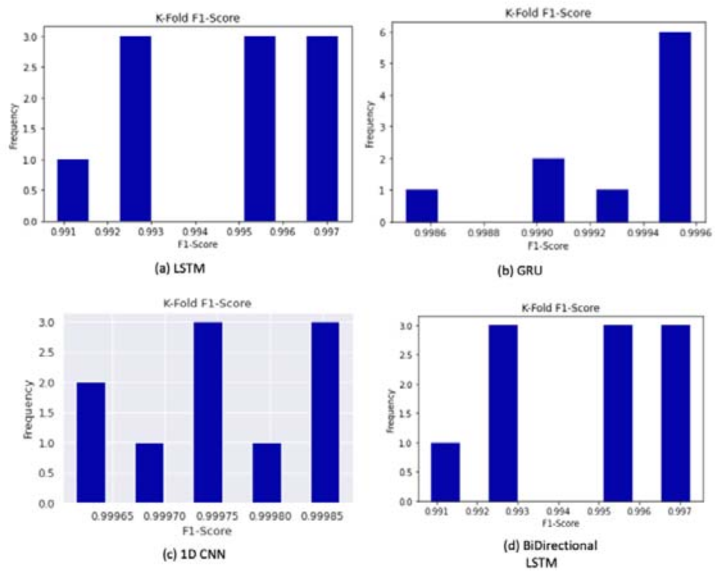

Fig. 3. 10-Fold Macro-F1 metrics

An analysis of the confusion matrices showed that Replay and Normal class were the most misclassified across the various methods.

6 Conclusion

While many ID models have been proposed for CAN networks, this paper has presented the best state-of-the-art results by using very conventional and small neural network models.

References

[1] I. Martínez, "The 5G Car," in *The Future of the Automotive Industry: The Disruptive Forces of AI, Data Analytics, and Digitization*, I. Martínez, Ed. Berkeley, CA: Apress, 2021, pp. 45–62. doi: 10.1007/978-1-4842-7026-4_3.
[2] "[HIDE]CAN-intrusion-dataset (OTIDS)." https://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset (accessed Aug. 07, 2021).
[3] "Car-Hacking Dataset." https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset (accessed Aug. 07, 2021).
[4] H. K. Kim, "Car Hacking: Attack & Defense Challenge 2020 Dataset." IEEE, Feb. 03, 2021. Accessed: Aug. 05, 2021. [Online]. Available: https://ieee-dataport.org/open-access/car-hacking-attack-defense-challenge-2020-dataset
[5] H. Lee, S. H. Jeong, and H. K. Kim, "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)*, Aug. 2017, pp. 57–5709. doi: 10.1109/PST.2017.00017.

[6] S. Jin, J.-G. Chung, and Y. Xu, “Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network,” in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2021, pp. 1–5. doi: 10.1109/ISCAS51556.2021.9401087.

[7] T. Moulahi, S. Zidi, A. Alabdulatif, and M. Atiquzzaman, “Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus,” *IEEE Access*, vol. 9, pp. 99595–99605, 2021, doi: 10.1109/ACCESS.2021.3095962.

[8] O. Avatefipour *et al.*, “An Intelligent Secured Framework for Cyberattack Detection in Electric Vehicles’ CAN Bus Using Machine Learning,” *IEEE Access*, vol. 7, pp. 127580–127592, 2019, doi: 10.1109/ACCESS.2019.2937576.

[9] X. Li *et al.*, “CAN Bus Messages Abnormal Detection Using Improved SVDD in Internet of Vehicle,” *IEEE Internet Things J.*, pp. 1–1, 2021, doi: 10.1109/JIOT.2021.3098221.

[10] X. He, Z. Yang, and Y. Huang, “A Vehicle Intrusion Detection System Based on Time Interval and Data Fields,” in *Artificial Intelligence and Security*, Cham, 2021, pp. 538–549. doi: 10.1007/978-3-030-78612-0_43.

[11] A. R. Javed, S. ur Rehman, M. U. Khan, M. Alazab, and T. R. G, “CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU,” *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1456–1466, Apr. 2021, doi: 10.1109/TNSE.2021.3059881.

[12] J. Song, F. Li, R. Li, Y. Li, Q. Zhou, and J. Zhang, “Research on CAN Bus Anomaly Detection Based on LSTM AndResNet,” *J. Phys. Conf. Ser.*, vol. 1757, no. 1, p. 012044, Jan. 2021, doi: 10.1088/1742-6596/1757/1/012044.

[13] F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone, and A. Santone, “CAN-Bus Attack Detection With Deep Learning,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–10, 2021, doi: 10.1109/TITS.2020.3046974.

[14] N. Leslie, “An Unsupervised Learning Approach for In-Vehicle Network Intrusion Detection,” in *2021 55th Annual Conference on Information Sciences and Systems (CISS)*, Mar. 2021, pp. 1–4. doi: 10.1109/CISS50987.2021.9400233.

[15] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, “CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data,” *IEEE Access*, vol. 8, pp. 58194–58205, 2020, doi: 10.1109/ACCESS.2020.2982544.

[16] E. Seo, H. M. Song, and H. K. Kim, “GIDS: GAN based Intrusion Detection System for In-Vehicle Network,” in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, Aug. 2018, pp. 1–6. doi: 10.1109/PST.2018.8514157.

[17] S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, “Deep Transfer Learning Based Intrusion Detection System for Electric Vehicular Networks,” *Sensors*, vol. 21, no. 14, Art. no. 14, Jan. 2021, doi: 10.3390/s21144736.

[18] *SynCAN Dataset*. ETAS, 2021. Accessed: Aug. 07, 2021. [Online]. Available: https://github.com/etas/SynCAN

[19] “Applied Sciences | Free Full-Text | Anomaly Detection of CAN Bus Messages Using a Deep Neural Network for Autonomous Vehicles | HTML.” https://www.mdpi.com/2076-3417/9/15/3174/htm (accessed Aug. 05, 2021).

[20] H. Qin, M. Yan, and H. Ji, “Application of Controller Area Network (CAN) bus anomaly detection based on time series prediction,” *Veh. Commun.*, vol. 27, p. 100291, Jan. 2021, doi: 10.1016/j.vehcom.2020.100291.

[21] M. Delwar Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “An Effective In-Vehicle CAN Bus Intrusion Detection System Using CNN Deep Learning Approach,” in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Dec. 2020, pp. 1–6. doi: 10.1109/GLOBECOM42002.2020.9322395.

[22] Y. Xun, Y. Zhao, and J. Liu, “VehicleEIDS: A Novel External Intrusion Detection System Based on Vehicle Voltage Signals,” *IEEE Internet Things J.*, pp. 1–1, 2021, doi: 10.1109/JIOT.2021.3090397.