A Lightweight Intrusion Detection System on In-Vehicle Network Using Polynomial Features

Baatarsuren Sukhbaatar[1], Md Rezanur Islam[1], Kamronbek Yuspov[1], Insu Oh[2], and Kangbin Yim[2](✉)

[1] Department of Software Convergence, Soonchunhyang University, Asan, Korea
{baatar56,arpureza,yuskarmron}@sch.ac.kr

[2] Department of Information Security Engineering, Soonchunhyang University, Asan, Korea
{catalyst32,yim}@sch.ac.kr

Abstract. Intrusion detection systems are critical to maintaining network security, especially for onboard vehicle networks. However, the complexity of existing systems often requires high computational power, making them impractical for many applications. In this study, we propose a simple yet effective approach for intrusion detection based on polynomial feature processing and a lightweight deep learning model. Our approach achieves significantly higher accuracy than other computationally intensive deep learning models, making it a practical solution for intrusion detection in low-resource environments. Our proposed method can be easily implemented and integrated into existing systems, providing a lightweight yet effective solution for network security.

1 Introduction

The automotive industry is growing and developing rapidly. Modern cars are becoming more intelligent and functional in their capabilities and movements. Equipping cars with new technologies should make them more comfortable and intelligent than previous generations. The development of computer technology, such as the electronic control unit (ECU) [1], has played an important role in achieving this goal. This technology is widely used in mechanical engineering, and with the help of the ECU, it is possible to monitor and control various vehicle systems, which can improve fuel efficiency and reduce noise and vibration during operation. To establish communication between vehicle components such as engine, transmission, and other systems, a communication protocol widely used in the automotive industry is used - Controller Area Network (CAN) [2]. However, despite its high reliability and data transmission rate, the CAN bus does not have a sufficient level of protection, making the system vulnerable to possible internal or external attacks. Modern transportation is a complex technological system that facilitates traffic management. However, due to the fact that the CAN bus used for communication in cars has a maximum load size of 8 bytes, the details of which can be found in [3], and does not provide encryption and authentication mechanisms, modern cars have become an attractive target for intruders. For example, if a hacker manages to

L. Barolli (Ed.): IMIS 2023, LNDECT 177, pp. 96–102, 2023.
https://doi.org/10.1007/978-3-031-35836-4_11

hack into the ECU, he can gain complete control over the vehicle's systems, including the engine, brakes, lighting, and other critical components. This can lead to dangerous situations on the road, such as the engine being turned off while the vehicle is in motion or the brakes coming off, which can lead to an accident. Intrusion Detection System (IDS) [4] is a system that enables the detection of intruders and the improvement of vehicle safety. IDS is based on deep learning algorithms that analyze data from vehicle sensors and systems to detect potential security risks. If an intruder attempts to hack into ECU and take control of the vehicle's systems, IDS can detect the intrusion, block access to critical systems, and notify the owner of the threat. However, a major drawback of current deep learning algorithms is their high computational power requirements, which the in-vehicle network cannot support due to low computational power with low power consumption. Table 1 shows some configurations of the onboard network devices [5].

Table 1. Accuracy scores according to classifying categories for different architecture models[5].

Device	Year	Android	CPU	Memory
Head Unit PNI A8020 (IVI)	2017	7.1	Quad-core 1.63 GHz Cortex A7	8 GB, 1 GB RAM
Head Unit Erisin ES8791V (IVI)	2019	10.0	Rockchips PX5 1512 MHz Cortex A53	64 GB, 4 GB RAM
Infineon Tricore TC224 (ECU)	2015	N/A	Single-core 133 MHz TriCore	1 MB, 96 KB RAM
Infineon Tricore TC397 (ECU)	2018	N/A	Hexa-core 300 MHz TriCore	16 MB, 2528 KB RAM
S12XE (ECU)	2006	N/A	Single-core 50 MHz S12X	1 MB, 64 KB RAM

To solve this problem, we propose a simple data processing method, polynomial features, and a lightweight deep learning model. Our previous study has shown that each attack has its features, and a lightweight model is sufficient to classify these features [6]. The overall accuracy of our proposed model is much higher than that of other deep learning models, which require a large amount of computation.

2 Related Works

In our modern world, where technology is advancing day by day, the concept of security is crucial. Especially for protection against external threats. One of the pressing problems in this area is to detect threats and eliminate them with little or no damage. In our section, we will look at IDS and what role it plays in mechanical engineering. In recent years, IDS has gained a lot of attention, and researchers working on IDS have made significant progress in the field of IDS. They are trying to improve the efficiency and accuracy of systems to create a more accurate model that can analyze and detect attacks or provide security.

Hyang et al. conducted a study to improve the performance of IDS [7] based on the analysis of the time intervals of CAN messages. Their research showed that there is a difference between the time intervals of CAN messages in normal mode and under attack. They proposed an efficient method for IDS analyzing the time intervals of CAN messages. In their research, Min et al. proposed a more efficient IDS system based on Deep Neural Networks (DNN) [8] to secure the automobile network. They trained the DNN parameters such that the DNN guarantees a high probability of correctly detecting intruders and ensures the security of the in-vehicle network. Md Delwar et al. developed an IDS system for the CAN bus [9] based on Deep Learning with Convolution Neural Networks (CNNs). Their study proves that the CNN-based model is more efficient and reliable than other approaches in detecting network attacks on the CAN bus and achieves a high speed of attack detection. Markus et al. conducted a study on CANet [10], a new neural network architecture that uses unsupervised learning to detect attacks and anomalies on the CAN bus. CANet is the first model in the literature that can process messages with different identifiers. For the CANet model to be used in real applications, it is important that it has a high true-negative rate, usually increasing by 0.99, and CANet meets this requirement. In addition to the high true-negative rate, CANet is also able to correctly detect many unknown attacks. Vita et al. presented an intrusion detection system for automotive communication networks based on the Kohonen SOM network [11], which has high accuracy in detecting messages about attacks on the CAN bus and a minimum number of false positives. This is particularly important for vehicle safety, as the system can effectively detect attacks on the CAN bus and prevent their negative consequences.

3 Data Pre-processing and Deep Learning Architectures

3.1 Data Pre-processing

The security of in-vehicle networks is a growing concern as vehicles become more interconnected and reliant on electronic systems. Cyberattacks on these networks can have serious consequences, such as compromising driver safety or stealing sensitive data. To address this issue, a recent study examined different types of attacks that could target in-vehicle networks. The study focused on several types of attacks, including low-speed and distributed denial-of-service (DoS) attacks, as well as data injection attacks such as fuzzing and replay attacks. These attacks are of particular concern because they are difficult to detect and defend against and can cause significant damage to onboard networks. To collect data for the attacks, the researchers used a unique approach to data collection. They recorded segments of 3to 5 s and injected a different number of data points per segment depending on the type of attack. For example, DoS attacks injected either 5000 or 1000 data points per segment, while fuzzing attacks injected either 100 or 500 data points per segment. For the replay attacks, only two random data points were injected. After collecting the data, the researchers analyzed it to gain insight into the effectiveness of different intrusion detection models in identifying and classifying these attacks. They found that some models were more effective than others and that the number of data points injected per segment had a significant impact on the accuracy of the models. These results have important implications for improving vehicle network security and developing more robust cybersecurity measures. In summary, the study sheds light on the growing threat of cyberattacks on in-vehicle networks and the need for improved security measures to protect against these attacks. The unique approach to data collection and analysis of various intrusion detection models provides valuable insights for future research in this area. Ultimately, the results of this study will be important for developing effective cybersecurity measures to ensure the safety of drivers and their vehicles.

In this study, we chose polynomial features as a means of feature extraction. Polynomial features can be defined as a transformation that takes an input vector or matrix of features, X, and produces a new matrix of polynomial features, X polynomial, according to the following formula:

$$X_{\text{polynomial}} = [1, \mathrm{X}, X^2, X^3, \ldots, X^d] \tag{1}$$

In this formula, X^{d} represents the d power of X, and the resulting matrix X polynomial contains all possible combinations of the input features up to degree d. The degree d is a hyperparameter indicating the maximum degree of polynomial features to be generated. To apply polynomial features in this study, we first converted the hexadecimal format of CAN ID to numeric data using a label encoder and then calculated the CAN ID time interval. We then scaled the data set to a range of 0 to 1 using a min-max scaler. Finally, we converted the resulting numerical values into polynomial features. This approach allows us to generate a broader range of features from the initial dataset, which can lead to improved performance in subsequent modeling steps.

3.2 Deep Learning Model Architecture

A dense neural network is a type of artificial neural network in which every neuron in one layer is connected to every neuron in the previous layer. This allows the network to learn complex representations of the input data [12]. Dense networks consist of multiple layers of densely connected neurons and are capable of solving a wide range of problems, such as image recognition, natural language processing, and speech recognition. The weights and biases of the connections between neurons are learned through a process called backpropagation, in which the network is trained using a large dataset. Dense networks have proven to be extremely effective in many machine-learning applications.

Mathematically, a dense layer can be defined as follows. Let X be the input data for the layer, with dimensionality (n, m), where n is the number of examples in the batch and m is the number of features in each example. Let W be the weight matrix of the layer, with dimensionality (m, k), where k is the number of neurons in the layer. Let b be the bias vector of the layer, with dimensionality (1, k). Then the output of the layer, denoted as Y, is given by:

$$\mathrm{Y} = \mathrm{XW} + \mathrm{b} \tag{2}$$

In this equation, the operation XW represents the matrix multiplication of X and W, resulting in an output matrix with dimensionality (n, k). The bias vector b is added element-wise to each row of the output matrix, resulting in the final output matrix Y with the same dimensionality as XW.

The main goal of this research is to develop a lightweight intrusion detection system so that the architecture was kept as simple as possible. The model consists of three layers, including two hidden layers and an output layer. The first layer is a dense layer of 32 neurons using the rectified linear unit (ReLU) activation function. The input shape for this layer is 5, which is determined by the shape of the input data. The second layer is also a dense layer with 16 neurons and the activation function ReLU. The output layer has a number of neurons equal to the number of classes and uses the softmax activation function that generates probabilities for each class. The model is built using the loss function categorical_crossentropy, the Adam optimizer, and accuracy as a metric for scoring. This architecture is commonly used in classification tasks and has been shown to be effective in various machine-learning applications. Figure 1 Shows the physical layout of the model architecture.

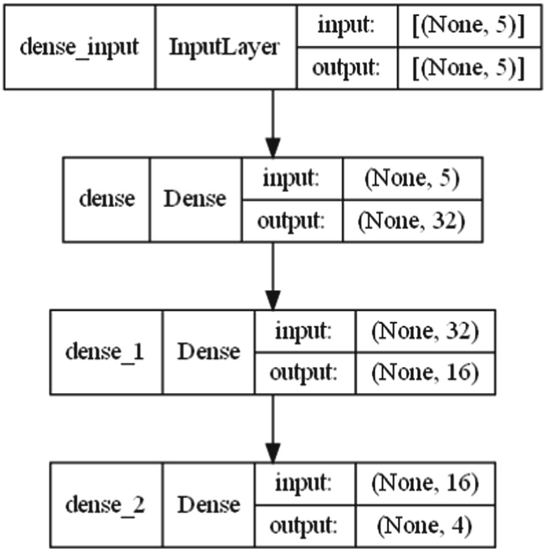
dense_input | InputLayer | input: | [(None, 5)] | output: | [(None, 5)]
dense | Dense | input: | (None, 5) | output: | (None, 32)
dense_1 | Dense | input: | (None, 32) | output: | (None, 16)
dense_2 | Dense | input: | (None, 16) | output: | (None, 4)

Fig. 1. Neural Networks.

4 Result Evaluation

Recently, there has been a lot of research on intrusion detection using advanced algorithms with high-dimensional features. This requires high computational power. However, this problem can be solved by using a simple algorithm model with low computational power. Our proposed model achieves an overall accuracy of 95% for three attack types, with lower accuracy for replay attacks than for the other attack types. Table 2 shows the performance evaluation of a classification model for a dataset with four different classes. The evaluation metrics include precision, recall, and F1 score for each class, as well as the macroscopic and weighted average of these metrics across all classes.

Figure 2 Shows the model achieves high precision and recall scores for all classes, with F1 scores ranging from 0.91 to 1.00. The overall accuracy of the model is 0.95, indicating that it is able to correctly classify the majority of examples in the dataset. These results indicate that the model can effectively distinguish between the different classes and has practical value in real-world applications.

Table 2. Accuracy scores according to classifying categories for different architecture models.

Types	Precision	Recall	F1-Score	Number of Packets
Normal	0.78	0.86	0.99	58211
Fuzz	0.93	0.98	1.00	58303
DoS	0.99	1.00	1.00	58356
Replay	0.18	0.39	0.97	58283
Overall Accuracy	0.95			233153
Macro avg	0.95	0.95	0.95	
Weighted avg	0.95	0.95	0.95	
ROC Score	0.9693			

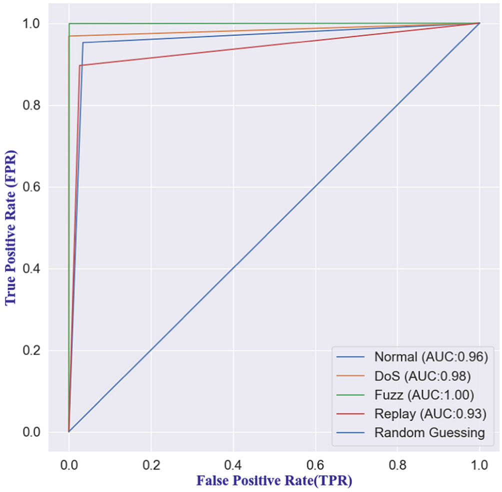

Fig. 2. ROC AUC Curve and Accuracy Score.

5 Conclusion

In conclusion, the article proposes a simple and lightweight intrusion detection system using a polynomial feature data processing method and a dense neural network model with three layers. The model is designed to classify the characteristics of different types of attacks with high accuracy while minimizing computational requirements. The proposed model's architecture is straightforward, with only two hidden layers and a small number of neurons. This architecture is commonly used in classification tasks and has proven to be effective in various applications of machine learning. Overall, the proposed method offers a promising approach to intrusion detection with a simple yet effective architecture that can be deployed in real-world systems.

Acknowledgments. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. 2021R1A4A2001810) and the Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (No. 2019-0-01343, Regional strategic industry convergence security core talent training business).

References

1. Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. Defcon 23, 2015, 1–91 (2015). http://illmatics.com/RemoteCarHacking.pdf
2. Bozdal, M., Samie, M., Jennions, I.: A survey on CAN bus protocol: attacks, challenges, and potential solutions. In: 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), pp. 201–205 (2018). https://doi.org/10.1109/iCCECOME.2018.8658720
3. BOSCH CAN Specification Version 2.0 (1991)
4. Aliwa, E., Rana, O., Perera, C., Burnap, P.: Cyberattacks and countermeasures for in-vehicle networks. ACM Comput. Surv. **54**(1), 1–37 (2021). https://doi.org/10.1145/3431233
5. Andreica, T., Curiac, C.-D., Jichici, C., Groza, B.: Android head units vs. In-vehicle ECUs: performance assessment for deploying in-vehicle intrusion detection systems for the CAN bus. IEEE Access **10**, 95161–95178 (2022). https://doi.org/10.1109/ACCESS.2022.3204746
6. Islam, M.R., Oh, I., Batzorig, M., Kim, S., Yim, K.: A concept of IDS for CAN protocol based on statics theory. In: Barolli, L. (ed.) BWCCA 2021. LNNS, vol. 346, pp. 294–302. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-90072-4_32
7. Song, H.M., Kim, H.R., Kim, H.K.: Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network (2016). https://doi.org/10.1109/ICOIN.2016.7427089
8. Kang, M.-J., Kang, J.-W.: Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE **11**(6), e0155781 (2016). https://doi.org/10.1371/journal.pone.0155781
9. Delwar Hossain, M., Inoue, H., Ochiai, H., Fall, D., Kadobayashi, Y.: An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach. In: GLOBECOM 2020 - 2020 IEEE Global Communications Conference, pp. 1–6 (2020). https://doi.org/10.1109/GLOBECOM42002.2020.9322395
10. Hanselmann, M., Strauss, T., Dormann, K., Ulmer, H.: CANet: an unsupervised intrusion detection system for high dimensional CAN bus data. IEEE Access **8**, 58194–58205 (2020). https://doi.org/10.1109/ACCESS.2020.2982544
11. Barletta, V.S., Caivano, D., Nannavecchia, A., Scalera, M.: Intrusion detection for in-vehicle communication networks: an unsupervised kohonen SOM approach. Futur. Internet **12**, 119 (2020). https://doi.org/10.3390/FI12070119
12. Charles, D., Fyfe, C., Livingstone, D., McGlinchey, S.: An introduction to artificial neural networks. In: Biologically Inspired Artificial Intelligence for Computer Games, pp. 12–23. IGI Global (2008)