Black Mamba: A Multi-class Random Forest for Automotive Intrusion Detection

Vita Santa Barletta*, Danilo Caivano*, Mirko De Vincentiis*, Antonio Piccinno*
*Department of Computer Science, University of Bari Aldo Moro, Bari, Italy
{vita.barletta, danilo.caivano, mirko.devincentiis, antonio.piccinno}@uniba.it

***Abstract*—The latest generation of vehicles incorporates advanced technologies that offer many benefits. One such innovation is the in-vehicle communication system called Controller Area Network (CAN) bus, which connects various components called Electronic Control Units (ECUs). The ECUs improve the vehicle's overall safety, security, and stability, ensuring enhanced protection for the driver and passengers. Since they provide critical functionalities, it is necessary to integrate the CAN bus with real-time Intrusion Detection Systems (IDSs) to prevent threats in vehicles. Most of the IDSs proposed in the literature use offline classification. Further, the in-vehicle networks need to be more robust for implementing IDS. For these reasons, this paper proposes an in-vehicle multi-class IDS aiming to detect cyber attacks that can be occurred on the CAN bus to perform a real-time identification.**

***Index Terms*—Automobile, Cybersecurity, Smart City, CAN Bus, IDS-multiclass**

I. Introduction

The automotive sector has been undergoing a radical transformation in recent years and several initiatives concerning smart mobility and autonomous driving are, indeed, experiencing increasing development in urban areas and smart city contexts [1], [2]. The vehicles are characterized by ECUs that provide different functionalities such as keyless entry, anti-lock braking system, power steering, anti-theft, traction control, telematic/navigation system, and parking assistant. These components communicate using different protocols, but the most used and studied is the CAN due to its safety and velocity of sending messages [3].

With advanced technologies installed in the new breed of automobiles, they became subject to numerous threats from attackers. In particular, with the increase of the semi-autonomous car, the number of threats is increasing. Although the CAN bus is responsible for stable, safe, and secure communication within the ECUs, some inherent vulnerabilities can still be exploited. For example, Denial of Service (DoS), eavesdropping, fuzzy, malfunction, and flooding, among others, [4]. To meet the demand for security, different techniques like IDSs, network segmentation, authentication, and encryption were proposed in the past couple of decades to combat cyberattacks on vehicles. Regarding IDS, Alshammari et al. [5] proposed two classification algorithms: KNN and Support Vector Machine (SVM) using the Car-Hacking Dataset. The results show that the KNN reached better performance than the SVM. Gundu and Maleski compared supervised machine learning algorithms and concluded that the Random Forest classifier outperforms both K-Nearest Neighbor and XG boost [6]. In addition, Mowla et al. [7] used Random Forest with a dynamic voting technique that presented better and more stable performance. Therefore, considering the literature, Random Forest proved an excellent candidate for multi-class classification techniques for IDS problems.

Random forest, thus, proved to be a good candidate for multi-class classification techniques for IDS problems. The principal challenge is to detect attacks on the CAN bus accurately and in real-time. The computational units or ECUs existing in the vehicles are primarily microcontrollers and possess very low computational power. Real-time IDS can be achieved only with an onboard, specialized, and dedicated IDS powerful enough to run complex Machine Learning (ML) tasks [8]. For this reason, this work proposed a multi-class IDS to identify attacks in real time. The multi-class technique offers an opportunity to improve vehicle attack detection and classification since most research proposes only binary classification solutions.

II. Black Mamba: a Multi-class IDS

A Random Forest (RF) classifier algorithm was used to identify threats on the CAN bus. The classifier consists of N decision trees, each of which will predict a class (vote). The class with the most votes will become the model's prediction. The model can predict the following classes: Normal, Flooding, Fuzzy, or Malfunction. To be more specific, for the Flooding attack, the CAN ID and the DATA field were set to zero; for the Fuzzy attacks, the values of CAN ID and DATA were generated randomly in hexadecimal form; and finally, for the Malfunction attack, the CAN ID corresponded to the IDs used by the Survival Analysis Dataset [9] instead, the DATA field was generated randomly like the Fuzzy attack. The training and the testing phase were performed offline because an ECU has limited computational power.

To replicate real-time identification, an Arduino Elegoo Uno R3 component simulates the behavior of the malicious actor by sending attack messages. In particular, 100 attack messages were sent to validate the model. The Raspberry Pi 4 analyzed the messages received from the CAN bus and determined whether the received message was an attack or not. Two Arduino MKR CAN Shields were used wherein one sent the messages (using the Arduino Elegoo Uno R3), and the other received those and transmitted them to the IDS (Raspberry Pi 4). The MKR CAN Shield consists of a microchip MCP2515

TABLE I
RESULTS OBTAINED CONSIDERING RANDOM FOREST AND ARDUINO ELEGOO UNO R3 (INJECTED MESSAGES).

Model	Label	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Random Forest	Normal	99.98	99.99	99.98	99.99
	Flooding		100	100	100
	Fuzzy		99.79	99.93	99.86
	Malfunction		99.90	99.98	99.94
Injected Messages	Flooding	85.71	100	100	100
	Fuzzy		57.14	100	72.72
	Malfunction		100	25	40

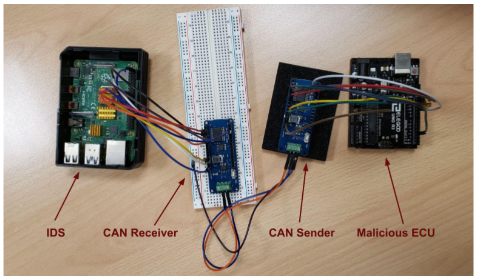

Fig. 1. Laboratory setup for the experimentation phase.

to transmit and receive the CAN message [10]. Figure 1 shows the laboratory setup to replicate real-time identification.

The RF model was trained and tested using a state-of-the-art dataset called Survival Analysis Dataset [9] because it contains CAN messages obtained from real vehicles: HYUNDAI YF Sonata, KIA Soul, and CHEVROLET Spark. This dataset contains *flooding*, *fuzzy*, and *malfunction* attacks. The attributes contained are **Timestamp** recorded times; **CAN ID** identifier of the CAN message in hexadecimal form; **DLC** the Data Field length from 0 to 8; **DATA** data value in hexadecimal format; **Flag**, T represents the injection message while R represents the normal message.

All the messages were merged from the analyzed dataset for multi-class classification. The CAN ID and the Data were transformed from hexadecimal to decimal form. Then, the Timestamp and the DLC were removed because they were unimportant for the model. Finally, the features are scaled into a range of $0, 1$. The dataset was split into training (70%) and testing (30%). After the RF model's training and testing, the final model was deployed into the Raspberry Pi 4 for real-time identification.

III. EVALUATION RESULT AND CONCLUSION

Prediction, Recall, and F1-Score were used as metrics to evaluate the Random Forest and the injected malicious messages. Table I shows the results using the traditional machine learning metrics for the Random Forest model and injected messages. Mostly, the predictions about the attack types were correct, apart from the Fuzzy attack, because of the randomness of the DATA field. The Arduino Elegoo Uno R3 only injected malicious messages to simulate the attack and validate the IDS when a vehicle is under attack. As seen in Table I, 75% of Malfunction messages were misclassified as Fuzzy. In the case of Malfunction messages, the CAN IDs are reused from the existing ones in the dataset, and the DATA field was randomly generated.

So, through this experiment, it was possible to see the feasibility of using an IDS inside a vehicle to detect possible attacks. This approach adopted a laboratory-based IDS system to be implemented in a real-world automotive scenario.

ACKNOWLEDGMENT

This study has been partially supported by the following projects: SSA (Codice 6ESURE5) and KEIRETSU (Progetto V9UFIL5) funded by ”Regolamento regionale della Puglia per gli aiuti in esenzione n. 17 del 30/09/2014 (BURP n. 139 suppl. del 06/10/2014); and SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

REFERENCES

[1] V. S. Barletta, D. Caivano, A. Nannavecchia, and M. Scalera, “Intrusion detection for in-vehicle communication networks: An unsupervised kohonen som approach,” *Future Internet*, vol. 12, no. 7, 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/7/119

[2] R. Du, P. Santi, M. Xiao, A. V. Vasilakos, and C. Fischione, “The sensable city: A survey on the deployment and management for smart city monitoring,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1533–1560, 2018.

[3] V. S. Barletta, D. Caivano, M. D. Vincentiis, A. Ragone, M. Scalera, and M. Á. S. Martín, “V-soc4as: A vehicle-soc for improving automotive security,” *Algorithms*, vol. 16, no. 2, p. 112, 2023.

[4] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, “Cybersecurity challenges in vehicular communications,” *Vehicular Communications*, vol. 23, p. 100214, 2020.

[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, no. 4, pp. 79–94, 2018.

[6] R. Gundu and M. Maleki, “Securing can bus in connected and autonomous vehicles using supervised machine learning approaches,” in *2022 IEEE International Conference on Electro Information Technology (eIT)*. IEEE, 2022, pp. 042–046.

[7] N. I. Mowla, J. Rosell, and A. Vahidi, “Dynamic voting based explainable intrusion detection system for in-vehicle network,” in *2022 24th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2022, pp. 406–411.

[8] H. Ma, J. Cao, B. Mi, D. Huang, Y. Liu, and S. Li, “A GRU-Based Lightweight System for CAN Intrusion Detection in Real Time,” *Secur. Commun. Netw.*, vol. 2022, Jun. 2022.

[9] M. L. Han, B. I. Kwak, and H. K. Kim, “Anomaly intrusion detection method for vehicular networks based on survival analysis,” *Vehicular Communications*, vol. 14, pp. 52–63, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209618301189

[10] Microchip, “MCP2515 Stand-Alone CAN Controller with SPI Interface,” Microchip Technology Inc, Chandler, Arizona, USA, Tech. Rep., 2019. [Online]. Available: https://ww1.microchip.com/downloads/en/DeviceDoc/MCP2515-Stand-Alone-CAN-Controller-with-SPI-20001801J.pdf