FedIoV: A Federated Learning-Assisted Intrusion Messages Detection in Internet of Vehicles

Ahmad Zainudin*†, Rubina Akter‡, Dong-Seong Kim§, and Jae-Min Lee§
*Department of Electronic Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea
§Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, Korea
‡ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea
†Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya, Surabaya, Indonesia
(zai*, rubinaakter2836, dskim, ljmpaul)@kumoh.ac.kr

***Abstract*—The internet of vehicles (IoV) has made cognitive services realize autonomous driving and advanced driver assistance for intelligent connected vehicles (ICVs). However, the fast growth of ICVs and the emergence of wireless interfaces have created vehicle networks vulnerable to cyber-attacks. This study proposes the following contribution, taking into account the privacy-preserving of the intelligent connected vehicles for intrusion message detection in the IoV. The proposed model was evaluated by in-vehicle network intrusion detection, the Car-Hacking dataset. The measurement results show the proposed model outperforms other FL-based messages intrusion detection systems.**

***Index Terms*—federated learning, intrusion messages detection, internet of vehicles (IoV)**

I. Introduction

The Internet of vehicles (IoV) is part of the internet of things (IoT) applications that allow a connection between automated vehicles and intelligent transportation network infrastructure. The fast growth of intelligent connected vehicles (ICVs) has created some security and privacy problems. Moreover, the increased use of software and the emergence of wireless interfaces have created vehicle networks vulnerable to cyber-attacks [1]. Securing shared information using efficient and reliable intrusion detection systems (IDSs) by leveraging a machine learning (ML) or deep learning (DL) model continues to be a crucial concern, particularly with the increasing use of vehicle networks [2]. However, scalability and acceptable latency cannot be provided by centrally managed cloud-based IDS. Additionally, a centralized learning scenario leads to clients' privacy issues [3]. Federated learning (FL) is a collaborative learning mechanism in which the learning model parameters are transferred to the aggregator, which is supposed to provide privacy in the IoV. FL-based IDS allows local training using the local model with its own network traffic data on the vehicles as the clients.

The authors [4] evaluated the deep convolution neural network (DCNN) model to detect IVNs' malicious attacks. The DCNN model was built by utilizing a reduced Inception-ResNet network structure. An ML-based DDoS Attack Detection model was implemented in an SDN-based VANET [5]. These models [4], [5] perform centralized-based learning that leads client data privacy issues. The federated LSTM-based in-vehicle networks (IVNs) intrusion detection was implemented to detect malicious activities based on the periodicity of the ID sequence [6]. The federated-LSTM model was evaluated using the CAN-intrusion (OTIDS) dataset. This model utilized multi-stack LSTM with a large number of neurons, causing a costly computing process. It is not acceptable to have constrained devices in an intelligent connected vehicle network.Considering the privacy-preserving requirement and the need for an efficient model for constrained devices in an intelligent connected vehicle network, this study has some contributions.

- We proposed a federated learning (FL)-assisted intrusion detection system (IDS) that can detect malicious messages in vehicle networks that enables privacy-aware using MLP model.
- We implemented an accurate MLP model with a low-complexity structure to enable the development of real-time intrusion message detection in IoV.

II. FL-based In-Vehicle Networks (IVNs) Intrusion Detection in IoV

An aggregation server and intelligent connected-vehicles acting as data owners make up the proposed federated architecture as shown in Fig. 1. The weight parameters w_0 as well as additional model training parameters are initiated by the aggregation server and shared with the vehicles V_k, where $k \in K = \{1, 2, 3.., K\}$. Furthermore, define the aggregate number of communication rounds R that occur during the aggregation procedure. The vehicle agents use received weight and other training parameters to train their network traffic features $D_k(k \in K)$ with size N_k. Following local model training, the vehicle agents upload each local deep learning model parameter w_{t+1}^k to the aggregation server. The aggregation server aggregates and calculates the model parameters using the federated averaging (FedAvg) algorithm as shown below.

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^k. \quad (1)$$

This study makes use of the Car-Hacking dataset [7], which includes the most recent IoV malicious message attacks. We suggest an FL-based Multilayer Perceptron (MLP) model for

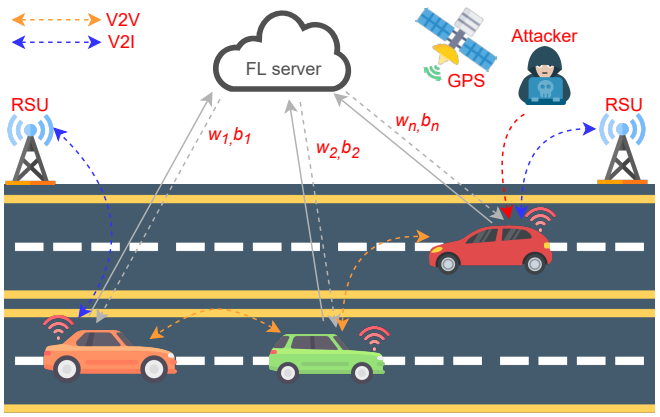

Fig. 1. FL-based intrusion messages detection in IoV

TABLE I
EXPERIMENTAL PARAMETERS SETTING OF THE PROPOSED MODEL

Parameters	Value	Parameters	Value
Total Features	9	Dense layers	3 (100, 50, 2)
Local epochs	2	Loss function	Sparse Categorical Crossentropy
Mini-batch size	32	Activation function	ReLU
Optimizer	SGD	Number of rounds	(2, 4, 6, 8, 10)
Learning rate	0.001		

classifying malicious messages. Parameters are provided in Table I.

III. EXPERIMENTAL RESULTS AND DISCUSSION

Table II describes the performance comparison of the proposed model with other models (3-Layer MLP, 7-Layer MLP, Multi-MLP) for malicious messages classification. For comparison purposes, we rerun the existing network structure model and apply a standard multi-MLP models using our environment. Based on the measurement results, the proposed model outperforms the existing models. The proposed model achieves the highest accuracy of 98.45% and loss 0.0441 when using ten communication rounds with five vehicle agent contributors.

IV. CONCLUSION

Based on the in-vehicles intrusion security branch-mark, the Car Hacking dataset, this study implements an FL-based architecture malicious messages detection in IoV. The measurement results show the proposed model outperforms the existing FL-based intrusion detection approaches in IoV with an accuracy of 98.45% and a loss of 0.0441.

TABLE II
PERFORMANCE COMPARISON OF MALICIOUS MESSAGES CLASSIFICATION WITH DIFFERENT MODELS

Model	Accuracy	Loss	AUC Score	Time Cost	Trainable Parameters
3-Layer MLP [8]	98.28%	0.0649	0.9828	1.203 ms	5.96K
7-Layer MLP [8]	98.31%	0.0534	0.9847	1.397 ms	22.6K
Multi MLP	98.38%	0.0559	0.9845	3.081 ms	45,2K
Proposed Model	**98.45%**	**0.0441**	**0.9845**	**1.321 ms**	**5.31K**

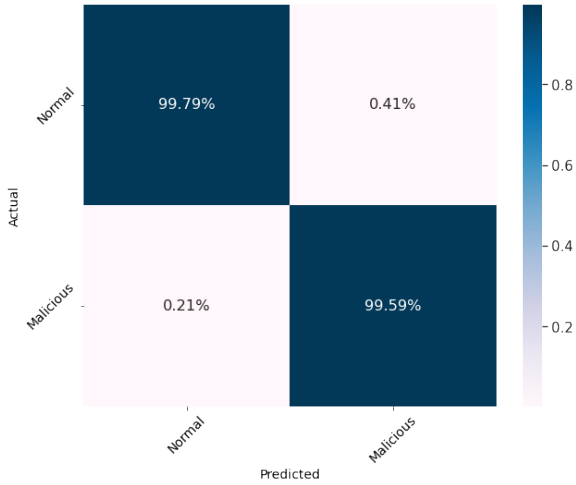

Fig. 2. Confusion matric FL-based intrusion messages detection

ACKNOWLEDGMENT

This work was supported by Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the MSIT (Ministry of Science and ICT) (2018R1A6A1A03024003), Korea and the Grand Information Technology Research Center support program (IITP-2022-2020-0-01612) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation.

REFERENCES

[1] S. Ullah, M. A. Khan, J. Ahmad, S. S. Jamal, Z. e Huma, M. T. Hassan, N. Pitropakis, and W. J. Buchanan, "HDL-IDS: A hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles," *Sensors*, vol. 22, no. 4, p. 1340, 2022.

[2] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Novel Hyper-tuned Ensemble Random Forest Algorithm for the Detection of False Basic Safety Messages in Internet of Vehicles," *ICT Express*, 2022.

[3] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, "An Efficient Hybrid-DNN for DDoS Detection and Classification in Software-Defined IIoT Networks," *IEEE Internet of Things Journal*, 2022.

[4] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle Network Intrusion Detection using Deep Convolutional Neural Network," *Vehicular Communications*, vol. 21, p. 100198, 2020.

[5] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Optimization of RBF-SVM Kernel using Grid Search Algorithm for DDoS Attack Detection in SDN-based VANET," *IEEE Internet of Things Journal*, 2022.

[6] T. Yu, G. Hua, H. Wang, J. Yang, and J. Hu, "Federated-LSTM based Network Intrusion Detection Method for Intelligent Connected Vehicles," in *ICC 2022-IEEE International Conference on Communications*. IEEE, 2022, pp. 4324–4329.

[7] H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, "Car Hacking and Defense Competition on In-Vehicle Network," in *Workshop on automotive and autonomous vehicle security (AutoSec) vol*, 2021, p. 25.

[8] T. Dong, S. Li, H. Qiu, and J. Lu, "An Interpretable Federated Learning-based Network Intrusion Detection Framework," *arXiv preprint arXiv:2201.03134*, 2022.