A Life-long Learning Intrusion Detection System for 6G-Enabled IoV

Abdelaziz Amara korba[2], Souad Sebaa[1], Malik Mabrouki[1], Yacine Ghamri-Doudane[2], and Karima Benatchba[1]

[1]*École nationale Supérieure d'Informatique, Algeria*
[2]*L3I, University of La Rochelle, France*

***Abstract*—The introduction of 6G technology into the Internet of Vehicles (IoV) promises to revolutionize connectivity with ultra-high data rates and seamless network coverage. However, this technological leap also brings significant challenges, particularly for the dynamic and diverse IoV landscape, which must meet the rigorous reliability and security requirements of 6G networks. Furthermore, integrating 6G will likely increase the IoV's susceptibility to a spectrum of emerging cyber threats. Therefore, it is crucial for security mechanisms to dynamically adapt and learn new attack patterns, keeping pace with the rapid evolution and diversification of these threats - a capability currently lacking in existing systems. This paper presents a novel intrusion detection system leveraging the paradigm of life-long (or continual) learning. Our methodology combines class-incremental learning with federated learning, an approach ideally suited to the distributed nature of the IoV. This strategy effectively harnesses the collective intelligence of Connected and Automated Vehicles (CAVs) and edge computing capabilities to train the detection system. To the best of our knowledge, this study is the first to synergize class-incremental learning with federated learning specifically for cyber attack detection. Through comprehensive experiments on a recent network traffic dataset, our system has exhibited a robust adaptability in learning new cyber attack patterns, while effectively retaining knowledge of previously encountered ones. Additionally, it has proven to maintain high accuracy and a low false positive rate.**

***Index Terms*—6G, IoV, Security, intrusion detection, Continual Learning, Life-long Learning, Federated Learning**

I. Introduction

As we enter the 6G era, the landscape of digital communications and interactions is undergoing a profound transformation. This evolution is particularly evident in the Internet of Vehicles (IoV) ecosystem, where the convergence of 6G technology with Connected and Automated Vehicles (CAVs) promises to significantly enhance efficiency, convenience, and user experience. However, this technological advancement is not without its risks. The adoption of 6G in the IoV potentially increases the vulnerability of CAVs to a multitude of emerging cyber threats, making security a major concern for this promising technology [1].

In the complex landscape of cybersecurity, Intrusion Detection Systems (IDS) hold a critical role. The transition from traditional signature-based IDS to anomaly-based systems, capitalizing on advancements in artificial intelligence (AI), represents a significant leap forward. This evolution has led to the development of IDS that can detect a wide array of cyberattacks with remarkable precision [2], [3]. Predominantly, these recent AI-driven IDS rely on deep learning techniques [3], [4], however an inherent limitation of DL: the challenge of incremental learning from continuously evolving data streams, often described as catastrophic forgetting [5]. This challenge is particularly relevant when the system must differentiate between classes that are not observed concurrently. In essence, the IDS must be capable of dynamically adapting to new types of attacks or variations in data patterns that were absent in its initial training dataset. This capability for dynamic learning and adaptability is a critical component for IDS to remain effective in the constantly changing landscape of cyber threats.

Continual Learning, also known as life-long learning, focuses on acquiring knowledge from a continuous stream of data, aiming to expand this knowledge base without the need for retraining from scratch [5]. This area of ML has grown due to its practical benefits, such as improving medical diagnoses, advancing autonomous driving, and accurately predicting financial trends. Its growth highlights its potential to enhance AI adaptability in diverse real-world situations [5]. However, few studies [6], [7] have investigated the application of continual learning for attack detection, the proposed solutions are not fully suited to the distributed and dynamic nature of the IoV. They rely on a centralized learning model that requires data collection, which raises privacy concerns.

This study aims to propose an adaptive IDS capable of learning new attack patterns while retaining those previously learned. We introduce a detection system that combines class-incremental learning (CIL) with federated learning (FL), ensuring adaptability and suitability for the distributed and dynamic environment of the IoV. To enable evolving detection of emerging cyber attacks, our approach integrates the Continual Learning with Experience And Replay (CLEAR) [8] method into our detection model. CLEAR effectively combines direct learning from recent data, ensuring the system remains adaptable, with indirect learning from historical data, enhancing its stability. We train this detection model using FL across local datasets from participating CAVs. In this setup, Multi-access edge computing (MEC) nodes play a pivotal role in coordinating the training process by acting as parameter servers for aggregating FL model updates. The effectiveness of the proposed solution is evaluated using the 5G-NIDD [9] dataset, which contains real-world 5G network traffic traces. To mimic real-world conditions as closely as possible, we initially train the model on a dataset containing a single type of attack mixed

with benign traffic. We then progressively introduce samples of various attack types, each time incorporating a new type. The results have demonstrably proven the IDS's ability to learn new patterns while maintaining high accuracy and a very low False Positive Rate (FPR).

The remainder of this paper is organized as follows. Section II describes related work. The design of our scheme is presented in Section III. Section IV depicts the performance evaluation results, and finally, Section V concludes the paper.

II. Related Work

A recent study by Osorio et al. [1] provided a thorough analysis of security and privacy in the 6G-enabled IoV. They explored how key technological enablers such as network softwarization, blockchain, and AI/ML enhance secure communication. To address the challenges associated with deploying machine learning in 6G-enabled IoV, Hoang et al. [4] proposed a secure and reliable integration of Transfer Learning into the 6G-enabled IoV framework. Addressing security threats in 6G IoV networks, Sedjlmaci et al. [2] developed a collaborative cybersecurity framework based on a multi-level FL algorithm and Stackelberg security games. In a similar vein, Zhang et al. [10] designed a sophisticated weight-based ensemble ML algorithm, optimized with many-objective techniques, for identifying anomalies in vehicular Controller Area Network (CAN) bus systems, thereby aligning with the high security demands of 6G networks. However, while these studies propose IDS solutions suitable for 6G-enabled IoV, they do not fully address the adaptability challenges in a such dynamic and constantly evolving environments where cyber threats are in continuous flux, with new ones emerging. A notable limitation of DL-based IDS is their struggle with incremental learning from continuously evolving data streams, a problem often termed as catastrophic forgetting [5].

To tackle the challenge of adapting IDS to new attack patterns and addressing catastrophic forgetting in DL-based IDS, the study by Prasath et al. [7] examines the effectiveness of continual learning models for the incremental learning of novel attack patterns. This research involved both experimental and analytical studies, focusing on three key continual learning methods: learning without forgetting, experience replay, and dark experience replay. Additionally, another significant effort in employing continual learning is the work by Ejaz et al. [6], which investigates the use of continual learning techniques for consistent phishing detection over time. This study trained a vanilla neural network (VNN) model with deep feature embedding of HTML content in a continual learning setup. The results indicate that continual learning algorithms effectively maintain accuracy over time, albeit with slight performance decline. However, these solutions predominantly utilize centralized learning models, which may not align with the specific demands of the IoV environment. These models often require high bandwidth and result in increased latency. Moreover, there are privacy concerns, as sensitive data might be compromised during transmission to central locations.

To align with the specific demands of the IoV environment, recent studies [11], [12] have proposed Federated Learning (FL)-based IDS for misbehavior detection in 5G and 6G-enabled IoV. Our solution uniquely combines FL and Continual Learning (CL) to ensure both adaptability and suitability within the distributed and dynamic environment of the IoV.

III. Proposed Solution

The proposed IDS is designed to operate on CAV, where it monitors network traffic. For each network flow, the system calculates a specific set of features. These primarily include attributes and statistics from packet headers, focusing on information from the network and transport layers. The aggregation of these feature vectors constitutes the local dataset, which is crucial for training the detection model during the development phase. In the deployment phase, the IDS classifies each vector as either benign or as a specific type of attack.

To enable evolving attack detection, we use the Continual Learning with Experience And Replay (CLEAR) [8] method for our detection model. This methods fuses direct learning from new experiences to preserve the system's adaptability with indirect learning from past experiences to bolster stability. Moreover, CLEAR strengthens the system's consistency by incorporating behavioral cloning, aligning the current operational guidelines with prior iterations. CLEAR is underpinned by an actor-critic training regime that leverages both fresh and historical experiences. Formally, the network parameters are denoted by θ, with π_θ indicating the network's current policy over actions a, and h_s representing the hidden state of the network at time s. The policy generating the observed experience is represented by μ. The V-Trace target v_s for this method is defined as follows [8]:

$$v_s := V(h_s) + \sum_{t=s}^{s+n-1} \gamma^{t-s} \left(\prod_{i=s}^{t-1} c_i \right) \delta V_t,$$

where $\delta V_t := \rho_t(r_t + \gamma V(h_{t+1}) - V(h_t))$ for truncated importance sampling weights $c_i := \min\left(\overline{c}, \frac{\pi_\theta(a_i|h_i)}{\mu(a_i|h_i)}\right)$, and $\rho_t := \min\left(\overline{\rho}, \frac{\pi_\theta(a_t|h_t)}{\mu(a_t|h_t)}\right)$ (with $\overline{c}$ and $\overline{\rho}$ constants). The policy gradient loss is:

$$L_{\text{policy-gradient}} := -\rho_s \log \pi_\theta(a_s|h_s)(r_s + \gamma v_{s+1} - V(h_s)).$$

The loss functions $L_{\text{policy-gradient}}$, L_{value}, and L_{entropy} are utilized for both new and replay experiences. Additionally, $L_{\text{policy-cloning}}$ and $L_{\text{value-cloning}}$ are incorporated exclusively for replay experiences.

In replay experiences, additional loss terms are incorporated to enable behavioral cloning between the network's current state and its historical counterparts. This is aimed at preventing deviations in the network's output on replayed tasks during the learning of new tasks. The methodology includes penalizing (1) the Kullback-Leibler (KL) divergence, which assesses the disparity between the historical and present policy distributions, and (2) the L2 norm, reflecting the variance between

historical and current value functions. Technically, this leads to the integration of specific loss functions [8]:

$$L_{\text{policy-cloning}} := \sum_{a} \mu(a|h_s) \log \frac{\mu(a|h_s)}{\pi_\theta(a|h_s)},$$

$$L_{\text{value-cloning}} := \|V(\theta_{h_s}) - V_{\text{replay}}(h_s)\|^2.$$

Algorithm 1: Federated Averaging Algorithm

Variables: K: index of clients, B: local batch size, E: number of local epochs, η : learning rate
Initialize w_0
for *each round* $t \in \{1, ..., N\}$ **do**
  $m \leftarrow$ max(C. K, 1)
  $S_t \leftarrow$ (random set of m CAVs)
  for *each CAV* $k \in S_t$ *in parallel* **do**
    $\beta_k \leftarrow$ (split P_k into batch of size B)
    for *each local epoch* $i \in \{1, ..., E\}$ **do**
      for *batch* $b \in \beta_k$ **do**
        $w_k \leftarrow w_k - \eta \nabla l(w_k; b)$
      end for
    end for
    $w_{t+1}^k \leftarrow w_k$
  end for
  $w_{t+1} \leftarrow \sum_{k=1}^{n} \frac{n_k}{n} w_{t+1}^k$
end for

The MEC nodes orchestrate the federated training process of the detection model by playing the role of parameters servers for model updates aggregation.First, the MEC server initializes the learning parameters of the detection model, including the number of layers, number of neurons, activation functions, and learning rate. These parameters are then shared with the participating CAVs. Each CAV trains the detection model on its local dataset using these parameters. Upon completion, each CAV sends its local model's parameters (weights) back to the MEC server. The MEC server aggregates these received local models using the Federated Averaging (FedAvg) algorithm [13] to generate a global learning model. This aggregated global model is then distributed back to the CAVs to initiate a new training round. The main steps performed by both the MEC server and each participating CAV, as well as the iterative training and aggregation process, are illustrated in Algorithm 1.

In our study, the federated learning problem involving multiple CAVs is formulated as a federated optimization problem. This problem is solved using the FedAvg algorithm, where each CAV calculates the average gradient of the model weights w for the current training round r using its local data. Subsequently, each CAV performs a local gradient descent on the model using its own data. Meanwhile, the MEC server aggregates these local updates to update the global model, which is then sent back to the CAVs for further training. This iterative process continues for a predefined number of rounds, initially set by the MEC server.

IV. Performance Evaluation

A. Dataset

We evaluated our system using the 5G Network-Intrusion Detection and Defense (5G-NIDD) [9] dataset. This dataset was selected for its recency, the variety of attack types it includes, and particularly because it contains real 5G traffic. Ideally, we would have preferred to use a dataset with 6G traffic, but to our knowledge, such a dataset is not yet available. The dataset includes examples of Denial of Service (DoS) attacks, such as ICMP Flood, UDP Flood, SYN Flood, HTTP Flood, and Slowrate DoS, as well as port scans, including SYN Scan, TCP Connect Scan, and UDP Scan. Following a comprehensive data preprocessing that involved cleaning, normalization, and feature engineering, the final dataset was refined to include 522,550 samples, each characterized by 81 features.

B. Experimental results

Initially, we assess the performance of the proposed detection model within a centralized training setup. Subsequently, we proceed to evaluate its accuracy in a federated training setup. To ensure a validation as realistic and closely aligned with real-world scenarios as possible, we begin by training the model on a dataset that includes only one type of attack along with benign traffic. Subsequently, we sequentially introduce samples of different attack types, each time integrating a new type. The order of the attacks' introduction is completely random. The model evaluation was based on the three metrics detailed below:

- Accuracy: $\frac{TP+TN}{TP+FN+FP+TN}$
- Recall: $\frac{TP}{TP+FN}$
- FPR (False Positive Rate): $\frac{FP}{FP+TN}$
- F1-Score: $F1\_Score = \frac{2\times TP}{2\times TP+FP+FN}$

TP, TN, FP, and FN denote true positive, true negative, false positive, and false negative, respectively.

1) Centralized training: We implemented and evaluated our proposed system within the Google Colab cloud environment, utilizing the Pytorch package to implement both local and federated learning models. The core of our system is a Multilayer Perceptron (MLP) model, intricately structured with three hidden layers. Each layer comprises 300 neurons, activated by the ReLU (Rectified Linear Unit) function. Throughout its training phase, it undergoes 1000 iterations. Additionally, we incorporated a buffer memory capable of storing up to 100 samples. This memory plays a crucial role in our implementation of CLEAR method. By preserving previously observed samples, it significantly mitigates the issue of catastrophic forgetting.

Figure 1 illustrates the performance dynamics as new types of attacks were incrementally introduced to the system. Initially, the system's handling of benign traffic and Lowrate DoS attack was exemplary, achieving 100% accuracy, a 0% FPR, and a detection rate of over 99%. Despite a slight decline in performance following the addition of UDP Flood and HTTP Flood attacks, the model successfully maintained high levels

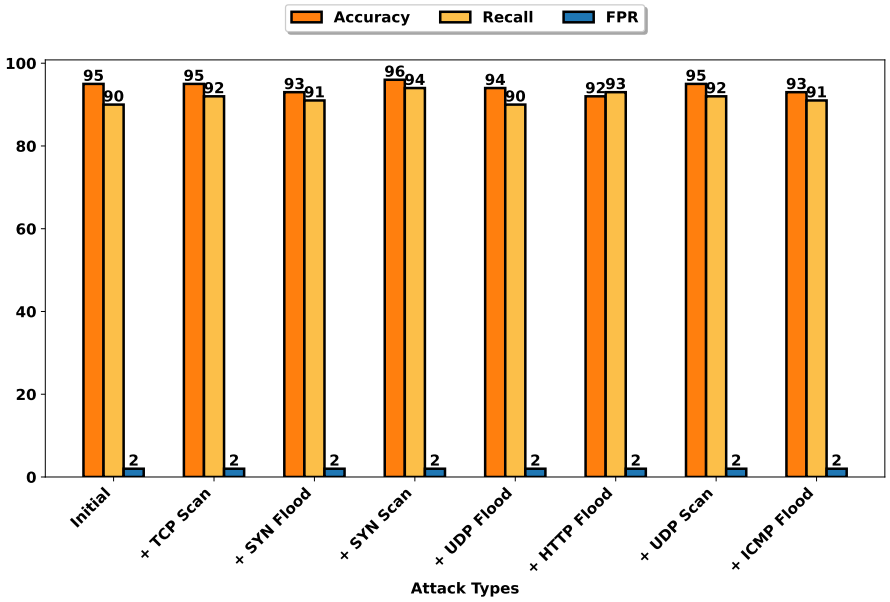
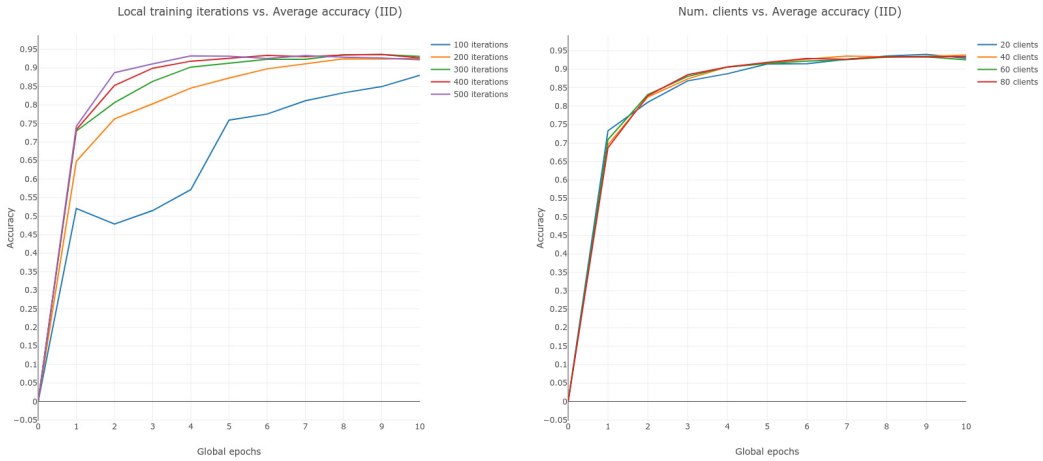


Fig. 1: Evaluation of Performance Throughout the Incremental Learning Process



(a) (b)

Fig. 2: Accuracy vs. Nb. clients & Nb. Iterations

of performance. Upon the final integration of all attack types, the detection model sustained robust performance, with both accuracy and recall exceeding 92%, while maintaining a very low FPR of 2%.

2) Federated training: In our federated training approach, we implemented an independent and identically distributed (IID) sampling setup. We followed the same testing strategy as our previous experiment, which involves both sequential and random observations of various attack types. In our initial setup, we considered 10 clients and conducted training over 10 rounds. We experimented with varying numbers of local iterations to assess the model's convergence. As shown in Figure 2a, it is evident that the model converges after 300 local iterations (across 10 FL rounds). This observation is corroborated by the swift learning rate and consistently high accuracy depicted in the plot.

For a comprehensive evaluation, we assessed the system in both binary classification (benign, malicious) and multi-class classification scenarios. In the multi-class context, we considered both Macro Recall and Weighted Recall. Macro Recall measures the average performance across all classes, treating each class equally. Weighted Recall, on the other hand, accounts for the frequency of each class, providing a more realistic evaluation in scenarios where some attacks are more prevalent than others. These metrics offer a well-rounded assessment, considering both majority and minority attacks, providing a comprehensive perspective on the model's capabilities and opportunities for improvement. As illustrated in Table I, the detection model shows very good performances with a high weighted recall of 0.931, showcasing its strong

It. locales	Multiclass Acc.	Macro Recall	Weighted Recall	Binary Acc.	Binary FPR	Binary Precision	Binary Recall	Binary F1-Score
100	0.839	0.642	0.839	0.960	0.025	0.969	0.941	0.955
200	0.919	0.854	0.919	0.980	0.014	0.983	0.973	0.978
300	0.931	0.874	0.931	0.985	0.020	0.976	0.991	0.984
400	0.926	0.875	0.926	0.980	0.031	0.964	0.993	0.978
500	0.921	0.874	0.921	0.975	0.040	0.954	0.993	0.973

TABLE I: Nb. of Local Iterations vs. Predictive performances

No. of Clients	Multiclass Acc.	Macro Recall	Weighted Recall	Binary Acc.	Binary FPR	Binary Precision	Binary Recall	Binary F1-Score
20	0.928	0.874	0.928	0.984	0.024	0.972	0.993	0.982
40	0.933	0.874	0.933	0.987	0.016	0.980	0.991	0.986
60	0.923	0.870	0.923	0.979	0.033	0.961	0.993	0.977
80	0.927	0.872	0.927	0.984	0.024	0.972	0.993	0.982

TABLE II: Nb. of Clients vs. Predictive performances

performance in identifying majority classes. While the macro recall is at 0.874, this still represents a commendable performance, especially in the context of less frequent classes.

To assess the system's scalability, we experimented with varying the numbers of FL CAVs. Figure 2b indicates strong scalability in the federated learning process. Despite increasing the number of clients per MEC node, from 20 to 80, there is no significant variance in accuracy, suggesting that the system can handle scaling horizontally—adding more clients—without a loss in performance. The quick convergence and stable high accuracy across all client configurations demonstrate the system's robustness and effectiveness in a distributed learning context. Table II demonstrates that the detection model maintains stable and high performance in both multiclass and binary classifications across varying numbers of clients. The model achieves high accuracy and precision, indicating its robustness. While the macro recall indicates a slightly lower performance in identifying less frequent attack types, the high F1-scores across all client groups suggest a well-balanced model. The consistent performance, regardless of the number of clients, affirms the model's scalability and effectiveness.

V. Conclusion

This study introduced a new adaptive Intrusion Detection System (IDS) designed for the constantly evolving Internet of Vehicles (IoV) security environment, in anticipation of the upcoming 6G technology shift. By integrating class-incremental and federated learning, which are well-suited to the IoV's distributed structure, the system achieved a detection rate exceeding 92%, while maintaining a very low false positive rate of 2%, as demonstrated in our tests using a recent dataset generated from a real test network. These results underscore the system's flexibility and represent a significant advancement in AI-driven cybersecurity for vehicular networks. Our efforts provide a foundational step towards enhancing IoV security in preparation for the new wave of cyber threats expected with 6G advancements.

Acknowledgment

This work was supported by the 5G-INSIGHT bilateral project (ID: 14891397) / (ANR-20-CE25-0015-16), funded by the Luxembourg National Research Fund (FNR), and by the French National Research Agency (ANR).

References

[1] Diana Pamela Moya Osorio, Ijaz Ahmad, José David Vega Sánchez, Andrei Gurtov, Johan Scholliers, Matti Kutila, and Pawani Porambage. Towards 6g-enabled internet of vehicles: Security and privacy. *IEEE Open Journal of the Communications Society*, 3:82–105, 2022.

[2] Hichem Sedjelmaci, Nesrine Kaaniche, Aymen Boudguiga, and Nirwan Ansari. Secure attack detection framework for hierarchical 6g-enabled internet of vehicles. *IEEE Transactions on Vehicular Technology*, 2023.

[3] Abdelaziz Amara Korba, Abdelwahab Boualouache, Bouziane Brik, Rabah Rahal, Yacine Ghamri-Doudane, and Sidi Mohammed Senouci. Federated learning for zero-day attack detection in 5g and beyond v2x networks. In *ICC 2023 - IEEE International Conference on Communications*, pages 1137–1142, 2023.

[4] Minrui Xu, Dinh Thai Hoang, Jiawen Kang, Dusit Niyato, Qiang Yan, and Dong In Kim. Secure and reliable transfer learning framework for 6g-enabled internet of vehicles. *IEEE Wireless Communications*, 29(4):132–139, 2022.

[5] Gido M van de Ven, Tinne Tuytelaars, and Andreas S Tolias. Three types of incremental learning. *Nature Machine Intelligence*, 4(12):1185–1197, 2022.

[6] Asif Ejaz, Adnan Noor Mian, and Sanaullah Manzoor. Life-long phishing attack detection using continual learning. *Scientific Reports*, 13(1):11488, 2023.

[7] Sai Prasath, Kamalakanta Sethi, Dinesh Mohanty, Padmalochan Bera, and Subhransu Ranjan Samantaray. Analysis of continual learning models for intrusion detection system. *IEEE Access*, 10:121444–121464, 2022.

[8] David Rolnick, Arun Ahuja, Jonathan Schwarz, Timothy Lillicrap, and Gregory Wayne. Experience replay for continual learning. *Advances in Neural Information Processing Systems*, 32, 2019.

[9] Sehan Samarakoon, Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, Sang-Yoon Chang, Jinoh Kim, Jonghyun Kim, and Mika Ylianttila. 5g-nidd: A comprehensive network intrusion detection dataset generated over 5g wireless network. *arXiv preprint arXiv:2212.01298*, 2022.

[10] Zhixia Zhang, Yang Cao, Zhihua Cui, Wensheng Zhang, and Jinjun Chen. A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6g. *IEEE Transactions on Vehicular Technology*, 70(6):5234–5243, 2021.

[11] Preeti Rani, Chandani Sharma, Janjhyam Venkata Naga Ramesh, Sonia Verma, Rohit Sharma, Ahmed Alkhayyat, and Sachin Kumar. Federated learning-based misbehaviour detection for the 5g-enabled internet of vehicles. *IEEE Transactions on Consumer Electronics*, 2023.

[12] L Jai Vinita and V Vetriselvi. Federated learning-based misbehaviour detection on an emergency message dissemination scenario for the 6g-enabled internet of vehicles. *Ad Hoc Networks*, 144:103153, 2023.

[13] H. B. McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *AISTATS*, 2017.