Evaluating the Robustness of ADVENT on the VeReMi-Extension Dataset

Hamideh Baharlouei
Faculty of Computer Science
Dalhousie University
Halifax, NS, Canada
hm729953@dal.ca

Adetokunbo Makanju
Department of Computer Science
New York Institute of Technology - Vancouver
Vancouver, BC, Canada
amakanju@nyit.edu

Nur Zincir-Heywood
Faculty of Computer Science
Dalhousie University
Halifax, NS, Canada
zincir@cs.dal.ca

***Abstract*—In this paper, we extend and evaluate the effectiveness of ADVENT (Attack/Anomaly Detection in VANETs), a machine learning-based system designed for early attack detection and malicious node identification in Vehicular Ad Hoc Networks (VANETs). ADVENT combines machine learning with federated learning to detect the onset of attacks while preserving user privacy. The system detects and reports malicious nodes to neighboring vehicles, allowing proactive defense against attacks. We focus on its robustness against various Distributed Denial-of-Service (DDoS) attacks. Using the Vehicular Reference Misbehavior Extension (VeReMi-Extension) dataset, we assess ADVENT across five distinct types of (D)DoS attacks, each representing diverse attack characteristics. Based on our findings, we enhance ADVENT by refining its malicious node detection step through a time slicing mechanism, improving both False Positive Rate (FPR) and F1-score metrics. Our evaluation shows that ADVENT consistently excels in detecting attack onsets and identifying attackers, even under different attack types. The results emphasize its adaptability and effectiveness in strengthening VANET security.**

***Index Terms*—VANET, (D)DoS,Malicious Node detection, Attack Onset Detection, Robustness, Machine Learning, Federated Learning.**

I. Introduction

Despite advancements in malicious behavior systems tailored for Vehicular Ad Hoc Networks (VANETs), there persists a crucial need to evaluate their robustness against diverse attack scenarios. Evaluating the performance of malicious behavior detection systems against different types of attacks is imperative for identifying vulnerabilities and enhancing the overall security posture of VANETs. In the literature, the Vehicular Reference Misbehavior Extension (VeReMi-Extension) dataset dataset serves as a comprehensive repository for assessing the effectiveness of malicious behavior detection systems in mitigating various types of (D)DoS attacks [10]. In our previous work [6], ADVENT (Attack/Anomaly Detection in VANETs) has been proposed and successfully tested against DoS attacks in various settings, i.e., different traffic conditions, road layouts, and attacker density etc. ADVENT uses a Machine Learning (ML)-based approach, in particular Federated Learning (FL), for malicious behavior detection. The results in [6] show ADVENT achieving an average F1-score of 99.66% in detecting when an attack commences i.e., Attack Onset detection and subsequently an average F1-score of approximately 97.85% in identifying the malicious actors (vehicles) i.e., Malicious Node detection.

While those results are promising, this paper introduces an update to our Malicious Node detection component aimed at effectively managing the False Positive Rate (FPR) and improving the F1-Score. Additionally, we provide further evaluations of ADVENT that demonstrate its robustness and effectiveness in detecting any type of distributed attack that affects the frequency of packet reception at each node. To this end, we employ the VeReMi-Extension dataset. The types of (D)DoS attacks in the VeReMi-Extension dataset include DoS, DoS Random, DoS Random Sybil, DoS Disruptive, and DoS Disruptive Sybil attacks. These attack types represent a wide range of mechanisms that might be used by an attacker to improve the effectiveness of the DoS attack or evade detection. Showing that ADVENT can also detect these attack types will demonstrate its effectiveness in countering different attack vectors and the robustness of the proposed system. In doing so, we aim to identify areas for enhancements and propose further improvements to strengthen misbehavior detection mechanisms in VANETs. In summary, apart from the results of the new evaluations with the VeReMi-extension dataset, this paper introduces a novel enhancement to ADVENT: We have enhanced our method to calculate thresholds for detecting malicious node behavior more effectively. This improvement allows us to manage normal traffic from long-time neighbors effectively, resulting in an increased F1-Score and decreased False Positive Rate (FPR). By ”long-time neighbors,” we refer to vehicles that have similar trajectories and thus spend a longer time than average close to each other while in the simulation. This results in them sending and receiving more packets from each other than usual.

The rest of this paper is organized as follows. Section II summarizes the related work. Section III introduces the methodology. Section IV details the evaluations and results. Finally, conclusions are drawn, and the future work is discussed in Section V.

II. Related Work

This section provides an overview of existing research efforts and contributions in the field of VANET security

978-3-903176-66-9 ©2024 IFIP

mechanisms and attack detection techniques, particularly those utilizing the VeReMi-Extension dataset for their evaluations.

Attar et al. [3] provide a comparative analysis of several ML algorithms for detecting DDoS attacks in connected vehicle environments using the VeReMi-Extension dataset. The algorithms were assessed based on detection accuracy and execution time. The results indicate that XGBoost is the most effective ML algorithm, followed by Random Forest and SVM. The study specifically focuses on differentiating normal Cooperative Awareness Messages (CAM) from flooding CAM attacks in a Vehicle-to-Infrastructure (V2I) setting. However, they focus on attack detection without addressing malicious node detection, the onset of attacks, or data privacy aspects.

Hasan et al. [8] propose a scheme that includes fuzzy logic-based factors and a novel data-centric parameter for enhanced trust computation accuracy in VANETs. Their scheme captures all malicious vehicle behaviors and effectively handles content tampering attacks. An inter-edge transfer mechanism ensures seamless trust evaluation when vehicles switch between edge servers, improving overall VANET performance. Validated through simulations using OMNet++ their method simulates a freeway VANET environment with vehicles and edge servers. Evaluations using the VeReMi dataset and its extension show their scheme detects 36% more malicious vehicles in DoS attacks, compared to existing methods.

Asensio-Garriga et al. [2] address security challenges in V2X environments using beyond-5G networks and multi-access edge computing. They utilized the VeReMi-extension dataset for evaluations, achieving F1 scores of 99.06% for DoS attacks, 97.97% for DoS Disruptive attacks, 92.56% for DoS Disruptive Sybil attacks, 99.77% for DoS Random attacks, and 94.46% for DoS Random Sybil attacks. While this provides a framework for detecting DDoS attacks targeting V2X services, they do not address the onset of attacks, detection of malicious nodes or data privacy related issues.

The work of Attar et al. supports our decision to use XGBoost in ADVENT [6] for ML-based attack onset detection, demonstrating its effectiveness compared to other supervised algorithms. The work of Hasan et al. [8] addresses attack onset detection and malicious node detection through different approaches. Our system, however, functions as a complete and robust solution, emphasizing real-time attack onset detection, model optimization, and a new data preprocessing method that enhances simplicity and effectiveness. In contrast to prior work, the previously proposed ADVENT system not only addresses attack detection and onset detection but also includes a component for malicious node detection, ensuring data privacy while keeping the system optimized.

These works collectively offer insights and methodologies for enhancing the security framework of VANETs for dependable and secure vehicular communications. Table I provides a comparison between our proposed system i.e., ADVENT and the prior works highlighted in this section.

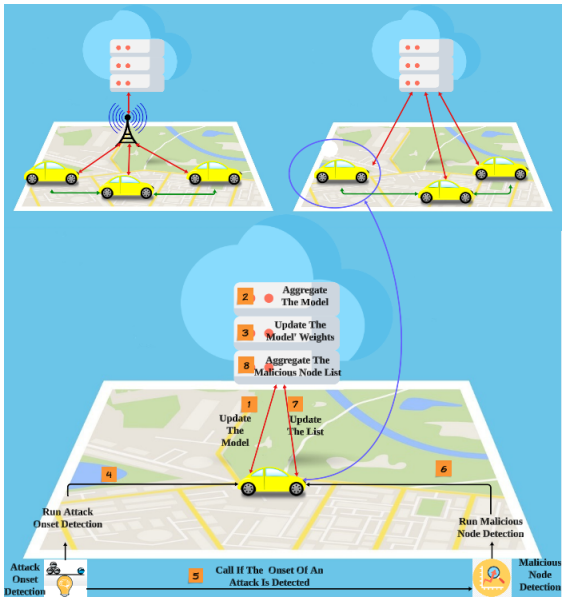

Fig. 1. Attack/Anomaly Detection in Vehicular NeTworks (ADVENT)

III. Methodology

In this section, we provide an overview of our previously proposed ADVENT system [6] and the datasets employed along with the different types of DDoS attacks evaluated in this work.

A. Overview of ADVENT

ADVENT [6] operates as a decentralized defense mechanism employing a federated learning approach for Attack Onset and Malicious Node Detection. Figure 1 offers an overview of the ADVENT system, illustrating its primary components and their interactions. ADVENT is effective both with or without Roadside Units (RSUs), and can be used in scenarios where cars communicate either with RSUs or directly with the cloud server via communication links. ADVENT provides comprehensive protection while preserving privacy [6]. Below we describe the primary components, shown in Figure 1, of ADVENT:

- **Vehicles (Nodes):** Each vehicle sends and receives packets to and from other vehicles, communicates with RSUs (if applicable), and interacts with the cloud server to update the model for attack onset detection. Vehicles also receive the final list for malicious nodes from the cloud server. For this study, we assume the vehicles are trustworthy, and verifying the trustworthiness of nodes is beyond the scope of this work.
- **Cloud Server:** The cloud server is the central component responsible for aggregating the models received from the vehicles. It updates the model weights and sends the updated models back to the vehicles, ensuring all vehicles use the same model for attack onset detection. After an attack is detected by any vehicle, it sends its list of nodes suspected to be involved in the attack to the cloud server

TABLE I
COMPARATIVE ANALYSIS OF RECENT ATTACK DETECTION WORKS ON VANETS

Paper Authors	VD	AD	DOA	MND	FE	SL	FL	DP	AM	OT	ID
Asensio-Garriga et al. [2]	*	*									
Attar et al. [3]	*	*				*					
Hasan et al. [8]	*	*	*	*	*				*	*	
ADVENT [6]	*	*	*	*	*	*	*	*	*	*	*

VD - VANET Dataset, AD - Attack Detection, DOA - Detecting the Onset of Attacks, MND - Malicious Node Detection, FE - Feature Engineering, SL - Supervised Learning, FL - Federated Learning, DP - Data Privacy, AM - Aggregation Method, OT - Optimization Techniques, ID - Imbalanced Data Handling

that aggregates these lists into one final list to share with all vehicles.

- **Communication Links:** Communication links are used for data transfer between vehicles and a central server, using technologies like cellular networks, low Earth orbit satellites, or radio communications depending on the situation. The system's adaptability to different communication methods ensures it can function in various environments. Since no sensitive data that could be reconstructed by attackers is shared, conventional communication security measures are deemed sufficient for protection.
- **Attack Onset Detection:** This component is an early warning system to flag suspicious activity enabling ADVENT to identify potential threats in near real-time,also it can be extended to handle DOS attacks carried out with short bursts of attack traffic.
- **Malicious Node Detection:** Upon flagging suspicious activity, ADVENT swiftly pinpoints potential malevolent vehicles (nodes) lurking within the network. Through a meticulous evaluation of individual vehicle behavior against pre-established benchmarks, it identifies anomalies and designates them as Malicious Nodes.
- **Federated Learning and Adaptation:** The ADVENT system utilizes federated learning for both attack onset and malicious node detection processes. The aggregation required for federated learning is carried out on the cloud server and enables the adaptation of vehicles to the changes in the VANETs.
- **Time Slicing Method:** This paper introduces a novel Time Slicing method within the ADVENT framework. The method is added to enhance the detection of malicious nodes by analyzing network behavior over discrete time intervals. Algorithm 1 describes the Time Slicing algorithm. The central idea is to monitor each node within these time slices and aggregate the results to make a final determination on whether a node should be classified as malicious.

ADVENT system underwent evaluations in [5], utilizing 24 simulated datasets [4] featuring varying ratios of one type of (D)DoS attack across four distinct city maps. The results of the evaluations showed ADVENT achieving an F1-score of 99.66% in attack onset detection and subsequently identifying malicious vehicles with an average F1-score of approximately 97.85%. These results are promising. Nonetheless, in this paper, we evaluate the robustness of ADVENT using the

Algorithm 1 Time-Slicing-Based Malicious Node Detection

Input:
    Nodes: List of network nodes
    Time Interval (T): 120 seconds (2 minutes)
    Slice Duration (x): 2 seconds
    Threshold (y): # Suspicious detections required to mark a node as malicious
    Detection Function: As described in Section III-A
Output:
    Malicious_Nodes: List of detected malicious nodes
Initialize:
    Suspicious_Counts[N] = 0
    Malicious_Nodes = []
Begin:
for *time_slice* in range(0, 120, 2) **do**
  for *each node* in *Nodes* **do**
    Status = Detection_Function(*node*, *time_slice*)
    if *Status* == "Suspicious" **then**
      Suspicious_Counts[node] += 1
      if *Suspicious_Counts[node]* $>y$ **then**
        if *node* not in *Malicious_Nodes* **then**
          Malicious_Nodes.append(node)
        end if
      end if
    end if
  end for
end for
Return *Malicious_Nodes*

VeReMi-Extension datasets which enables us to compare it to the state-of-the-art from the literature with a spectrum of (D)DoS attacks.

B. VeReMi-Extension Dataset

The dataset utilized in this work i.e., VeReMi-Extension dataset, is generated using the Framework For Misbehavior Detection (F2MD) [9]. F2MD is an extension of VEINS [1]. VEINS is an open-source simulator for Inter-Vehicular Communication based on OMNeT++ and SUMO [11], [13]. In these datasets, the simulation scenarios are set in Luxembourg City, with a subsection of the LuST network (Luxembourg SUMO Traffic), covering an area of 1.61 km² and a peak density of 67.4 Veh/km². Sensor error models are incorporated into the datasets to render the data more realistic, including position, velocity, acceleration, and heading errors. The VeReMi-

Extension dataset comprises 39 publicly available subsets that capture various types of misbehavior during rush hour and low traffic periods, along with a complete test bench for simulating an entire day. Based on Luxembourg network simulations with a 30% attacker penetration rate, these datasets can be replicated or expanded using the open-source F2MD tool on GitHub. We have also tested the ADVENT with different portions of attackers in our previous papers [5], [6].

Each type of attack, including DDoS, Data Replay, Disruptive attacks, Eventual Stop, and Traffic Congestion Sybil, is simulated at different times of day, resulting in two subsets for each attack type: one for rush hour (7-9 AM) and one for low traffic (2-4 PM), labeled with the suffixes 0709 and 1416, respectively. These datasets are publicly available.

- **(D)DoS** These attacks flood VANETs with messages exceeding permissible frequency limits set by IEEE or ETSI, causing network congestion and disrupting critical communications, which can compromise road safety and traffic management.
- **(D)DoS Disruptive** Malicious vehicles flood the network by replaying data from random neighbors, obstructing genuine message broadcasts and complicating the differentiation between legitimate and malicious communications.
- **(D)DoS Disruptive Sybil** These attacks combine disruptive DoS tactics with Sybil deception, where attackers replay data from neighboring vehicles while frequently changing identities. This dual approach overwhelms the network with fake messages, making detection and mitigation difficult, thus threatening VANET security and reliability.
- **(D)DoS Random** A variant of DoS attacks where malicious vehicles send messages with random values to disrupt VANET operations. In Sybil mode, attackers constantly change identities, further complicating the identification of malicious activity.
- **(D)DoS Random Sybil** These attacks mix random flooding with Sybil tactics, where attackers send random messages while changing identities to evade detection. This dual strategy exploits VANET vulnerabilities, posing a significant threat to network reliability and security.

While all of the above are (D)DoS attacks, they exhibit distinct characteristics and behaviors, making it essential to test each type comprehensively with the ADVENT system. This ensures a thorough assessment of its robustness and effectiveness in safeguarding VANETs against various threats.

IV. Evaluations and Results

In this section, the results of the evaluations focusing on Attack Onset detection and Malicious Node detection using ADVENT across various DDoS attack scenarios in the VeReMi-Extension datasets are presented. In this context, four key metrics are utilized to assess the performance of the system: Detection Rate (DR), False Positive Rate (FPR), False Negative Rate (FNR) and F1-score. These metrics are widely recognized in the evaluation of ML models. To provide clarity, each metric serves a distinct purpose: DR measures the proportion of true positive instances correctly identified, FPR quantifies the proportion of false alarms, FNR evaluates the rate of false negatives, i.e., missed attacks, and the F1-score offers a balanced assessment of precision (positive predictive value) and recall (Sensitivity or True Positive Rate). The calculation of these metrics involves specific formulas, where True Positive (TP), True Negative (TN), False Negative (FN), and False Positive (FP) denote various classification outcomes. By employing these metrics, we ensure a comprehensive evaluation of the effectiveness of ADVENT.

$$DR = \frac{TP}{TP + FN} \tag{1}$$

$$FPR = \frac{FP}{FP + TN} \tag{2}$$

$$FNR = \frac{FN}{TP + FN} \tag{3}$$

$$F1 - score = \frac{2 \times TP}{2 \times TP + FP + FN} \tag{4}$$

A. Attack Onset Detection

This section discusses results from two different scenarios. The first scenario, Centralized Training (CT-AOD), presents results where the ML model is on a centralized server on the cloud and all vehicles send all their data to this model for attack detection purposes. In CT-AOD, 70% of each dataset was used to train the detection model, while the remaining 30% was used to test the system on a per-vehicle basis. In the second scenario, to respect the privacy of the vehicles, their raw data are not shared with other nodes or the server. Instead, FL-AOD allows each vehicle to train its model locally, then to share the model parameters with the cloud server. The server aggregates these parameters to create a global model, which is then distributed back to the vehicles. In this case, both the training and testing occur locally, but using FedXGBllr [12], the cloud server optimizes the final model for ensuring privacy while maintaining efficiency. FeXGBllr is a version of XGBoost that incorporates Federated Learning. Both the CT-AOD and FL-AOD methods represent viable options for ADVENT's Attack Onset detection. Both approaches were evaluated in our prior evaluations of ADVENT [6] and are used again for our evaluations in this work.

Figure 2 presents the detection rate for both the CT-AOD and FL-AOD approaches. The results demonstrate that while ADVENT enhances privacy using FL-AOD, its performance is still comparable to the centralized approach, CT-AOD. ADVENT achieves this without requiring all the data of all the vehicles, whereas the CT-AOD requires all the data from all the vehicles. Additionally, these results highlight the consistency of ADVENT in detecting the onset of all attack types studied in this research. This also shows that utilizing data balancing techniques significantly improves efficiency.

Figure 3 presents the F1-score results for all the attacks in the VeReMi-Extension datasets. Similar to the detection

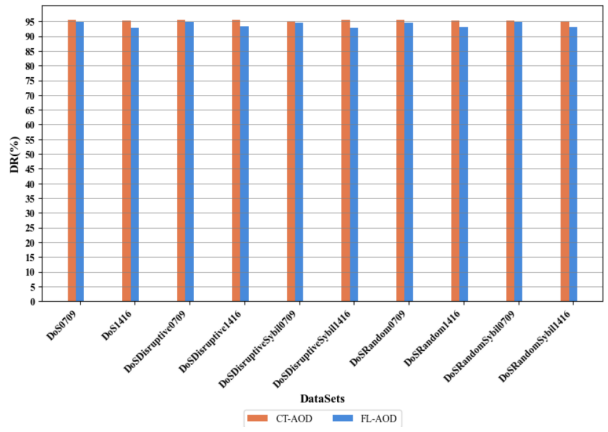

Fig. 2. Attack Onset Detection: Detection Rate

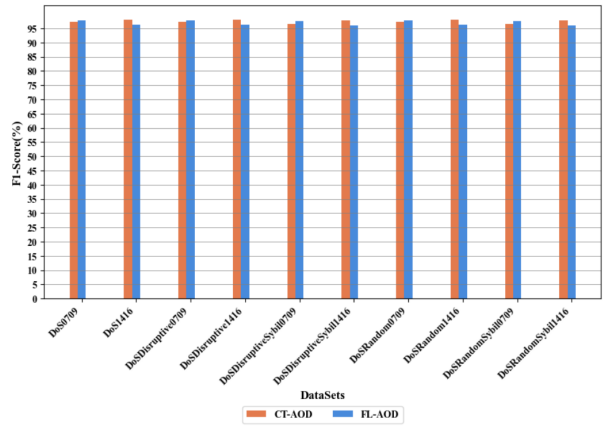

Fig. 3. Attack Onset Detection: F1-Score

rate (DR) results, the F1-score results demonstrate consistency, showcasing the effectiveness and robustness of the ADVENT system across different types of attacks evaluated. This consistency highlights ADVENT system's ability to effectively and robustly detect and mitigate various attack types, further emphasizing its robustness in securing VANETs.

Table II presents the False Positive Rate (FPR) and False Negative Rate (FNR) for different attacks. The results demonstrate a consistent performance across all attacks, with the FPR for the FL-AOD being lower than that of the CT-AOD. This indicates that the FL-AOD approach not only enhances privacy but also reduces false positive rate more effectively compared to the CT-AOD.

However, the results reveal an average of 1.5% higher FNR for the FL-AOD system compared to the CT-AOD system. This outcome is expected, as the FL-AOD models are trained on local data rather than the entire dataset used by the CT-AOD approach. In our prior work [6], we addressed the high FNR caused by local training using Synthetic Minority Oversampling Technique (SMOTE) [7]. By employing SMOTE to balance the data, we successfully reduced the FNR from an average of 2.41% to 0.35% in the datasets.

Although we balance the dataset locally, this seems to indicate a trade-off between enhanced privacy and FNR. Future research will analyze this phenomenon in more detail.

TABLE II
ATTACK ONSET DETECTION: (FNR AND FPR)

ID	Attack	CT FNR	FL FNR	CT FPR	FL FPR
1	DoS0709	4.51	5.10	2.54	1.39
1	DoS1416	4.57	6.98	1.41	0.76
2	DoSDis0709	4.47	5.15	2.61	1.48
2	DoSDis1416	4.26	6.58	1.41	0.78
3	DoSSyb0709	4.86	5.46	3.48	1.63
3	DoSSyb1416	4.42	6.98	2.08	0.95
4	DoSRan0709	4.32	5.36	2.71	1.46
4	DoSRan1416	4.73	6.83	1.41	0.82
5	DoSRanSyb07	4.77	5.19	3.47	1.62
5	DoSRanSyb14	4.97	6.96	1.94	0.88

B. Malicious Node Detection

In this section, we perform malicious node detection evaluations using two approaches: Node-Based, and Federated Learning Technique (FLT) Based. In the Node-Based approach, we employ the Malicious Node identification method on each node to detect malicious nodes (vehicles). On the other hand, in the FLT-Based approach, we aggregate the results from each node to create a global malicious node list on the cloud server. As with the Attack Onset evaluations, both the Node-Based and FLT-Based approaches represent possible approaches that can be used by ADVENT for Malicious Node Detection and were evaluated in our prior evaluations of ADVENT [6]. They are used again for our evaluations in this work. We tested the FLT-Based approach, each evaluation is called using FLT-X-Y, with X and Y as previously discussed in III-A. In previous work [4]–[6] a time slice concept was not included in the ADVENT system; instead, a threshold was calculated based on all packets received in the last two minutes, once an attack onset was detected. It's important to note that each node could respond differently upon detecting an attack onset. Some nodes might block traffic temporarily before identifying the malicious nodes, allowing them to mitigate potential issues during this 2 minutes detection period.

In this paper, we compare our new time-slicing approach with the FLT-0-2 method, which indicates no time slicing is used, as presented in [4]–[6]. We introduce FLT-2-2, FLT-2-5 and FLT-2-7, where the two-minute interval is divided into 2-second slices to calculate the threshold in each slice. In this case, if a node is detected as malicious in two time slices, its ID is added to the malicious node list, culminating in the final list. This proposed method prevents the misidentification of normal neighboring vehicles traveling on the same road, who might be sending a large number of messages over a prolonged period, as malicious nodes.

Employing the concept of time slices enables ADVENT to identify malicious behavior more accurately. In short, when a car detects the onset of an attack, it initiates the malicious node detection method based on the number of connections received from each node in the last two minutes. This two-minute interval is divided into 2-second slices. The car repeats

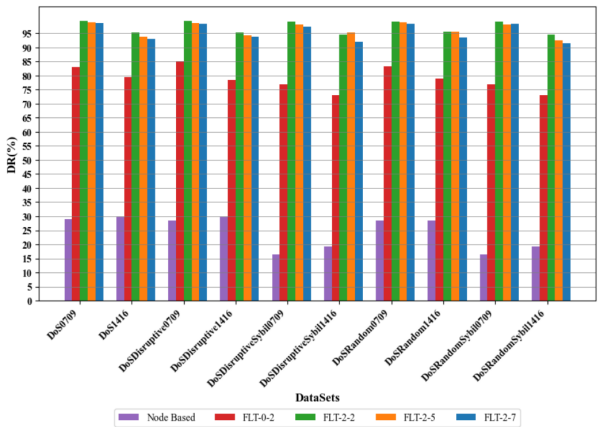

Fig. 4. Malicious Node Detection: Detection Rate

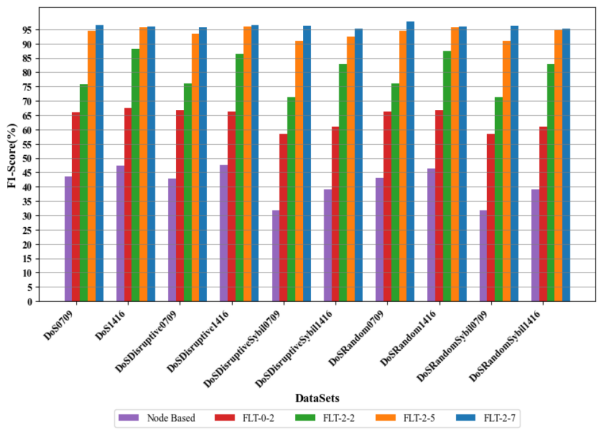

Fig. 5. Malicious Node Detection: F1-Score

the detection process for each slice and compiles a list of suspected malicious nodes, which contains the ID of malicious nodes and the number of times they are detected as malicious. Then, it applies the threshold 2, filtering out all the nodes reported less than 2 times as malicious to create the final list. This threshold can be adjusted based on the network conditions and parameters. However, we set it to 2, as it represents the minimum number of reports required to classify a node as malicious. At the end of this process, the car shares its compiled list with the server. The server aggregates the lists received from all nodes using the value of parameter Y, and adds the nodes reported by more than Y nodes to its list. It then reports this final aggregated list back to the vehicles. Vehicles can then use this list to identify and respond to malicious nodes.

Please note that we assume all nodes reporting to the cloud server are reliable. Verifying the trustworthiness of each node is beyond the scope of this paper.

Figure 4 demonstrates that using thresholds contribute to sustained high detection rates, indicating the effectiveness of continuous monitoring in identifying malicious nodes. Also, this highlights the efficacy of a higher threshold in maintaining consistently high detection rates.

Figure 5 illustrates different levels of efficacy among distinct detection techniques and thresholds. Notably, FLT-2-7 (where X=2 and Y=7) consistently achieves the highest F1-Score surpassing other methods across various iterations. This implies that increasing the threshold for number of reports for each suspected node enhances the capability to effectively identify malicious nodes.

Figure 6 underscores the critical role of the chosen detection method and the duration of the detection interval in effectively mitigating malicious activities within the network. Specifically, increasing the threshold (Y) used for number of reports received for each suspected node demonstrates a marked enhancement in the system's ability to identify and address potential threats.

Figure 7 shows the importance of selecting appropriate detection methods and optimizing detection parameters (X and Y) to effectively identify and mitigate malicious activities within the network. Increasing the Y factor raises the risk of losing detection of malicious nodes that are attacking fewer neighbors.

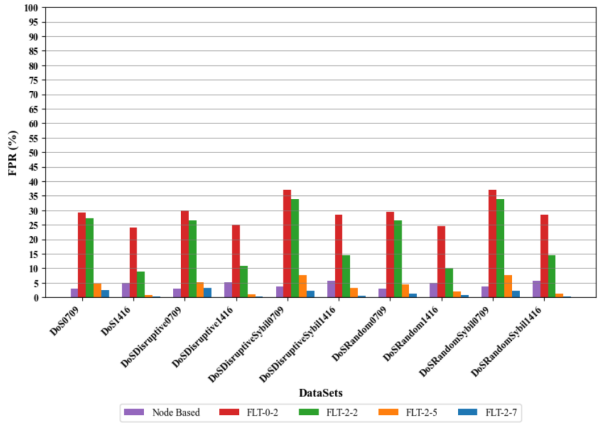

Fig. 6. Malicious Node Detection: False Positive Rate

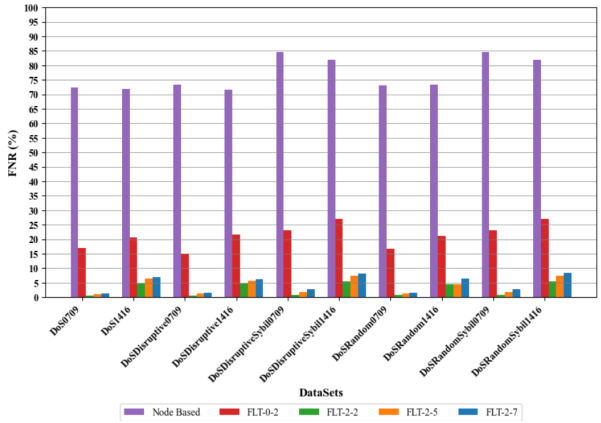

Fig. 7. Malicious Node Detection: False Negative Rate

TABLE III
ADVENT RESULTS IN CONTRAST WITH ASENSIO-GARRIGA ET AL. [2]

Attacks	[2]	ADVENT(07-09)	ADVENT(14-16)
DoS	99.06%	96.59%	96.03%
Disruptive	97.97%	95.7%	96.45%
Disruptive Sybil	92.56%	96.2%	95.3%
Random	99.77%	97.84%	95.85%
Random Sybil	94.46%	96.2%	95.28%

V. CONCLUSION

In conclusion, the comprehensive evaluations conducted in this paper demonstrate the robustness and efficacy of ADVENT in countering a range of (D)DoS attacks prevalent in VANETs. By leveraging a combination of sophisticated detection mechanisms and strategic server thresholds, ADVENT proves to be highly effective in identifying and mitigating malicious nodes within the network. Specifically, when employing malicious node detection at 2 seconds time slices and utilizing the number of vehicle reporting thresholds set at 2, 5, and 7 in the server, ADVENT exhibits consistent and robust performance across different types of (D)DoS attacks.

These findings highlight the significance of the timely and accurate detection ADVENT provides in fortifying VANETs against evolving security threats. By promptly identifying and isolating malicious nodes, ADVENT contributes to the overall robustness and security of vehicular communication networks, thereby enhancing road safety and security in dynamic and unpredictable environments.

Overall, the findings of this research show the role an advanced detection system like ADVENT can have in safeguarding VANETs against potential disruptions and vulnerabilities. Through its effective and robust performance and adaptive capabilities, ADVENT emerges as a promising solution for enhancing the security posture of vehicular communication networks and ensuring secure exchange of critical information among vehicles and infrastructure components. Table III compares the results of ADVENT with those of Asensio-Garriga et al. While Asensio-Garriga et al. did not clearly specify whether their results pertain to rush hour times (07:00-09:00) with higher traffic and more messages or to low traffic times (14:00-16:00) with fewer vehicles and less message transfer, we compare their results with our evaluations. Our evaluations demonstrate that the proposed ADVENT system is robust, effectively detecting both DoS family attacks and Sybil attacks. Additionally, ADVENT performs well during both rush hour and normal traffic times. It is also pertinent to mention that unlike ADVENT, the work of Asensio-Garriga et al. does not address detecting the onset of attacks, data privacy, or malicious node detection. Based on our evaluations of ADVENT to date, it has proven capable of detecting different kinds of (D)DoS attacks. This demonstrates that ADVENT can identify attacks with different characteristics.

We believe we can generalize that ADVENT's attack onset detection step is capable of identifying any VANET attack that is distributed in nature and that affects the frequency of packet reception at each node. Following this, the malicious node detection step should effectively identify the malicious nodes. In future research, we aim to explore this assumption by testing the efficacy of ADVENT in detecting other VANET attacks that posses these characteristics and are not necessarily (D)DoS attacks. Such evaluations, if successful, will further confirm the effectiveness of ADVENT in diverse scenarios. Additionally, our future endeavors will focus on refining the ADVENT system for model updates, prioritizing simplicity and efficiency to maintain optimal performance.

ACKNOWLEDGMENT

This research is made possible through the support of the Mitacs funding program. The research is conducted at the Dalhousie Network Information Management and Security (NIMS) Lab and the Cybersecurity Lab at New York Institute of Technology in Vancouver, Canada.

REFERENCES

[1] "Instant Veins Virtual Machine ". http://veins.car2x.org/, accessed:Dec. 2021.

[2] Rodrigo Asensio-Garriga, Pol Alemany, Alejandro Zarca, Roshan Sedar, Charalampos Kalalas, Jordi Ortiz, Ricard Vilalta, Raúl Muñoz, and Antonio Skarmeta. Zsm-based e2e security slice management for ddos attack protection in mec-enabled v2x environments. *IEEE Open Journal of Vehicular Technology*, PP:1–12, 01 2024.

[3] Ali EL Attar, Ayoub Wehby, Fadlallah Chbib, Hassane Aissaoui Mehrez, Ahmad Fadlallah, Joel Hachem, and Rida Khatoun. Analysis of machine learning algorithms for ddos attack detection in connected cars environment. In *2023 Eighth International Conference On Mobile And Secure Services (MobiSecServ)*, volume CFP23RAC-ART, pages 1–7, 2023.

[4] Hamideh Baharlouei, Adetokunbo Makanju, and Nur Zincir-Heywood. Exploring realistic vanet simulations for anomaly detection of ddos attacks. In *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, pages 1–7, 2022.

[5] Hamideh Baharlouei, Adetokunbo Makanju, and Nur Zincir-Heywood. Exploring real-time malicious behaviour detection in vanets. In *Proceedings of the Int'l ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, DIVANet '23, page 1–8, New York, NY, USA, 2023. Association for Computing Machinery.

[6] Hamideh Baharlouei, Adetokunbo Makanju, and Nur Zincir-Heywood. Advent: Attack/anomaly detection in vanets, 2024.

[7] Nitesh V Chawla, Kevin W Bowyer, Lawrence O Hall, and W Philip Kegelmeyer. Smote: Synthetic minority over-sampling technique. *Journal of artificial intelligence research*, 16:321–357, 2002.

[8] Md. Mahmudul Hasan, Mosarrat Jahan, and Shaily Kabir. A trust model for edge-driven vehicular ad hoc networks using fuzzy logic. *IEEE Transactions on Intelligent Transportation Systems*, 24(12):14037–14050, 2023.

[9] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. Ben Jemaa, and P. Urien. Simulation framework for misbehavior detection in vehicular networks. *IEEE Transactions on Vehicular Technology*, 2020.

[10] Joseph Kamel, Michael Wolf, Rens W. van der Hei, Arnaud Kaiser, Pascal Urien, and Frank Kargl. Veremi extension: A dataset for comparable evaluation of misbehavior detection in vanets. In *2020 IEEE International Conference on Communications (ICC)*, pages 1–6, 2020.

[11] Pablo Alvarez Lopez, Michael Behrisch, Laura Bieker-Walz, Jakob Erdmann, Yun-Pang Flötteröd, Robert Hilbrich, Leonhard Lücken, Johannes Rummel, Peter Wagner, and Evamarie Wießner. Microscopic traffic simulation using sumo. In *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, 2018.

[12] Chenyang Ma, Xinchi Qiu, Daniel Beutel, and Nicholas Lane. Gradient-less federated gradient boosting tree with learnable learning rates. In *Proceedings of the 3rd Workshop on Machine Learning and Systems*, EuroMLSys '23, page 56–63, NY, USA, 2023. Association for Computing Machinery.

[13] Andras Varga. *OMNeT++*, pages 35–59. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.