International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Optimal Attack or Malicious Activity Detection in VANET Using Ensemble Machine Learning Approach

[1]Raghunath M. Kawale, [2]Dr. Ritesh V. Patil, [3]Dr. Surendra A. Mahajan

Submitted: 03/12/2023 **Revised**: 15/01/2024 **Accepted**: 26/01/2024

Abstract: In a Vehicular Ad-Hoc Network (VANET), a large number of moving and stationary automobiles form a wireless network. It's a cheap and straightforward way to get data on traffic and cars to command centers. VANET employs a set of protocols to safely transmit data and connect vehicle nodes to the internet. It's not uncommon for VANETs to make use of the Ad-hoc on-demand Distance Vector Protocol (AODV). It is a machine language paradigm that requires minimal processing time and memory. OBUs on vehicles carry out the necessary protocols and procedures for sending messages between vehicles, while RSUs are the fixed links that allow vehicles to communicate with one another. When multiple vehicles transmit data on a single vehicle at the same time, some of the data may be garbled or lost. However, the nodes' roles shiftregularly, making routing difficult when a vehicle's software or hardware fails. New attack detection in VANET is developed to address the aforementioned problems. At first, we compiled the information from several online resources. Data cleansing is the process of scrubbing information of duplicates or irrelevant details. By contrasting the results of the developed machine learning-based attack detection in VANET with those of previously established methods and algorithms, we can verify the effectiveness of the latter.

Keywords: *Malicious Activity Detection, Vehicular Ad-Hoc Network, Ensemble Machine Learning Model.*

1. Introduction

In a Vehicular Ad-Hoc Network (VANET) [9], for example, automobiles connect to one another by Road Side Units (RSUs) and On-Board Units (OBUs), making it a type of Mobile Ad Hoc Network (MANET). The Onboard Bus Unit (OBU) implements communication protocols and techniques in cars, allowing them to communicate with one other through predetermined routes or other locations connected to roadways (RSU) [10]. Roadside units (RSUs) are secure infrastructure pieces that have communication tools installed so they can receive data from automobiles. More specifically, RSU can be installed at intersections, on roadside barriers, or at traffic lights [11]. The foundation of an Intelligent Transportation System (ITS) is any vehicle that can start and stop communicating depending on the information that has to be exchanged [12]. With the advancement of ITS communication technology, VANET is a concept in its early stages of development. An essential component of smart city infrastructure, VANET integration with mobile apps is delivering web apps over the internet while simultaneously increasing bandwidth and decreasing latency [13]. Vehicles participate in data analysis using cloud computing by acting as nodes and contributing computing power [14]. In addition, VANET provides a range of cloud services, including as computation and storage, from the vehicles' locations, which helps to minimize backbone network congestion and delay [15]. Hence, VANET opens doors to capitalizing on big data for a range of smart city uses, including infotainment, real-time traffic monitoring, and surveillance [16]. At the same time, since VANET connections necessitate engagement and cooperation between cars and other cloud entities, this makes them attractive targets for attackers.

1.1 VANET has a distributed

It is the responsibility of the infrastructure to ensure that all security parameters are properly managed while data is exchanged between the dispersed nodes in the vehicular network. VANET security characteristics such as authentication, integrity, and availability are susceptible to numerous attacks, such as Distributed Denial-of-Service (DDoS), Sybil Attack (SA), Man-In-The-Middle (MITM), and jellyfish attacks [17]. To make the ad hoc vehicular system more secure and efficient, it is necessary to provide a way to detect and block all of these harmful attacks in the network, taking into account all of the dangers in the VANET [18]. Every year, DDoS assaults take new forms and target different resources, such as system resources, network bandwidth, and others. That being said, the primary danger to system availability is a distributed denial of service attack [19]. Developing a scalable, dependable, and strong network intrusion detection system to effectively combat distributed

[1]*Research Scholar, SKNCOE Vadgaon (Bk.), Pune.*
raghunathkawale22@gmail.com
[2]*Principal, PDEA's College of Engineering Manjari (Bk.), Pune.*
rvpatil3475@yahoo.com
[3]*Associate Professor,*
PVGCOET & GKPIOM,Pune.
sa_mahajan@yahoo.com

denial of service assaults is crucial for ensuring the high availability of virtual area networks (VANETs).

As technologies like the cloud, the IoT, and AI continue to advance, cybercriminals will be able to conduct massive DDoS attacks with relative ease and cheap cost. Data denial of service (DDoS) assaults is harder to identify and counter. Additionally, DDoS network traffic often resembles regular network traffic. Finding a way to distinguish DDoS attacks from the deluge of network traffic is, thus, an extremely difficult and intricate task [20]. There have been reports of AI techniques like Genetic Algorithm (GA), Artificial Neural Network (ANN), and Fuzzy Sets (FS) being employed to identify malicious attacks on networks. They include ANN as one of their spokespeople [21]. One benefit of employing ANN algorithms for unsupervised learning is its potential to detect DDoS assault packets pretty effectively. But when data is big and network structure is complicated, these kinds of solutions won't scale well. When training, over-fitting is easy to do [22]. In order to identify intrusions, numerous conventional machine learning (ML) methods have been used, such as Decision Tree (DT), Support Vector Machine (SVM), Naïve Bayes (NB), and many more. Their detection performance, though, is heavily dependent on features [23]. Traditional Network Intrusion Detection Systems (NIDS) are unable to handle the data processing demands of DDoS attack detection due to the rise of big data technologies, which allow governments, businesses, and academic communities to tap into massive amounts of digital data [24]. A lot of research in recent years has concentrated on using big data frameworks for DDoS attack detection and defense. To meet the data processing needs of DDoS attack detection in the cloud, studies combine big data technology with ML technology [25]. However, Current research has numerous issues, such as detecting system performance limitations, system stability and scalability, and processing enormous amounts of data.

2. Related works

For the purpose of VANET attack categorization, Kaur and Kakkar [1] created a Deep Maxout Network (DMN) in 2022 using hybrid optimization. A custom-built hybrid optimization technique was used to select and route Cluster Heads (CH). In order to carry out an efficient classification process, the feature selection procedure was more crucial. Furthermore, an optimization approach was implemented to teach DMN how to classify attacks. Improved accuracy, recall, energy efficiency, and trust in routing were all outcomes of the optimization-based DMN model's development.

An updated machine learning approach for intrusion detection systems (IDSs) was suggested by Bangui et al. [2] in 2022. It makes use of Random Forest (RF) and coreset-based posterior detection to boost detection efficiency and accuracy. When compared to traditional machine learning methods, the experimental findings reveal that the suggested model considerably improves detection accuracy.

A deep learning-centered intrusion detection system (IDS) using CMEHA-DNN to identify SA in VANET was proposed by Velayudhan et al. [3] in 2022. Cluster Formation (CF), CH selection, attack detection, and VANET security are the four pillars of the suggested method. As a first step, the vehicles are clustered using the MKHM algorithm. In the next step, the Floyd-Warshall Algorithm (FWA) chose the cluster's CH item. After the CH was chosen, the malicious CH was located using the deep learning model CMEHA-DNN by obtaining the relevant parameters of the CH. Finally, after identification, with a normal CH, the data contained within it was securely transferred to the cloud using the MD5-ECC. In comparison to previous approaches, the presented study achieves a higher level of accuracy.

Alsarhan et al. [4] used SVM to detect intrusions in VANET in 2023. Some of the many computational benefits of SVM's structure include the irrelevance between algorithm complexity and sample dimension and its specific direction at a finite sample. The VANET intrusion detection challenge was combinatorial and nonconvex. The accuracy value of the SVM classifier was therefore optimized using three intelligence optimization strategies. Ant Colony Optimization (ACO), GA, and PSO are all examples of optimization methods. Based on their findings, GA is clearly the superior optimization algorithm.

3. Problem Definition

Network security is compromised by malicious assaults. There must be a system in place to detect and stop these cybersecurity breaches. Attack classification information is often lost in most deep learning-based detection methods, which in turn lengthens the time it takes to identify attacks. The current assaults or malicious activities based on machine learning are listed in Table 1. recognized in VANET, as well as the characteristics and difficulties associated with them. Even when there are more

vehicles, DMN [1] still uses less computing time. Misconduct within the network can be mitigated with its help. However, the price tag is steep. When used to massive amounts of vehicle data, RF [2] effectively identifies malicious activity. With its help, real-time attack detection becomes more precise. However, it demands more resources and processing capacity, as well as more time for training. By integrating the vehicles, DNN [3] strengthens the network. Encrypting the data stored in the nodes requires less time. More data is needed to do the analysis, and it is still difficult to understand the results. The space dimension difficulties can be solved and the network's robustness can be increased with the help of SVM [4]. The problem is that it struggles when trained using actual huge data derived from vehicle communication. Reducing misclassification results and facilitating efficient data transfer without protocols are two uses for convolutional neural networks (CNNs) [5]. However, with a limited dataset, performance becomes complicated and generalizability suffers. Data may be efficiently sent without protocols using CNN [6]. The results of misclassification are decreased. However, due to inaccuracies in the raw data, the forecast findings were inaccurate.

Table 1: Features and challenges of existing machine learning-based attack or maliciousactivity detection in VANET

Author [citation]	Methodology	Features	Challenges
Kaur and Kakkar [1]	DMN	The computation time is less even in more number of vehicles. It is used to reduce the misconduct behaviours inside the network.	Cost requirement is high.
Bangui *et al.* [2]	RF	It efficiently detects the malicious activity in large amount of vehicular data. It provides better accuracy in real-time attack detection.	It requires more training time. It needs more resources and computational powers.
Velayudhan *et al.* [3]	DNN	It is used to improve the stability of the network by connecting the vehicles. It takes less time to encrypt the node data.	It is complex to interpret the results. More number of data is required to perform.
Alsarhan *et al.* [4]	SVM	It is used to rectify the space dimension problems. It is used to increase the robust of the network.	It does not perform well on real big data collected from vehicular communication for training.

4. Research Methodology

An affordable and simple solution for intelligent traffic management and failure protection measures is the Vehicular Ad-Hoc Network (VANET) paradigm. While VANET nodes do not often rely on routing protocols for performance, they do make use of broadcast protocols to efficiently transmit safety information. An aggressive vehicle may intentionally transmit malicious packets in an attempt to cause harm, leading to the aforementioned misbehavior. In addition, unexpected misbehavior might happen as a result of software or hardware failures in vehicles, which is caused by the dynamic behavior of nodes in VANET and routing issues. We will create new attack detection in VANET to fix the aforementioned problems. [6] The data will first be collected from various online sources. Data cleaning will be carried out to remove any superfluous elements from the data. The normalization approach will be used to organize the data. Using Improved Green Anaconda Optimization (IGAO) [26], the best weighted features will be chosen from this data set. The newly created ensemble machine learning-based method will be used to detect attacks. Merging the Multi-Layer Perceptron (MLP), Support Vector Machine (SVM), Adaboost, and Bayesian network will create it. The next step is to categories the various VANET attacks using the fuzzy ranking algorithm. Last but not least, we will compare the created machine learning-based attack detection in VANET to existing methodologies and algorithms to validate its performance. Figure 1 shows an architectural illustration of the proposed VANET attack detection system that uses machine learning.

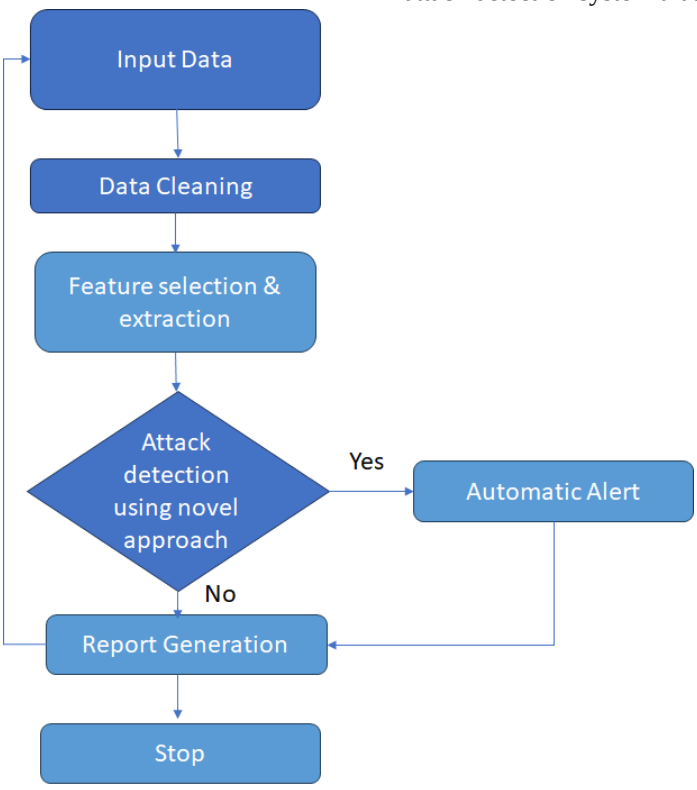

Fig 1: Architectural representation of proposed machine learning-based attackdetection in VANET

5. Result:

An ensemble machine-learning model in Python has been used to detect malicious behaviour in VANETs using the described technique. The execution was carried out by contrasting the final results with several conventional algorithms and methodologies.

The implemented model was run with a maximum of 50 iterations, a chromosomal length of 10, and a population size of 10. The experimental results were compared with the detection of malicious activity in VANET using a variety of algorithms and techniques.

Evaluation of the confusion matrix

Fig. 2 illustrates the study of the confusion matrix, which is used to determine the effectiveness of the approach based malicious activity detection in VANET. Using anticipated and real values in the confusion matrix, the created model achieved high prediction in identifying malicious activities in VANET, according to analysis verification.

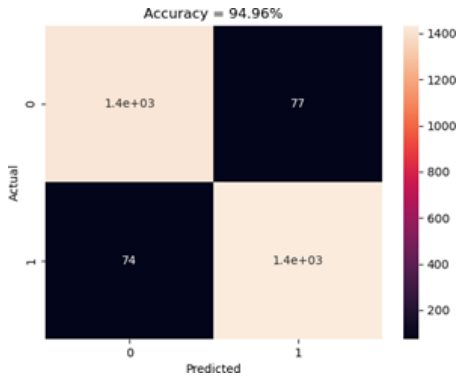

Fig 2. Confusion matrix study utilizing an ensemble machine learning model for thesuggested malicious activity detection in VANET

5.1 Comparison of Methods and Algorithms for Efficiency

Table II gives a detailed examination of how well various strategies and algorithms perform in comparison to the suggested model MRP-GAO-EMLM for detecting hostile activityin VANET. When compared to HHO-EMLM, DA-EMLM and the suggested Proposed harmful activity detection achieved a 10 to 11 percentage point increase in precision value. As a result, the suggested approach improves VANET's ability to detect harmful actions. Extensive results are presented for all the positive and negative measures, in contrast to the conventional algorithms.

Table 02: Comparison of Developed Malicious Activity Detection Algorithms in VAnetPerformance measures

Performance measures	HHO- MLM	DA- MLM	Proposed approach
Accuracy	86.07	90.63	94.97
Recall	85.77	90.54	94.90
Specificity	86.37	90.73	95.03
Precision	86.46	90.84	95.09
F1-Score	86.11	90.69	95.00
MCC	72.14	81.27	89.93

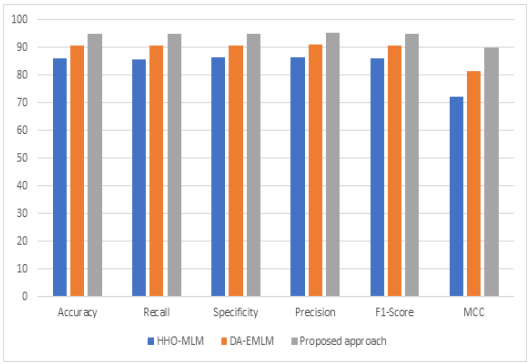

Fig 03: Comparative analysis of existing approach with proposed using some parameter

6. Conclusion:

Newly developed malicious activity detection in VANET has been implemented to detect malicious activity using an ensemble machine learning approach with a fuzzy ranking model. These proposed models improve the efficiency of communication between the vehicles. The raw data are collected from online sources and applied to the data cleaning process. The approach was used to optimize the weights and select the features to maximize the variances and correlation function. The optimized weighted features were given to the classification stage, where four classifiers were used. Finally, the outputs from four different classifiers were ensemble using a fuzzy-based ranking method. Resultant outcomes were compared with various techniques and algorithms to verify the attack detection performance of the proposed scheme.

References

[1] Gurjot Kaur and Deepti Kakkar, "Hybrid optimization enabled trust- based secure routing with deep learning- based attack detection in VANET," Ad Hoc Networks, vol.136, pp.102961, November 2022.

[2] Hind Bangui, Mouzhi Ge and Barbora Buhnova, "A hybrid machine learning model for intrusion detection in VANET," Computing, vol.104, pp.503– 531, 2022.

[3] Velayudhan, N.C., Anitha, A. and Madanan, "Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC," Journal of Ambient Intelligence and Humanized Computing, vol.14, pp.1297–1309, 2023.

[4] Ayoub Alsarhan, Mohammad Alauthman, Esra'a Alshdaifat, Abdel- Rahman Al- Ghuwairi and Ahmed Al- Dubai, "Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks," Journal of Ambient Intelligenceand Humanized Computing, vol.14, pp.6113–6122, 2023.

[5] J. Bhuvana, Hina Hashmi, Rachit Adhvaryu, Sneha Kashyap, Savita Kumari and Durgesh Wadhwa, "Intelligent analytics algorithms in breach detection systems for securing VANETs and data for smart transportation management, Soft Computing, 2023.

[6] Erfan A. Shams, Ahmet Rizaner and Ali Hakan Ulusoy, "Flow-based intrusion detection system in Vehicular Ad hoc Network using context-aware feature extraction," Vehicular Communications, vol.41, pp.100585, June 2023.

[7] Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," IEEE Access, vol. 7, pp. 154560-154571, 2019.

[8] Ankit Kumar, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh Choudhary, V.D. Ambeth Kumar, B.K. Panigrahi and Kalyana C. Veluvolu, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," Microprocessors and Microsystems, vol.80, pp.103352, February 2021.

[9] Manoj kumar Pulligilla and C. Vanmathi, "An authentication approach in SDN- VANET architecture with Rider-Sea Lion optimized neural network for intrusion detection," Internet of Things, vol.22, pp.100723, July 2023.

[10] B.A. Tosunoglu and C. Kocak, "feature selection for clustering and classification based attack detection systems in vehicular ad-hoc networks," Microprocessors and Microsystems, pp.104808, February 2023.

[11] Yantao Yu, Xin Zeng, Xiaoping Xue and Jingxiao Ma, "LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection," IEEE Transactions on Intelligent Transportation Systems, vol. 23, pp. 23906-23918, December 2022.

[12] T. Zhou, R. R. Choudhury, P. Ning and K. Chakrabarty, "P2DAP — Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 29, pp. 582-594, March 2011.

[13] Nie L, Li YK and Kong Xiangjie, "Spatio-temporal network traffic estimation and anomaly detection based on convolutional neural network in vehicular ad-hoc networks," IEEE Access, vol.6, pp.40168–40176, 2018.

[14] Sedjelmaci H and Senouci SM, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," Computers Electrical Engineering, vol.43, pp.33– 47, 2015.

[15] Omar Abdel Wahab, Azzam Mourad, Hadi Otrok and Jamal Bentahar, "SVM-based intelligent detection model for clustered vehicular ad hoc networks," vol.50, pp.40–54, 2016.

[16] David A. Schmidt, Mohammad S. Khan, Brian T. Bennett, "Spline-based intrusion detection for VANET utilizing knot flow classification," Internet technology letters," vol.3, June 2020.

[17] Xiaoyun Liu, Gongjun Yan, Danda B Rawat and Shugang Deng, "Data Mining Intrusion Detection in Vehicular Ad Hoc Network,"IEICE Transactions on Information and Systems, vol.7, pp.1719-1726, July 2014.

[18] Rupareliya J, Vithlani S and Gohel C, "Securing VANET by preventing attacker node using watchdog and Bayesian network theory," Procedia computer science, vol.79, pp.649–656,

2016.

[19] Hasan MAM, Nasser M, Pal B and Ahmad S, "Support vector machine and random forest modeling for intrusion detection system (IDS)," Journal of Intelligent Learning Systems and Applications, Vol.6 February 2014.

[20] Sonali D.Patil, Atul B.Kathole, Savita Kumbhare, Kapil Vhatkar, Vinod V. Kimbahune,"A Blockchain-Based Approach to Ensuring the Security of Electronic Data", International Journal ofINTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING, IJISAE, 2024, 12(11s), 649–655.

[21] Atul Kathole, Dinesh Chaudhari "Secure Hybrid Approach for Sharing Data Securely in VANET", Proceeding of International Conference on Computational Science and Applications pp 217–221, © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[22] Atul Kathole, Dinesh Chaudhari "Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach", Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021) pp 447–457 © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[23] Atul Kathole , Dinesh Chaudhari "Securing the Adhoc Network Data Using Hybrid Malicious Node Detection Approach", Proceedings of the International Conference on Intelligent Vision and Computing (ICIVC 2021) pp 447–457 © 2022 The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd.

[24] Mohammad Dehghani, PavelTrojovský and Om Parkash Malik, "Green Anaconda Optimization: A New Bio-Inspired Metaheuristic Algorithm for Solving Optimization Problems," Biomimetics, vol.8, March 2023.