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

A Comparative Analysis of a Novel Security Framework for Misbehaviour Detection in Vehicular Ad Hoc Networks

Ila Naqvi*[1], Alka Chaudhary[2], Anil Kumar[3]

Submitted: 27/12/2023 **Revised**: 03/02/2024 **Accepted**: 11/02/2024

Abstract: This research introduces a novel Security Framework for Misbehaviour Detection (SFMD) in Vehicular Ad Hoc Networks (VANETs) and presents a comparative analysis of the proposed framework. Leveraging a hybrid approach with Genetic Algorithms (GAs) and Deep Learning (DL), SFMD addresses the critical need for robust security in VANETs. The novelty in this research study is the use of Genetic Algorithms in misbehaviour detection in VANETs. Traditionally, the complexity of defining a suitable fitness function for GAs in this context has deterred their application. However, SFMD overcomes this challenge by introducing an innovative solution: employing an Artificial Neural Network (ANN) as the fitness function for GAs. This paradigm shift opens new avenues for efficient and effective feature selection, marking the first instance in VANET research where GA plays a pivotal role in misbehaviour detection. The synergy between these two cutting-edge approaches, coupled with the integration of contextual data and the utilization of an ANN-based fitness function in GA, equips SFMD to address the unique challenges posed by VANETs, where rapid decision-making and adaptability are paramount. By integrating contextual data, including vehicle positions, speed, and communication patterns, SFMD utilizes GAs for feature selection and DL for real-time misbehaviour detection. The 10- fold CV used enabled the whole system to be unbiased, achieving precision, recall, and F1 scores of 0.9999 in binary classification and 0.9976, 0.9977, and 0.9977 in multiclass classification respectively. Comparative analysis with recent works underscores SFMD's superiority, highlighting its potential to enhance the security landscape of VANETs. The study emphasizes the importance of context awareness, paving the way for future real-world validations and large-scale experiments. Future research can explore SFMD's practicality in diverse VANET scenarios, validating its effectiveness. However, limitations include the dependence on simulated datasets and the need for real-world deployment to uncover potential challenges.

Keywords: *Artificial Neural Network, Genetic Algorithm, Hybrid Detection, Misbehavior Detection, Security in VANETs, Vehicular ad hoc Networks*

1. Introduction

The Vehicular Ad-Hoc Network (VANET), a subset of Mobile Ad-Hoc Network (MANET), facilitates communication between vehicles (V2V) and between vehicles and infrastructure (V2I) [1]. The implementation of high-definition mapping, intelligent transportation apps, and autonomous and coordinated driving have all been made possible by VANETs because of the advances in the field of telecommunications [2]. Simultaneously, VANETs exhibit distinctive features like highly dynamic topology, decentralized networking, and self-organization [3]. Hence the security and safety requirements in these networks are different and more complex than the traditional networks [4, 5]. Messages exchanged in vehicular communication networks, encompassing navigation, traffic safety, and event-oriented messages, are often transmitted without encryption [6]. Consequently, the open nature of VANETs exposes vulnerabilities to various attacks like false reporting, denial-of-service (DoS), and forgery, potentially leading to traffic disruptions or accidents [7–9]. Moreover, malicious nodes may exploit participants' messages and identities, posing a considerable threat to drivers. Consequently, in the context of security preservation, it becomes imperative to trace and penalize malicious vehicles in response to any misbehaviour [10, 11].

Attacks in VANET could be categorised as intravehicular or intervehicle based on the attackers' target location. Intravehicular attacks occur when the malicious activities are targeted within a specific vehicle in the network. For example, falsifying GPS data or disabling the steering or braking system of an autonomous vehicle through compromised Electronic Control Unit (ECU), is extremely dangerous [12]. Intervehicle attacks are more sophisticated than intravehicular attacks as these involve malicious activities that target the communication and interactions between multiple vehicles in the VANET. [13]. In the dynamic world of vehicular communication, vehicles, Roadside Units (RSUs), and cloud platforms exchange crucial traffic-related information to enhance the management of vehicular networks. This includes sharing data on accident notifications, traffic congestion, and road conditions. However, this interconnected system is vulnerable to misbehaviour, particularly in the form of deceptive messages originating from malicious nodes.

[1] *AIIT, Amity University, Noida, Uttar Pradesh, INDIA*
ORCID ID : 0000-0002-0887-1906
[2] *AIIT, Amity University, Noida, Uttar Pradesh, INDIA*
ORCID ID : 0000-0003-2617-3279
[3] *DIT University, Dehradun, Uttarakhand, INDIA*
ORCID ID : 0000-0003-0982-9424
** Corresponding Author Email: naqviila92@gmail.com*

These spurious messages, either unintentionally triggered by misbehaving nodes or intentionally relayed through fraudulent means, can have significant and potentially harmful consequences. The primary focus of this study is intervehicle misbehaviour, which is a growing concern.

In VANETs, technologies ensuring security aim to tackle the security concerns associated with VANETs. These technologies are broadly classified into proactive and reactive processes [14]. The proactive approach prevents potential outside attackers from accessing the system, enforcing security policies through methods such as access control mechanisms, integrity and authenticity checks (e.g., cryptographic signature verification), and Public Key Infrastructures (PKIs). PKIs issue key material and certificates only to approved vehicles and entities, establishing a trusted environment. However, if an attack originates from an insider, like injecting a false message to warn vehicles of a non-existent hazard, proactive security alone may fall short, necessitating active safety measures. The reactive security mechanism involves detection and response, addressing threats not prevented by proactive security [15], with misbehaviour detection being a prominent reactive security mechanism [16].

The landscape of VANET security has traditionally leaned on static security measures like fixed encryption algorithms and access control policies. However, with the rise of machine learning solutions for misbehaviour detection, there's a notable shift towards more dynamic and adaptive approaches. Despite these advancements, there remains a research gap in the development of comprehensive, context-aware frameworks that can seamlessly integrate context awareness, considering factors like real-time traffic conditions, communication patterns, and the dynamic positions of vehicles.

While some studies explore Deep Learning (DL) for VANET security, there is a distinct lack of research leveraging Genetic Algorithms (GAs) in the context of misbehaviour detection in VANETs. The research community has not fully explored the potential synergy between GAs and DL for optimizing feature selection and enhancing classification accuracy in this domain. This study uniquely contributes to filling this void by proposing the novel Context-Aware Security Framework for Misbehaviour Detection (SFMD), which pioneers the integration of GAs and DL. This innovative approach seeks to address the existing gap by introducing a cohesive framework that harnesses the strengths of both techniques for enhanced security in VANETs.

The core motivation behind SFMD is to create a framework that not only identifies misbehaviour but also adapts to evolving threats and changing network conditions, all while considering the rich contextual data present in VANETs. Contextual data, including vehicle positions, speed, and communication patterns, serves as a critical foundation for the framework's decision-making processes. GA is employed as a feature selection mechanism, optimizing the relevance and dimensionality of the dataset, while DL models are harnessed in the classification module for accurate and real-time misbehaviour detection. The synergy between these two cutting-edge approaches, coupled with the integration of contextual data and the utilization of an ANN-based fitness function in GA, equips SFMD to address the unique challenges posed by VANETs, where rapid decision-making and adaptability are paramount.

Section 2 of this paper presents the materials and methods used in the study including the dataset, the communication architecture and the proposed framework. Section 3 presents the results that include a comprehensive exploration of SFMD, experimental evaluation and a series of experiments that demonstrate the framework's effectiveness in detecting misbehaviour across a range of scenarios. Furthermore, in Section 3 we provide evidence of SFMD's superiority over traditional machine learning models and existing misbehaviour detection methods, underscoring the critical role of context-awareness and the ANN-based fitness function in VANET security. The conclusion of the paper is provided in Section 4.

2. Material and Methods

2.1. Dataset

For this study, the VeReMi Extension dataset [17] has been used. VeReMi extension provides contextual as well as behavioural data. Features including speed, speed noise, position, and position noise are contextual features.

This dataset is available online for researchers free of cost. The VeReMi Extension dataset was created to provide an initial baseline against which detection algorithms may be evaluated and contrasted. This not only shortens the amount of time needed for researchers to carry out simulation studies of high quality, but it also makes it much simpler for the researchers to put the strategy into practice.

The dataset was produced with the help of LuST (Version 2) and VEINS. The Luxembourg traffic scenario (LuST), which was initially presented by Codeca et al. [18], was developed to provide a realistic framework for the assessment of VANET applications. F2MD has been utilized throughout the process of producing the dataset. F2MD [19] is an extension to VEINS that enables the reconstruction and detection of a wide variety of different types of misbehaviour detection use cases. OMNeT++ and SUMO are the foundations upon which VEINS, an open-source simulator for Inter-Vehicular Communication, is built. Table. 1 provides a short overview of the parameters

of the VeReMi Extension dataset. The files in the dataset are encoded in JSON.

```
{"type":ℤ[0,20],
"rcvTime":ℝ[0,+∞],
"sendTime":ℝ[0,+∞],
"sender":ℤ[0,+∞],
"senderPseudo":ℤ[0,+∞],
"messageID":ℤ[0,+∞],
"pos":[ℝ[−∞,+∞],ℝ[−∞,+∞],ℝ[−∞,+∞]],
"pos_noise":[ℝ[0,+∞],ℝ[0,+∞],ℝ[0,+∞]],
"spd":[ℝ[−∞,+∞],ℝ[−∞,+∞],ℝ[−∞,+∞]],
"spd_noise":[ℝ[0,+∞],ℝ[0,+∞],ℝ[0,+∞]],
"acl":[ℝ[−∞,+∞],ℝ[−∞,+∞],ℝ[−∞,+∞]],
"acl_noise":[ℝ[0,+∞],ℝ[0,+∞],ℝ[0,+∞]],
"hed":[ℝ[−∞,+∞],ℝ[−∞,+∞],ℝ[−∞,+∞]],
"hed_noise":[ℝ[0,+∞],ℝ[0,+∞],ℝ[0,+∞]]}
```

Fig 1: Parameters in VeReMi Extension dataset [21]

The VeReMi Extension dataset contains the message logs for each vehicle, each of which contains GPS data of the local nodes as well as BSM messages received from other nodes via DSRC, labelled as type 2 and type 3 respectively. It accomplishes two key goals: first, it acts as a baseline to evaluate the effectiveness of misbehaviour detection techniques on a city scale, and second, it helps save a significant number of computational resources.

For our experiment, some minor adjustments are made for data labelling to help with the classification. Another parameter was added named “misbehaving”: $R_{[0,1]}$, where 0 means that a particular message is from a vehicle that is normal while 1 represents the message that came from a misbehaving vehicle.

The VeReMi extension dataset is available as JSON files. The data files must be changed into a .csv format to be used in our system. The data files were converted from JSON to csv format using Gigasheet.co. We extracted 30,000 message logs from the VeReMi Extension dataset. The dataset contained 33 features that made a dimensionality of the dataset as 30000 x 33.

2.2. Communication Architecture of Proposed Framework

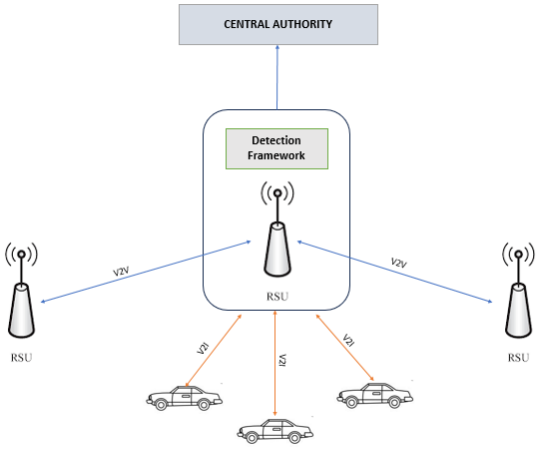

Fig 2: Communication Architecture

The communication architecture of the proposed framework for misbehaviour detection is illustrated in Figure 2. Each vehicle registers with the regional authorization party or certificate authority, which provides it with appropriate credentials for communication. BSMs (Basic Safety Messages) are periodic beacon messages that are periodically generated by authorized vehicles and digitally signed before they are broadcasted. All vehicles and RSUs within the communication range of the sender vehicle receive these BSMs. A wired backbone network connects the RSUs in the network and other infrastructure nodes. While existing methods rely on individual vehicle OBUs to detect misbehaviour, the proposed scheme deploys the detection framework at the RSUs. RSUs are configured to receive BSMs from vehicles and then combine GPS information with BSM data to identify misbehaving or attacking vehicles using the hybrid detection module. The RSU generates an alert message to inform nearby vehicles and infrastructures every time a vehicle is classified as a "misbehaving" vehicle. In response to such alert messages from RSUs, each vehicle adds this information to the OBU's local log of flagged vehicles. Afterwards, the certificate authorities and other nodes may take additional actions depending on their network policies, which are beyond the scope of this study.

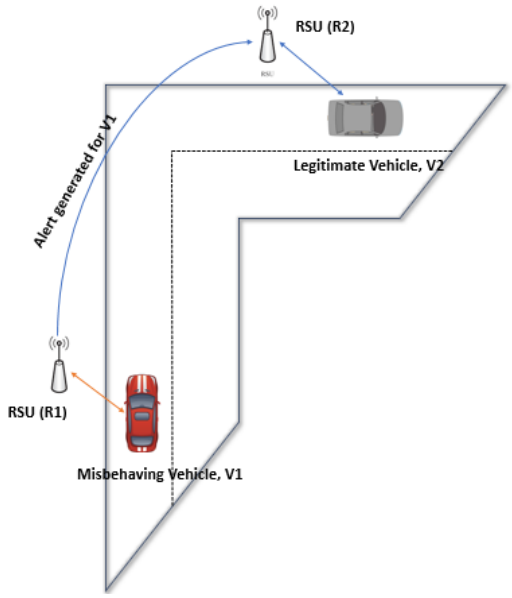

Fig 3: Alert Generation by RSU

While vehicle OBUs are more resource constrained, RSUs have more computational capabilities available for misbehaviour detection. The proposed method also has the benefit of notifying a vehicle about a potential attacker even before they get within communication range. For instance, as depicted in Fig. 3, vehicle V1 is outside of vehicle V2’s communication range. However, depending on the data R1 has received, the RSU can detect the misbehaviour and alert vehicle V2 as necessary. The RSU just needs to emit one "alert" message to neighbouring RSUs and vehicles if misbehaviour is discovered. We

assume that the nodes of the infrastructure are secure. Instead of RSUs, we focus on misbehaving vehicles because vehicles are more vulnerable to attacks than RSUs.

2.3. Proposed Misbehaviour Detection Framework

The core contribution of this study is the framework for misbehaviour detection for the VANETs. The performance efficiency and the effectiveness of the suggested security framework are both significantly impacted by the entire features that are employed by the detection system. Detection accuracy, computational time and memory requirements have been identified as the primary factors for which the reduction in the total number of features is required by the system.

The proposed framework (Fig. 4) consists of four modules which include:

- Data collection module: This module collects the behavioural data, and the contextual data from the network and sends it to the pre-processing module.
- Pre-processing Module: To obtain the initial data, the network's raw traffic is handled in a predetermined manner.
- Hybrid Detection: This module primarily consists of a hybrid model, which analyses the data, filters out the irrelevant characteristics, and reconstructs a low-dimensional feature dataset then uses supervised algorithms to categorize traffic, judge if it is being subjected to an attack, and decide whether to provide a warning in response to the findings.
- Feedback module: Using the machine's output status and alarm information, this module modifies its operations.

2.3.1.1. Context Sensing and Behavioural Data Collection

Contextual elements at times impede a vehicle's regular operations. As a result, we have devised a framework that acquires and logs contextual data that is combined with a vehicle's inherent behaviour to establish whether the vehicle is exhibiting malicious intent. A range of contextual data types hold the potential to significantly influence a vehicle's actions. These include the position coordinates, altitude, speed, status of the channel, temperature, weather conditions etc. The impact of each contextual factor on a vehicle's actions is outlined below:

- GPS coordinates and altitude, in combination, offer insight into the geographic location of mobile vehicles. This data aids in identifying instances where a vehicle might engage in misbehaviour due to its position. For instance, if a mobile vehicle moves to the far side of a hill relative to its communication peer, it might have to drop a packet due to the obstruction caused by the hill.
- Speed (velocity) denotes a vehicle's motion, and we've observed that higher speeds hinder collaborative interactions with other vehicles.
- Channel status indicates the congestion level of the transmission channel over a specific timeframe. Given that all vehicles within the radio range share this channel, increased congestion elevates the likelihood of dropped data packets.
- Temperature and wind speed are crucial in determining whether a vehicle's misbehaviour can be attributed to

  harsh weather. For instance, a mobile vehicle is more prone to malfunctions in conditions where the temperature is 20°F and wind speed is 40mph, compared to conditions of 70°F and 5mph wind.

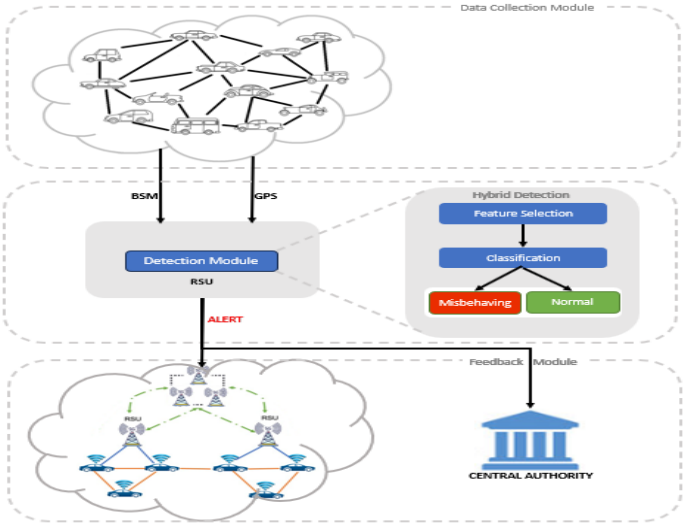

Fig 4: SFMD Framework

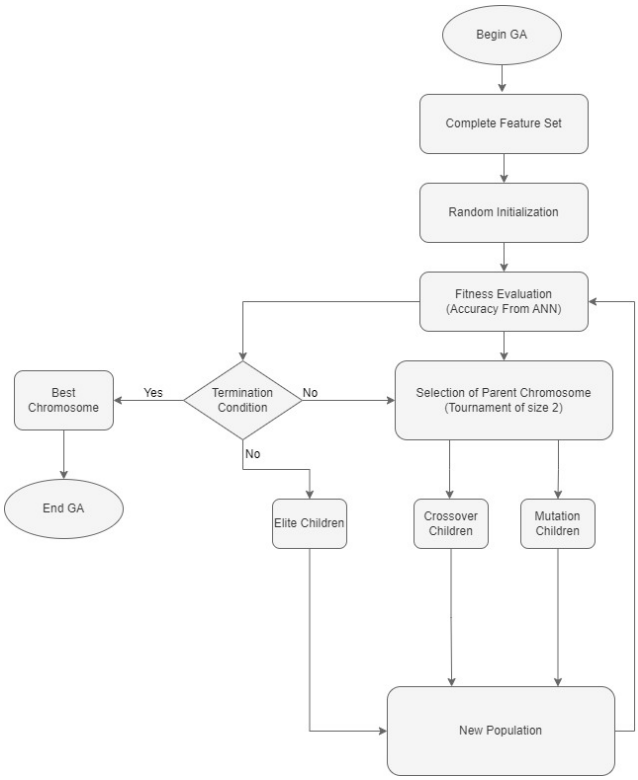

Fig 5: GA Based Feature Selection

The behavioural data collection module is responsible for the collection of vehicle behaviors through the BSM (Basic Safety Messages) that are broadcasted by the vehicles and the context sensing module collects the contextual data through GPS.

2.3.1.2. Data Pre-processing

It is required to reduce the features from high-dimensional feature sets because this may directly challenge systems for pattern recognition. In other words, having a lot of features may often lower the detection system's accuracy rate because some of them may be redundant or otherwise pointless [20]. Several combinatorial sets are required to preserve the optimal combination and achieve the highest level of accuracy.

2.3.1.3. Hybrid Detection

2.3.1.3.1 Feature Selection using ANN Fitness function-based Genetic Algorithm

Genetic algorithms (GA) are population-based and algorithmic search heuristics that imitate the process of human evolution in nature [21]. By employing the process of natural selection along with genetic functions like crossovers and mutations, GA repeatedly uses one population to produce a new population of chromosomes (In a manner like Charles Darwin's theory of evolution, which emphasizes the importance of reproduction, genetic recombination, and the survival of the fittest). In terms of human genetics, chromosomes can be compared to bit strings, genes to features, alleles to feature values, loci to bit positions, genotype to encoded strings, and phenotype to decoded genotype [22].

A function "fitness function" or "Objective function" is used to assess the fitness of the chromosomes. In other terms, the fitness function provides numeric values that are used to rank the chromosomes. Chromosomal encoding, initializing the population, measuring fitness, selecting individuals, and conditions to terminate the GA are the five key processes in the Genetic Algorithm. In a manner like how humans naturally evolve, the algorithm manipulates the finite binary population. First, an initial population is generated randomly and assessed using the fitness function.

A Feature Subset Selection is a map or an operator F_{Sub} from an x-dimensional input space to a y-dimensional output space given as:

$$F_{Sub}: R^{n \times x} \rightarrow R^{n \times y} \quad (1)$$

where $x \geq y$ and $x, y \in Z^{+}$, $R^{n \times x}$ is any dataset containing the initial feature set containing n instances or observations with x number of features and $R^{n \times y}$ is the feature set after reduction containing n observations with y features in the subset selection.

The feature selection by GA is shown in Fig. 5. In relation to the binary chromosome utilized in this study, if the gene value is '1' shows that the specific feature identified by the position of the '1' is chosen. Conversely, if the gene value is '0', the feature is not selected. The ranking is carried out

and the top 'n' most fit individuals are chosen to survive and move on to the next generation, a process known as elitism. Once the elite individuals have been transferred to the successor generation, the individuals left in the population are utilized to generate the rest of the next generations by a combination of crossover and mutation. Crossover refers to combining the genetic information from two individuals to create a new crossover offspring. On the other hand, the mutation operator perturbs the genes within each chromosome by flipping bits, with the probability of flipping determined by the mutation probability.

2.3.1.3.2 Generation of Initial Population

Initially, the population consists of a matrix with dimensions Size of Population x Genome Length, where the elements are randomly generated binary digits. The Size of Population refers to the number of chromosomes (individuals) in the population, while the Genome Length (also referred to as Chromosome Length) indicates the number of bits (genes) within every chromosome [23]

2.3.1.3.3 Fitness Evaluation

For the Genetic Algorithm (GA) to reduce the features and choose a subset, a fitness function is required, which serves as a guiding factor for the GA, to assess the discriminatory capability of each feature subset. The fitness of every chromosome within the population is evaluated using an ANN-based fitness function.

During each iteration of the GA, the individuals (subset of features) in the current population are assessed, and their fitness is determined based on the accuracy of classification obtained from the ANN. Individuals with high fitness values have a higher likelihood of surviving and being included in the next generation. The iterations of the GA aim to gradually reduce the error rate and select the individuals with the best fitness values (highest accuracy). This is accomplished by reporting the accuracy rate for each involved chromosome C, and ultimately selecting the chromosome with the highest accuracy rate as determined by Eq 2.

$$FF(C) = \frac{1}{N}\sum_{i=1}^{N} \alpha_i * 100 \qquad (2)$$

Where, α = ANN-based classification accuracy

N = Cardinality of chosen features

This function takes a chromosome C (represented by the subset of selected features) as input evaluates its fitness using a function (which includes the neural network training and evaluation) and returns the mean accuracy as the fitness value.

The mathematical structure of this equation guarantees that the Genetic Algorithm is capable of learning, minimizing errors, and selecting a reduced number of features.

2.3.1.3.4 Generation of New Children

Table 1 shows the parameters of the GA used in this study. According to Table 1, the chromosome length for the experimental dataset is 33, which corresponds to the number of features extracted from the VeReMi extension dataset. To prevent the GA from getting stuck in local optima, the maximum number of generations was set to 500. The GA follows a sequential Elitism, Crossover, and Mutation process to generate a new population.

Table 1. Parameters used in Genetic Algorithm.

Parameter	***Value***
Genome length	33
Population size	300
Number of generations	500
Mutation	Uniform Mutation
Mutation Probability	0.1
Crossover	Arithmetic Crossover
Crossover Probability	0.8
Fitness Function	ANN-Based Classification Accuracy
Selection scheme	Tournament of size 2
Elite Count	2

2.3.1.3.5 Summary of the Approach.

Here's a summary of the approach:

Genetic Algorithm (GA):

The genetic algorithm is responsible for evolving a population of solutions (feature subsets) over generations. The fitness of each solution is determined by an Artificial Neural Network (ANN) trained on the selected features.

ANN as Fitness Function:

The ANN, embedded in the fitness function, evaluates the performance of a feature subset in terms of misbehaviour detection.

The goal of the genetic algorithm is to find feature subsets that lead to high accuracy in misbehaviour detection based on the ANN's evaluation.

Misbehaviour Detection:

The ANN, trained during the fitness evaluation, implicitly serves as the classifier for misbehaviour detection. A feedforward neural network with one hidden layer containing 10 neurons was used in the study, and it was trained using the Levenberg-Marquardt algorithm [24].

The features selected by the genetic algorithm guide the ANN in making predictions related to misbehaviour. In this approach, the genetic algorithm is responsible for optimizing the features fed into the ANN, and the ANN itself is responsible for learning the patterns related to misbehaviour. An additional classifier for misbehaviour detection is not needed.

The feedback module handles the detected misbehaviours by generating an alarm and informing the authority for detected misbehaving nodes in the network.

3. Results

The proposed system employed a dataset of 30,000 records to define the normal and misbehaving vehicles in VANETs. We passed the extracted 33 features from the dataset to the Genetic algorithm for the feature reduction phase. The genetic algorithm reduced the feature space to 14 features thus reducing the dimensionality of the dataset to 30,000 x 14.

The VeReMi Extension dataset exhibits an imbalance, encompassing data on legitimate vehicles as well as attacker vehicles [25]. Recognizing that accuracy is insufficient for evaluating imbalanced datasets, we employ metrics outlined in equations (1) to (3) to assess and compare the effectiveness of the proposed framework.

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \ldots\ldots (3)$$

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \ldots\ldots (4)$$

$$F1\ Score = \frac{Precision * Recall}{Precision + Recall} \ldots\ldots (5)$$

different classes corresponding to the type of misbehaviour a node exhibits.

3.1. Comparison of different classifiers for fitness function

In this section, we compare the chosen ANN classifier with six popular classifier algorithms (Logistic Regression, Naïve Bayes, K Nearest Neighbour, Decision Tree, SVM [26], and Random Forest) and use them as fitness functions in Genetic algorithm to check if we selected correct classifier to be used as fitness function. The results are summarised in Table 2 and visually represented in Fig.6.

TABLE 2: Simulation Results

Model	Precision	Recall	F1 Score
Logistic Regression	0.925	0.846	0.883738
Naïve Bayes	0.964	0.963	0.96349974
K-Nearest Neighbour	0.965	0.958	0.96148726
Decision Tree	0.989	0.975	0.9819501
SVM	0.991	0.991	0.991
Random Forest	0.993	0.989	0.99099596
Artificial Neural Network	0.9976	0.9977	0.99765

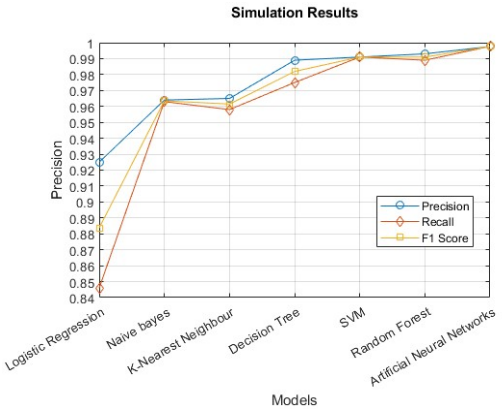

Fig 6: Simulation Results of different fitness functions

Based on the simulation results reported above, the ANN yielded the best results among all classifiers. So, ANN has been chosen to be used as a fitness function in the Genetic algorithm in our framework.

3.2. Binary Classification Results

Figures 7 and 8 show the results of the binary classification of the proposed framework. The detection accuracy of the SFMD using the binary classification method is 99.99%. Analysing the ROC shows the AUC (Area under curve) near 1which means the framework has an excellent measure of separability.

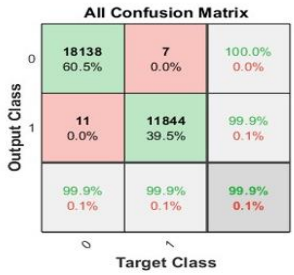

Fig 7: Confusion Matrix

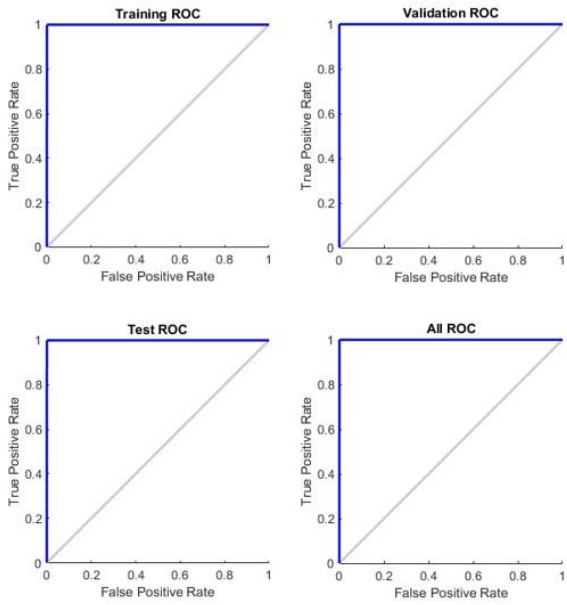

Fig 8: Receiver Operating Characteristics graph

3.3. Multiclass Classification Results

Figures 9 and 10 show the results of the multiclass classification of proposed framework. The detection accuracy of the SFMD using the multiclass classification method is 99.76%. The AUC is near to 1 which means the framework is performing excellently in terms of multiclass classification as well.

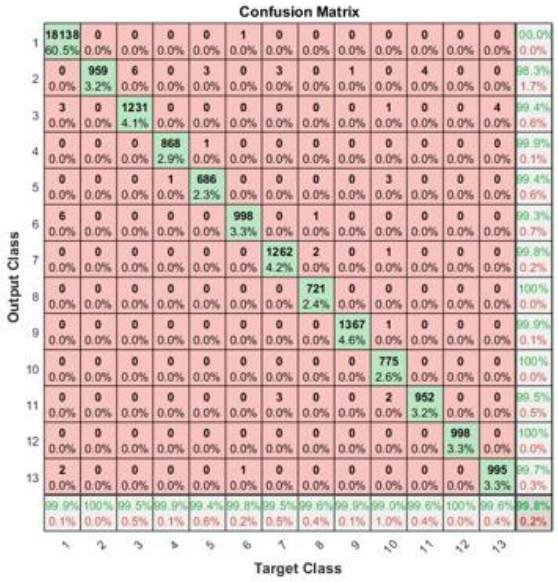

Fig 9: Confusion Matrix

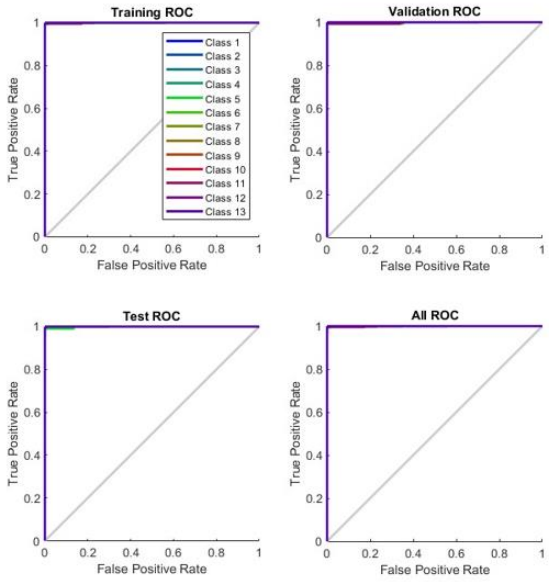

Fig 10: Receiver Operating Characteristics graph

3.4. Results with different misbehaving nodes densities

To evaluate our framework's performance under different misbehaviour node densities, we created five datasets with 10%, 20%, 30%, 40% and 50% misbehaving nodes percentage in each dataset respectively and tested the performance of SFMD. The results of the simulation have been shown in Figure 11. The results have shown that when the percentage of misbehaving nodes was only 10% of the total number of nodes, the framework showed 100% accuracy with precision, recall and F1 score all point to 1. As more and more misbehaving nodes were introduced into the dataset, there was a decrease in the precision, recall and F1 score values. However, at 50% misbehaving nodes, the framework's performance was reduced as compared to the 10% scenario, still, it has shown the precision, and F1 score as 0.9966 and recall as 0.9967.

This shows that our framework is giving excellent results even in the worst scenarios when misbehaving nodes percentage is 50% of the total nodes.

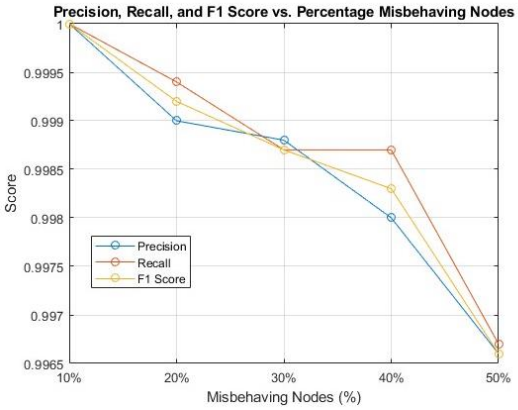

Fig 11: SFMD Results with different misbehaving nodes percentage.

3.5. Comparison with existing works

Table 3 compares the precision, recall and F1 scores obtained using the SFMD with techniques reported in some recent papers. Figure 11 presents a graphical representation of the comparison work. As clear from the results, Paper 2 [28] has shown very low precision, recall and F1 score values as compared to all other frameworks. Paper 5 [11] performed similarly to the proposed model and generated a high precision value of 0.9999 however, showed comparatively less recall value and F1 Score. The proposed model showed the best performance, compared to existing techniques, which was classified with 0.9976, 0.9977, and 0.9977 precision, recall and F1 scores respectively using multiclass classification while with binary classification the framework has shown the precision, recall and F1 scores as 0.9999 for all three metrics.

4. Conclusion

In a landscape where secure and reliable communication is essential for the success of VANETs, the proposed security framework, SFMD offers a promising avenue for advancing the state of security within these networks. We use contextual as well as behavioural data of the vehicles in the network to train the ANN classifier, and then use the trained ANN classifier as a fitness function in the Genetic Algorithm. This technique helped us to reduce features to a significantly low level and distinguish misbehaving nodes from well-behaved nodes. Experimental results show that the framework, SFMD, achieves a good performance in terms of high precision, recall and F1-score. What sets SFMD apart and renders it truly innovative is its unwavering focus on the contextual aspects of misbehaviour detection, facilitated by the utilization of an ANN-based fitness function within the Genetic Algorithm. Through this study, we aim to contribute to the ongoing efforts to secure the future of VANETs, where the right information at the right time can make all the difference. Future work can validate the proposed framework in real-world VANET scenarios to assess its practicality and effectiveness. Conducting large-scale experiments and deployment in diverse urban and suburban settings would provide valuable insights into the framework's real-world performance and potential challenges.

TABLE 3: Comparison of SFMD with existing works

Paper	Precision	Recall	F1 Score
Proposed Framework (with Binary Classification model)	0.9999	0.9999	0.9999
Proposed Framework (with Multiclass Classification model)	0.9976	0.9977	0.9977
Paper 1 [27]	0.988	0.99	0.988999
Paper 2 [28]	0.887	0.616	0.727069
Paper 3 [29]	0.978	0.932	0.954446
Paper 4 [25]	0.9886	0.8277	0.901023
Paper 5 [11]	0.9999	0.9554	0.977144

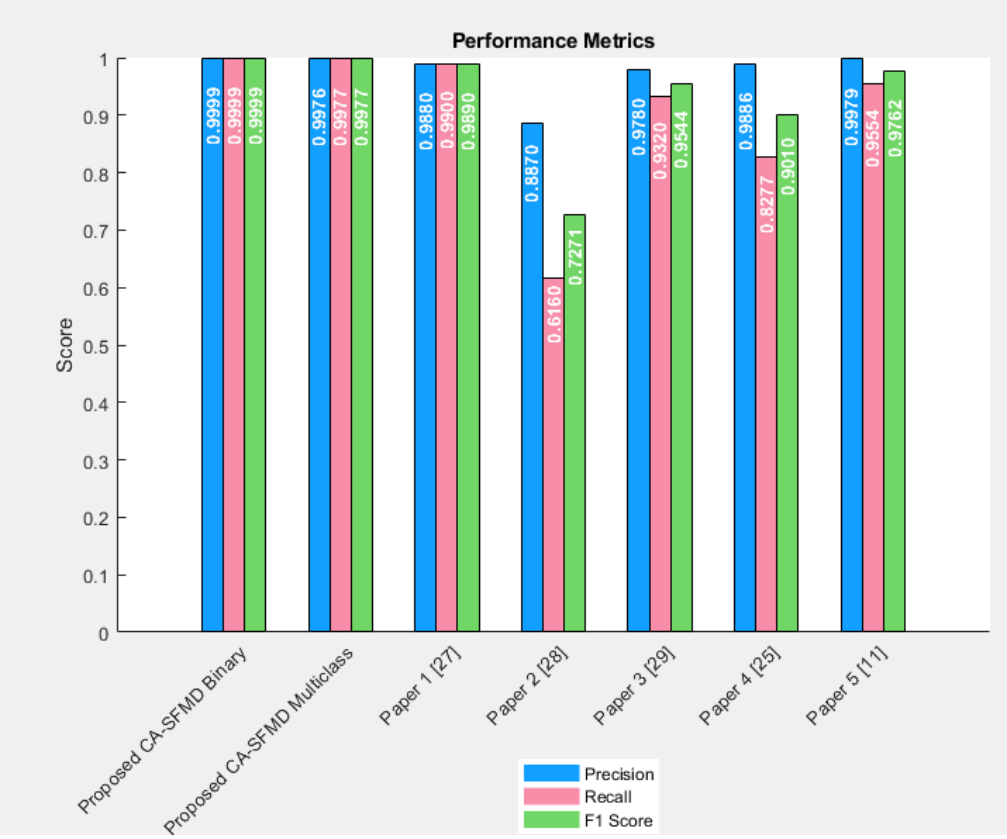

Fig 11: Comparison Chart of SFMD and other works

Acknowledgements

This research was partially supported by Gigasheet.co. We thank gigasheet.co for providing us with enterprise access to their website for converting json data to csv.

Author contributions

Ila Naqvi: Conceptualization, Methodology, Software, Implementation **Alka Chaudhary:** Data preparation, Writing-Original draft preparation, Validation **Anil Kumar:** Comparative study, Writing-Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest

References

[1] I. Naqvi, A. Chaudhary, and A. Kumar, "A Systematic Review of the Intrusion Detection Techniques in VANETS," *TEM Journal*, pp. 900–907, May 2022, doi: 10.18421/tem112-51.

[2] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, "Smart Transportation: An Overview of Technologies and Applications," Sensors, vol. 23, no. 8, p. 3880, Apr. 2023, doi: 10.3390/s23083880

[3] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, "Challenges and Solutions for Cellular Based V2X Communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 222–255, 2021, doi: 10.1109/comst.2020.3029723.

[4] D. He, S. Zeadally, B. Xu, and X. Huang, "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015, doi: 10.1109/tifs.2015.2473820.

[5] M. Clavijo-Herrera, J. Banda-Almeida, and C. Iza, "Performance Evaluation in Misbehaviour Detection Techniques for DoS Attacks in VANETs," *Proceedings of the 18th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks*, Nov. 2021, **Published**, doi: 10.1145/3479240.3488510.

[6] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, Feb. 2014, doi: 10.1109/jiot.2014.2306328.

[7] Z. Yang, K. Zhang, L. Lei, and K. Zheng, "A Novel Classifier Exploiting Mobility Behaviors for Sybil Detection in Connected Vehicle Systems," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2626–2636, Apr. 2019, doi: 10.1109/jiot.2018.2872456.

[8] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Real-Time Detection and Estimation of Denial of Service Attack in Connected Vehicle Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018, doi: 10.1109/tits.2018.2791484.

[9] M. S. Sheikh, J. Liang, and W. Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–25, Jan. 2020, doi: 10.1155/2020/5129620.

[10] X. Xu, Y. Wang, and P. Wang, "Comprehensive Review on Misbehavior Detection for Vehicular Ad Hoc Networks," *Journal of Advanced Transportation*, vol. 2022, pp. 1–27, Apr. 2022, doi: 10.1155/2022/4725805.

[11] C. Mangla, S. Rani, and N. Herencsar, "A misbehavior detection framework for cooperative intelligent transport systems," *ISA Transactions*, vol. 132, pp. 52–60, Jan. 2023, doi: 10.1016/j.isatra.2022.08.029.

[12] Sheikh, Liang, and Wang, "A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)," *Sensors*, vol. 19, no. 16, p. 3589, Aug. 2019, doi: 10.3390/s19163589.

[13] I. Naqvi, A. Chaudhary, and A. Rana, "Intrusion Detection in VANETs," *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Sep. 2021, **Published**, doi: 10.1109/icrito51393.2021.9596141.

[14]]M. Obaidat, M. Khodjaeva, J. Holst, and M. Ben Zid, "Security and Privacy Challenges in Vehicular Ad Hoc Networks," *Connected Vehicles in the Internet of Things*, pp. 223–251, 2020, doi: 10.1007/978-3-030-36167-9_9.

[15] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (CACC)," *2017 IEEE Vehicular Networking Conference (VNC)*, Nov. 2017, **Published**, doi: 10.1109/vnc.2017.8275598.

[16] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, Jun. 2015, doi: 10.1109/mcom.2015.7120028.

[17] J. Kamel, M. Wolf, R. W. van der Hei, A. Kaiser, P. Urien, and F. Kargl, "VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, Jun. 2020, **Published**, doi: 10.1109/icc40277.2020.9149132.

[18] L. Codeca, R. Frank, S. Faye, and T. Engel, "Luxembourg SUMO Traffic (LuST) Scenario: Traffic Demand Evaluation," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 2, pp. 52–63, 2017, doi: 10.1109/mits.2017.2666585.

[19] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation Framework for Misbehavior Detection in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6631–6643, Jun. 2020, doi: 10.1109/tvt.2020.2984878.

[20] A. Choudhury, "Curse Of Dimensionality And What Beginners Should Do To Overcome It," *Analytics India Magazine*, Dec. 09, 2019. https://analyticsindiamag.com/curse-of-dimensionality-and-what-beginners-should-do-to-overcome-it/

[21] Lambora, K. Gupta, and K. Chopra, "Genetic Algorithm- A Literature Review," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Feb. 2019, **Published**, doi: 10.1109/comitcon.2019.8862255.

[22] S. Mirjalili, Evolutionary Algorithms and Neural Networks. Springer, 2018.

[23] H. M and S. M.N, "A Review on Evaluation Metrics for Data Classification Evaluations," *International Journal of Data Mining & Knowledge Management Process*, vol. 5, no. 2, pp. 01–11, Mar. 2015, doi: 10.5121/ijdkp.2015.5201.

[24] J. Brownlee, "A Gentle Introduction to Imbalanced Classification," *MachineLearningMastery.com*, Jan. 14, 2020. https://machinelearningmastery.com/what-is-imbalanced-classification/

[25] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "VeReMi: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 318–337, 2018, doi: 10.1007/978-3-030-01701-9_18.

[26] I. Naqvi, A. Chaudhary, and A. Kumar, "Genetic Algorithm Optimized SVM for DoS Attack Detection in VANETs," *Lecture Notes in Electrical Engineering*, pp. 47–57, 2023, doi: 10.1007/978-981-99-5080-5_5.

[27] A. Sharma and A. Jaekel, "Machine Learning Based Misbehaviour Detection in VANET Using Consecutive BSM Approach," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1–14, 2022, doi:

10.1109/ojvt.2021.3138354.

[28] S. So, P. Sharma, and J. Petit, “Integrating Plausibility Checks and Machine Learning for Misbehavior Detection in VANET,” *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Dec. 2018, **Published**, doi: 10.1109/icmla.2018.00091.

[29] S. Gyawali, Y. Qian, and R. Q. Hu, “Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8871–8885, Aug. 2020, doi: 10.1109/tvt.2020.2996620.