International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Hybrid Approach for Detecting of Intrusion in Vanet Using Machine Learning with Optimization Approach

Ganga T G[1], Dr. Anuja Beatrice [2]

Submitted: 29/01/2024 **Revised**: 07/03/2024 **Accepted**: 15/03/2024

Abstract: In recent times, there has been a growing focus among researchers on VANET (Vehicular Ad-hoc Network) and its diverse applications, including the improvement of traffic safety through the collection and distribution of traffic event information. Malfunctions in vehicles significantly affect both human safety and road safety, underscoring the importance of addressing vehicle network security as a crucial challenge. The significance of carefully analyzing the Machine Learning (ML) methods used to improve the security aspects of intrusion detection systems (IDSs) is highlighted by this delicate research focus in VANET. This entails dealing with issues like the computational complexity of machine learning difficulties brought on by the increase in vehicle data. In order to better address the issues raised by rapid development, this research presents a hybrid machine learning approach intended to enhance the efficacy of intrusion detection systems (IDSs). This network's main goals are to improve general privacy and thwart vulnerable attacks. Support Vector Machine with Fish Swarm Optimization (SVM-FSO), a cutting-edge machine learning approach, is used in our suggested system to identify DDoS attacks and provide vehicle information while maintaining anonymity. The CICIDS 2017 IDS dataset is used for the evaluation, and MATLAB is used to implement the unique machine learning technique. When performance evaluation takes into account parameters like latency, network lifetime, throughput, delivery ratio, and drop, the results are better than with other approaches like SVM, ANN, KNN, and DNN.

***Keywords**: Intrusion Detection Systems (IDS), Support Vector Machine with Fish Swarm Optimization (SVM-FSO), ANN, KNN, and DNN.*

1. Introduction

Vehicular Ad Hoc Networks (VANETs) represent a groundbreaking paradigm in modern transportation systems, empowering vehicles to communicate seamlessly and share vital information for enhanced road safety and traffic efficiency. As the integration of communication technologies in vehicles continues to advance, so does the imperative to address the security challenges inherent in the dynamic and open nature of VANETs. This research article endeavors to delve into the critical domain of secure data dissemination within VANETs, acknowledging the necessity of safeguarding the integrity and privacy of transmitted information.

By introducing novel approaches, methodologies, and frameworks, this study aims to contribute to the development of robust solutions that fortify the security posture of VANETs, ensuring the reliability of the communication infrastructure.

The pervasive connectivity of vehicles in VANETs opens up avenues for efficient information exchange, ranging from traffic updates and road conditions to emergency notifications. However, this interconnectedness also exposes the network to potential threats such as data tampering, impersonation attacks, and unauthorized access. In this context, the introduction of cryptographic techniques emerges as a fundamental aspect of secure data dissemination. By leveraging cryptographic algorithms such as digital signatures and secure hash functions, the integrity and authenticity of transmitted data can be ensured, laying the groundwork for a secure and trustworthy communication environment.

This article embarks on an exploration of comprehensive cryptographic solutions within the VANET context to establish a resilient defense against potential security breaches. Moreover, the research recognizes the pivotal role of trust management in fostering secure communication among vehicles in VANETs. As vehicles rely on information received from other sources within the network, assessing the trustworthiness of these sources becomes paramount. Trust management mechanisms, integrated into the communication framework, enable vehicles to make informed decisions about the reliability of incoming data, mitigating the impact of malicious actors.

This introduction sets the stage for an in-depth exploration of trust-based approaches, coupled with efficient key management strategies, to enhance the security of data dissemination in VANETs. By addressing the multifaceted challenges in this dynamic environment, the research endeavors to pave the way for a safer and more secure future of intelligent transportation systems.

[1] Research Scholar, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.
Email: gangatgphd@gmail.com
[2]Associate Professor , Head, Department of Computer Applications, Sri Krishna Arts and Science College, Coimbatore.
ORCID: 0009-0005-1640-782X

The main focus of this study:

- To use machine learning in conjunction with a hybrid optimization technique to detect DDoS attacks in vehicular ad hoc networks (VANETs).
- We propose a method where network learning is achieved by employing a Support Vector Machine for intrusion detection, and the Fish Swarm Optimization (FSO) algorithm is used to optimize the SVM parameters.
- A thorough evaluation of the proposed methodology's success is provided by considering many factors, including message drop, network lifetime, delivery ratio, throughput, and message delay.

The paper is organized as follows in the sections that follow: A brief summary of privacy preservation in attack detection is provided in Section 2. The suggested hybrid detection strategy using machine learning techniques is described in Section 3. In Section 4, the experimental setup is described in detail, and the experiment findings are discussed. Concluding thoughts are provided in Section 5, outlining possible research directions for VANET security. Last but not least, Section 6 offers a synopsis of the work and suggests topics for more investigation.

2. Literature Survey

A secure message distribution system based on node trust score was proposed by Ullah et al. [1]. Based on their social utilities, vehicular nodes receive scores that are kept track of at RSU. Vehicles submit messages to RSU, and depending on the originating vehicle's trust score, RSU chooses whether to forward it or drop the message.

At RSU, trust must be constantly built and kept, since there is no safeguard against social utility fraud. With this method, capture and replay of attacks can't be stopped either. Instead of using broadcast, Due et al. [2] used forwarding on a dependable path to solve the issue of message distribution. Path dependability is computed through the application of game theory. Two significant problems with this strategy are increased processing complexity and path congestion.

Using traffic flow theory as a foundation, Liu et al. [3] developed a machine learning classifier to identify bogus messages and stop their spread within VANETs. The purpose of a Bayesian classifier is to identify the probability that an event is untrue. The method is not suitable for other events and is limited to traffic flow scenarios. In order to detect misleading messages based on occurrences from cars moving in each direction from the perspective of the source vehicle, Park et al. [4] employed a cooperative technique. Despite not requiring any infrastructure and being spread, the technology can only be used in highway circumstances.

A fake message detection approach based on machine learning was proposed by Arshad et al. [5]. The Bayesian classifier uses the witness information gathered from the incident to categorize the likelihood of the false event. However, faith in the cars supplying the witness was not taken into account in the task. A cryptographic technique was employed by Mohamed et al. [6] to authenticate messages and stop the spread of bogus messages. For key exchange from RSU to automobiles, the Diffe-Hellman protocol was employed. Prior to propagation, each communication from the vehicle is key-encrypted and validated at RSU. Since replay threats were not taken into consideration, message authentication and key exchange are highly complex processes.

The collaborative trust evaluation methodology was presented by Chen et al. [7] to confirm the message's authenticity. This approach's message validation has a higher latency because it involves numerous parties. Zhang et al. [8] dropped the message from the untrusted source and utilized the Dempster-Shafer theory to assess the message source's trustworthiness. However, this approach needs trust information to be universally available across all RSUs and only works well over time.

A trust-based message validation system for automotive networks was suggested by Asian et al. [9]. In this work, the message is classified by the application of genetic programming. The method has zero-day difficulties and only works after some time. Muhammad et al. [10] used radio signal strength (RSS) to confirm the message's authenticity. To determine whether a message is authentic, the predicted distance from RSS is compared to the message's event consistency.

The method fails against capture and replay assaults, even though it is effective against Sybil attacks. Rassam et al. [11] used a machine learning classifier to determine whether the message was genuine.

Using the K-means method, context features that are retrieved from the message and the vehicle node are clustered into two classes: real and fraudulent. There is no temporal association; just the spatial context is used. Similar to it, context information was employed by Ghaleb et al. [12] to identify bogus messages. To categorize phony communications, misbehaving context data is gathered and a Bayesian model is built. With this method, computational complexity is increased.

Using entropy change and flow sampling, Sharshembiev et al. [13] identified vehicle nodes that were acting strangely. A classifier is constructed to identify misbehaving nodes based on statistical differences in flow among misbehaving and regular activity.

Large training dataset volumes are required for the model, and outlier detection wasn't taken into account in this study. A trust management approach was presented by Guo et al. [14] to identify phony messages.

Reinforcement learning is used to continuously update the trust management strategy. We identify fake messages about road conditions. But this method has more latency. Using a rule-based methodology, Sedjelmaci et al. [15] identified fraudulent messages in VANETs. RSU has established the guidelines for identifying malicious vehicle nodes, and RSU can identify harmful vehicle nodes.

Even though the method is easy to implement, periodic rule upgrades are necessary because it is not adaptive. Zaidi et al. [16] suggested using statistics to find fraudulent messages in VANETs. Messages from attack scenarios are gathered, and behavioral characteristics are taken out of them.

It is used to create statistical rules that identify potential attack scenarios. The method is inflexible and unable to adapt to small modifications in the attack environment. In order to identify fraudulent messages in VANET, Liang et al. [17] employed a hidden generalized mixture model. On the basis of the expected future state of the vehicle's processing of bogus messages, fake messages are identified. It is discovered that there is a temporal link between the messages across time.

2. Dataset Used:

The assessment of intrusion detection was conducted using the CICIDS 2017 IDS dataset [18]. Both intrusion prevention systems (IPSs) and intrusion detection systems (IDSs) are essential security capabilities when it comes to defending against increasingly complex network threats.

This dataset of actual traffic includes the most recent and common attack scenarios, which are recreated in seven different attack families: web assault, infiltration attack, botnet, DoS attack, DDoS attack, brute force attack, and heartbleed attack. The data in the PCAP file was used to create a complete set of 80 features. 273,097 recordings were used in total for the experiment. Table 1 shows the number of records in CICIDS 2017 dataset.

Table1: Number of records in CICIDS 2017 Dataset

Type	**Label**	**Number of instances**
Normal	BENIGN	233107
DoS/DDoS Attacks	DDoS, DoS, DoS slow Loris, DoS Slow, Http test, DoS Hulk, DoS Golden Eye, Heart bleed	24 350
Botnet Attack	Bot	1560
PortScan Attack	PortScan	8000
Brute Force Attack	FTP-Patator, SSH-Patator	4000
Infiltration Attack	Infiltration	30
Web Attacks	Web Attack-Brute Force, Web Attack - XSS, Web Attack-SQL Injection	2050
Total of Instances:		273 097

4. Proposed Method:

This part developed a dynamic condition for VANET to find the best route for every node. To improve routing accuracy, information for every node was also obtained. Early DDoS attack detection was achieved by using an Ant Colony Optimization modified SVM that was security-based. Comparing the suggested method to other available methodologies, the latter showed greater accuracy in identifying vehicle information. The study proves to be the best approach for stability in automotive networks after extensive validation. It is quick and reliable in forecasting DDoS attacks.

4.1 Fish Swarm Optimization:

By mimicking their social search behaviors, artificial fish (AF) simulate the migrations of actual fish toward locations with more consistent food sources [19]. Approximately four social behaviors—prey behavior, follow behavior, swarm behavior, and jump behavior—that AF exhibits are used to analyze and clarify the issue [20].

If each artificial fish has its state represented as a vector F, then we may write $F = (f^1, f^2, \dots, f^n)$,where $f^i(i = 1,2, \dots n)$ is the fishes' optimization variable. $Y = X(F)$, where Y is the target function's value, is the expression for the food concentration at the artificial fish's current location. Step is the furthest an AF may go, whereas visual denotes the range in which AFs can seek. The distance between two AFs, denoted as and, is expressed using the Euclidean distance formula as follows:

$$D^{i,j} = \left| F^i - F^j \right| \qquad (1)$$

The crowd factor can be denoted as parameter γ $(0 < \gamma < 1)$ is a control factor to control AF tend to gather around a specific position, and the optimal position discovered by these AF will be stored or recorded. The behavior of AF can be described as:

4.1.1 Prey Behavior: This can be calculated using $F^j = F^i + visual \times r(0,1)$ (2)

This is used to find the food for the fish. F^j is the position of AF j randomly. $F^i$is the current position of $i. Y = X(F)$ is the objective function where $Y^j\ and\ Y^i$ is the food concentration by determining it with F.

If $Y^i < Y^j$, AF move forward a next position from the current position F^j by

$$F^i(m+1) = F^i(m) + \frac{F^j(m) - F^i(m)}{\|F^j(m) - F^i(m)\|} \times step \times r(0,1)$$

(3)

If $Y^i > Y^j$, whether its food consistency meets the specified criteria. else, after a certain number of attempts, the AF remains dissatisfied with the given criteria, it engages in leap behavior.

4.1.2 Swarm Behavior: Artificial fish strive to approach the central position during each iteration. The central position is determined as

$$F^c = \frac{1}{N} \sum_1^N F^i \qquad (4)$$

Where, N→ Size of the population F^c → Average of all AF population

If $Y^c > Y^i$, the center position of the population has better food and no crowd. So i advances a step toward the central position with its companion by

$$F^i(m+1) = F^i(m) + \frac{F^c - F^i(m)}{\|F^c - F^i(m)\|} \times step \times r(0,1)$$

(5)

else do 4.1.1.

4.1.2 Follow Behavior: While an artificial fish is in motion, if one or several fish discover food, the neighboring fish will promptly follow and converge on the identified position. This can be expressed using equation (3).

4.1.3 Leap Behavior: Leap behavior serves as a fundamental approach to explore food or companions across extensive ranges, effectively guarding against local optima. The artificial fish jumps, changing its settings to get out of its current place. To avoid local extreme values, it chooses a state that is within its visual range and travels toward this state. This can be expressed as

$$F^j(m+1) = F^i(m) + visual \times r(0,1) \qquad (6)$$

4.2 Support Vector Machine:

It has been established that Support Vector Machines (SVM) [21] are an effective and reliable paradigm for categorization. A crucial mathematical model that may be used for both regression and classification tasks is provided by SVM. Figure 1 shows the classification of classes using Support vector Machine with its components

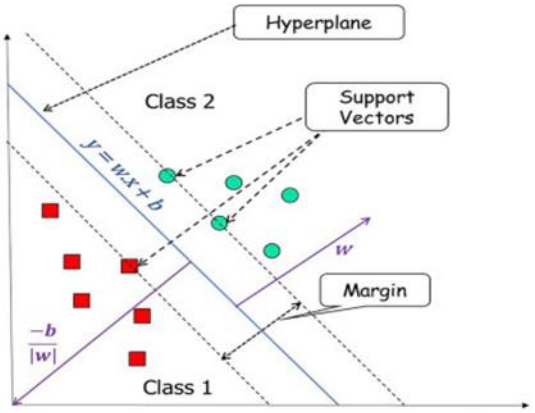

Figure 1: Components of SVM

The underlying idea of Support Vector Machines (SVMs) is that a non-linear mapping function makes a non-linear issue linearly separable in a higher-dimensional feature space. SVM does the classification by searching for a hyperplane in the feature space that separates two different kinds of data. To increase classification accuracy, SVM optimizes the distance between the closest data points of each type and the hyperplane. The support vectors were created using the original data samples, which had sufficient information to build the hyperplane. Once the support vectors have been identified, the remaining data points can be removed. With fewer initial data points, an SVM can thus attain excellent classification accuracy.

4.3 Proposed Algorithm: SVM with the FSO

The primary objective of this algorithm is to mitigate vulnerable attacks and enhance the privacy of the VANET. Support Vector Machine (SVM), K-nearest neighbor (KNN), Artificial Neural Networks (ANN), Deep Neural Networks (DNN), and Bayesian Networks (BN) are employed for comparison with the proposed SVM with Fish Swarm Optimization (FSO) in the context of privacy preservation.

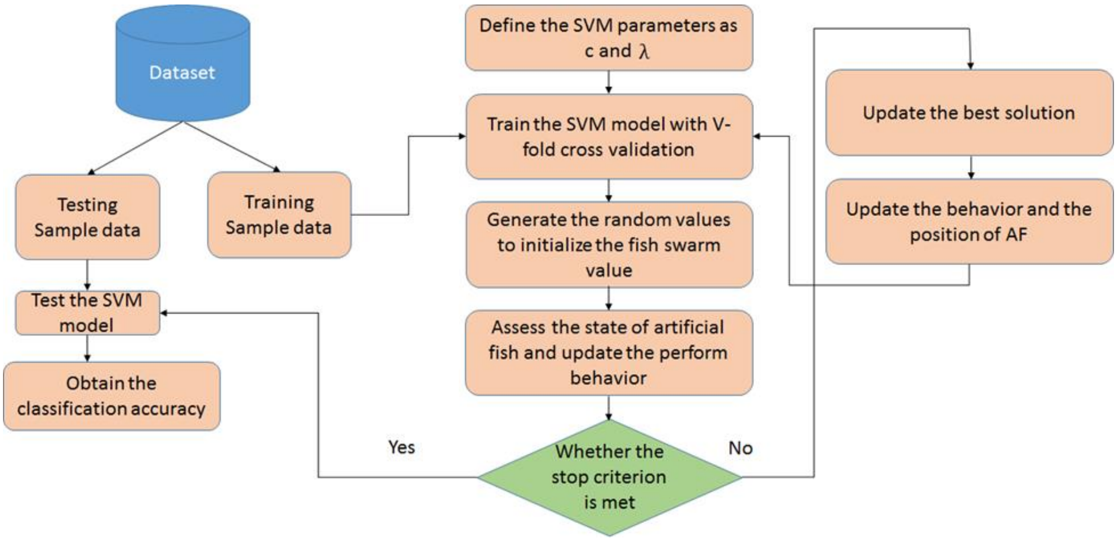
Dataset
Testing Sample data
Training Sample data
Test the SVM model
Obtain the classification accuracy
Define the SVM parameters as c and λ
Train the SVM model with V-fold cross validation
Generate the random values to initialize the fish swarm value
Assess the state of artificial fish and update the perform behavior
Whether the stop criterion is met
Yes
No
Update the best solution
Update the behavior and the position of AF

Figure 2: Flowchart for Proposed Algorithm (SVM with FSO)

- Step 1Define the kernel parameter δ and the error penalty c of the SVM as the particle positions to specify the SVM parameters. Here, a two-dimensional feature space is taken into consideration.

- Step 2: Use groups of training samples to train the SVM model, altering the parameter pairs (c, δ) to reflect the movement of the particles.

- Step 3: Initialize the Fish swarm by setting parameters such as food concentration, position, Number of Iteration, Population Size, and Visual range.

- Step 4: Compute and evaluate the fitness value using the Gaussian function $p(f) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{f-\mu}{\sigma}\right)^2}$. The fitness value is employed to assess intrusion detection with the parameters δ and c.

- Step 5: Evaluate the fish neighbors based on the crowd factor value and the behavior of Artificial Fish (AF) using equations (2), (3), and (4).

- Step 6: Establish the stopping condition, wrap up the iteration, and, if the required accuracy is attained, determine the best SVM parameters. If not, carry out the iterative computation.

- Step 7: Either go back to Step 5 or adjust the particle's best using Equation (5) to update the parameters.
- Step 8: Utilizing Equation (6), update the local extreme values and determine the best outcomes.
- Step 9: Using a small number of testing samples and the determined optimal parameter combinations, δ and c, validate the SVM model.

5. Results & Discussion:

The dataset CICIDS 2017 is already described in the Dataset description section. The proposed SVM-FSO model has been evaluated in the MATLAB R2023b environment. 30% of the dataset is used to test the model, while the remaining 70% is used for training. Specifically for network intrusion detection systems, we thoroughly tested our suggested model against a range of machine learning methods, such as SVM, ANN, KNN, BN, and DNN. Metrics including accuracy (ACY), precision (PRN), recall (REC), specificity (SPY), and F-measure (F_M) are used to evaluate the performance of IDSs. In order to provide a thorough summary of the model's performance, individual indicators are used to create a confusion matrix. The metrics have been described in this section are as:

5.1 Measures of Performance:

5.1.1 Accuracy (ACY):

$$ACY = \frac{TP+TN}{TP+FP+TN+FN} \quad (7)$$

5.1.2 Precision (PRN):

$$PRN = \frac{TP}{TP+FP} \quad (8)$$

5.1.3 Recall (REC):

$$REC = \frac{TP}{TP+FN} \quad (9)$$

5.1.4 Specificity(SPY):

$$SPY = \frac{TN}{TN+FP} \quad (10)$$

5.1.5 F-measure (F_M):

$$F_M = 2 \times \frac{PRN \times REC}{PRN+REC} \quad (11)$$

Where, TP→ True Positive

TN→False Positive

FP→ False Positive

FN→ False Negative

5.2 Network Performance Metrics:

Also we have taken the parameters for analyzing the performance of the VANET such as Packet Drop, Throughput, Delay and Delivery Ratio.

5.2.1 Packet Drop:

$$packet_{drop} = \frac{\sum_i sp^i - \sum_i rp^i}{\sum_i sp^p} \times 100 \quad (12)$$

5.2.2 Throughput:

$$t_{put} = \frac{\sum_i rp^i}{\sum_i tp^i} \quad (13)$$

5.2.3 Delay:

$$delay = {}^{lat}/_{bw} \quad (14)$$

5.2.4 Delivery Ratio:

$$pd_{ratio} = \frac{\sum_i rp^i}{\sum_i sp^i} \times 100 \quad (15)$$

where, sp^i→ Send Packet

rp^i→ Received Packet

tp^i→ Transmission Packet

lat→ Latency

bw→ Bandwidth

5.3 Simulation Setup:

Table 2: Simulation parameters used

S.No	Parameters	Values
1.	Packet Size	600
2.	Simulation Time	100s
3.	Network Area	2500X2000
4.	Simulator	SUMO,NS-2
5.	Routing Protocol	AODV

The Network parameters have been taken into the account for identifying the attack in VANET. This is happened based on transmit of data between the nodes. The following parameters such as Drop packet, Throughput, Delay, and packet delivery ratio have been used for analyzing the attack and compare proposed method with the existing classifiers.

Table 3: Comparison of Network Performance Parameters with existing approaches

Network Performance Parameters	**Classifiers Used**	**Nodes**			
		25	**45**	**65**	**90**
Drop packet	SVM-FSO	0.56674	0.28171	0.25759	0.15804
	SVM	0.76124	0.68541	0.54127	0.44124
	KNN	0.81412	0.76584	0.68142	0.54321
	ANN	0.92993	0.546114	0.436911	0.401246
	DNN	0.74684	0.48014	0.32314	0.19421
	BN	5.129421	12.156547	21.184789	19.458451
Throughput (bps)	SVM-FSO	42156	47651	32741	38560
	SVM	16540	18541	13584	22320
	KNN	18472	16541	18741	19841
	ANN	13142	14751	16472	16661
	DNN	38741	40147	32741	29412
	BN	11010	13210	14715	18412
Delay (s)	SVM-FSO	0.321163	11.15305	18.11668	18.13164
	SVM	0.987410	19.25847	26.94710	31.25478
	KNN	1.258410	10.684171	18.247869	36.14251
	ANN	4.87412	29.25841.	24.175641	32.10475
	DNN	0.314271	14.12471	21.30147	22.32456
	BN	9.942181	15.123477	29.771381	24.159857
Packet Delivery Ratio (%)	SVM-FSO	0.841751	0.86988	0.901602	0.937219
	SVM	0.814121	0.83868	0.854661	0.871229
	KNN	0.715156	0.786964	0.8142461	0.834349
	ANN	0.801308	0.857601	0.828196	0.852961
	DNN	0.837690	0.845678	0.876985	0.906210
	BN	0.690142	0.712048	0.781941	0.825787

Table 4: Comparison table of Performance Measures of Proposed SVM-FSO algorithm

Performance Measures	**SVM-FSO**	**SVM**	**KNN**	**ANN**	**DNN**	**BN**

Accuracy (%)	97.5	85.3	82.1	79.45	92.5	74.02
Precision (%)	91.6	79.6	84.25	81	89	71.5
Recall (%)	88.6	72.5	81.78	78.19	84.59	75.63
Specificity (%)	86.17	70.39	74.15	71.26	81.91	70.58
F-measure (%)	89.65	79.31	80.57	77.47	70.58	72.93

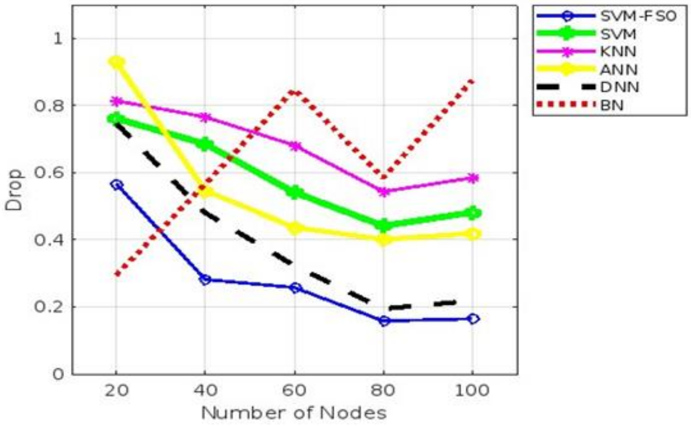

Figure 3: Drop

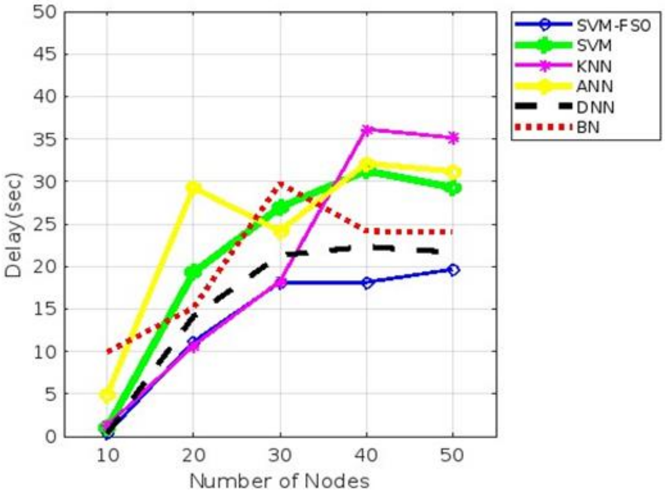

Figure 4: Delay

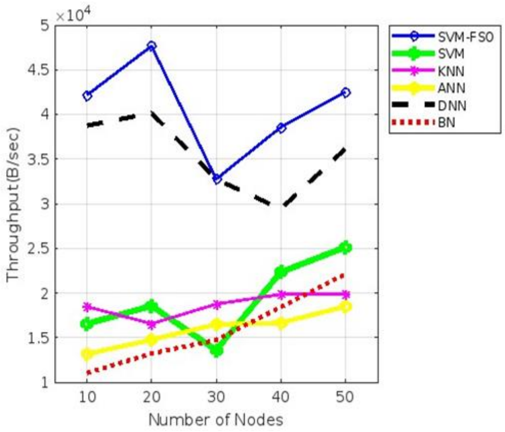

Figure 5: Throughput

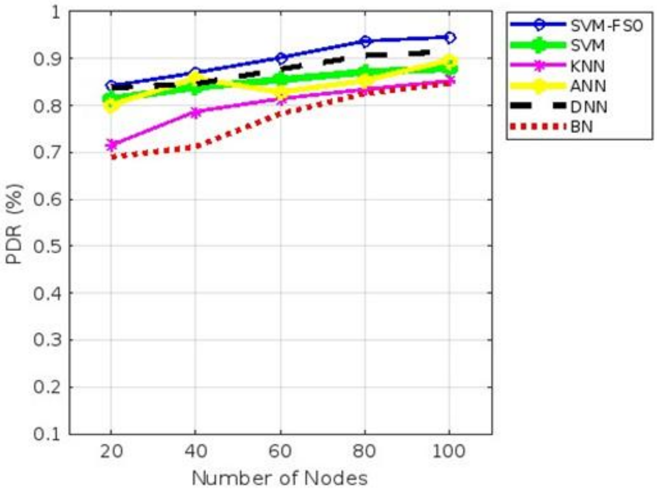

Figure 6: Packet Delivery Ratio (PDR)

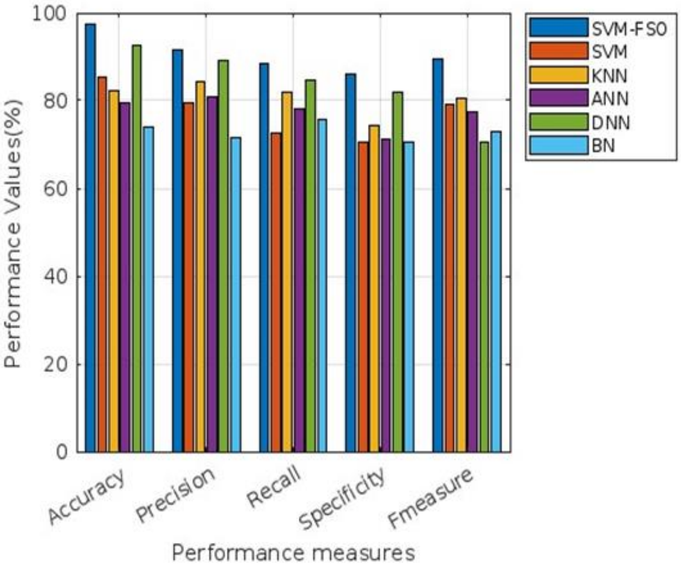

Figure 7: Comparison analysis of Proposed SVM-FSO for Intrusion Detection System

As shown in Figures 3-6, comparisons were made between the node performance of the suggested methodology and the state-of-the-art methods with respect to drop rates, throughput, delay durations, and packet delivery ratios. The measured values, which include the values of the proposed and current method nodes in Table 3, are shown in the table below. The primary objective of these performance studies was to evaluate the mobility prediction capability of the proposed model in VANETs. Table 3 summarizes comparison findings with the most advanced mobility prediction techniques currently used in VANETs, highlighting the advantages of the suggested strategy. The suggested model's effectiveness in predicting mobility within VANETs is confirmed by the performance measures. Table 3 clearly shows that the proposed hybrid optimization strategy combined with machine learning performs better than previous approaches in forecasting mobility within VANETs. The observed figures show that the suggested technique produces improved throughput: at node 90, the drop rate is 0.15804; at node 45, the throughput is 47651 bps; at node 45, the delay is 11.15305 seconds; and at node 90, the packet delivery ratio is 0.937210%. Furthermore, the suggested strategy achieves a higher throughput than the current techniques.

In Table 4 and Figure 7, we present the assessment metrics, including Accuracy, Precision, Recall, Specificity, and F-measure. Our proposed method demonstrates the highest accuracy at 97.5%, while Bayesian-networks exhibit the lowest at 74.02%. The precision of our method is 91.6%, surpassing existing classification models such as SVM, KNN, ANN, DNN, and BN. The recall of our method stands at 88.6%, outperforming other classifiers. The specificity of our method exceeds that of existing classifiers, with values of 15.78%, 6.82%, 10.41%, 4.26%, and 15.59%, respectively. Additionally, the F-measure attains 89.65% in our proposed method, surpassing the lowest in DNN. Consequently, the hybrid learning approach, aided by the approximate technique, yields improved results for Intrusion Detection System (IDS) models.

6. Conclusion:

Vehicle-related problems directly affect traffic and human safety, which emphasizes how important it is to keep car networks secure. Vehicular Ad Hoc Networks, or VANETs, have become more and more significant in recent years. They are essential for allowing intelligent transport systems, maintaining traffic safety, and averting collisions. The primary objective of this study is intrusion detection in the VANET environment. To protect data privacy and identify attacks during communication, the SVM-FSO technique is used.

The suggested SVM with FSO performs well in mass simulations for both network intrusion detection and optimization. The SVM system allows for secure communication between unauthorized users and the trusted authority (TA) with the right training. Accurately labeling attacks and differentiating between attack and normal outputs is achieved using supervised learning. As a result, the SVM-FSO-based technique's security improves the VANET system's overall security. At node 90, the proposed system achieves a packet delivery ratio of 0.937210%, a drop rate of 0.15804, a throughput of 47651 bps, a delay of 11.15305 seconds at node 45, and a throughput of 47651 bps. These results outperform those of existing machine learning (ML) techniques, such as SVM, ANN, KNN, DNN, and BN. Moreover, compared to the existing methods, the proposed strategy produces a higher throughput. We plan to apply it to real-world scenarios in the future and conduct tests with more optimal solutions that respect computing time limitations.

References:

[1] Ullah, Noor & Kong, Xiangjie&Tolba, Amr&Alrashoud, Mubarak & Xia, Feng. (2020). Emergency warning messages dissemination in vehicular social networks: A trust-based scheme. Vehicular Communications.100199. 10.1016/j.vehcom.2019.100199.

[2] Dua, N. Kumar, S. Bawa, Reidd: reliability-aware intelligent data dissemination protocol for broadcast storm problem in vehicular ad hoc networks, Tele commun. Syst. 64 (3) (2017) 439–458

[3] Liu J, Yang W, Zhang J, Yang C. Detecting false messages in vehicular ad hoc networks based on a traffic flow model. International Journal of Distributed Sensor Networks. 2020;16(2).

[4] S. Park and C. C. Zou, "Reliable Traffic Information Propagation in Vehicular Ad-Hoc Networks," *2008 IEEE Sarnoff Symposium*, Princeton, NJ, USA, 2008, pp. 1-6

[5] Arshad, M., Ullah, Z., Ahmad, N. et al. A survey of local/cooperative-based malicious information detection techniques in VANETs. J Wireless Com Network 2018, 62 (2018).

[6] Mr. R. Senthil Ganesh. (2019). Watermark Decoding Technique using Machine Learning for Intellectual Property Protection. International Journal of New Practices in Management and Engineering, 8(03), 01 - 09. https://doi.org/10.17762/ijnpme.v8i03.77.

[7] Mohamed TM, Ahmed IZ, Sadek RA. Efficient VANET safety message delivery and authenticity with privacy preservation. PeerJ Comput Sci. 2021 May 4;7:e519

[8] Chen (2010). A Trust-based Message Evaluation and Propagation Framework in Vehicular Ad-Hoc Networks. UWSpace. http://hdl.handle.net/10012/4929

[9] C. Zhang, K. Chen, X. Zeng and X. Xue, "Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs," in *IEEE Access*, vol. 6, pp. 59860-59870, 2018

[10] Aslan, M., Sen, S. (2019). Evolving Trust Formula to Evaluate Data Trustworthiness in VANETs Using Genetic Programming. In: Kaufmann, P., Castillo, P. (eds) Applications of Evolutionary

[11] Computation.EvoApplications 2019. Lecture Notes in Computer Science (), vol 11454. Springer, Cham

[12] Mujahid Muhammad, Paul Kearney, Adel Aneiba, Junaid Arshad, Andreas Kunz. RMCCS: RSSI-based Message Consistency Checking Scheme for V2V Communications. In Sabrina De Capitani di Vimercati, PierangelaSamarati, editors, Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, July 6-8, 2021. pages 722-727, SCITEPRESS

[13] Rassam, Murad&Ghaleb, Fuad&Zainal, Anazida& Maarof, Mohd. (2019). Detecting Bogus Information Attack in Vehicular Ad Hoc Network: A Context-Aware Approach.

[14] Mohannad O. Rawashdeh, Sayel M. Fayyad, Sulieman Abu-Ein, WaleedMomani, ZaidAbulghanam, A. M. Maqableh. (2023). Intelligent Automobiles Diagnostic System. International Journal of Intelligent Systems and

Applications in Engineering, 11(4s), 458–465. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2703.

[15] Ghaleb, F.A.; Maarof, M.A.; Zainal, A.; Al-Rimy, B.A.S.; Saeed, F.; Al-Hadhrami, T. Hybrid and Multifaceted Context-Aware Misbehavior Detection Model for Vehicular Ad Hoc Network. IEEE Access 2019, 7, 159119–159140.

[16] Sharshembiev, K.; Yoo, S.M.; Elmahdi, E.; Kim, Y.K.; Jeong, G.H. Fail-Safe Mechanism Using Entropy Based Misbehavior Classification and Detection in Vehicular Ad Hoc Networks. In Proceedings of the 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Atlanta, GA, USA, 14–17 July 2019; pp. 123–128

[17] Guo, J.; Li, X.; Liu, Z.; Ma, J.; Yang, C.; Zhang, J.; Wu, D. TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet Things J. 2020, 7, 6647–6662.

[18] University of New Brunswick, Canadian Institute for Cybersecurity: Intrusion Detection Evaluation Dataset (CICIDS 2017), Accessed 15 September 2020

[19] R. Azizi, "Empirical study of artificial fish swarm algorithm," Computer Science, vol. 17, no. 6, pp. 626–641, 2014.

[20] Y. Gao, L. Guan, and T. Wang, "Triaxial accelerometer error coefficients identification with a novel artificial fish swarm algorithm," Journal of Sensors, vol. 2015, Article ID 509143, 17 pages, 2015.

[21] V Vapnik. The nature of statistical learning theory. New York: Springer-Verlag Press, 2000.