Collaborative based Vehicular Ad-hoc Network Intrusion Detection System using Optimized Support Vector Machine

Azath M, Vaishali Singh
Department of Computer Science & Engineering-School of Engineering & Technology,
Maharishi University of Information Technology, Lucknow, Uttar Pradesh 226013, India

***Abstract*—The Vehicular Ad hoc Network (VANET) can be used to provide secured information to the user vehicles. However, these days the immunity of safeguarding the information from vulnerabilities and threats are of great challenge. Therefore, it is necessary to provide a secured solution for the improvement of security with the deployment of advanced technology. In context with this, a blockchain based VANET structure for secured communication incorporated with the enhancement of confidentiality, scalability, and privacy is planned. The k-means clustering model forms cluster formation. The cluster head selection is carried out with Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm. The proposed approach aims to mitigate the delay with the enhancement of throughput and energy efficiency. Meanwhile, the deployed blockchain will enhance reliability and security. Moreover, the novel War Strategy Optimization (WSO) based Support Vector Machine (SVM) model (Optimized SVM) can be used for the trust-based collaborative intrusion detection in the VANET. Our work targets to detect the intrusion and non-intrusion classes. Meanwhile, our proposed work can be used for the prevention of repetitive detection processes and therein it enhances the security by rewarding the vehicles. An experimental analysis is carried out to ensure its usage in detecting the malicious node from the resource constraint vehicles and also used to achieve better security, energy utilization and end-to-end delay.**

Keywords*—Vehicular Ad hoc network; intrusion detection; tabu search based particle swarm optimization; war strategy optimization; support vector machine

I. INTRODUCTION

The emerging trend of vehicular technology leads to the addition of smart equipment in vehicles and advancement of the intelligent transportation system and self-driving vehicles. The communication among vehicles and the roadside unit (RSU) can be accomplished with the VANET which alerts the drivers about the traffic, emergency alerts, and safety messages [1, 2]. The increase in mobility of vehicles, intricate topology, and diverse communication are the major possibilities of the VANET system to have been attacked by intruders. The main purpose of the intruders is to break the smart communication between the vehicles and RSUs. This might lead to damage in the VANET system and overcoming this intrusion detection system is the best choice [3].

The performance of the IDS relies on its deployed location in the cluster head, vehicles, and RSU and the conventional IDS contains three various architectures including distributed centralized and hybrid IDS [4]. Most probably the detection of various attacks by the traditional approaches is limited and it is necessary to design a precise approach to detect all types of abnormalities in the system. The centralized approach of software-defined networking (SDN) provides better flexibility and security throughout the network; however, a system bottleneck occurs due to failure in the single point. The issues in the SDN such as reliability and scalability are visibly moved by the distributed networks [5, 6]. Moreover, the communication and computation overhead of the SDN controllers are also tackled by the distributed SDN via VANET. It also possesses some demerits and it is necessary to overcome them [7].

The securities of the vehicles are the most challenging ones since most of the vehicles are designed without considering the security system. However, they can perform communication without any delay but still increases the attacks [8]. This can be dealt with the conventional approaches such as encryption and neglecting the irrelevant nodes. Recently the vehicles are linked in the VANET and thus detect the attacks. So to secure the communication between the vehicles and RSUs a Blockchain-based collaborative intrusion detection approach is introduced for the VANETs. Different kinds of swarm-based optimization models such as particle swarm optimization, fish swarm optimization, Cuckoo Search algorithm, Glowworm Swarm Optimization (GSO), Genetic Algorithms (GA) etc. contains more searchability, less cost, less time execution and it is easy to solve the optimization problems. Tabu search creates a metaheuristics search technique that could really evaluate the optimum solution in addition to local optimization problems. The critical feature of Tabu Search is the use of adaptable storage to produce a much more adaptable behavior. PSO is the motion, which is controlled by two factors: information from particle to particle and iteration to iteration. The intrusion detection can be achieved with the SVM-based WSO approach. Prior to this the cluster head and cluster formulation are done with the Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm. This approach collaboratively trains the samples and achieves better detection.

The major contribution of this study is summarized as follows:

- The cluster formation in VANET is performed via the k-means clustering model.

- The Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm selects the optimal cluster heads.
- The blockchain-based security performs VANET security. Both intrusion and non-intrusion are detected via the novel War Strategy Optimization (WSO) based Support Vector Machine (SVM) model.

A. Problem Statement

Most vehicles are created without taking into account the security system, it is one of the most difficult areas to secure. They can communicate instantly, which makes attacks more common. Traditional methods, like encryption and ignoring unnecessary nodes, can be used to handle this. Recently, vehicles have been connected to the VANET, allowing them to detect threats.

Therefore, the existing studies created a Blockchain based collaborative intrusion detection approach for the VANETs to secure the connection between the cars and RSUs. The searchability, cost, and execution time of various swarm-based optimization models, such as fish swarm optimization, particle swarm optimization, glowworm swarm optimization, Cuckoo Search algorithm, genetic algorithms, and others, are higher. Tabu search develops a metaheuristics search method that can effectively access both the ideal solution and local optimization issues. The use of adaptable storage to create a significantly more adaptive behavior is a key component of Tabu Search. The SVM-based WSO technique can be used to detect intrusions.

II. Literature Review

A hybrid machine learning model was suggested by Bangui et al. [9] for the detection of intrusion in VANET. The Random Forest (RF) models were used to improve the accuracy of IDS. Compared to other methods, this RF model considerably improves the accuracy of detection based on the CICIDS2017 dataset. The detection accuracy is increased and the computational time is decreased but it failed to describe any security concept.

A hybrid data-driven model was introduced by Bangui et al. [10] for VANET intrusion detection. The explosive development in computing power deals to improve the IDS performance. The possible novel intruders were detected with the help of the post-detection stage. The corsets-based clustering and data classification were combined via a hybrid data-driven model. The computational overhead was less but the execution time was higher and had more complicated process.

In VANET, Zaidi et al. [11] suggested Host-based intrusion detection (H-ID). The statistical and graphical techniques represent the collection of extensive data. The rogue nodes were easily detected with the usage of different traffic conditions. According to the cooperative information, the application layer IDS were observed and evaluated with respect to the state-of-art results. Due to increased vehicular data, the computational complexity was also higher.

Based on ToN-IoT dataset, the machine learning (ML) techniques were suggested by Gad et al. [12] to detect the VANET intrusion. The ML techniques are the combination of Naive Bayes (NB), Support Vector Machine (SVM), XGBoost, Logistic Regression (LR), and k-Nearest Neighbor (kNN) and Decision Tree (DT). Both multi-class and binary classification issues were easily solved by using this ToN-IoT dataset. The class balancing was performed with the usage of the Synthetic minority oversampling technique. The higher feature dimensionality increases the overall complexity.

The deep learning (DL) model was suggested by Aboelfottoh et al. [13] for intrusion detection in ACVs and VANETs. More accurate and smarter IDS were made via deep learning thereby providing an efficient intrusion detection model but it failed to satisfy the security process. Based on the time series classification approach, the LSTM model was introduced by Yu et al. [14] for the VANETs intrusion detection system. The classification model of LSTM was used to enhance the false emergency message detection accuracy. For both collusion attack and normal scenarios, the time series feature vectors train and the traffic incident classifier were designed to identify traffic parameter patterns with higher computational difficulties.

The context of an intrusion detection system in VANET was designed by Gonçalves et al. [15]. Based on the geographic region, the publicly available VANET datasets were evaluated. The far more popular security policy was used to employ conventional instruments which can aid in the prevention of threats. In vehicular ad hoc networks, Alsarhan et al. [16] suggested an SVM-based intrusion detection system. This model outperformed classification accuracy with a better intrusion detection model and higher execution time than the existing methods such as PSO, ACO and GA. The distributed ensemble learning model was introduced by Ghaleb et al. [17] for misbehavior-aware on-demand collaborative IDS. The remote and locally trained classifiers were encompassed with the weighted random forest-based classifiers. Compared to the previous CIDS model, this distributed ensemble learning approach delineated 97% F1 score performances but the computational cost was higher and it needed more security during intrusion detection.

III. Proposed Methodology

The VANET are critical enablers of eventual collaborative transportation systems. Vehicles on VANETs exchange actual information regarding its location, congestion, and traffic conditions. Nevertheless, VANETs are vulnerable to threats that can result in existing circumstances. IDS depending on automotive collaboration to detect attackers in VANET were the most frequently proposed privacy model. The schematic diagram of the proposed intrusion detection model is shown in Fig. 1. The proposed methodology includes four stages namely cluster formation, cluster head selection, VANET security and Collaborative intrusion detection. Each of these stages is delineated in the following section.

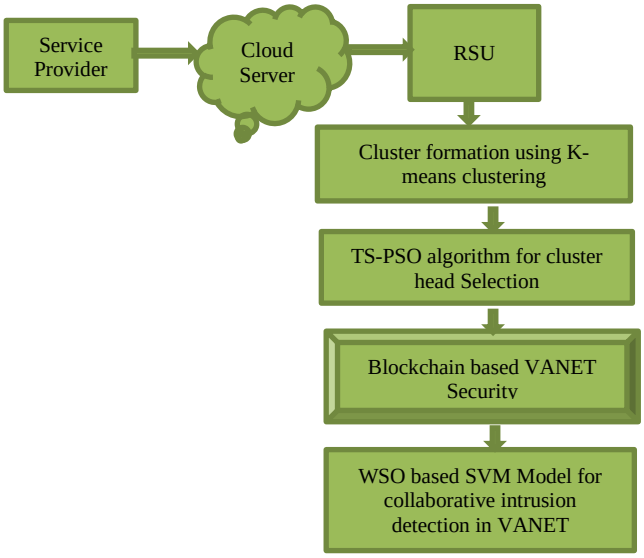

Fig. 1. Proposed intrusion detection framework.

A. Cluster Formation

The stable vehicle cluster formations are the major step of this study. In this study, the K-means clustering algorithm was used to perform cluster formation. The edges were represented by using the distances between vehicles and the graph vertex act as each vehicle [18]. Based on roadside units (RSU) transmission region, the cluster formation of each vehicle was calculated. In the d-dimensional real vector, the observation set is $(A_1, A_2, .., A_m)$ [14]. Within cluster square sum (WCSS) is minimized via the m observation partition into K-sets $(K \le m) s = \{s_1, s_2, ..., s_K\}$.

$$WCSS = \arg\min_{s} \sum_{j=1}^{K} \sum_{A_i \in s_j} \left\| A_i - \chi_j \right\|^2 \quad (1)$$

During cluster formation, the points mean S_j in is Xj.

B. Cluster Head Selection

The space solution apart from local optimality was analyzed via Tabu Search (TS) to represent the search process. The component of TS is an adaptive memory, which is more efficient. In a similar period, the respective optima were not attained with multiple objectives. In a rapid manner, the TS had hard combinatorial optimization problems and which led to select the solution design [19]. The particle swarm optimization (PSO) model contains several advantages in case of a direction to initial converging towards local optima, less population diversity, resolving optimization and greater convergence [20]. Tabu Search is a powerful stochastic efficient algorithm that, in theory, might aggregate monotonically to a global optimum, but it required a lot of time to reach the close-to-global minimum. The algorithm can maintain population variety by incorporating TS into PSO as a local development phase, which prevented it from leading to an incorrect local optimal solution.

In this study, Tabu Search based Particle Swarm Optimization (TS-PSO) algorithm was used for the selection of cluster heads in VANET. While compared to the PSO algorithm, the TS takes less computational time with the average energy consumption during CH selection [21]. The tradeoff between both PSO and TS can be neglected by combining the TS-PSO algorithm.

The following steps explain the TS-PSO model for cluster head selection.

- Initialize the base station location and energy nodes.
- The TS-PSO algorithm with a maximum number of iterations is initialized.
- The base station corresponding to the node's distances is calculated via the cluster formation.
- Determine the local best position of the PSO algorithm.
- Tabu memory entries to zero. The initialization of the PSO solution with the Tabu list calculates the global best solution.
- In the Taby memory, create the entry and routes are swapped.
- Evaluate the fitness function of the next position and note the fitness value in the Tabu list.
- The most effective solution from the Tabu list is eliminated.
- Tabu Search based Particle Swarm Optimization (TS-PSO) algorithm is used to optimally select the cluster heads in VANET.

C. VANET Security based on Blockchain Model

The blockchain is made up of a collection of blocks that are linked together. A block is a decentralized network ledger that is connected simultaneously [22]. The actions inside the block are irreversible and unchangeable. Each block inside the blockchain is connected by the subsequent block's hash. Any changes to a single block will have an impact on the rest network. Furthermore, the information loaded into blocks are entirely open. The data transfer from one vehicle to another is the major security issue in VANET. No necessary data is detected by the vehicles before sharing in the VANET task manager. Consequently, there was a probability for updated data to be uploaded into the Vehicular network [23]. This blockchain security model that successfully maintains the security across the system, to overcome these issues. Blockchain is the distributed immutable ledger that can be used to record transactions and asset tracking.

If the vehicle user transfers through one RSU zone to the next, that following RSU requires the vehicle users to be really authorized. This one will substantially add significant cost and reduce the VANET system's performance. The assets might include tangible and intangible. The values in the blockchain can be tracked virtually by the authenticated user thus mitigating the risk and cost. With the distributed data sharing and storage capacity, it can also avoid the hazards of an attack and outage at a single location [24]. Furthermore, the integrity

and validity of the initial global strategy can be guaranteed using the open ledger in the blockchain. Based on the reward and punishment system, the cars in the VANET system submit exact information. This stops false information from being uploaded. It is simple to trace the features of each transaction.

D. Intrusion Detection

This section describes the war strategy optimization (WSO) based support vector machine (SVM) for collaborative intrusion detection in VANET.

1) Support Vector Machine (SVM): The machine learning approach SVM [25] was used for intrusion detection in our proposed approach. This proposed approach is based on the WSO-SVM-based collaborative to detect the attacks and normal traffics. The data were represented in n-dimensional space and detection of intrusion was conducted by detecting the hyper-plane first and classifying the malicious node as intrusion and others as normal. The workflow of the proposed SVM is shown in Fig. 2.

To spate, the various points from the input the SVM utilizes the free parameters which rely on the separation margin as depicted in Fig. 3 [26]. However, there occur over fitting issues which can be rectified by the introduction of the WSO algorithm. The main reasons for utilizing the SVM are speed and scalability and also reduced complexity.

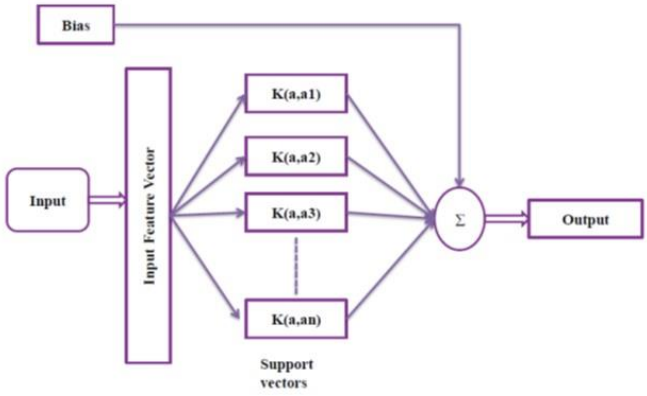

Fig. 2. Flowchart representation of the SVM model.

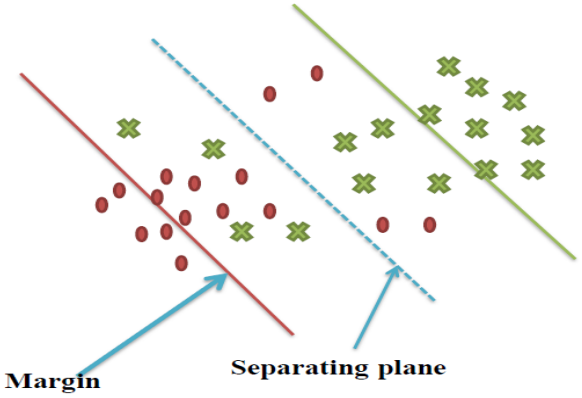

Fig. 3. Separating plane model of SVM.

2) War Strategy Optimization (WSO)

a) This WSO is based on the war strategy followed by the ancient kings based on the mission objectives, struggles, threats, and prospects. War is a continuous process in which the armed soldiers simply get together and fight the enemies.

The numerical expression followed by the strategy that the troops follow the king or commander on the war field. To avert falling prey to local troops the soldiers follow the combined movement tactics along with the king and the commanders.

- Attack Strategy

The war strategies have two models in which the former follows the updated locations of the soldiers with respect to the locations of the king. The soldier with high attack and fitness abilities are considered king. At first, all the soldiers possess the same rank and position and update the ranking location based on the finishing of war strategy. At end of the war the soldier, commander, and king all pretend to be close to each other and can be formulated as,

$$A_i(t+1) = A_i(t) + 2\times\tau\times(D-L) + ran\times(V_i\times L - A_i(t)) \quad (2)$$

The current location of the soldiers is Ai and the updated locations are depicted as A_i (t+1) the location of the commander is D and L is the location of the king with the weight of V*i*.

- Up-gradation of rank and weight

The location of the soldiers can be updated with the location of the attack force. If the new location of the fitness (Fn) is lower than the current location (Fc) then the soldier will remain in the previous location [27].

$$A_i(t+1) = (A_i(t+1))\times(F_n \geq F_c) + (A_i(t))\times(F_n < F_c) \quad (3)$$

Then the rank of the soldier is updated as shown below,

$$S_i = (S_i + 1)\times(F_n \geq F_c) + (S_i)\times(F_n < F_c) \quad (4)$$

The estimation of weights based on the rank can be performed as,

$$V_i = V_i \times \left(1 - \frac{S_i}{Max\_iter}\right)\beta \quad (5)$$

- Defense strategy

The latter strategy was based on the up-gradation of locations of the king, commander, and a random soldier. The ranking and weight-up gradation follow the same strategy.

$$A_i(t+1) = A_i(t) + 2\times\tau\times(L - A_{ran}(t)) + ran\times V_i\times(D - A_i(t)) \quad (6)$$

- Weak Soldiers replacement/relocation

The detection of the worst soldiers is performed for each iteration and replaced with a random soldier as shown below,

$$A_v(t+1) = LC + ran\times(UC - LC) \quad (7)$$

The next approach is to reposition the weak soldier to the median of the whole army as shown below,

$$A_v(t+1) = -(1-rann) \times (A_v(t) - median(A)) + L \quad (8)$$

3) Enhancement of WSO-based SVM for intrusion detection.

- This proposed approach maintained the balance between exploitation and exploration.
- Each soldier (solution) maintained a unique weight with respect to the rank.
- After finishing the fitness step the weight of the soldiers got updated.
- At the starting stage of iteration the weights changed in large amount and decreases towards the end and this will result in a global optimum value.
- The stated approach simply increases the convergence speed and leads to less computation complexity.

4) Optimized SVM-based collaborative intrusion detection: The machine learning approach SVM provides efficient intrusion detection, and swift implementation, and is simple in nature. However, it possessed some shortcomings like over fitting issues and higher complexities [28]. These were tackled by the WSO algorithm which increased the convergence speed and searchability and increased the detection speed and accuracy. Thus the merging of WSO and SVM is performed in this proposed collaborative intrusion detection approach. The position parameters of SVM are updated by the fitness function of the proposed WSO algorithm. The schematic structure of the proposed WSO-SVM-based collaborative intrusion detection in VANET is illustrated in Fig. 4.

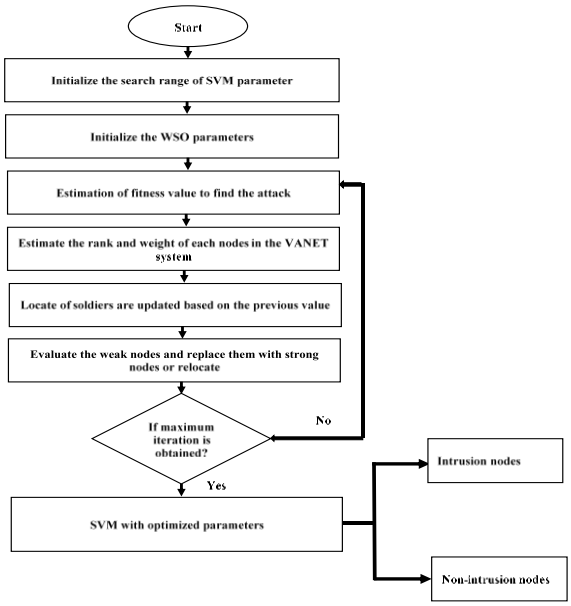

Fig. 4. Schematic overflow of proposed optimized SVM-based collaborative intrusion detection approach in VANET.

IV. Result and Discussion

This section discusses the experimental investigation of a proposed framework based on collaborative intrusion detection in VANET. The GTX1050 GPU at 16GB RAM and Intel Core i5-8300H CPU with Tensorflow 1.15 on a GPU-based computer based on NS-2 implement the experimental results [29]. Table I explains the parametric description based on the proposed framework.

In this study, the KDD99 dataset was used for experimental investigation [30]. There were five million records involved in the KDD99 dataset and 41 features described these records.

TABLE I. Parameter Description

Parameters	Ranges
Number of population	50
Maximum number of iteration	100
Number of nodes	50
Simulation range	1.5 kms * 1.5 kms
Kernel function	Gaussian
Regularization	0.01

A. Performance Measures

The performance metrics such as accuracy (A), precision (P) and recall (R) are used to validate the effectiveness of proposed framework [30], [31]. The following equations explain all these performance measures for intrusion detection performance efficiency.

$$A = \frac{T_N + T_P}{F_N + T_N + F_P + T_P} \quad (9)$$

$$P = \frac{T_P}{F_P + T_P} \quad (10)$$

$$R = \frac{T_P}{F_N + T_P} \quad (11)$$

Where, the number of correctly predicted intrusion and the number of correctly predicted non-intrusion classes are true positive (T_P) and true negative (T_N). Moreover, a number of incorrectly predicted intrusion and the number of incorrectly predicted non-intrusion classes are true positive (F_P) and true negative (F_N).

B. Evaluation based on Performance

The analysis of accuracy is plotted in Fig. 5. A different number of nodes such as 10, 20, 30, 40 and 50 are used for the analysis of accuracy. The methods like RF, HDDM, H-ID, and ML are proposed. However, these proposed method offers superior accuracy than previous methods like RF, HDDM, H-ID, and ML in terms of all nodes.

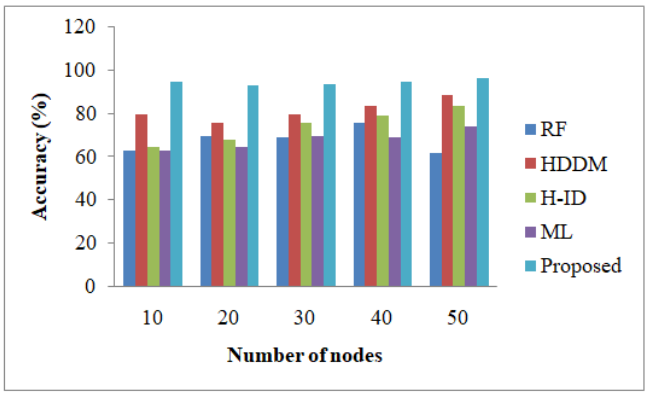

Fig. 5. Graphical representation of accuracy results.

The graphical representation of energy consumption results is plotted in Fig. 6. The methods including RF, HDDM, H-ID, and ML with proposed methods are taken as the state-of-art methods. There are 50 nodes which were taken for this investigation. The proposed method consumed less energy while comparing to the existing methods such as RF, HDDM, H-ID, and ML.

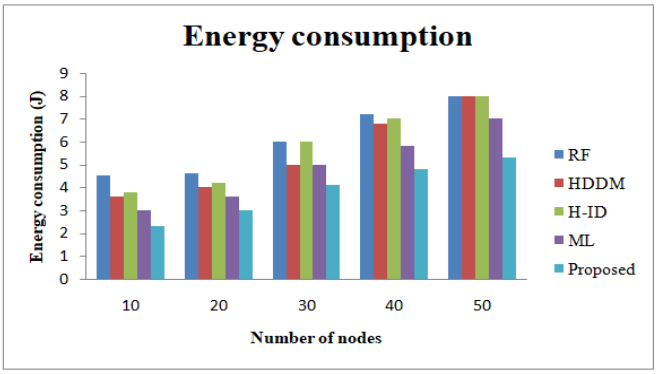

Fig. 6. Graphical representation of energy consumption results.

Fig. 7 represents the graphical representation of end-to-end delay results. The state-of-the-art methodologies include RF, HDDM, H-ID, and ML with proposed methodologies. For this examination, 50 nodes were taken and the delay is represented in time seconds. When compared to existing technologies like RF, HDDM, H-ID, and ML, the proposed method demonstrated minimum delay.

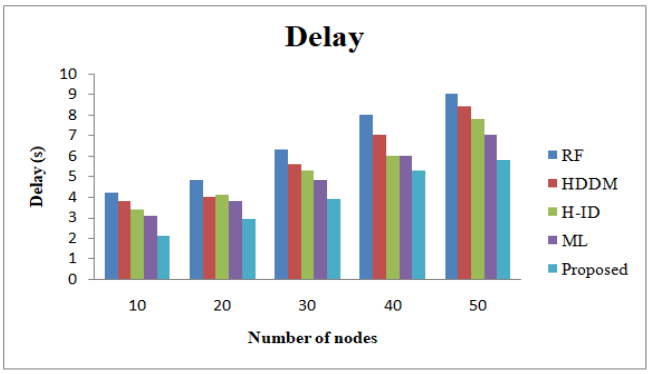

Fig. 7. Graphical representation of end-to-end delay results.

The performance evaluation of this proposed technique based on security was analyzed and compared with state-of-art work such as RF, HDDM, H-ID, and ML and reported in Table II. Since this proposed work utilized a collaborative blockchain-based WSO-SVM technique, it effectively secured the VANET system and avoided the vehicles from attacking. The security of the proposed approach is 95.89% and the other approaches RF, HDDM, H-ID, and ML provide security of 91.9%, 89.06%, 90.56%, and 93.23% respectively.

TABLE II. EVALUATION BASED ON SECURITY

Methods	Security (%)
RF	91.9
HDDM	89.06
H-ID	90.56
ML	93.23
Proposed	95.89

The evaluation based on the performance metrics was estimated and compared with state-of-art works such as RF, HDDM, H-ID, and ML, as stated in Table III. From the table III, it is clear that due to the inclusion of WSO along with the SVM classifier our approach provided better accuracy, precision, and recall of about 96.48%, 95.89%, and 96.56% respectively. Meanwhile, the other existing approaches show lacking strategies for above-stated metrics than this proposed approach.

TABLE III. EVALUATION BASED ON RECALL, PRECISION, AND ACCURACY

Methods	Recall (%)	Precision (%)	Accuracy (%)
RF	87.78	89.37	90.38
HDDM	91.09	90.56	92.77
H-ID	89.09	91.45	89.55
ML	93.45	90.76	93.00
Proposed	96.56	95.89	96.48

V. CONCLUSION

This article introduced a collaborative-based vehicular ad hoc network intrusion detection system using an optimized support vector machine. The cluster formation has been performed via k-means clustering. The Tabu Search-based Particle Swarm Optimization (TS-PSO) algorithm has been used to select the cluster heads for the formulated cluster. The suggested strategy helped to reduce the delay in the transmission of data by improving throughput and energy efficiency. The security of the proposed VANET system has been accomplished with the utilization of blockchain and enhanced its reliability. Additionally, the trust-based collaboration intrusion detection on the VANET can be performed using the optimized SVM model. The KDD99 dataset has been utilized and simulated with NS-2 software to analyze the performance of the proposed work. The proposed method offers minimum energy consumption as well as an end-to-end delay compared to the existing methods such as RF, HDDM, H-ID, and ML with the consideration of 50 nodes. The proposed strategy has a security level of 95.89%, while the

other approaches—RF, HDDM, H-ID, and ML—offer security levels of 91.9%, 89.06%, 90.56%, and 93.23% correspondingly.

This study has few challenges in which the efficiency and accuracy of the intrusion detection framework can be enhanced via granularity and in-depth monitoring. The usage of different protocols and data diversity of the modern VANET networks induces a high level of complexity when identifying the intrusions in future.

REFERENCES

[1] Tonguz, Ozan, Nawapom Wisitpongphan, Fan Bai, Priyantha Mudalige, and Varsha Sadekar, "Broadcasting in VANET," Mobile networking for vehicular environments, pp. 7-12. IEEE, 2011.

[2] Lee, M. and Atkison, T., "Vanet applications: Past, present, and future," Vehicular Communications, 28, p.100310, 2021.

[3] Hasrouny, Hamssa, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti, "VANet security challenges and solutions: A survey," Vehicular Communications, 7, 7-20, 2017.

[4] Calandriello, G., Papadimitratos, P., Hubaux, J.P. and Lioy, A., "Efficient and robust pseudonymous authentication in VANET," In Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks (pp. 19-28), 2007.

[5] Shu, Jiangang, Lei Zhou, Weizhe Zhang, Xiaojiang Du, and Mohsen Guizani, "Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach," IEEE Transactions on Intelligent Transportation Systems 22, no. 7, 4519-4530, 2020.

[6] Raja, G., Anbalagan, S., Vijayaraghavan, G., Theerthagiri, S., Suryanarayan, S.V. and Wu, X.W., "SP-CIDS: Secure and private collaborative IDS for VANETs," IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4385-4393, 2020.

[7] Maglaras, Leandros A, "A novel distributed intrusion detection system for vehicular ad hoc networks," International Journal of Advanced Computer Science and Applications 6, no. 4, 101-106, 2015.

[8] Shu, J., Zhou, L., Zhang, W., Du, X. and Guizani, M., "Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach," IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4519-4530, 2020.

[9] Bangui, H., Ge, M. and Buhnova, B., "A hybrid machine learning model for intrusion detection in VANET," Computing, 104(3), pp.503-531, 2022.

[10] Bangui, H., Ge, M. and Buhnova, B., "A hybrid data-driven model for intrusion detection in VANET," Procedia Computer Science, 184, pp.516-523, 2021.

[11] Zaidi, K., Milojevic, M.B., Rakocevic, V., Nallanathan, A. and Rajarajan, M., "Host-based intrusion detection for VANETs: A statistical approach to rogue node detection," IEEE transactions on vehicular technology, 65(8), pp.6703-6714, 2015.

[12] Gad, A.R., Nashat, A.A. and Barkat, T.M., "Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset," IEEE Access, 9, pp.142206-142217, 2021.

[13] Aboelfottoh, A.A. and Azer, M.A., "Intrusion Detection in VANETs and ACVs using Deep Learning," In 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (pp. 241-245). IEEE, 2022.

[14] Yu, Y., Zeng, X., Xue, X. and Ma, J., "LSTM-Based Intrusion Detection System for VANETs: A Time Series Classification Approach to False Message Detection," IEEE Transactions on Intelligent Transportation Systems , Vol. 23, Issue 12, 2022.

[15] Gonçalves, F., Macedo, J. and Santos, A., "Evaluation of VANET Datasets in context of an Intrusion Detection System," International Conference on Software, Telecommunications and Computer Networks (SoftCOM) (pp. 1-6). IEEE, 2021.

[16] Alsarhan, A., Alauthman, M., Alshdaifat, E., Al-Ghuwairi, A.R. and Al-Dubai, A., "Machine Learning-driven optimization for SVM-based intrusion detection system in vehicular ad hoc networks," Journal of Ambient Intelligence and Humanized Computing, pp.1-10, 2021.

[17] A. Ghaleb, F., Saeed, F., Al-Sarem, M., Ali Saleh Al-rimy, B., Boulila, W., Eljialy, A.E.M., Aloufi, K. and Alazab, M., "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," Electronics, 9(9), p.1411, 2020.

[18] Hussain, I. and Chen, B., "Cluster formation and cluster head selection approach for vehicle ad-hoc network (VANETs) using K-means and floyd-Warshall technique," International Journal of Advanced Computer Science and Applications, 8(12), 2017.

[19] Kandali, K., Bennis, L. and Bennis, H., "A new hybrid routing protocol using a modified K-means clustering algorithm and continuous hopfield network for VANET," IEEE Access, 9, pp.47169-47183, 2021.

[20] Alinaghian, M., Tirkolaee, E.B., Dezaki, Z.K., Hejazi, S.R. and Ding, W., "An augmented Tabu search algorithm for the green inventory-routing problem with time windows," Swarm and Evolutionary Computation, 60, p.100802, 2021.

[21] Pervaiz, S., Ul-Qayyum, Z., Bangyal, W.H., Gao, L. and Ahmad, J., "A systematic literature review on particle swarm optimization techniques for medical diseases detection," Computational and Mathematical Methods in Medicine, Vol. 2021, Article ID 5990999, 2021.

[22] Vijayalakshmi, K. and Anandan, P., "A multi objective Tabu particle swarm optimization for effective cluster head selection in WSN," Cluster computing, 22(5), pp.12275-12282, 2019.

[23] Maria, A., Rajasekaran, A.S., Al-Turjman, F., Altrjman, C. and Mostarda, L., "Baiv: An efficient blockchain-based anonymous authentication and Integrity Preservation Scheme for secure communication in VANETs," Electronics, 11(3), p.488, 2022.

[24] Alkadi, O., Moustafa, N. and Turnbull, B., "A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions," IEEE Access, 8, pp.104893-104917, 2020.

[25] Liang, J. and Ma, M., "Co-maintained database based on blockchain for idss: A lifetime learning framework," IEEE Transactions on Network and Service Management, 18(2), pp.1629-1645, 2021.

[26] Safaldin, Mukaram, Mohammed Otair, and Laith Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," Journal of ambient intelligence and humanized computing Vol. 12, no. 2 (2021): 1559-1576, 2021.

[27] Ayyarao, Tummala SLV, N. S. S. RamaKrishna, Rajvikram Madurai Elavarasan, Nishanth Polumahanthi, M. Rambabu, Gaurav Saini, Baseem Khan, and Bilal Alatas, "War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization," IEEE Access 10 (2022): 25073-25105, 2022.

[28] Ayyarao, Tummala SLV, and Polamarasetty P. Kumar, "Parameter estimation of solar PV models with a new proposed war strategy optimization algorithm," International Journal of Energy Research 46, no. 6 (2022): 7215-7238, 2022.

[29] Zhang, T. and Zhu, Q., "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," IEEE Transactions on Signal and Information Processing over Networks, 4(1), pp.148-161, 2018.

[30] Belenko, V., Krundyshev, V. and Kalinin, M., "September. Synthetic datasets generation for intrusion detection in VANET," International conference on security of information and networks (pp. 1-6), 2018.

[31] Shu, J., Zhou, L., Zhang, W., Du, X. and Guizani, M., "Collaborative intrusion detection for VANETs: A deep learning-based distributed SDN approach," IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4519-4530, 2020.