Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS-2025)
IEEE Xplore Part Number: CFP25K74-ART; ISBN: 979-8-3315-1208-8

2025 International Conference on Intelligent Computing and Control Systems (ICICCS) | 979-8-3315-1208-8/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICICCS65191.2025.10984526

Discrete Hopfield Neural Network Model for Secure Electrical Routing in VANETs to Avoid Blackhole Attacks

Chennaiah Kate[1], Arvind Tudigani[2], Sarala Raghavendra[3], A. Lizy[4], M. Malathi[5], Lalit Johari[6],
[1] Department of Computer Science and Engineering, St.Peter's Engineering College, Hyderabad, Telangana 500043, India. chennaiahkate@gmail.com
[2] Department of Computer Science, University College of Science, Saifabad, Hyderabad, Telangana 500004, India. mr.arvind@rediffmail.com
[3] Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana 501401, India. raghava.sarala@gmail.com
[4] Department of Artificial Intelligence and Machine Learning, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu 600062, India. lizyliju@gmail.com
[5] Department of Mathematics, Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu 638401, India. malathim@bitsathy.ac.in
[6] Department of Computer Applications, IFTM University, Lodhipur Rajput, Uttar Pradesh 244102, India. lalit.johari@gmail.com

***Abstract*— Intelligent Transportation Systems (ITS) depend heavily on Vehicle Ad Hoc Networks (VANETs) to establish vehicle-to-vehicle communication because these networks improve both safety performance on the roads and the reduction of traffic congestion. Black hole attacks represent one of the major cyber threats that affect the secure operation of Vehicle Ad Hoc Networks. Black hole attacks against VANET networks represent critical threats to security which can generate data packet losses along with network instability even with current security evolution efforts. Security measures based on conventional practices lead to substantial false detection situations while their response times remain slow thus preventing real-time mitigation strategies. This study develops a novel Discrete Hopfield Neural Network with Termite Alate Optimization (DHNN-TAO) model to address the mentioned issues. The Mountaineering Team-Based Optimization (MTBO) is the initial procedure that combines network nodes to establish enhanced network stability and effective transmission between nodes. Discrete Hopfield Neural Network (DHNN) identifies black hole attacks through effective detection of malicious nodes after the clustering process ends. The optimization process of hyperparameters in DHNN uses Termite Alate Optimization (TAO). After identification of malicious activity Light Spectrum Optimizer (LSO) works to find secure communication routes between attack-free network segments. The suggested DHNN-TAO attains 1600 kbps throughput, 0.42s routing delay, 7.4ms execution time, 99.1% accuracy, 0.96 packet delivery ratio, and 0.59 control overhead, surpassing the current techniques.**

Keywords*— *black hole attacks, Discrete Hopfield Neural Network, Light Spectrum Optimizer, Mountaineering Team-Based Optimization, Termite Alate Optimization.

I. INTRODUCTION

The cornerstone of Intelligent Transportation Systems and real-time communications for vehicular safety and traffic enhancement is Vehicular Ad Hoc Networks (VANETs). The routing issues in VANETs remain challenging because these networks differ from standard wireless systems through their high mobility along with their frequently changing topologies and decentralized architecture and their time-dependent communications [1]. The characteristic features of VANETs demand high priority for secure and prompt data exchange because network disturbances from malicious attacks lead to severe penalties including traffic accidents as well as congestion and information loss. Among many different security threats the Blackhole Attack (BHA) emerges as the most damaging denial-of-service attack that affects VANETs [2].

The Blackhole Attack makes nodes believe that a dishonest node holds the quickest route to a final destination through false advertising of superior connectivity which leads source nodes astray. The blackhole node acts as a data poisoner by ignoring packets so that data loss and network outage and packet delay occur [3]. The absence of route authentication prior to establishing a path makes AODV extremely exposed to Black Hole Attacks. Protecting real-time VANET-based applications from security threats has become essential because their widespread implementation in actual scenarios. The combination of cryptographic mechanisms and rule-based anomaly detection systems fails to deliver sufficient performance for VANETs because they cause expensive computations and high topology changes and cannot benefit from centralized control [4]. Without a central administrator in VANETs it becomes challenging to implement traditional security methods. Research groups have implemented advanced machine learning (ML) and deep learning (DL) systems to detect and stop Blackhole Attacks on VANETs because the previous methods failed to solve the existing limitations. Scientists use Deep Neural Networks (DNNs) as their top choice for detecting malware and patterns because they excel at precise detection. The IDS system powered by a DNN inspects network traffic patterns to identify suspicious activity which can foresee Blackhole Attacks [5].

DNN models surpass traditional rule-based systems by acquiring new attack patterns which leads to high effectiveness in securing VANET communication. Clustering-based routing protocols represent another method

to enhance security for VANET routing protocols as described in [6]. The process of grouping vehicles based on shared characteristics improves both network performance and resource utilization under the concept known as clustering. A VANET that implements clustering methodology allows Cluster Heads to handle data exchange pathways while enabling them to transfer information securely with other CHs or gateway nodes. Trust-based clustering approaches establish the ability to detect suspicious nodes during segregation processes which subsequently denies entry to BHAs [7]. Available solutions fail to resolve VANET routing protocol security issues because of adaptive attack methods combined with temporary vehicle network characteristics. The research creates a safety protocol for VANET to detect and fight blackhole attacks effectively with minimal performance degradation.

Novelty and contribution,

- A Discrete Hopfield Neural Network with Termite Alate Optimization (DHNN-TAO) serves as the proposed method which detects and stops black hole attacks in VANETs through secure data transmission.
- The mountaineering team-based optimization (MTBO) algorithm dynamically makes stable clusters which improve network structure and decrease overhead in VANET environments.
- Through its DHNN-based intrusion detection system the network successfully detects black hole attacks along with minimizing false positives to safeguard network security.
- The optimization method referred to as TAO enhances the learning potential of DHNN along with its ability to handle different VANET scenario changes.
- The implementation of Light Spectrum Optimizer (LSO) creates the most secure routing channels by lowering delay while boosting packet delivery ratio.
- DHNN-TAO has been developed to enhance network stability and performance with reduced attack effects while boosting both throughput and latency and success ratio of packets in VANETs.

The framework of the research study is as follows: Brief reviews of the most recent studies on the topic are given in Section 2. Additional information regarding the methods employed is given in the third part of the paper. Some examples of the circumstances that arise out of applying the proposed techniques are given in Section 4. Argument in favor of the outcome of the study is given in Section 5.

II. LITERATURE SURVEY

Cluster-Based Wireless Sensor Network and Variable Selection Ensemble Machine Learning Algorithms (CBWSN_VSEMLA) is an attack detection framework in Wireless Sensor Networks (WSNs) proposed by Ayuba John et al. [8] in 2024. FCM clustering is employed in the CBWSN model to remove the single node effects, and the optimal number of clusters is determined using fuzzy coefficient partitioning (FCP). To detect grayhole, blackhole, flooding, and scheduling threats, Variable Selection Ensemble Machine Learning Algorithm (VSEMLA) applies Bagging, LogitBoost, and Random Forest with Principal Component Analysis (PCA) for feature selection. Nevertheless, the model's low ability to adapt to evolving threats, high computational complexity due to FCM, and high data loss through PCA are its limitations.

In 2022, Gebrekiros Gebreyesus Gebremariam et al. [9] presented a Security Localization using Optimized Multilayer Perceptron Artificial Neural Network (MLPANN) detection and localization framework for attacks. The model tracks and identifies malicious nodes by combining machine learning and localization approaches. The target field is simulated by a hierarchical structure of beacon, sensor, and malicious nodes. The suggested strategy works well in large-scale WSNs. But there are drawbacks, such as difficulties with scalability, computing complexity, and flexibility in response to changing attack type.

In 2022, Shereen Ismail et al. proposed a lightweight ensemble-based machine learning approach, Weighted Score Selector (WSS), for cyber-attack detection. WSS dynamically promotes the most effective supervised classifier to improve detection performance efficiently. The approach was compared against Boosting-based, Bagging-based, and Stacking-based ensemble techniques, evaluating various performance metrics. The results highlight WSS's effectiveness in optimizing detection speed and accuracy. However, limitations include computational overhead, dependency on classifier diversity, and potential challenges in real-time adaptability. Future enhancements could focus on reducing model complexity, improving robustness against evolving attacks, and optimizing resource efficiency for better security.

In 2024, Ayyasamy Pushpalatha et al. [11] suggest an Optimized Memory Augmented Graph Neural Network-based DoS Attack Detection. The model utilizes the WSN-DS dataset for training. A secure adaptive event-triggered filter is employed for data preprocessing, handling negation and stemming. A nested patch-based feature extraction method is then applied to obtain optimal features, which are fed into MAGNN for classifying blackhole, flooding, grayhole, scheduling, and normal traffic. The weight parameters of MAGNN are optimized using gradient-based optimizers to improve accuracy. Limitations include computational complexity, potential overfitting due to feature extraction, and reliance on dataset quality.

A. Problem statement

In Vehicular Ad Hoc Networks (VANETs), homogeneous and heterogeneous nodes are quite dynamic in nature, so secure and efficient data transfer becomes a necessity. Routing efficiency is usually impaired by unreliable intermediary nodes, insecure routes, and packet delay. Moreover, mobility and hop count issues also impact the smooth flow and reception of information. VANETs are also susceptible to many security attacks such as Distributed Denial of Service (DDoS) attacks, flooding attacks, and black hole attacks. In the case of a black hole attack, an attacker node misadvertises a best path, catching and discarding packets rather than forwarding them. Consequently, the information vanishes, resulting in substantial disruption in communication and lowering overall network performance.

III. PROPOSED METHODOLOGY

Secure routing in VANETs receives improvements through the DHNN-TAO method which enables efficient black hole attack response. MTBO generates strong clusters

to enable optimal network organization as the initial procedure of the method. The identification of black hole attacks by Discrete Hopfield Neural Network (DHNN) begins after clustering is achieved through the network. The Termite Alate Optimization (TAO) algorithm improves DHNN hyperparameters through optimization to enhance performance during environmental change. The Light Spectrum Optimizer (LSO) serves as the last component which selects secure routes for data transmission with maximum security and minimized interruption to VANET communications. The proposed architecture structure appears as figure 1.

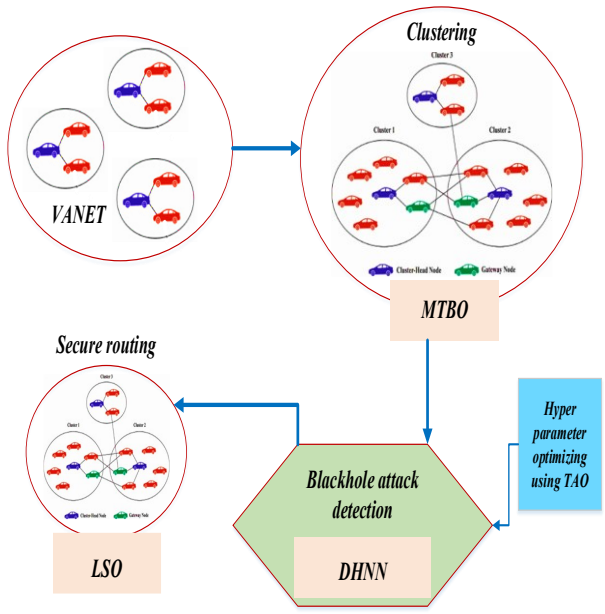


Figure.1.Proposed DHNN-TAO architecture

A. Clustering using Mountaineering Team-Based Optimization (MTBO)

Efficient clustering reduces expenses and enhances network stability in a VANET by ensuring reliable communication. Inspired by the synchronized movement of a mountaineering team in an attempt to climb a summit, the Mountaineering Team-Based Optimization (MTBO) [12] algorithm provides a dynamic clustering approach. Here, the cluster objective is alike achieving optimal network structure with less interference and high connection, and every vehicle in the VANET is equivalent to a climber. The cluster members (CMs) are directed toward an optimum structure by the cluster head (CH), which represents the optimum solution in a specific iteration.

a. Cluster Formation

Being the leader of the team, the most experienced climber leads the others to the summit of the mountain. The cluster head (CH) is the leader in VANET clustering and is selected based on attributes including excellent connection, minimum mobility, and optimal communication range. Every vehicle (mountaineer) j that is begun from Y_j moves toward the cluster head Y_{CH}, per equation (1).

$$Y_j^{new} = Y_j + rand \times \left(Y_{CH} - Y_j\right) \quad (1).$$

where the current location of vehicle j is represented by Y_j. The position of the cluster head is denoted by Y_{CH}. It is guaranteed to exhibit stochastic behavior as $rand$ is a random number between 0 and 1. Each vehicle is additionally affected by its closest neighbor, as per equation (2), ensuring smoother clustering.

$$Y_j^{new} = Y_j + rand \times \left(Y_{CH} - Y_j\right) + rand \times \left(Y_{jj} - Y_j\right) \quad (2).$$

where the position of the closest neighboring car in the cluster is denoted by Y_{jj}. The movement probability in this phase, guarantees that every vehicle has a specific possibility of adhering to the clustering procedure.

b. Mobility and Cluster Instability

A climbing team may experience mobility difficulties due to natural disasters as avalanches. Similarly, problems like channel fading, sudden disconnections, and excessive vehicle movement can lead to cluster instability in VANETs. To simulate these interruptions, a vehicle with connection issues (such as an avalanche) will move away from the worst position Y_{worst} or an affected region $Y_{avalanche}$, according to equation (3).

$$Y_j^{new} = Y_j - rand \times \left(Y_{avalanche} - Y_j\right) \quad (3).$$

where $Y_{avalanche}$ stands for the location of a node that has either weak connection or significant mobility. Rand guarantees a random departure from the impacted area.

c. Cluster Stability Improvement

One of the main characteristics of MTBO is cooperative conduct, in which mountaineers help stranded colleagues. Cooperation techniques in VANET clustering assist unstable nodes in regaining stable connection by aligning with the average location (Y_{team}) of the cluster. This behavior may be explained by equation (4).

$$Y_j^{new} = Y_j + rand \times \left(Y_{team} - Y_j\right) \quad (4).$$

where, to ensure stability, Y_{team} stands for the average position of the cars in the cluster.

d. Cluster Member Reassignment

A climber might not survive a disaster in extreme circumstances. Comparably, with VANET clustering, a vehicle that leaves the cluster or loses connectivity is swapped out for a new vehicle that enters the coverage area. The random start of this new member inside the network range is explained by equation (5).

$$Y_j^{new} = Y\left(Y_{\max} - Y_{\min}\right)_{\min} \quad (5).$$

where the bounds of the network are defined by $Y_{\max}$ and $Y_{\min}$. In this stage, the high mobility of VANETs is dynamically adjusted to preserve cluster stability. Once the clusters are constructed, the next step is to make the resistant to possible Blackhole assaults.

B. Blackhole attack detection using Discrete Hopfield Neural Network (DHNN)

The Discrete Hopfield Neural Network (DHNN) [13] is used to detect Blackhole attacks by analyzing the node activity inside each cluster after cluster development. The DHNN illustrates the attack detection problem as an optimization process, where each neuron represents a network node and its state is iteratively updated to identify nodes as either normal nodes or Blackhole nodes. Every node j in the network has a neuron with state T_j that is updated by synaptic weights $X(j,k)$and a threshold ρ_j. The updating rule is defined in equation 6).

$$T_j = \begin{cases} if \sum_{k}^{o} X_{(j,k)} T_k \geq \rho_j & 1 \\ otherwise & -1 \end{cases} \quad (6).$$

where $T_j = 1$ represents a normal node. The representation of the malignant Blackhole node is $T_j = -1$ displays the trust weight between nodes i and j. For best result ρ_j, the decision threshold, is set at 0. During the detection phase, a cost function $F_{\Gamma_{s2\text{Satisfiability}}}$ guides the network to stabilize in an optimal state, as shown in equation (7).

$$F_{\Gamma_{S2\text{Satisfiability}}} = \sum_{j=1}^{\lambda} \prod_{k=1}^{v+w} r_{jk} \quad (7).$$

where the misclassification error in attack detection is represented by $F_{\Gamma_{s2\text{Satisfiability}}}$. The number of node-to-node connections, or constraints, is denoted by λ. r_{jk} determines if a node satisfies a particular trust criterion. $F_{\Gamma_{s2\text{Satisfiability}}} = 0$, the network has correctly classified each node. If not, neurons continue to update until they reach a stable state. The effect of neighboring neurons on the state update of each neuron is determined by the local field equation (8).

$$i_j(u) = \sum_{k=1, j=k}^{v+w} X_{(j,k)}^{(2)} T_k + X_{(j)}^{(1)} \quad (8).$$

where $i_j(u)$is the local field that affects neuron j at time u. In neurons j and k, the higher-order weight is $X_{(j,k)}^{(2)}$. The bias reflected by $X_{(j)}^{(1)}$is based on prior trust values. Neurons utilize Hyperbolic Tangent Activation Function (HTAF) to update the states to ensure non-linear attack classification, as explained in equation (9).

$$T_j(u) = \begin{cases} \tan i(i_j) \geq 0 & 1 \\ otherwise & -1 \end{cases} \quad (9).$$

where the decision boundary for categorizing Blackhole nodes is controlled by $\tan i(i_j)$. When the network achieves a stable state, the Lyapunov energy function makes sure that malicious nodes are accurately detected in equation (10).

$$M_{\Gamma_{2\text{Satisfiability}}} = -\frac{1}{2} \sum_{j=1, j\neq k}^{o} \sum_{k=1, k\neq j}^{o} X_{(j,k)}^{(2)} T_j T_k - \sum_{j=1}^{o} X_{(j)}^{(1)} T_j \quad (10).$$

where a stable categorization is indicated by a low $M_{\Gamma_{s2\text{Satisfiability}}}$. Neurons keep updating if $T_j T_k$ is high until stability is reached. To improve neuron state convergence and classification accuracy, Termite Alate Optimization (TAO) is used to adjust the hyperparameter ($M_{\Gamma_{S2}}$) of the Discrete Hopfield Neural Network (DHNN).

C. Hyper parameter optimizing using Termite Alate Optimization (TAO)

The hyper parameter ($M_{\Gamma_{S2}}$) in Deep Hopfield Neural Networks (DHNN) regulates learning rate adjustments, weight stability, and synaptic regularization. To maximize this, Termite Alate Optimization (TAO) [14] replicates termite dispersal behavior so that there is a balance between exploitation and exploration. The swarm behavior of flying termites where individuals venture into the new region while remaining in touch with the group is what inspires TAO. With its best knowledge and global expertise, every termite modifies its position. Through adjusting movement dynamics, the algorithm achieves a trade-off between exploitation and exploration to ensure optimal ($M_{\Gamma_{S2}}$) tuning. Reduction of loss is employed in fitness determination, and the process is iterated until a stopping condition is met. Through improved generalization, minimization of errors, and optimization of learning efficiency, the technique enhances DHNN performance. The TAO process is described in algorithm 1.

Algorithm 1: TAO
Initialize termite alates with random values of ($M_{\Gamma_{S2}}$) within a defined range
Evaluate fitness of each termite alate using the DHNN model
Set the brightest (best) and darkest (worst) termite alates based on fitness
For each iteration until $\max\_itr$ or convergence:
For each termite alate j :
Select the best (brightest) and worst (darkest) termite alates
Generate random factors r1 and r2 in range [0,1]
Update position of termite alate using:

$alate_j^{\mu+1} = alate_j^{\mu} + s_1\left(alate_{best}^{\mu} - alate_j^{\mu}\right) - s_2\left(alate_{worst}^{\mu} - alate_j^{\mu}\right)$
Ensure($M_{\Gamma_{S2}}$) is within valid boundaries (clamping)
Evaluate fitness of updated termite alates
Sort alates based on fitness
Perform elimination process:
Remove (pe) of worst-performing termite alates
Replace them with new alates in brighter regions:
$alate_{new} = alate_b + \beta\left(alate_c - alate_d\right)$
Ensure new alates remain within valid boundaries
Update the brightest and darkest termite alates
Check stopping criteria (max_itr or minimal fitness change)
Return the best value

D. Secure Routing using Light Spectrum Optimizer (LSO)

The secure routing path is established by the Light Spectrum Optimizer (LSO) [15], which simulates the refraction and dispersion of light rays, once blackhole assaults in VANET have been detected. Initialize the routing paths using a randomized dispersion model to explore several secure routes. Potential pathways are shown in equation (11).

$$\vec{y}^{0} = mc + SW_1\left(vc - mc\right) \tag{11}.$$

The initial candidate secure routing path is indicated by y^0 . The lower and upper boundaries of the potential routing space are denoted by mc , vc. In order to ensure equitable investigation of potential pathways, SW_1 denotes a random variable between 0 and 1. Normal vectors derived from secure pathways are used by each vehicle to fine-tune its routing direction. These vectors aid in determining the optimal course, as shown in equations (12), (13), and (14).

$$\vec{y}_{oB} = \vec{yu8i}_u^s / norm\left(\vec{y}_u^s\right) \tag{12}.$$

$$\vec{y}_{oC} = \vec{y}_u^q / norm\left(\vec{y}_u\right) \tag{13}.$$

$$\vec{y}_{oD} = \vec{y}^{*} / norm\left(\vec{y}^{*}\right) \tag{14}.$$

The Normalized vector for a path free of random attacks is denoted by y_{oB} . The Normalized vector for the current vehicle's routes is displayed by y_{oC} . The normalized vector of the best secure route in the world is denoted by y_{oD} . The magnitude (norm) of the vector is indicated by the notation y_u^s, which ensures normalization to unit length. Following that, the mean secure path for every vehicle in the VANET is determined using equation (15).

$$Y_{mean} = \frac{\sum_j^O \vec{y}_j}{O} \tag{15}.$$

The average of all unattacked paths is denotes as Y_{mean} . y_j is utilized for the final normalized mean secure route. The light refraction and reflection model dynamically adjusts the trajectory after calculating possible pathways. The refractive index may be dynamically adjusted using equation (16).

$$l^s = l^{red} + SW_1\left(l^{violet} - l^{red}\right) \tag{16}.$$

For refraction changes informed by the light spectrum, l^{red} , l^{violet} denotes the predefined bounds. SW_1 represents the random variable that secures adaptive changes in routing direction. Continuous adaptation is ensured by dynamically changing the routing path using equation (17).

$$\vec{y}_{u+1} = \vec{y}_u + \varepsilon SW_2^o HJ\left(\vec{y}_{M2} - \vec{y}_{M3}\right) \times \left(\vec{y}_{s3} - \vec{y}_{s4}\right) \tag{17}.$$

The routing path at that moment is denoted by y_u . The scaling factor governing the transition to an attack-free route is shown by ε . The exploration term, HJ makes sure the algorithm stays out of local optima. The randomized reference points impacting route adaptation are indicated

by y_{M2}, y_{M3}, y_{s3}, and y_{s4}. The LSO-based routing dynamically chooses safe routes in VANETs by simulating the dispersion, refraction, and reflection of light. In order to prevent blackhole assaults and guarantee effective communication, it assesses several routes and modifies direction vectors. In vehicle networks, this flexible strategy improves dependability, reduces latency, and maximizes security.

IV. RESULT

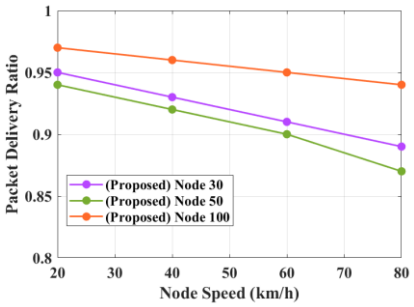
The proposed DHNN-TAO secure routing mechanism for VANET was simulated with the NS3 simulator. The simulation was performed on the Intel Core i5 processor (3.0 GHz) having 8GB RAM. The network environment was 1000 x 1000 m, and the simulation time was 1000 seconds. The packet size was 1024 bits, and the number of nodes was 30, 50, and 100. The transmission range was kept at 250 meters to analyze the effectiveness of the proposed framework in black hole attack detection and prevention.

A. Dataset description

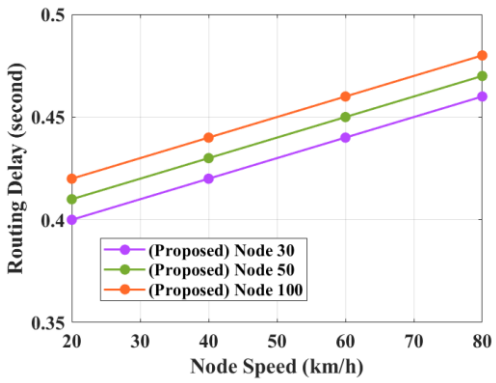
Black hole attacks form the subject of this research which employed WSN-DS dataset obtained from Kaggle. The dataset contains 18 essential elements for spotting attacks that include multiple characteristics from both network and node domains. All network features serve an essential role when analyzing both network patterns and black hole attack behaviors. Through the utilization of these features the study successfully detects attacks during thorough examination of trend patterns. The database allows researchers to conduct exhaustive testing about the black hole attack vulnerabilities of VANETs together with DHNN-TAO secure routing protocol behavior.

B. Performance analysis

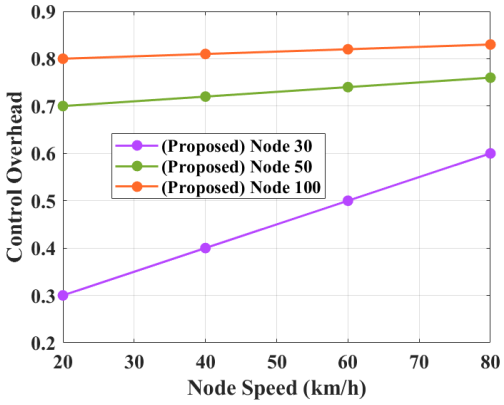
The proposed DHNN-TAO method receives evaluation against CBWSN_VSEMLA [8], MLPANN [9], WSS [10], and MAGNN [11] performance testing. Major performance indicators including routing delay, execution time, accuracy, packet delivery ratio and control overhead determine the basis for comparison. The research discusses how the suggested method increases network efficiency and security in VANETs. Experimental results prove improvements in packet delivery and minimized delay over conventional methods.



(a)



(b)



(c)

Figure.2.Proposed (a) Packet delivery ratio (b) Routing delay (c) Control overhead

The performance assessment of the given DHNN-TAO solution for VANETs in terms of Packet Delivery Ratio (PDR), Routing Delay, and Control Overhead using varying node velocity (20–80 km/h) and number of nodes (30, 50, and 100) is represented through figure 2. In Figure 2(a), the PDR decreases as node speed increases. For 30 nodes, it drops from 0.96 at 20 km/h to 0.86 at 80 km/h, while for 50 nodes; it declines from 0.97 to 0.87, and for 100 nodes, from 0.98 to 0.89. Figure 2(b) shows that the routing delay rises with speed; for 30 nodes, it increases from 0.38s to 0.44s, for 50 nodes, from 0.39s to 0.46s, and for 100 nodes, from 0.40s to 0.48s. Lastly, Figure 2(c) indicates an increase in control overhead with node speed. For 30 nodes, it rises from 0.3 to 0.5, for 50 nodes, from 0.6 to 0.7, while for 100 nodes, it remains around 0.8 to 0.85.

TABLE I. PERFORMANCE COMPARISON OF THE PROPOSED DHNN-TAO METHOD WITH EXISTING APPROACHES

Method	Throughput (kbps)	Routing Delay (s)	Execution Time (ms)	Accuracy (%)	Packet Delivery Ratio	Control Overhead
CBWSN_VSEMLA	1250	0.65	12.5	91.2	0.85	0.75
MLPANN	1345	0.58	10.8	93.5	0.88	0.71
WSS	1400	0.55	9.7	94.8	0.90	0.69
MAGNN	1485	0.50	8.9	96.3	0.92	0.65
Proposed DHNN-TAO	1600	0.42	7.4	99.1	0.96	0.59

Table 1 presents the performance comparison of the proposed DHNN-TAO method with existing approaches, including CBWSN_VSEMLA, MLPANN, WSS, and MAGNN. The proposed DHNN-TAO achieves the highest throughput of 1600 kbps, outperforming MAGNN (1485 kbps) and CBWSN_VSEMLA (1250 kbps). It also minimizes routing delay to 0.42s, compared to MAGNN (0.50s) and CBWSN_VSEMLA (0.65s). The execution time is significantly lower at 7.4 ms, whereas WSS and MAGNN have 9.7 ms and 8.9 ms, respectively. Additionally, accuracy reaches 99.1%, surpassing MAGNN (96.3%) and MLPANN (93.5%). The packet delivery ratio is 0.96, compared to WSS (0.90) and CBWSN_VSEMLA (0.85). Finally, DHNN-TAO reduces control overhead to 0.59, demonstrating its efficiency over MAGNN (0.65) and CBWSN_VSEMLA (0.75).

V. CONCLUSION

The suggested DHNN-TAO framework improves VANETs secure routing by resisting black hole attacks via an improved clustering and detection mechanism. The MTBO algorithm effectively constructs stable clusters, facilitating well-organized network management. The DHNN detects black hole attacks effectively by detecting malicious nodes, with the hyperparameters optimized via TAO, improving adaptability in dynamic environments. Secure routing is attained via the LSO, which identifies optimal paths, guaranteeing safe data transmission. The suggested approach reaches 1600 kbps throughput, 0.42s routing delay, 7.4ms execution time, 99.1% accuracy, 0.96 packet delivery ratio, and 0.59 control overhead, showcasing superior performance. Main benefits are high accuracy, low delay, and enhanced network security. The results prove that DHNN-TAO is a valid solution for protecting vehicular networks. Nevertheless, computational complexity is still a drawback, affecting real-time implementation. Future research will be directed towards identifying other threats like Sybil and wormhole attacks, improving computational efficiency, and extending the framework to 5G-enabled VANETs.

REFERENCES

[1] A. Amalia, Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "A deep-learning-based secure routing protocol to avoid blackhole attacks in VANETs," Sensors (Basel), vol. 23, no. 19, p. 8224, Oct. 2 2023. DOI: 10.3390/s23198224

[2] R. K. Dhanaraj, S. H. Islam, and V. Rajasekar, "A cryptographic paradigm to detect and mitigate blackhole attack in VANET environments," Wirel. Netw., vol. 28, no. 7, pp. 3127–3142, 2022. DOI: 10.1007/s11276-022-03017-6

[3] S. Younas, F. Rehman, T. Maqsood, S. Mustafa, A. Akhunzada, and A. Gani, "Collaborative detection of black hole and gray hole attacks for secure data communication in VANETs," Appl. Sci. (Basel), vol. 12, no. 23, p. 12448, 2022. DOI: 10.3390/app122312448

[4] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal, and G. Mehmood, "An efficient approach for the detection and prevention of gray-hole attacks in VANETs," IEEE Access, vol. 11, pp. 46691–46706, 2023. DOI: 10.1109/ACCESS.2023.3274650

[5] G. Kaur and D. Kakkar, "Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET," Ad Hoc Netw., vol. 136, p. 102961, 2022. DOI: 10.1016/j.adhoc.2022.102961

[6] M. Yazdanypoor, S. Cirillo, and G. Solimando, "Developing a Hybrid Detection Approach to Mitigating Black Hole and Gray Hole Attacks in Mobile Ad Hoc Networks," Appl. Sci. (Basel), vol. 14, no. 17, p. 7982, 2024. DOI: 10.3390/app14177982

[7] M. S. Azhdari, A. Barati, and H. Barati, "A cluster-based routing method with authentication capability in Vehicular Ad hoc Networks (VANETs)," J. Parallel Distrib. Comput., vol. 169, pp. 1–23, 2022. DOI: 10.1016/j.jpdc.2022.06.009

[8] A. John, I. F. B. Isnin, S. H. H. Madni, and M. Faheem, "Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms," Intell. Syst. Appl., vol. 22, p. 200381, 2024. DOI: 10.1016/j.iswa.2024.200381

[9] Emayavaramban, G., Divyapriya, S., Mansoor, V. M., Amudha, A., Ramkumar, M. S., Nagaveni, P., & SivaramKrishnan, M. (2021). SEMG based classification of hand gestures using artificial neural network. *Materials Today: Proceedings*, *37*, 2591-2598.

[10] G. G. Gebremariam, J. Panda, and S. Indu, "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network," Wirel. Commun. Mob. Comput., vol. 2023, no. 1, p. 2744706, 2023. DOI: 10.1155/2023/2744706

[11] S. Ismail, Z. El Mrabet, and H. Reza, "An ensemble-based machine learning approach for cyber-attacks detection in wireless sensor networks," Appl. Sci. (Basel), vol. 13, no. 1, p. 30, 2022. DOI: 10.3390/app13010030

[12] A. Pushpalatha, S. Pradeep, M. V. Pullarao, and S. Sankar, "Optimized memory augmented graph neural network-based DoS attacks detection in wireless sensor network," Network, vol. •••, pp. 1–27, Oct. 28 2024. DOI: 10.1080/0954898X.2024.2392786

[13] I. Faridmehr, M. L. Nehdi, I. F. Davoudkhani, and A. Poolad, "Mountaineering team-based optimization: A novel human-based metaheuristic algorithm," Mathematics, vol. 11, no. 5, p. 1273, 2023. DOI: 10.3390/math11051273

[14] S. S. Muhammad Sidik, N. E. Zamri, M. S. Mohd Kasihmuddin, H. A. Wahab, Y. Guo, and M. A. Mansor, "Non-systematic weighted satisfiability in discrete hopfield neural network using binary artificial bee colony optimization," Mathematics, vol. 10, no. 7, p. 1129, 2022. DOI: 10.3390/math10071129

[15] A. Majumder, "Termite alate optimization algorithm: A swarm-based nature inspired algorithm for optimization problems," Evol. Intell., vol. 16, no. 3, pp. 997–1017, 2023. DOI: 10.1007/s12065-022-00714-1

[16] M. Abdel-Basset, R. Mohamed, K. M. Sallam, and R. K. Chakrabortty, "Light spectrum optimizer: A novel physics-inspired metaheuristic optimization algorithm," Mathematics, vol. 10, no. 19, p. 3466, 2022. DOI: 10.3390/math10193466