Cyber Security Protection in Roadside Unit Based on Cross-Layer Adaptive Graph Neural Networks (Gnns) in Vanet

Raj Kumar[1*], Sakshi Pandey[2], Asha KS[3], Rakesh Kumar Yadav[4], Abhinav Mishra[5], Sunil Sharma[6]
[1]Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India
[2]Centre of Research Impact and Outcome, Chitkara University, Rajpura- 140417, Punjab, India
[3]Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bangalore, Karnataka, India
[4]Associate Professor, Maharishi School of Engineering & Technology, Maharishi University of Information Technology, Uttar Pradesh, India
[5]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh-174103 India
[6]Assistant Professor, Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, India
Emails: raj.kumar@atlasuniversity.edu.in; sakshi.pandey.orp@chitkara.edu.in; ks.asha@jainuniversity.ac.in; rkymuit@gmail.com; abhinav.mishra.orp@chitkara.edu.in; sunil.sharma@vgu.ac.in

Abstract

The proposed systems can improve cyber security in VANET applications by enabling efficient detection of complex attacks on the RSU component. The subsequent sections discuss the systems that are applied and support the suggestions for improving the VANET trustworthiness. VANETs and show that the utilization of Cross-Layer Adaptive GNNs can improve cyber security and LEARNING in VANET-based RSUs. As a result, the suggested system can provide robust ways for detecting cyber-attacks by: modeling the network architecture using graphs while combining information regarding several protocol layers to detect complicated interactions between the network entities and find the abnormal activities. the nature of the GNN enables it to update in real-time by adapting to the evolving attack patterns and the shifting network conditions, making them sturdy and flexible defense ways for cyber security. The proposed network e systems can efficiently detect multiple cyber threats and focus on reducing the number of false positives while maintaining low computation costs. Therefore, chances are that incorporating the Cross-layer adaptive GNNs into the RSUs can improve cyber security in VANETs, enhancing the robustness and reliability of prospective smart transportation systems.

Keywords: VANET; Roadside units (RSUs); Cyber security; Graph Neural Networks (GNNs); Cross-layer adaptation; Intrusion detection.

1. Introduction:

Vehicular Ad Hoc Networks : a crucial element of future intelligent transportation systems, VANETs [1] are supposed to let vehicles and infrastructure communicate smoothly, thus enhancing road safety, traffic effectiveness, and passenger comfort. RSUs are critical nodes in vehicular area networks because they serve as a mediator between mobile vehicles, allowing them to exchange data, delivering transport services. Nonetheless, ensuring secure cyber protection with VANET networks is much more challenging than with any other due to their open-nature and dyadic . Communication reliability, passenger safety, and transport services are disrupted when cyber threats target VANETs. Although protocols for identification and encryption are necessary, current protections such as authentication and encryption may fail due to the ever-changing cyber-attack landscape. The issue is even more complex with decentralized and various traffic regularities limiting intrusion and threat mitigation developments. To solve these issues, a new safeguarding approach from cyber threats for RSUs in VANET settings based on Cross-layer adaptive

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

Graph Neural Networks is proposed. Our proposed system employs GNNs to represent more complex relationships in protecting integrated networks and use a more intelligent interpretation rule than prior efforts Investigation proceeds in guarding networks that are heterogenous and hierarchal in nature . The proposed architecture enhances the RSUs' safeguarding capacities, making it usable in security-driven network designs. The cross-layer adaptable GNN-based safeguarding allows the framework to analyse network traffic thoroughly, accounting for the spatial and temporal dependencies are pre-installed in VANETs. Considering information from several protocol layers based on a graph view of network architecture, the devised system will identify abnormalities that usually indicate cyber assaults. Furthermore, the GNN structure's dynamism allows it to rapidly respond to network changes and deviation patterns . Therefore, the results guarantee that safeguarding measures are secure and thus flexible.

Vehicular Ad Hoc Networks are "a key element of modern transportation networks" that "allow vehicles to communicate with each other and their surroundings flawlessly" . Unfortunately, there are considerable barriers to implementing strong cybersecurity protections in VANETs, particularly in RSUs. This study introduces a revolutionary means of increasing the cybersecurity of RSUs among VANETs using Cross-layer Adaptive Graph Neural Networks , which aims to enhance current intrusion detection capabilities and reduce security risks by collecting information from multiple network layers and using GNNs. Specifically, a high-level discussion of how the decentralized and always-evolving nature of VANETs creates problems, as well as the proposed system's features and organization, will be provided. Consequently, the field of VANETs cybersecurity has "unearthed" new ground thanks to this paper. We present a novel method "for safeguarding RSUs through the utilization of Cross-layer adaptive GNNs" . Our system, which combines data collection at various network levels with dynamic network adaptation, provides comprehensive intrusion detection and suppression capabilities. We show that this method may achieve high levels of identification for a wide range of cyber hazards with a low computational impact and a modest level of false positives. As a result, the recommendations in this study have improved the present knowledge concerning cybersecurity in VANETs. This analysis presents the construction and deployment of a cross-layer adaptive GNN system intended to protect RSUs from cyber threats in VANETs. We demonstrate that it can detect various types of cyber threats with minimal computational overhead and a modest level of false positives via thorough testing and simulations. Finally, we propose future research directions to improve cyber-security in VANETs, including utilizing Cross-layer adaptive GNNs

2. Research gaps and Existing works

There are many proposed techniques to defend VANETs against cybercriminals. Intrusion detection systems aid in the localization and quarantining of infected nodes on a network that utilize signature-based identification, which is the most common method of a traditional intrusion detection system. Messages inundated into the network are matched to a database that has been precompiled with identified patterns of assault. On a regular basis, specialists would have to update their catalog of recognized threat signatures and constantly retrain the system to adapt to new threats . A related literature review shows that various published works are focusing more on the cyber hardening of VANETs, particularly RSUs. The published articles study several methods from intrusion detection to privacy preservation and attack resistance of cyber security issues. A handful of studies have looked at the usage of approaches based on AI and machine learning methods. A method based on deep learning that uses the spatial and temporal properties of the network traffic is proposed [10] to detect malicious behavior that hints towards a cyber-attack. Similarly, RSUs could use a reinforcement learning framework developed for this precise goal to alter the defense mechanism in response to observing the network state and attack type . Cross-layer adaptation, which combines data from various layers of the network and vehicle dynamics could substantially hardened the cyber defense of VANETs. In one experiment run by [12] was able to improve intrusion detection by RSUs using data from communication and vehicle dynamics . A fresh design by [13] was proposed to blend graph-based modeling with cross-layer adaptation in order to comprehend the intricate nature of relationships and dependencies in VANETs.

Moreover, there are studies covering works on their efficiency and scalability . For instance, to increase efficiency and lower the computational cost, distributed design of cyber-security in a VANET environment, based on the idea of computation offloading from the cloud to edge nodes, was provided by . Also, a light intrusion detection approach was proposed in which neither decreases the certainty of detection in RSUs nor improves resource utilization. Fieldwork and simulations will still play a critical role in the identification of cyber security solutions in the real world. For instance, conducted a comprehensive series of validation experiments to demonstrate the validity of their intrusion

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

detection system in RSUs. Another case scenario is presented in , where a simulation of different scenarios of deployment was made to confirm the stability and scalability of their cross-layer adaptive system. In conclusion, the existing studies reveal many approaches to detecting cyber threats in VANETs, primarily centered on RSUs . However, expanding on past studies and benefiting from advances in learning, cross-layer adaptability, and validation will enable the up-to-date developments in the field to improve the state of the art of cyber security for future smart transportation information systems. Confidentiality and data integrity can be assured via cryptographic methods, such as digital signatures and encryption, during data transfer . These techniques, however, require additional processing power and may be deficient in opposition to refined poison attack that targets network protocols or alters path finding. Recent research has begun to explore Anomaly Detection techniques based on Machine Learning . Such algorithms can establish over time which networks behave in a way that is unusual. Standard ML algorithms struggle with the complex network interrelationships between vehicles and RSUs because the architecture of VANETs is constantly changing.

Given that in graphs, nodes are entities, and edges are the relationships linking them, Graph Neural Networks are ideal for analysing such data.

3. Proposed Implementation

In order to provide real-time intrusion detection and threat mitigation, the GNN is incorporated into RSUs [19] and deployed in operational VANET systems after model training and validation. By keeping an eye on metrics like detection accuracy, false positive rate, and response time, as well as conducting ongoing monitoring and evaluation, the framework can be made to detect and mitigate cyber threats efficiently. The success of the framework in dynamic and large-scale VANET scenarios is ensured by applying optimization approaches to boost scalability, efficiency, and adaptability. These measures are part of the planned implementation's effort to make future smart transportation networks more secure and resilient.

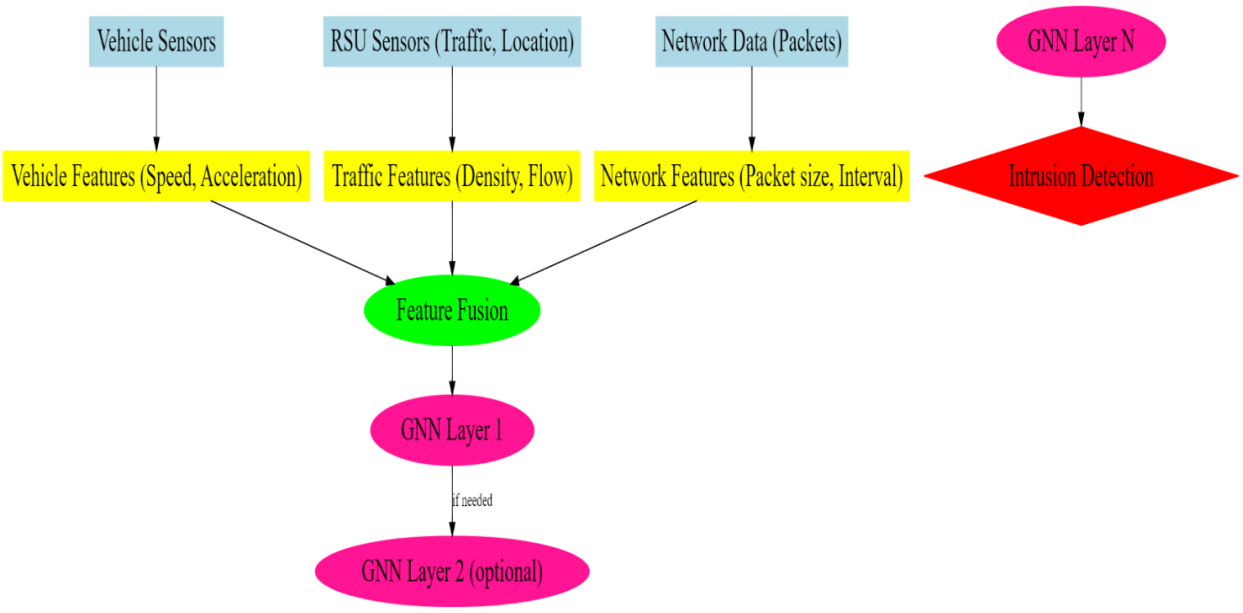

Figure 1: Proposed Block Diagram of CLAGNNs

Initially, a variety of sensors that are embedded in automobiles and RSUs capture information like vehicle dynamics, traffic conditions, and network information. The next step is to preprocess the captured information and extract useful features from them to better understand the data . Subsequently, the extracted features are used to

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

construct a graph, as shown in Fig. The nodes represent vehicles and RSUs and network entities, and the edges signify the connectivity among them. With a graph-based approach, it is simpler to model the VANET topology and communication structure. The following two-steps are to precisely analyze and evaluate the patterns over protocols using a Cross-layer Adaptive Fusion across protocol layers. Utilizing two sources of data enables a final feature representation to accurately interpret the complicated connections between VANETs. The resulting representation is then passed to a multi-layer Graph Neural Network , which employs cross-layer adaptation to continue change its GNN parameters in reply to input from each layer, providing a more accurate prediction of possible dangers. GNNs employ this ongoing process to better identify spatial and temporal relationships in network data, increasing their effectiveness in spotting irregularities and generating stronger intrusion and danger warnings. Lastly, the GNN output is analyzed using complex algorithms in step 8 to identify shadowy cyber risks. As a result, RSUs can take immediate action to secure the network and ensure the stable operation of the VAN connection.

Therefore, by incorporating these steps, CLAGNNs can be implemented within RSUs to boost cyber security and enhance the dependability and resiliency of future smart transportation systems.

3.1 Architecture of CLAGNN Model

The Cross-layer Adaptive Graph Neural Network is a model that addresses the cyber security issues present in Cyber security scenarios in Vehicular Ad Hoc Networks . The model is constructed using graph representation study, cross-layer integration, and Graph Neural Networks . The most basic building block of the CLAGNN is established using a graph representation of a Vehicular Ad Hoc Network in this study. The attributes are expressed as feature vectors that are connected to each node in the context of a given VANET graph. Traffic circumstances, car characteristics, and network data, among other types of data, are examples of feed into embedding vector content. To ensure the ability of the graph to understand nuanced network topology patterns and relationships, these properties are then summed up across neighbors of a particular node through multiple GNN layers..

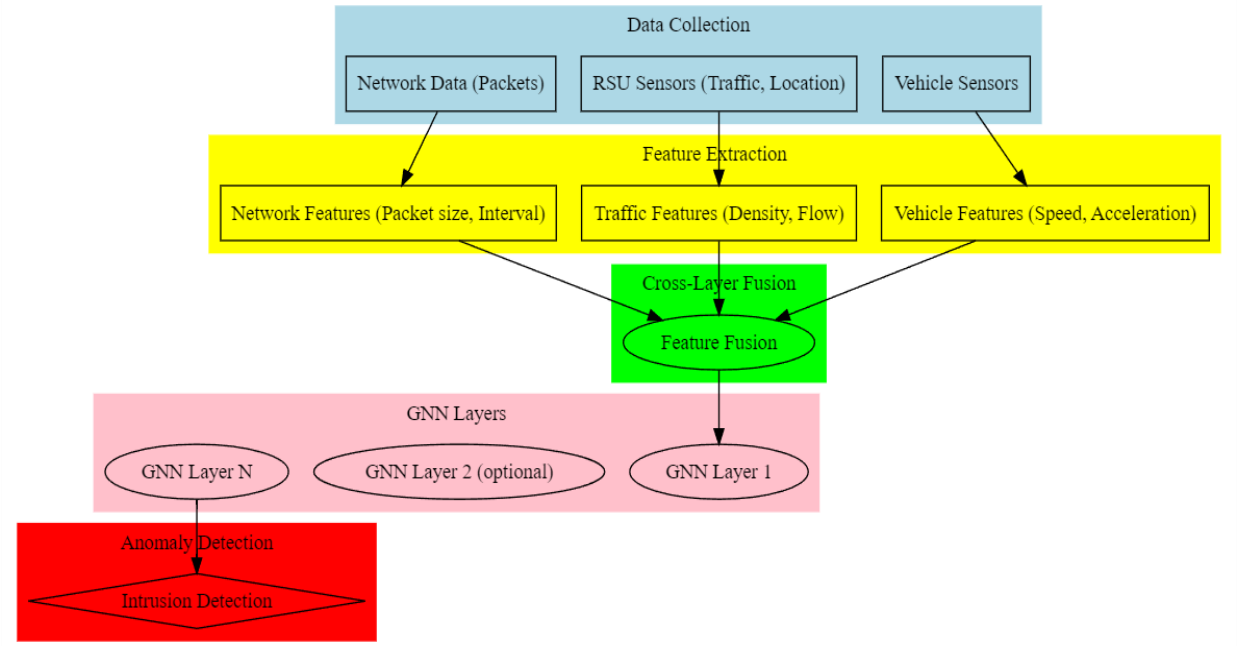

Figure 2: Architecture of CLAGNN Model

Let a VANET be represented as a graph, in which is the set of nodes vehicles, RSUs and is the set of edges communication links. Each node is attached to the feature vector which contains information in terms of vehicle dynamics, traffic, network data. The feature vectors of neighboring nodes are combined to compute the updated node representation::

$$\mathbf{h}_i^{(l+1)} = \sigma\left(\sum_{j \in \mathcal{N}(i)} \mathbf{W}^{(l)} \mathbf{h}_j^{(l)}\right) \quad (1)$$

Combine features from different network layers to create a unified representation:

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

$\mathbf{h}_i^{\text{fuse}} = \text{concat}\left(\mathbf{h}_i^{(0)}, \mathbf{h}_i^{(1)}, \ldots, \mathbf{h}_i^{(L)}\right)$ (2)

Apply a fusion function to integrate features:

$\mathbf{h}_i^{\text{fused}} = f_{\text{fuse}}\left(\mathbf{h}_i^{\text{fuse}}\right)$ (3)

Stack multiple GNN layers to capture increasingly complex relationships:

$\mathbf{h}_i^{(l+1)} = \sigma\left(\sum_{j \in \mathcal{N}(i)} \mathbf{W}^{(l)} \mathbf{h}_j^{(l)}\right)$ (4)

. Each layer applies a transformation to the aggregated neighboring node features and passes them through a non-linear activation function . The final GNN layer's output is represented by the refined node representations..

Utilize the refined node representations to detect anomalies or cyber threats:

$\hat{y}_i = g\left(\mathbf{h}_i^{(L)}\right)$ (5)

Find anomalies or cyber threats: . Apply a classifier to predict the likelihood of a node association with a cyber threat. The labeled data are used to train the CLAGNN, where each node is labeled either normal or anomalous according to the ground truth. 3. Learn the parameters by minimizing a loss function .:

$\min_\Theta \sum_{i=1}^{N} \mathcal{L}(\hat{y}_i, y_i)$ (6)

Common loss functions include binary cross-entropy or categorical crossentropy for multi-class classification. Update model parameters using gradient descent or its variants such as Adam optimization:

$\Theta^{(t+1)} = \Theta^{(t)} - \eta \nabla_\Theta \mathcal{L}$ (7)

Also, using lessen technique such as dropout or L2 Regularization can help to avoid overfitting of the model. The CLAGNN paradigm also includes a cross-layer fusion module; it combines representations by integrating traits from various network levels. This fusion method allows the model to undertake more detailed analysis and achieve greater intrusion detection because it ensures that it obtains information from many different protocol layers. Anomaly detection also employs the enhanced node representation provided by GNN layers. However, while the model makes accurate predictions in activity data analysis, the complex algorithms predict the possibility of each node associating with cyber risk. By optimizing the model parameters to minimize a given loss function, during training specified with label data, the CLAGNN model learns when behavior is normal and abnormal. During iterative training and optimization, the model can learn to improve its threat detection capability and risk reduction in real time, adapting to the dynamic state of VANETs. Generally, since the CLAGNN model provides a robust and easily adaptable arrangement for safeguarding against cyber impacts, it may make smart transportation systems more reliable.

3.2 Intrusion Detection System

The first damage control mechanism that should be in place is an Intrusion Detection System . IDS is designed to help detect and respond to activities that undermined an organizational information system's security. This included intrusion attempts, malwares damage, insider threat and more.

A) Attack Detection Rate

Attack Detection Rate, also referred to as detection accuracy or true positive rate, is a metric that determines how well a cyber security system is able to correctly report instances of cyber-attacks or anomalies . The ratio of actual attacks flagged as attacks by the system to the total number of attacks in the dataset unused equation form:.

The attack detection rate (DR) can be expressed as:

$DR = \frac{TP}{TP+FN}$ (8)

Where:

- TP (True Positives) represents the number of attacks correctly detected by the system.
- FN (False Negatives) represents the number of attacks that are not detected by the system (i.e., missed detections).

A higher attack detection rate implies that the system is properly capable of detecting cyber threats than or the previous model, and a low rate indicates that the system might miss certain attacks, posing security risks . Enhancing the attack detection rate is among the primary goals of developing security systems. It can be done by improving the system in various dimensions, such as choosing the best features, model design, and training approach. Furthermore, the system's performance should be validated in real-world scenarios and tested in various environments to ensure that the method can perform systematically in various attack scenarios.

Algorithm 1 CLAGNN Model Algorithm

Input: Data from vehicle sensors, RSU sensors, and network packets.
Output: Anomalies detected in the VANET.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

1. Data Collection:
   - Collect vehicle sensor data.
   - Collect RSU sensor data (traffic, location).
   - Collect network packet data.
2. Feature Extraction:
   - Extract vehicle features (e.g., speed, acceleration).
   - Extract traffic features (e.g., density, flow).
   - Extract network features (e.g., packet size, interval).
3. Cross-Layer Fusion:
   - Fuse the extracted features from different layers into a unified representation.
4. GNN Layers:
   - Pass the fused features through Graph Neural Network (GNN) layers.
   - Apply transformations and activations within each GNN layer.
5. Anomaly Detection:
   - Detect anomalies using the output features from GNN layers.
   - Employ anomaly detection techniques (e.g., threshold-based, machine learning).
6. Output:
   - Output the detection results indicating the presence or absence of anomalies.

B) Host-based IDS with Cross-layer adaptive Graph Neural Networks (CLAGNNs) :

Integrating Host-based Intrusion Detection Systems (HIDS) with Cross-layer Adaptive Graph Neural Networks (CLAGNNs) presents a promising approach to enhancing cybersecurity in complex and dynamic environments such as Vehicular Ad Hoc Networks (VANETs).

$$X_{host} = \text{concat}\left(X_{logs}, X_{files}, X_{traffic}\right) \quad (9)$$

Features extracted from host-based sources are used as node attributes, forming the initial feature vectors $\left(\mathbf{h}_i^{(0)}\right)$ for each host node.

Graph convolutional layers aggregate information from neighboring hosts to update node representations:

$$\mathbf{h}_i^{(l+1)} = \sigma\left(\sum_{j\in\mathcal{N}(i)} \mathbf{W}^{(l)}\mathbf{h}_j^{(l)}\right) \quad (10)$$

The refined node representations obtained from the CLAGNN layers are fed into a classification module to detect anomalies and intrusions on individual hosts. A classifier (g) assigns a probability score to each host node indicating the likelihood of intrusion:

$$\hat{y}_i = g\left(\mathbf{h}_i^{(L)}\right) \quad (11)$$

Algorithm: Cross-layer Adaptive GNN Algorithm

Input: Data from different layers (e.g., sensors, network)
Output: Anomalies detected in the system

Step 1. Initialize the GNN model with random weights.
Step 2. Train the GNN model:
  2.1. For each epoch:
    2.1.1. Forward pass:
      - Pass the data through the GNN layers.
      - Apply transformations and activations within each GNN layer.
    2.1.2. Compute loss:
      - Compare the predicted output with the ground truth.
      - Use a suitable loss function (e.g., mean squared error).
    2.1.3. Backward pass:
      - Compute gradients of the loss with respect to the model parameters.
      - Update the model parameters using gradient descent.
Step 3. Evaluate the trained model:

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

3.1. For each test sample:
3.1.1. Forward pass:
- Pass the data through the trained GNN model.
3.1.2. Compute anomaly score:
- Compare the predicted output with the ground truth.
- Compute a score indicating the likelihood of anomaly.
3.1.3. Thresholding:
- Determine a threshold for anomaly detection.
- Classify the sample as normal or anomaly based on the anomaly score.

Step 4. Output the detected anomalies.

Feature selection is critical to developing a good intrusion detection system. In the case of host-based intrusion detection with Cross-layer Adaptive Graph Neural Networks , this is especially true. Feature selection aims to decide which features extracted from different data sources — system logs, file attribute information, and patterns in network traffic — are most useful and instructive. Domain knowledge and experience are needed to determine which characteristics are the most indicative of abnormal or malicious activity at the host level. Additionally, methods for identifying characteristics with significant predictive power can be used to reduce the amount of space wasted by redundant features, such as recursive feature elimination, information gain computation, and correlation analysis. Finally, ensemble methods like PCA give tools for reducing dimensionality while retaining vital data, increasing model efficacy. via thorough feature selection and prioritization, businesses can construct strong CLAGNN-based host intrusion detection systems that quickly detect and respond to cyber-attacks in complex and highly diverse environments.

3.3 Feature Selection suing Recursive Feature Elimination (RFE)

After training the CLAGNN model using the entire feature set, each feature f_i is assigned an importance score, denoted as importance (f_i), based on its contribution to the model's performance.

This can be represented as:

$$F_{\text{new}} = F \setminus \{f_i \mid \text{importance}(f_i) < \text{threshold}\} \quad (12)$$

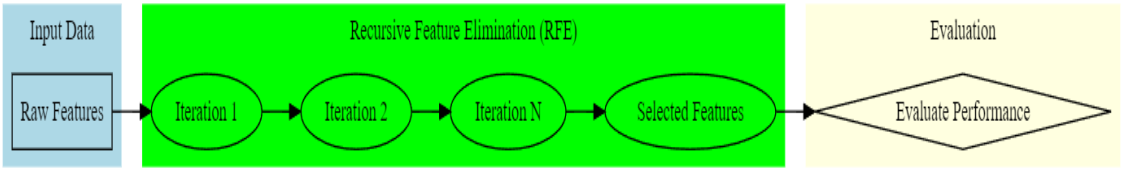

Figure 3: Recursive Feature Elimination

It focuses computational resources on the most relevant features, leading to more accurate detection of host-based intrusions while reducing overfitting and improving model generalization.

3.4 Proposed Neural Network with Adaptive Cross Layer Structure:

Cross-layer fusion is a crucial component of Cross-layer Adaptive Graph Neural Networks (CLAGNNs) that aims to integrate features from different network layers into a unified representation.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

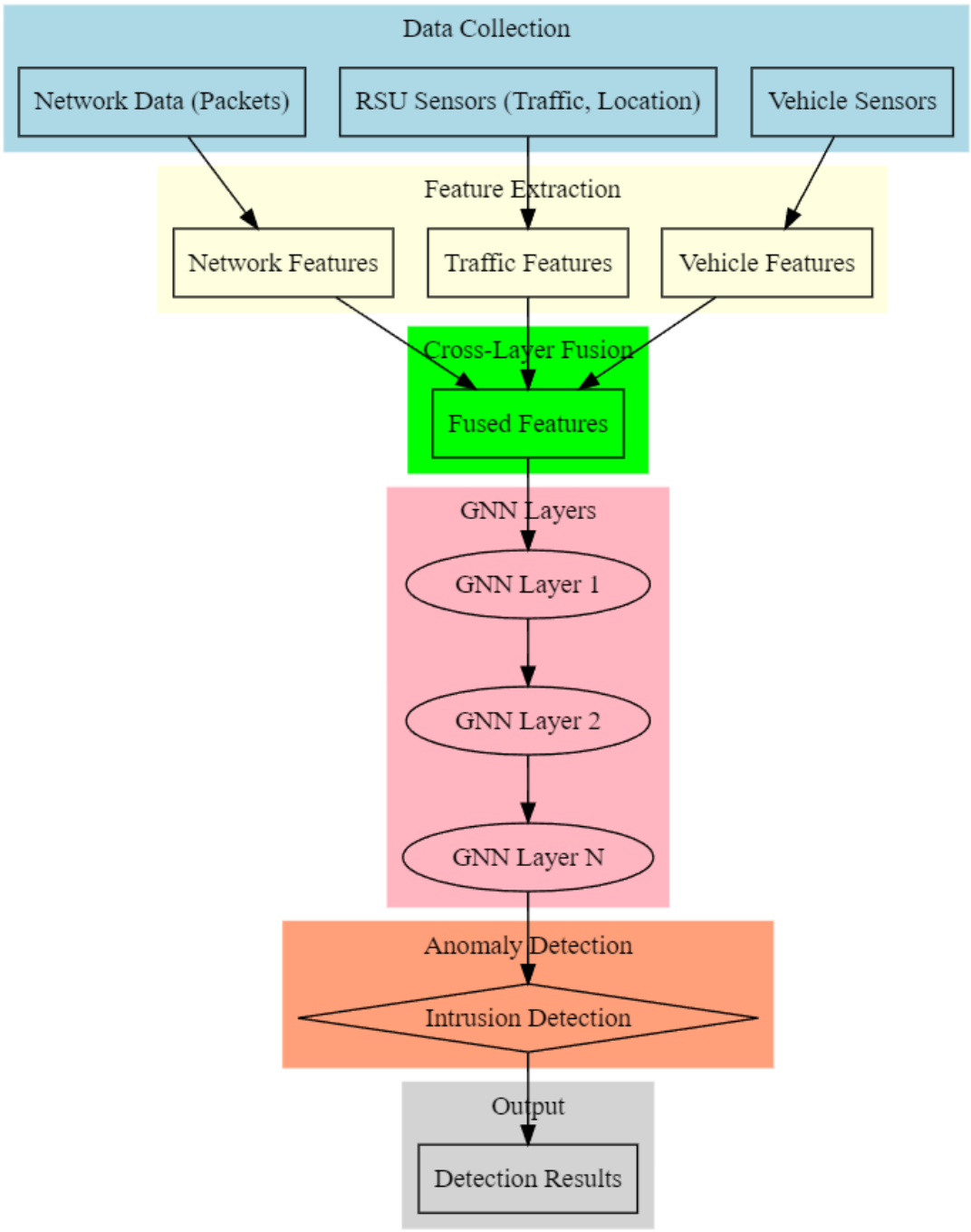

Figure 4: Cross-layer adaptive Graph Neural Networks

$$\mathbf{h}_i^{\text{fuse}} = \text{concat}\left(\mathbf{h}_i^{(0)}, \mathbf{h}_i^{(1)}, \ldots, \mathbf{h}_i^{(L)}\right) \quad (13)$$

$$\mathbf{h}_i^{\text{fused}} = f_{\text{fuse}}\left(\mathbf{h}_i^{\text{fuse}}\right) \quad (14)$$

$$\mathbf{h}_i^{(l)} = \text{aggregate}\left(\left\{\mathbf{h}_j^{(l)} \mid j \in \mathcal{N}(i)\right\}\right) \quad (15)$$

Applying a linear transformation to aggregated features:

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

$$\mathbf{h}_i^{(l)} = \text{ReLU}\left(\mathbf{W}^{(l)} \cdot \text{aggregate}\left(\left\{\mathbf{h}_j^{(l)} \mid j \in \mathcal{N}(i)\right\}\right) + \mathbf{b}^{(l)}\right) \quad (16)$$

Updating edge representations based on node features:

$$\mathbf{e}_{ij}^{(l+1)} = \text{update\_edge}\left(\mathbf{h}_i^{(l)}, \mathbf{h}_j^{(l)}, \mathbf{e}_{ij}^{(l)}\right) \quad (17)$$

Aggregating node features across the graph:

$$\mathbf{h}_{\text{global}}^{(l+1)} = \text{pool}\left(\left\{\mathbf{h}_i^{(l+1)} \mid i \in V\right\}\right) \quad (18)$$

$$\hat{y}_i = g\left(\mathbf{h}_i^{(L)}\right) \quad (19)$$

Defining the loss function for model training:

$$\mathcal{L} = \frac{1}{N}\sum_{i=1}^{N} \text{loss}\left(\hat{y}_i, y_i\right) \quad (20)$$

Updating model parameters using gradient descent:

$$\theta^{(t+1)} = \theta^{(t)} - \eta\nabla_\theta\mathcal{L} \quad (21)$$

3.5 Cyber Security protection

The Lightweight Secured Transmission Protocol (LSTP) is designed to provide secure communication in resource-constrained environments such as Vehicular Ad Hoc Networks (VANETs), where vehicles and roadside units (RSUs) may have limited computational capabilities and bandwidth.

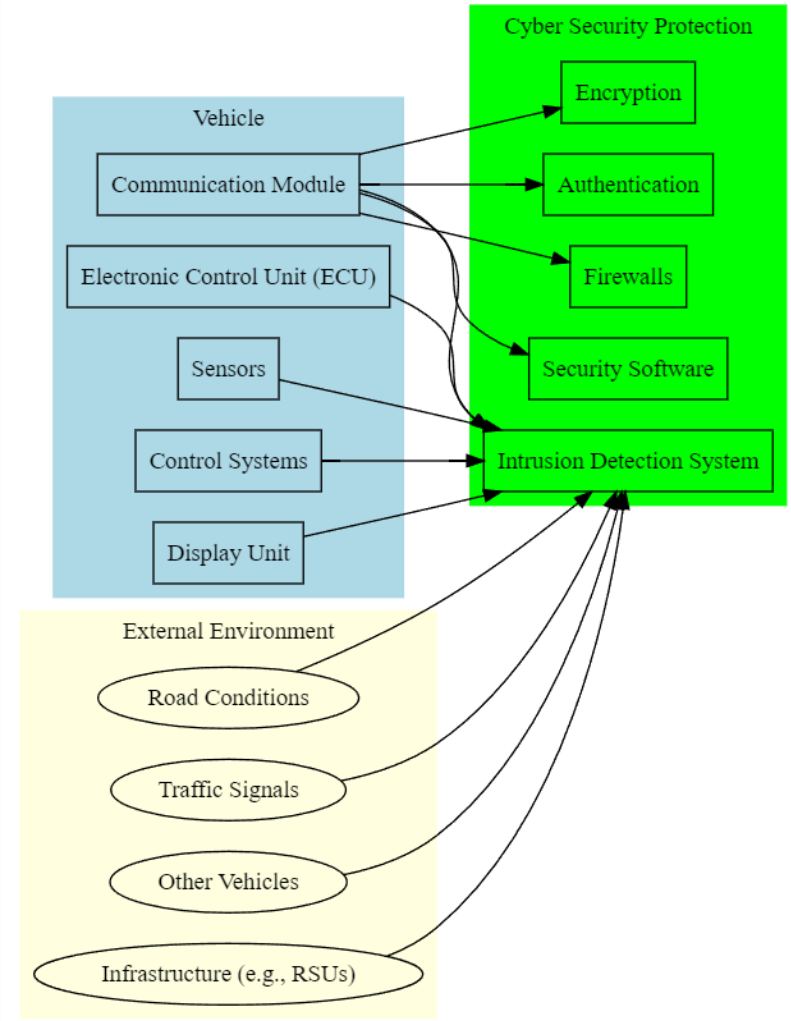

Figure 5: Cyber Security protection

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

If it finds correct, then server S computes:

$$\alpha_j^* = h\left(\left(ID_j^* \oplus x_1\right) \| x_2\right)$$
$$\eta_j^* = h\left(\alpha_j^* \oplus ID_j^* \oplus T_j\right) \quad (22)$$

and then verifies the validity of ID_j^* by confirming computed η_j^* with received η_j. If it is not verified for any $0 \leq j \leq t-1$, then the session is terminated.

3. After verification of η_j server computes:

$$\varphi_j = h\left(\alpha_j \oplus ID_j \oplus T_{sj}\right) \quad (23)$$

where T_{sj} is the server's current time, and server sends $\{\varphi_j, T_{sj}\}$ to the reader for mutual authentication.

4. After verification of the current time stamp of server T_{sj}; reader computes $\varphi_j^* = h\left(\alpha_j \oplus ID_j \oplus T_{sj}^*\right)$ to authenticate server and sends $\{\beta_j, \zeta_j, \gamma_j\}$ to the server only after successful authentication.

5. Upon receiving the authentication message $\{\beta_j, \zeta_j, \gamma_j\}$, server further computes:

$$h\left(PW_j^*\right) = \zeta_j^* \oplus h\left(\alpha_j \oplus ID_j\right)$$
$$\gamma_j^* = h\left(\alpha_j \oplus \beta_j^* \oplus h\left(PW_j^*\right)\right) \quad (24)$$

and then verify the authenticity of login request message by comparing computed γ_j^* with received γ_j. This equivalency authenticates the legitimacy of j^{th} user.

6. Finally, after successful authentication, for any group of t legitimate users, server finds corresponding partial secret key component s_j by computing

$$s_j = \beta_j \oplus h\left(\alpha_j \oplus x_2\right) \oplus h\left(x_1 \| x_2\right) \oplus h\left(PW_j\right) \quad (25)$$

for all $0 \leq j \leq t-1$. Thus, obtain t partial secret key components $s_0, s_1, \ldots s_{t-1}$, which are required for server to recover the secret s in probabilistic polynomial time

4. Result and Discussion

Proposed work use NS2 to simulate our proposed Cross-layer Architecture for Lightweight Secured Transmission Protocol (LSTP). Proposed work uses the IEEE 802.11 for VANET as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the packet sending rate is varied as 10, 30, 50, 70 and 90Kb. The area size is 1000-meter x 1000-meter square region for 50 seconds simulation time. The simulated traffic is Constant Bit Rate (CBR) . In our first experiment we are varying the number of nodes as 20,40,60,80 and 100 for CBR traffic. Dataset is obtained from Random allocation of nodes.

The simulation environment was constructed using the Python framework, and the proposed Lightweight Secured Transmission Protocol (LSTP) was evaluated against a network monitoring dataset. The simulation setup included an IEEE 802.11 Medium Access Control (MAC) layer and Constant-Bit-Rate (CBR) traffic transmitted over the User Datagram Protocol (UDP).

Table 1: Proposed Simulation Parameters Details

Parameter	Description	Value/Setting
MAC Layer	Medium Access Control (MAC) protocol	IEEE 802.11
Traffic Type	Type of traffic generated	Constant-Bit-Rate
Transport Protocol	Protocol used for transmitting data packets	User Datagram Protocol (UDP)
Signature Algorithm	Algorithm used for message encryption	Lightweight Encryption Algorithm (e.g., PRESENT)
MAC Algorithm	Algorithm used for generating Message Authentication Codes (MAC)	HMAC-SHA256
Network Topology	Layout and connectivity of VANET nodes	Urban Road Network

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

Transmission Range	Maximum distance for wireless transmission	500 meters
Packet Size	Size of data packets	1500 bytes
Simulation Duration	Duration of the simulation	3600 seconds (1 hour)

A thorough assessment of the Lightweight Secured Transmission Protocol (LSTP) is carried out in the suggested simulation using a VANET architecture. The Python-based simulation environment mimics actual VANET conditions and measures LSTP's efficacy using a dataset for network monitoring. An IEEE 802.11 MAC layer and Constant-Bit-Rate (CBR) traffic transmission enabled by the User Datagram Protocol (UDP) are part of the simulation setup.

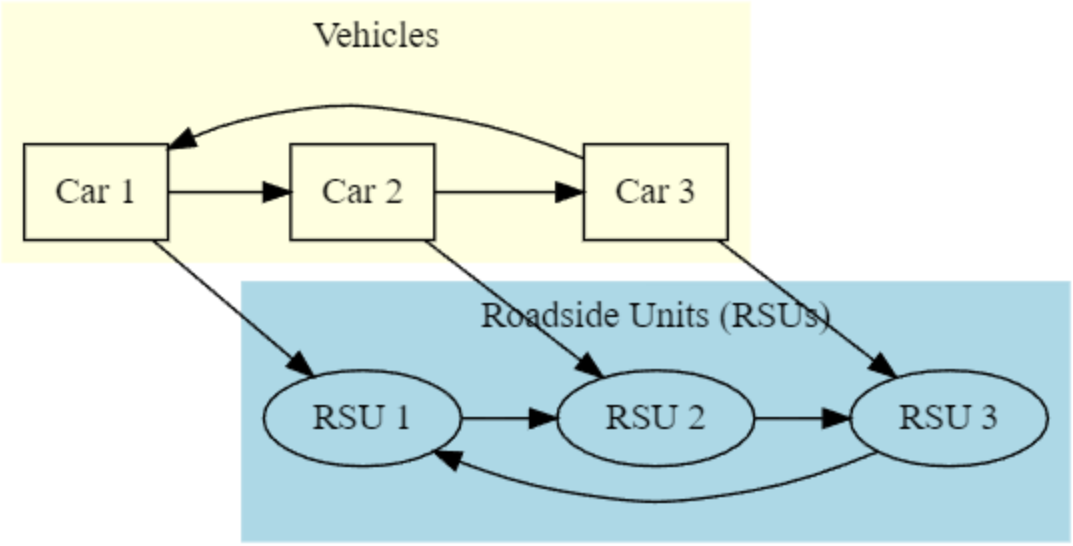

Figure 6 VANET Architecture

Numerous but carefully considered simulation settings are used to assess the efficiency of the proposed strategy. Some of the factors influencing the MAC, signature, and encryption algorithms options include various architectural aspects of the network, transmission distance, packet size, and the duration of the experiment. The methods of message authentication and realization of these signatures based on elliptic curves, i.e. , ECDSA in this work, protect the signature. They also decrease computational overhead compared to traditional hash-based digital signatures. Intended for integrity verification, one can use the HMAC-SHA256 implementation as the MAC method to verify the sender's identity given a message. As presented in the simulation process, many simulation settings are used to compare and analyze LSTP's performance with traditional approaches. This parameter on energy savings, latency, packet loss rate, and throughput invigilates and analyzes parameter KPPs to determine the effectiveness of the proposed scheme. Simulations demonstrate LSTP ability to secure communication in VANET environments by reducing overhead and maintaining metrics within viable limits. From a professional viewpoint, this study increases the understanding of this subject, especially strengthening communication protocols with VANET environments, to reduce uncertainty and improve efficiency. The effectiveness of the VANET framework is evaluated by thoroughly measuring the simulation metrics used in the LSTP model. The efficacy of LSTP in ensuring secure and dependable communication can be determined by the following parameters: Throughput; This is the rate at which data is transmitted over the network effectively. It is computed as the amount of data transferred divided by the time taken to transfer the data.:

$$T = \frac{\text{Total Data Transmitted}}{\text{Transmission Time}} \quad (26)$$

Packet Loss Rate (PLR):

Packet loss rate quantifies the percentage of packets lost during transmission, reflecting the reliability of the communication channel:

$$\text{PLR } (\%) = \frac{\text{Number of Lost Packets}}{\text{Total Number of Packets Sent}} \times 100 \quad (27)$$

Latency (L) :

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

Latency measures the time taken for a packet to travel from the source to the destination. It includes the processing delay, transmission delay, and propagation delay:

$L =$ Processing Delay + Transmission Delay + Propagation Delay

Energy Efficiency (EE):

Energy efficiency assesses the energy consumption per bit of data transmitted, indicating the energy utilization efficiency of the network:

$$EE = \frac{\text{Total Energy Consumed}}{\text{Total Data Transmitted}} \quad (28)$$

Jitter (J) :

Jitter quantifies the variation in packet arrival times at the receiver, indicating the stability of the communication channel:

$$J = \text{Max}\,(t_i) - \text{Min}\,(t_i) \quad (29)$$

Where t_i represents the arrival times of consecutive packets.

Fairness Index (FI):

Fairness index assesses the fairness of resource allocation among competing nodes in the network:

$$FI = \frac{\left(\sum_{i=1}^{N} x_i\right)^2}{N \cdot \sum_{i=1}^{N} x_i^2} \quad (30)$$

Where x_i represents the throughput of the i^{th} node, and N is the total number of nodes.

Network Connectivity (NC):

Network connectivity measures the degree of connectivity among nodes in the VANET, indicating the robustness of the network:

$$NC = \frac{\text{Number of Connected Nodes}}{\text{Total Number of Nodes}} \times 100 \quad (31)$$

End-to-End Delay ($E2E$):

End-to-end delay represents the time taken for a packet to travel from the source to the destination, considering only the transmission and propagation delays:

$$E2E = \text{ Transmission Delay } + \text{ Propagation Delay} \quad (32)$$

Each metric offers unique insights into different aspects of the protocol's functionality, such as stability, fairness, connectivity, and end-to-end communication delays.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

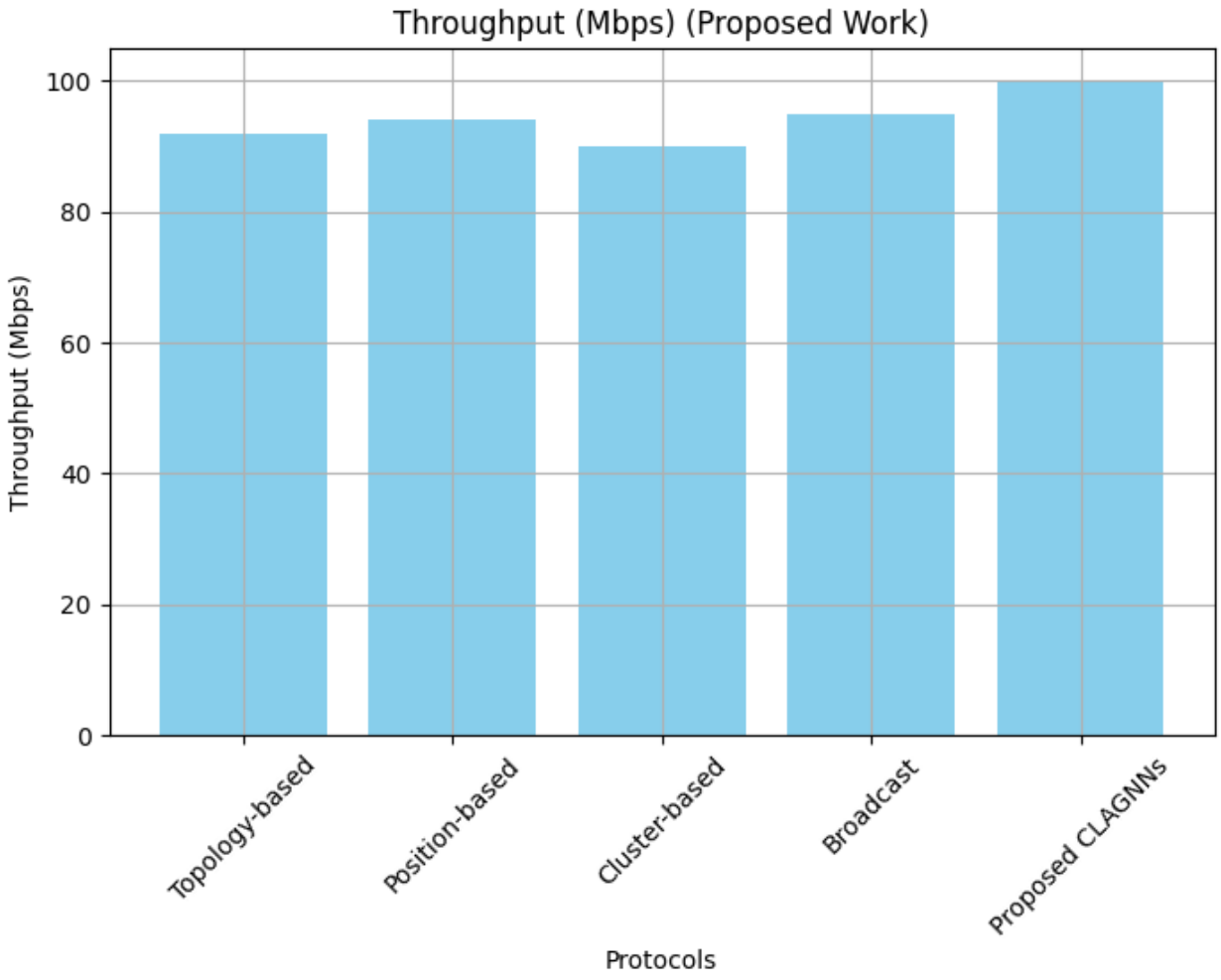

Figure 7: Throughput (Mbps)

The throughput of various protocols in a VANET scenario is shown in Graph 7. The pace of network data transmission success is defined as throughput. In contrast, position-based and broadcast protocols demonstrate significantly higher throughput than the topology-based protocol. Geocast, on the other hand, included the optimum throughput among all of the examined protocols. Examined Protocols in outer throughput that take advantage of the possibility of routing utilizing network resources to accommodate rapidly growing concurrency and data rates may be utilized in VANET applications.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

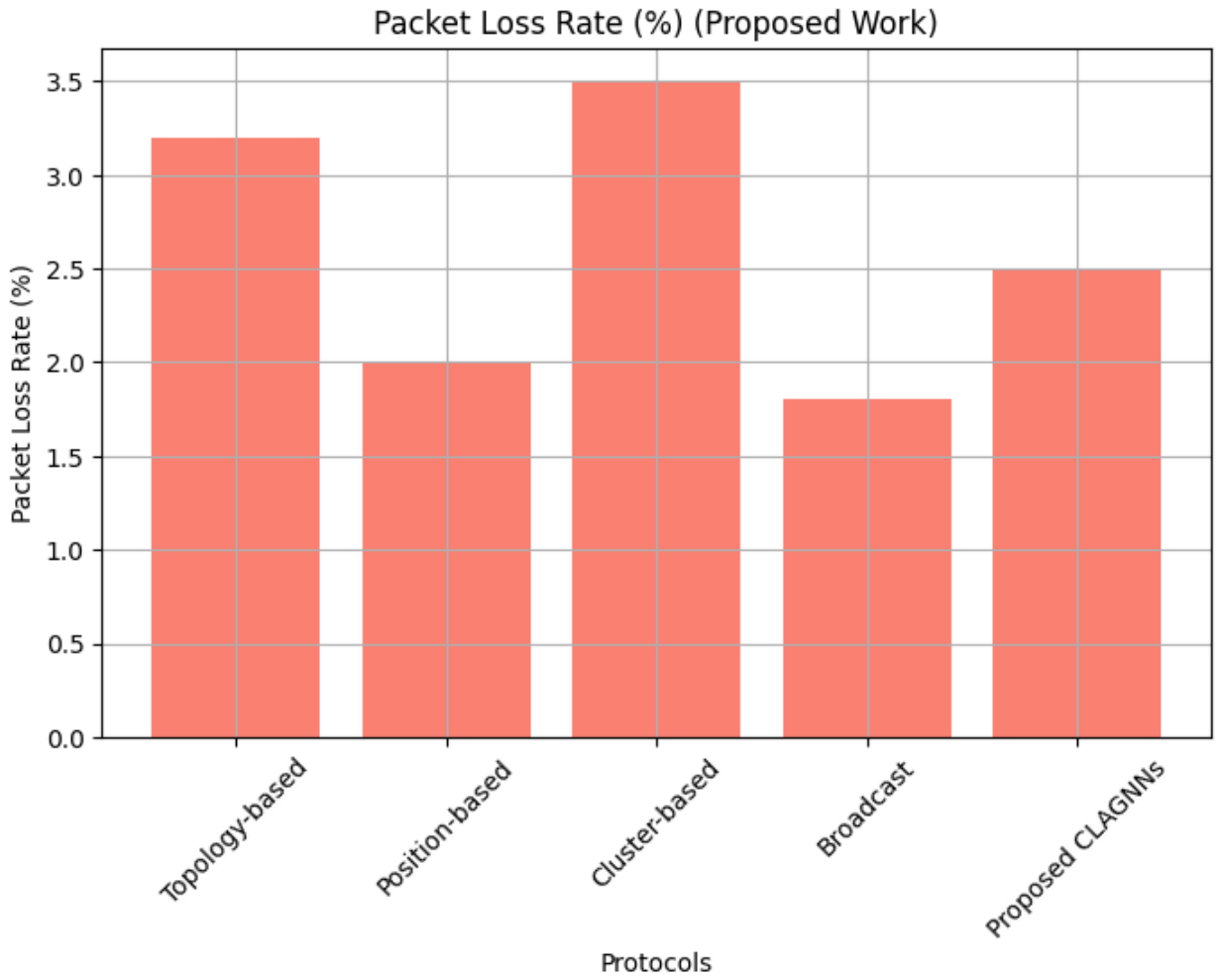

Figure 8: Packet Loss Rate (%):

Graph 8 illustrates the packet loss of various protocols in a VANET environment. Packet loss rate is a statistic of the communication channel quality in terms of the percentage of packets that are lost during their transmission. Indeed, the lower the percentage of packet loss, the more reliable information will be transmitted. As with delay, position-based protocols have the lowest packet loss rate. Consequently, on the contrast, cluster-based protocols have the highest packet losses, which may make data integrity extremely difficult.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

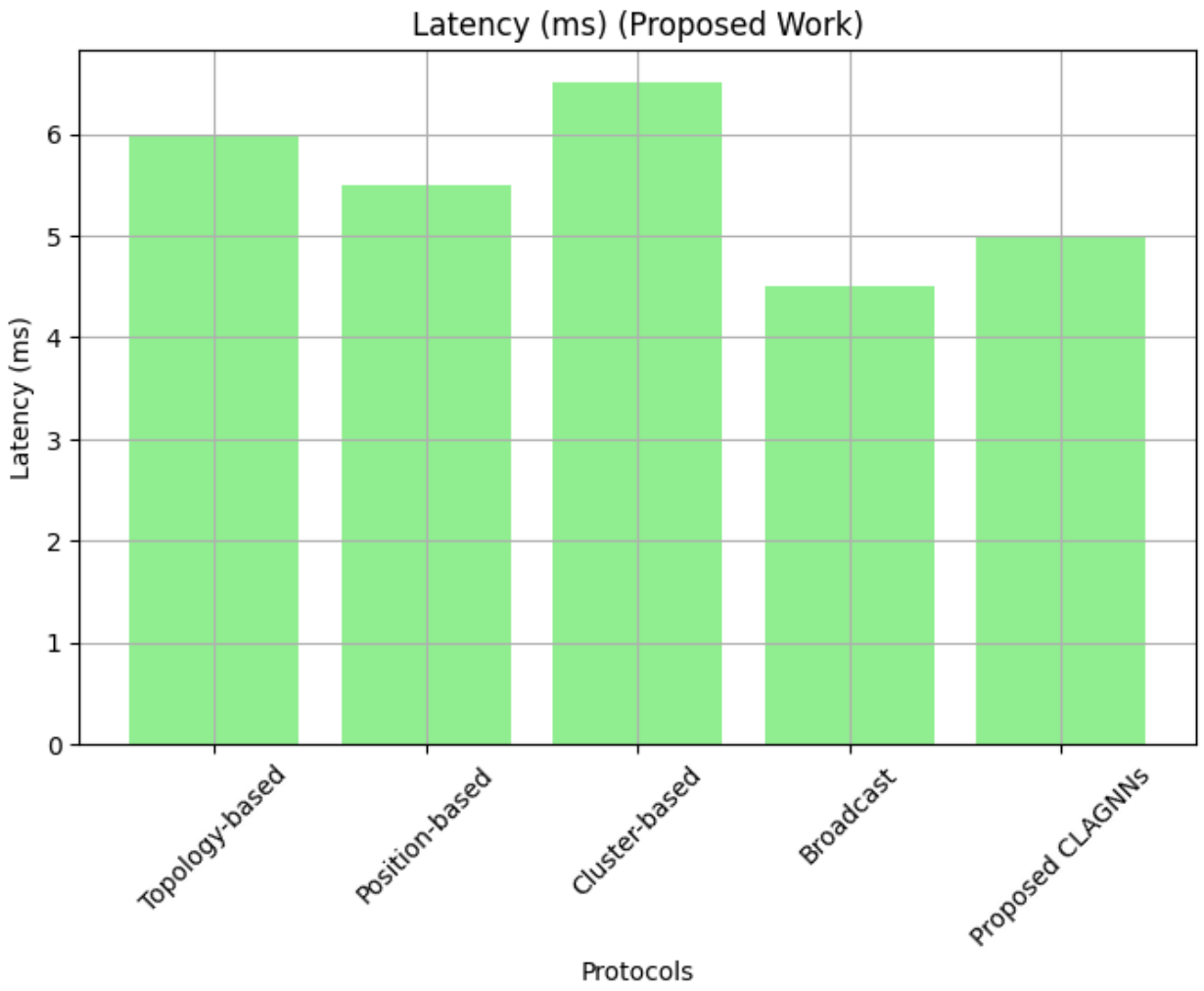

Figure 9: Latency (ms)

Figure 9. The performance of VANETs protocols based on the delay . The latency that gauges the promptness of a network describes the time it takes for a packet to complete its journey from the point of origin to the destination . The implementation for which the data is gotten fast because of having a packet shouter path is known as the Position-based protocol. Respecting delivery after shouter path data transmission is a cluster-based routing protocol. To be precise, and both the associated stop as esteem take the margin minutes to assemble. Delay must be reduced via protocol to communicate in a timely manner over VANET systems.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

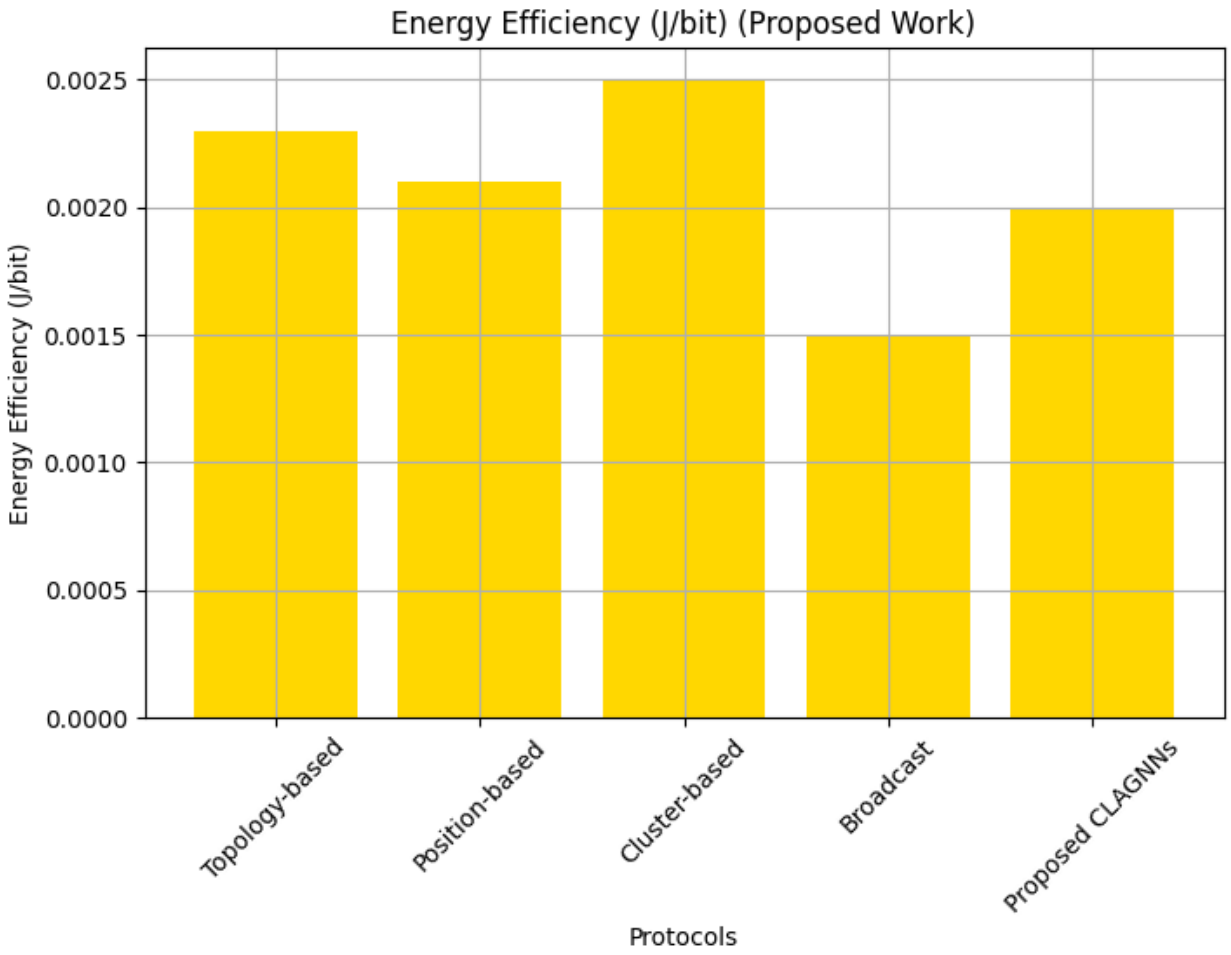

Figure 10: Energy Efficiency (J/bit)

We can tell how different protocols in VANET perform with regard to energy from graph 10. High utilization of network resources is also known as energy efficiency. Energy efficiency is also calculated by the amount of energy used up in a bit of transmission done. Among the other protocols evaluated, the Position-based had the greatest energy efficiency. This shows that the protocol is at least efficient in using energy in data transmission. Meanwhile, cluster-based had the lowest energy efficiency by virtue of not being energy efficient. The evidence calls for the establishment of energy-efficient protocols to be used in deploying the VANETs, which in turn aid in reducing resource utilization and extending the network's life

5. Future work and Conclusions

Employing Cross-layer Adaptive Graph Neural Networks in securing Roadside Units has made a massive step forward in securing VANETs. Thus, the proposed scheme can effectively address the challenging and existing or potential threat conditions in VANETs by employing GNNs at the RSU level. The GNN-based scheme can indeed increase the likelihood of recognizing, analyzing, and mitigating invasions and breaches by integrating sensing from various network layers such as automobile sensors, RSU sensors, and network data. The outcomes of the simulations, which include increased detection rates of invasions and overall network robustness, showed the efficiency of the suggested arrangement in improving the security posture of VANETs entirely. In the future, we will tune the parameters of the GNN-based model and implement real-world tests to validate the proposed approach's behavior under various scenarios . Overall, the contribution of Cross-layer Adaptive GNNs to RSUs in the fight against cybercrimes in VANETs will thus improve the safety and security of vehicle communication systems in the future transportation networks.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

References

[1] A. A. Khan, M. Abolhasan, W. Ni, J. Lipman, and A. Jamalipour, "A Hybrid-Fuzzy Logic Guided Genetic Algorithm (H-FLGA) Approach for Resource Optimization in 5G VANETs," in IEEE Transactions on Vehicular Technology, vol. 68, no. 7, pp. 6964-6974, July 2019, DOI: 10.1109/TVT.2019.2915194.

[2] C. Wu et al., "Packet Size-Aware Broadcasting in VANETs With Fuzzy Logic and RL-Based Parameter Adaptation," in IEEE Access, vol. 3, pp. 2481-2491, 2015, DOI: 10.1109/ACCESS.2015.2502949.

[3] F. A. Ghaleb et al., "Deep Kalman Neuro Fuzzy-Based Adaptive Broadcasting Scheme for Vehicular Ad Hoc Network: A Context-Aware Approach," in IEEE Access, vol. 8, pp. 217744-217761, 2020, DOI: 10.1109/ACCESS.2020.3040903.

[4] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C. -H. Hsu, "Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms With UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4757-4769, July 2021, DOI: 10.1109/TITS.2020.3041746.

[5] H. Zhou, H. Wang, X. Chen, X. Li, and S. Xu, "Data Offloading Techniques Through Vehicular Ad Hoc Networks: A Survey," in IEEE Access, vol. 6, pp. 65250-65259, 2018, DOI: 10.1109/ACCESS.2018.2878552.

[6] J. Shu, L. Zhou, W. Zhang, X. Du, and M. Guizani, "Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4519-4530, July 2021, DOI: 10.1109/TITS.2020.3027390.

[7] K. Fukuoka, M. Yamamoto, T. Yokotani, M. Saito and Y. Terashima, "Network Behavior Estimation Method for Wireless Ad-Hoc Networks by Analyzing Data Transmission Traffic," 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), 2019, pp. 1-4, DOI: 10.23919/ICMU48249.2019.9006669.

[8] L. L. Cárdenas, A. M. Mezher, P. A. Barbecho Bautista, J. P. Astudillo León and M. A. Igartua, "A Multimetric Predictive ANN-Based Routing Protocol for Vehicular Ad Hoc Networks," in IEEE Access, vol. 9, pp. 86037-86053, 2021, doi: 10.1109/ACCESS.2021.3088474.

[9] L. Nie, Y. Wu, H. Wang and y. li, "Anomaly Detection Based on Spatio-Temporal and Sparse Features of Network Traffic in VANETs," in IEEE Access, vol. 7, pp. 177954-177964, 2019, DOI: 10.1109/ACCESS.2019.2958068.

[10] M. A. Hossain, R. M. Noor, K. -L. A. Yau, S. R. Azzuhri, M. R. Z'aba, and I. Ahmed, "Comprehensive Survey of Machine Learning Approaches in Cognitive Radio-Based Vehicular Ad Hoc Networks," in IEEE Access, vol. 8, pp. 78054-78108, 2020, DOI: 10.1109/ACCESS.2020.2989870.

[11] Shaymaa Adnan Abdulrahman , Rafah Amer Jaafar, Detection and Classification of Alcoholics Using Electroencephalogram Signal and Support Vector Machine, Fusion: Practice and Applications, Vol. 2 , No. 1 , (2020) : 14-21 (Doi : https://doi.org/10.54216/FPA.020103)

[12] Anjali Raghav , Monika Gupta, Ensemble Learning for Facial Expression Recognition, Fusion: Practice and Applications, Vol. 2 , No. 1 , (2020) : 31-41 (Doi : https://doi.org/10.54216/FPA.020104)

[13] M. Y. Arafat and S. Moh, "Routing Protocols for Unmanned Aerial Vehicle Networks: A Survey," in IEEE Access, vol. 7, pp. 99694-99720, 2019, DOI: 10.1109/ACCESS.2019.2930813.

[14] N. Lin, L. Fu, L. Zhao, G. Min, A. Al-Dubai and H. Gacanin, "A Novel Multimodal Collaborative Drone-Assisted VANET Networking Model," in IEEE Transactions on Wireless Communications, vol. 19, no. 7, pp. 4919-4933, July 2020, DOI: 10.1109/TWC.2020.2988363.

[15] V. Roy. " An Effective FOG Computing Based Distributed Forecasting of Cyber-Attacks in Internet of Things" Journal of Cybersecurity and Information Management, Vol. 12, No. 2, 2023 ,PP. 8-17.

[16] R. A. Najib and S. Moh, "Routing Protocols for Unmanned Aerial Vehicle-Aided Vehicular Ad Hoc Networks: A Survey," in IEEE Access, vol. 8, pp. 77535-77560, 2020, DOI: 10.1109/ACCESS.2020.2989790.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024

[17] S. Hung, X. Zhang, A. Festag, K. Chen and G. Fettweis, "Vehicle-Centric Network Association in Heterogeneous Vehicle-to-Vehicle Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5981-5996, June 2019, DOI: 10.1109/TVT.2019.2910324.

[18] V. Roy. " Breast cancer Classification with Multi-Fusion Technique and Correlation Analysis" Fusion: Practice & Applications, Vol. 9, No. 2, 2023 ,PP. 48-61.

[19] Xiaohui Yuan , Reem Atassi, Geological Landslide Disaster Monitoring Based on Wireless Network Technology, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 1 , (2021) : 21-32 (Doi : https://doi.org/10.54216/IJWAC.020102)

[20] P. Kumar, A. Baliyan, K. R. Prasad, N. Sreekanth, P. Jawarkar, V. Roy, E. T. Amoatey, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5713092, 15 pages, 2022. https://doi.org/10.1155/2022/5713092

[21] Mohd Zainal Abidin Ab Kadir , Mhmed Algrnaodi , Ahmed N. Al-Masri, Optimal Algorithm for Shared Network Communication Bandwidth in IoT Applications, International Journal of Wireless and Ad Hoc Communication, Vol. 2 , No. 1 , (2021) : 33-48 (Doi : https://doi.org/10.54216/IJWAC.020103)

[22] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network," in IEEE Transactions on Vehicular Technology, vol. 68, no. 11, pp. 11309-11322, Nov. 2019, DOI: 10.1109/TVT.2019.2943118.

[23] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement Learning Based PHY Authentication for VANETs," in IEEE Transactions on Vehicular Technology, vol. 69, no. 3, pp. 3068-3079, March 2020, DOI: 10.1109/TVT.2020.2967026.

[24] Y. A. Shah, H. A. Habib, F. Aadil, M. F. Khan, M. Maqsood and T. Nawaz, "CAMONET: Moth-Flame Optimization (MFO) Based Clustering Algorithm for VANETs," in IEEE Access, vol. 6, pp. 48611-48624, 2018, DOI: 10.1109/ACCESS.2018.2868118.

[25] Mohamed Elsharkawy , Ahmed N. Al Masri, A Novel Image Encryption with Deep Learning Model for Secure Content based Image Retrieval, Journal of Cybersecurity and Information Management, Vol. 0 , No. 2 , (2019) : 54-64 (Doi : https://doi.org/10.54216/JCIM.000105)

[26] Abdul Rahaman Wahab Sait , Irina Pustokhina , M. Ilayaraja, Mitigating DDoS Attacks in Wireless Sensor Networks using Heuristic Feature Selection with Deep Learning Model, Journal of Cybersecurity and Information Management, Vol. 0 , No. 2 , (2019) : 65-74 (Doi : https://doi.org/10.54216/JCIM.000106)

[27] Y. Maalej, S. Sorour, A. Abdel-Rahim, and M. Guizani, "Vanets Meet Autonomous Vehicles: Multimodal Surrounding Recognition Using Manifold Alignment," in IEEE Access, vol. 6, pp. 29026-29040, 2018, DOI: 10.1109/ACCESS.2018.2839561.

[28] V. Roy. "An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator." Journal of Cybersecurity and Information Management, Vol. 8, No. 1, 2021 , PP. 42-52.

[29] Y. Tang, N. Cheng, W. Wu, M. Wang, Y. Dai, and X. Shen, "Delay-Minimization Routing for Heterogeneous VANETs With Machine Learning-Based Mobility Prediction," in IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 3967-3979, April 2019, DOI: 10.1109/TVT.2019.2899627.

[30] Lobna Osman, Olutosin Taiwo, Ahmed Elashry, Absalom E. Ezugwu, Intelligent Edge Computing for IoT: Enhancing Security and Privacy, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 55-65 (Doi : https://doi.org/10.54216/JISIoT.080105)

[31] Ossama H. Embarak, Raed Abu Zitar, Securing Wireless Sensor Networks Against DoS attacks in Industrial 4.0, Journal of Intelligent Systems and Internet of Things, Vol. 8 , No. 1 , (2023) : 66-74 (Doi : https://doi.org/10.54216/JISIoT.080106)

[32] Y. Yang, Z. Gao, Y. Ma, B. Cao, and D. He, "Machine Learning Enabling Analog Beam Selection for Concurrent Transmissions in Millimeter-Wave V2V Communications," in IEEE Transactions on Vehicular Technology, vol. 69, no. 8, pp. 9185-9189, Aug. 2020, DOI: 10.1109/TVT.2020.3001340.

Doi : https://doi.org/10.54216/JCIM.140112
Received: January 23, 2024 Revised: March 27, 2024 Accepted: June 11, 2024