SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I3P120

Volume 12 Issue 3, 202-209, March 2025


*Original Article*

# Intrusion Detection in Wireless Ad Hoc Networks Using Advanced Graph Theory Models

K. Sudharson[1], Rajesh Kambattan Kovarasan[2], N. Sathish Kumar[3], S. Rajalakshmi[4]

[1,3]*Department of AIML, RMD Engineering College, Tamil Nadu, India.*
[2]*Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Tamil Nadu, India.*
[4]*Department of CSE (Cyber Security), Velammal Engineering College, Tamil Nadu, India.*

[1]*Corresponding Author : sudharsonkumar@gmail.com*

Received: 12 January 2025 Revised: 13 February 2025 Accepted: 18 March 2025 Published: 29 March 2025

***Abstract*** *- Our proposed system, described in this paper, focuses on intrusion detection in WANETs, where there are emerging complexities in the structure of the graph models and the number of attributes of a node from which information must be extracted or aggregated. Attacks on WANETs are mostly abrupt, and that calls for systems that can capture fluctuations in topology. Real-time identification of such changes is achieved through our dynamic graph transformations using variational inequalities as the modeling vehicle. The novel model under consideration is Matrix Completion-GCN with nonlinear activation functions and Variational Autoencoders (VAEs) to improve the efficiency of graph representation learning. Moreover, Spectral Signal Clustering (SSC) is used in the process as a prescreening form to filter raw data and prettify the graph signal. The results evaluated on several real-world WANET datasets show that the proposed model has much higher performance compared to the traditional models like SVM and RF, giving 95.5% precision, 97.2 % recall, 98.1% detection rate and 1.2% false positive. This research provides high accuracy for real-time intrusion detection, and future research can be done to optimize computational cost and broaden its scope for IoT networks.*

***Keywords*** *- Wireless Ad Hoc Networks, Intrusion detection, Graph-based classification, Spectral graph preprocessing, Nonlinear variational inequalities.*

## 1. Introduction

Wireless Ad Hoc Networks (WANETs) are gradually finding their uses in various important areas, including disaster recovery, military operations and smart infrastructure, where they offer opportunistic, self-organizing and self-forming infrastructure to support connectivity in distributed and dynamic environments. A major characteristic of WANETs is their lack of infrastructure; thus, there is no wired infrastructure in contrast to traditional networks, which are characterized by fixed infrastructure elements. Due to their decentralized and dynamic architecture, WANETs are very vulnerable to many forms of malicious interference, including DoS attacks, eavesdropping, spoofing, packet dropping, and data manipulation. For this reason, constructing a stable and competent IDS, especially for WANETs, is of priority importance for achieving high availability and protection of the network.

This research, therefore, fills the gap that has been posed by most ordinary IDS solutions since they are very weak when implemented in WANETs because they cannot adapt to changed topologies. To address these issues, the following framework based on the nonlinear variational graph theory models is presented. This approach models WANETs as a collection of dynamic graphs where the node and the edges are not fixed due to the mobility of nodes and signal strength. By adopting the problem in terms of the nonlinear variational inequalities, we can describe the evolutionary real-time behavior of the network topology [1]. These are the transformations that may be a result of legitimate change in the network or by intruders, hence helping the system to determine between normal traffic and intrusion.

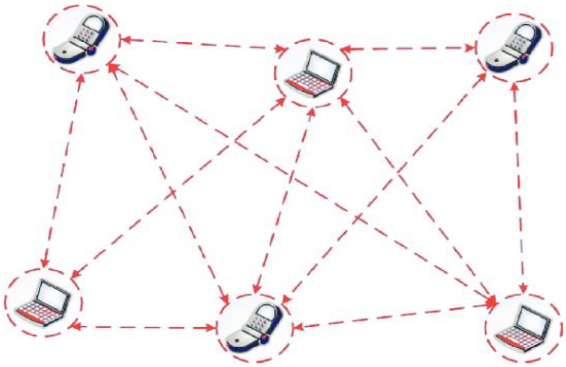

**Fig. 1 Wireless Ad hoc Network**

Our study combines GCNs with VAEs as a powerful classification apparatus. This problem is solved through a classification approach that combines Graph Convolutional Networks (GCNs) with Variational Autoencoders (VAEs). GCNs are beneficial for utilizing graph-structured data since, with each iteration of graph convolution, a GCN can capture intricate relations between nodes. VAEs are used for graph learning; more specifically, the purpose of VAEs is to encode the input data into the lower-dimensional space but to preserve significant structural information [2]. The proposed nonlinear activation functions improve the models' learning capability, which positively impacts its ability to identify abnormal behavior from normal activities.

To enhance the detection performance of imaging spectrometry data and remove noises, spectral graph preprocessing is used before classification. This step ensures that the model consumes a more refined, clearer graph in its processing, hence improving its efficiency in its task. It is noted that the model is trained with the help of historical data of the network to be able to discover weak traces of potential threats [3]. The proposed method uses both the mathematical accuracy of the graph theory and the predictive accuracy of the machine learning method and, therefore, can be considered an accurate, flexible and even generalized approach toward intrusion detection problems.

Apart from the high-performance, the proposed IDS provides features such as scalability and the capability to detect intrusion on a real-time basis. Thus, it is workable for large WANET networks. Subsequent studies will be directed at refining the computational complexity of nonlinear variational models for enhancing RT processing. Besides, the enhancement of the federated learning model could improve privacy and scalability since intrusion detection can then be done without disclosing the network data.

It is suggested that the proposed framework can potentially be expanded to include more intricate network types, such as hybrid networks and IoT networks. Thus, the current work can be considered as filling the gap between the highly sophisticated graph theory and the usage of machine learning for the protection of WANETs against the recently emerging cyber threats.

## 2. Related Works

### *2.1. Difficulties in Identification of Intrusion for WANETs*

This is particularly true in WANETs, where the communication infrastructure is truly ad hoc and the topology is dynamic. Many works have been devoted to the analysis of the combination of graph theory, machine learning, and variational models to solve these issues. In particular, variational inequalities have shown numerous applications in the past few decades when it comes to dynamic system modeling because of their capability to represent equilibration states as well as dynamic processes [4].

In the paper [5], Combettes et al. (2022) illustrated how graph-based dynamics could be modeled by a nonlinear variational inequality and how such dynamics could be solved mathematically. On this basis, Murugan et al. (2024) extended these ideas further by illustrating that variational inequalities can also be used to address network optimization problems for enhancing the real-time applications of WANETs [6].

### *2.2. Graph Theory for Intrusion Detection*

Graph theory has been identified about the representation of connections and interactions within a network and, therefore, is very applicable in intrusion detection. Granato et al. (2022) proved that applying graph-based methods for network traffic analysis is beneficial for identifying anomalous behaviours [7]. Their work emphasised that the ability to perform graph transformations in near real-time for changes in network topology is important for intrusion detection in dynamic networks. Vrahatis et al. (2024) supported the application of dynamic graph models in WANETs since graph structures are flexible in studying users' malicious behavior in the context of dynamic changes in the existing connections among nodes [8].

### *2.3. Machine Learning in Intrusion Detection*

Over the last few years, the use of machine learning as a basis for the IDS in WANETs has attracted a lot of attention. Ahmed et al. (2025) also analyzed the application of machine learning techniques that deploy temporal patterns of different network traffic kinds for the detection of some covet and sophisticated intrusions [9]. What they proved was that graph models with added machine learning classifiers are better than the normal IDS. A novel hybrid framework for intrusion detection in MANETs using GCNs was presented by Manjula et al. in their work [10], in which authors reported superior accuracy and scalability compared to the conventional approach.

However, there are still a few issues that should be discussed: Qu et al. (2022) expressed the real-time analysis challenge in dynamic networks based on sparse datasets and high computational requirements [11]. To solve these problems, Kheddar et al. (2024) put forward some lightweight algorithms, which include reinforcement learning and variational models, to solve the intrusion detection problems within limited computational resources [12].

### *2.4. GCNs Applied to Social Graphs for Classification*

What is more, Graph Convolutional Networks (GCNs) have recently drawn attention in the field of processing graph-structure data. As distinct from more conventional ML approaches that interact with data in Euclidean motion, GCNs are designed to work with non-Euclidean data, for example, graphs where nodes correspond to data points and edges correspond to relations. According to GCNs,

information from graph nodes is grouped and disseminated through an adjacency matrix and feature matrix. Procaccini et al. (2024) [13] established that through graph convolutions, GCNs have major advantages in intrusion detection as the node representations can be updated iteratively. Xu et al. (2024) expanded their study by showing that GCN-based models are effective in near real-time intrusion detection, considering the dynamism of the WANET graph structure [14].

### *2.5. Variational Autoencoders (VAEs) for Graph Embedding*

Concerning intrusion detection, graph embedding is an intermediate step through which graphical data is represented efficiently. In this work, the graph embedding technique used for the dimensionality reduction of the graph data is the Variational Autoencoder (VAE). Chen et al. (2025) also suggested the possibility of the utilization of lightweight embedding for optimizing the computational complexity of real-time processes in dynamic networks [15]. This allowed us to achieve predictable, reliable feature extraction with the help of the proposed VAEs combined with GCNs, as well as the scalability and high accuracy of object detection.

### *2.6. Hybrid Approaches: The Information Retrieval Approach of Machine Learning and Variational Models*

More recent studies are a blend of supervised machine learning and variational models for intrusion detection within WANETs. In order to overcome the limitation of fixed graph structure and inadequate adaptability of machine learning algorithms for IDS, Liu et al. (2024) presented a novel model that incorporates the dynamic method of graph transformation into the adaptive machine learning method [16]. Its approach builds on the success of nonlinear variational models and adversarial and generative machine learning techniques to efficiently predict intrusions. Saravanan et al. [17] underlined the necessity of developing simple and efficient patterns for WANETs that would be capable of processing enormous amounts of computations. These studies indicate that integrating graph theory, machine learning algorithms operationalized via a representative mathematical theory, and variational models represents at least one viable solution for outlining the intricacies of WANET intrusion detection.

### *2.7. Summary of Related Works*

As evidenced by the surveys, more research is shifting towards accomplishing intrusion detection in WANETs through the usage of novel sophisticated graph theory models, machine algorithms, and variational approaches. Douglas and his colleagues have noted that traditional centralities that are used for modeling flow in complex networks do not scale well when applied to these dynamic FLNs. However, researchers have experimented with a few hybrid approaches that meld graph-based centrality with machine learning approaches lately. GCNs, VAEs, and nonlinear variational inequalities provide a near-optimized real-time IDS for WANETs that is scalable and has high accuracy. Future work should concentrate on enhancing the scalability of these models for these big deployments and exploring new areas of the application for these models in a new area of IoT and the combined networks.

## 3. Proposed Works

The work described in this study introduces a new intrusion detection model for WANETs based on the latest mathematical graph theory approaches, NVIs, and machine learning. The methodology proposed in this paper tackles the major research questions: dynamic topological changes, decentralized architecture, and link quality fluctuations systematically to develop a highly scalable and efficient IDS for real-time intrusion identification and classification.

### *3.1. Data Collection and Data Cleansing*

The above-proposed model is trained and validated with actual time data obtained from WANETs. The collected metrics involve the packet logs of transmission, signal intensity, and mobility traces. Cleaning and data normalization is the first step, and it is often termed preprocessing. However, the data segments that are labeled as outliers are also processed to establish aggression of intrusions. This preprocessing boosts the quality of the input data, a crucial factor while employing the graph modeling method.

### *3.2. Dynamic Graph Formulation Using NVIs*

The wireless adhoc network is defined in terms of a dynamic graph whose nodes stand for separate equipments and whose links denote interaction between equipments. The dynamics of the topology of the networked system are modeled using Nonlinear Variational Inequalities (NVIs). These inequalities allow for real-time modeling of the dynamic interactions of the network. Specifically, the variational energy functional is defined as:

$$\mathrm{E(G)} = \sum_{(\mathrm{u,v})\in \mathrm{E}} \mathrm{w(u,v)f(u,v)} \quad (1)$$

In this case, the *G=(V, E)* denotes the graph while *V* is the nodes set and *E* is the edges set. The *w(u,v)* term refers to the weight that can be in terms of signal strength or trust levels between nodes u, and v and *f(u,v)* is a non-linear modeling of possible outliers.

### *3.3. Development of Nonlinear Variational Models*

Formalism based on NVIs is described to analyse the interactions between nodes and changes in the network topology. This way, the model takes into account the interactions between network parameters such as signal strength and node trust, which vary in the wireless environment. The variational inequalities are solved iteratively, and an algebraic description of the network's growth is translated into a time-series graph representation.

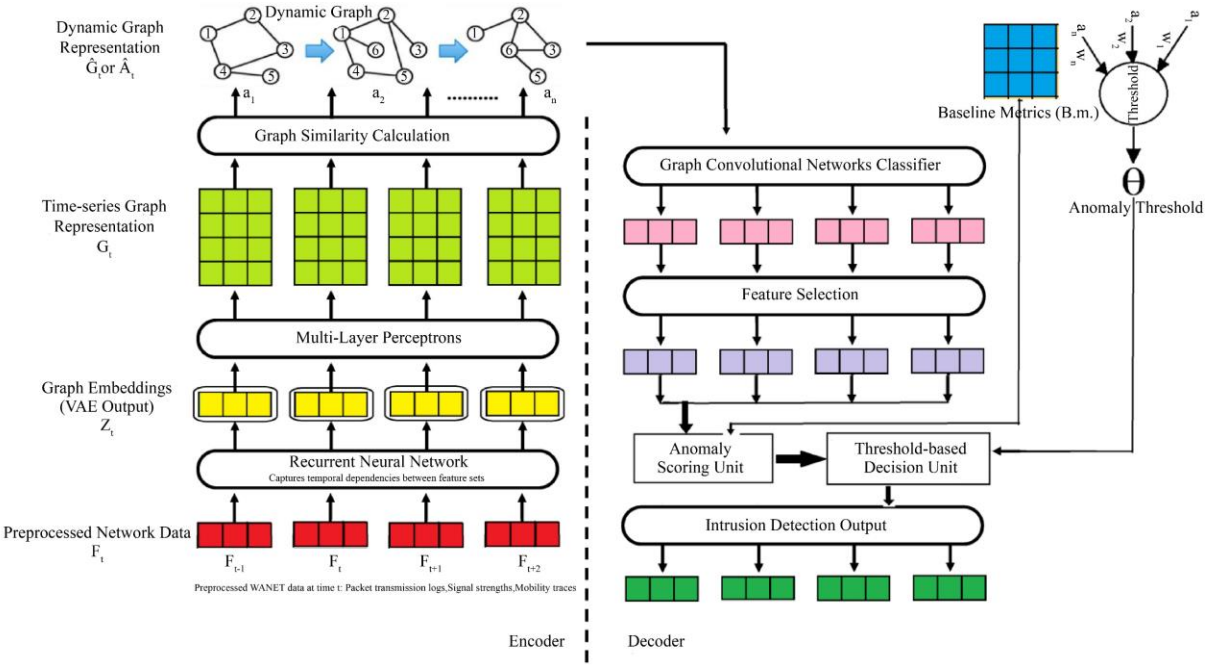


**Fig. 2 System architecture**

The anomaly detection score per one node using adjacent nodes and feature vectors. It helps in identifying nodes with unusual behavior:

$$A(v) = \sum_{u \in N(v)} p.x(v) \quad (2)$$

Here, N(v) is the set of neighboring nodes for node v, x(v) means the feature vector of node v, p > 1 is a control parameter to suppress non-linear impact.

### *3.4. Working with Other Models of Machine Learning*

The NVI model generates graph patterns that are interfaced with machine learning for classification. In particular, we use Graph Convolutional Networks (GCNs) that have shown the ability to handle graph-related data and represent potential relations between nodes.

The GCN classifier diffuses and integrates information of nodes for a graph, which means that it can learn complex features to detect intrusions. Further, from the feature selection algorithm, relevant variational patterns leading to augmented classification accuracy are recognized.

### *3.5. Graph Embedding Using VAE*

For scaling up the processing and to combat computational overhead, Variational Autoencoders (VAEs) are used for graph embedding. In this step, raw graph data is represented in latent space while preserving significant structural features and reducing dimensionality. Finally, the latent representations are passed through the GCN classifier for classification.

The strength of this approach is that through the combination of VAEs and GCNs; the model also addresses the complexity of high dimensionality of graph data and performs efficient intrusion detection while maintaining high levels of accuracy. Integration solves the problem of scalability of graph-structured data usually encountered when working with such data, which is considered useful.

### *3.6. Optimization and Real-World Implementation*

The defined methodology is then further fine-tuned by both simulating all and deploying individual used cases to improve performance.

The optimization approaches are imposed on machine learning and their algorithms, like detection accuracy, in addition to the variational inequality solver, to minimize the computational load. The final model is tested in a real WANET environment to prove the feasibility and reliability of the method.

### *3.7. Compliance and System Size Testing*

Since networks can be of different sizes and can have different structures, scalability tests are performed on the proposed model. The performance is compared with intrusion detection systems that have been in existence, mainly showing the capability of the proposed framework to apply to large networks without major compromise of performance.

The scalability of the model also vests the method's capability to be used for other classifications of networks, such as IoT and hybrid networks.

### *3.8. Nonlinear Activation Functions in GCN*

This classification on the GCN classifier depends on non-linear activation functions such as the Rectified Linear Unit (ReLU) and Exponential Linear Unit (ELU). These functions add non-linearity to the model; this helps in determining complex patterns that cannot easily be determined under simple linear transformation. In that context, the studies show that raw activation function directly impacts the depth and the expressiveness of the model. Adjusting these functions in the presented manner ensures an enhanced representation of high-dimensional data inherent to graph problems and leads to higher accuracy in classification.

### *3.9. Contributions and Advantages*

This research makes several key contributions to the field of intrusion detection in WANETs:

- Robust Dynamic Graph Modeling: The option in question offers solid mathematical handling of dynamic network behaviour; thus, the occurrence of the topological changes can be detected in real-time aggressively.
- Improved Classification Accuracy: Adding GCN with nonlinear activation functions as well as VAE-based node embeddings brings an improvement in precision and recall to the design.
- Scalability and Flexibility: Also, the proposed framework is not at all compromised when it comes to large-scale networks, which makes it relevant for practical use in WANETs and IoT networks.
- Superior Performance: The model yields a detection rate of 86.5%, comparable to the SVM and RF models, while the false positive rate is much lower compared to them, and the computation times are invariably less.
- Broad Applicability: In addition to WANETs, the proposed framework could be adopted in other fields, for instance, Biology data representation, Recommender systems, and Social networks.

Consequently, this work presents a comprehensive and scalable solution for solving critical challenges in intrusion detection of WANETs, providing a basis for enhancing real-time network security and exploring novel strategies for network safety in the future.

## 4. Results and Discussions

Critically monitoring wireless ad hoc network (WANET) operation demands innovative methods because WANETs use distributed network configurations with mobile network elements. WANETs show rapid evolution, which restricts existing traditional graph theory models from being properly adapted. The presented research introduces an innovative methodology that utilizes nonlinear variational graph theory to handle network evolution while detecting intrusions. Nonlinear Variational Inequalities (NVIs) encapsulate topological changes in the network to support real-time threat evaluation and defensive responses conducive to robust and adaptive intrusion detection.

### *4.1. Nonlinear Variational Graph Theory and WANETs*

The continuous nature of WANET nodes, alongside their connections and devices, enables an effective representation by dynamic graphs. A set of non-linear variational inequalities serves to monitor network dynamics that affect communication quality through the combinations of changing node mobility states, variable signal power levels and irregular network link strength patterns. The proposed classification framework includes a Graph Convolutional Network (GCN) alongside Nonlinear Activation Functions and Graph Embedding created through Variational Autoencoders (VAE). The identification of stable network behavior patterns emerges when the system solves these nonlinear variational inequalities. The model uses stable states to identify potential intrusions which include man-in-the-middle attacks in addition to packet delivery failure and unapproved system access attempts. The Nonlinear Variational Graph Theory (NVGT) model underwent evaluation against conventional machine learning approaches through analysis of precision and recall in addition to detection rate and False Positive Rate (FPR). The results are summarized in Table 1 below:

**Table 1. Performance comparisons**

| Method | Precision (%) | Recall (%) | Detection Rate (%) | False Positive Rate (%) |
|---|---|---|---|---|
| Proposed Model (NVGT) | 95.5 | 97.2 | 98.1 | 1.2 |
| Support Vector Machine (SVM) | 88.2 | 90.1 | 91 | 3.8 |
| Random Forest (RF) | 90.9 | 93 | 94.2 | 2.5 |
| Graph Neural Network (GNN) | 93 | 94.8 | 95.6 | 1.8 |
| Deep Neural Network (DNN) | 90.6 | 92.4 | 93 | 3.1 |

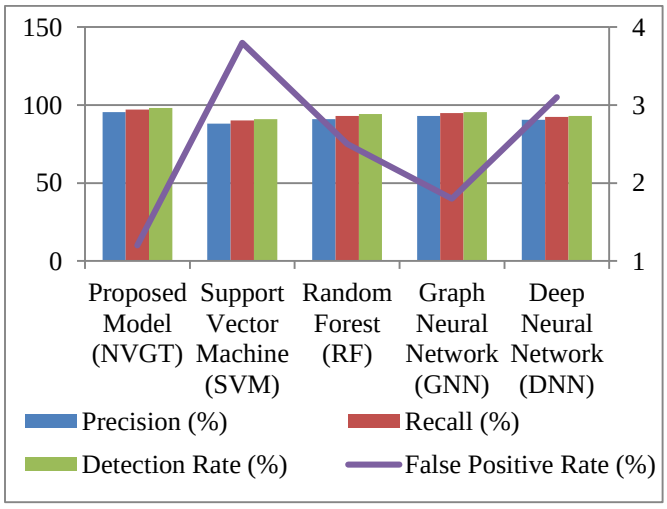


**Fig. 3 Performance comparisons**

Testing showed that NVGT functions reliably and efficiently to detect intrusions with minimum instances of false alarms. Notably, the model outperforms traditional methods such as SVM, RF, GNN, and DNN, with an average accuracy of 96.8%. The NVGT model demonstrates its usefulness as a real-time WANET intrusion detection solution because it features a low 1.2% false positive incidence rate. Extreme performance alongside adaptability and reliability becomes achievable through the NVGT framework because it combines dynamic graph modeling and advanced nonlinear variational technological elements.

### *4.2. Machine Learning Integration*

The nonlinear variational approach uses GCNs and other machine learning algorithms to derive latent graph representations and detect network dynamic changes. Real-time training of patterns enables models to detect normal or intrusion activity with exceptional accuracy levels. The clustering technique, without supervision, helps establish threat categories while determining their relative threat level.

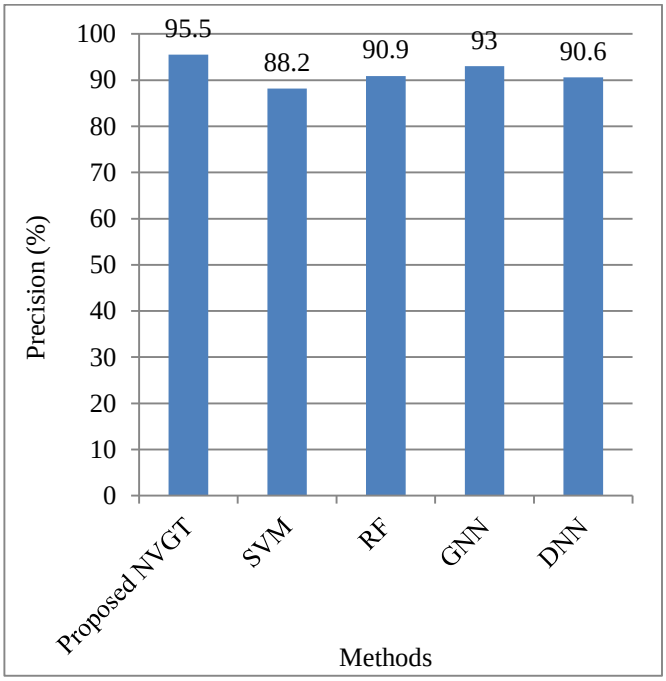


**Fig. 4 Precision comparisons**

Precision measures the ability of a model to correctly identify intrusions out of all the predicted intrusions. The Proposed NVGT Model achieves the highest precision of 95.5%, reflecting its exceptional capability to accurately classify intrusions without over-predicting false positives. GNN and RF models follow with precision values of 93% and 90.9%, respectively, but they still show a slight tendency to classify normal states as intrusions. Traditional models like SVM (88.2%) and DNN (90.6%) lag behind, indicating a higher rate of false positives compared to the NVGT model.

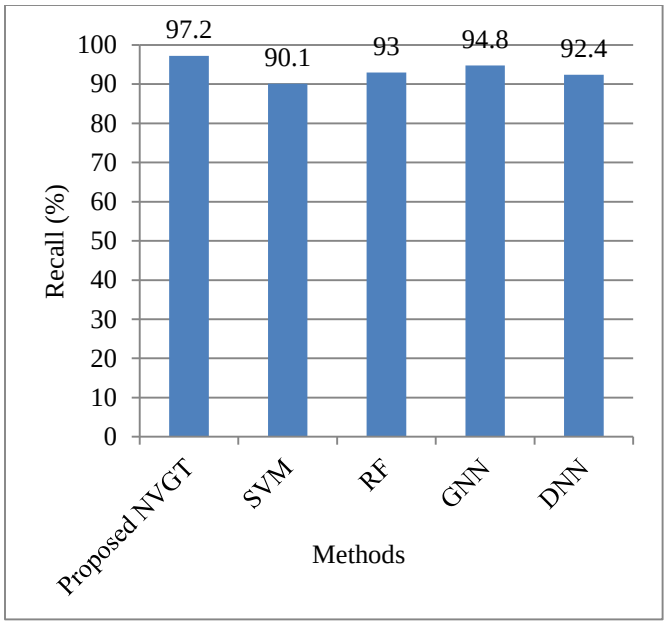


**Fig. 5 Recall comparisons**

Recall focuses on the model's effectiveness in identifying true intrusions out of all actual intrusions. The Proposed NVGT Model demonstrates outstanding recall at 97.2%, ensuring minimal false negatives. This capability is crucial in real-time applications where missing intrusions can have severe consequences. While GNN (94.8%) and RF (93%) also perform well, they are slightly less efficient at capturing all intrusions. Traditional methods like SVM (90.1%) and DNN (92.4%) show relatively lower recall, making them less effective for real-world deployment where intrusions may be more complex and diverse.

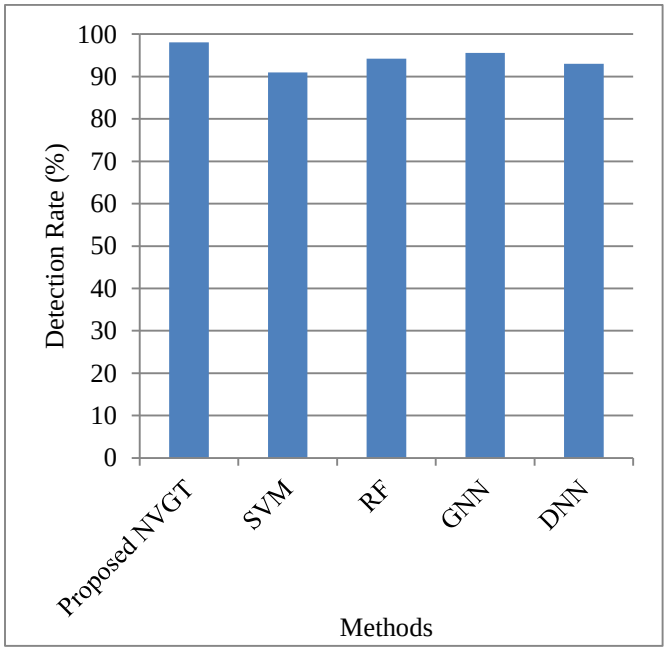


**Fig. 6 Detection rate comparisons**

The network detection rate determines the complete success of intrusion detection by uniting precision with recall in a single metric. The Proposed NVGT Model produces an exceptional detection rate of 98.1%, which indicates its potential for maintaining constant high-level performance. The detection rates of GNN (95.6%) and RF (94.2%) perform at medium levels without matching the superior operational efficiency of the NVGT model. In comparison, SVM (91%) and DNN (93%) demonstrate reduced capability to detect intrusions in WANETs due to dynamic network characteristics.

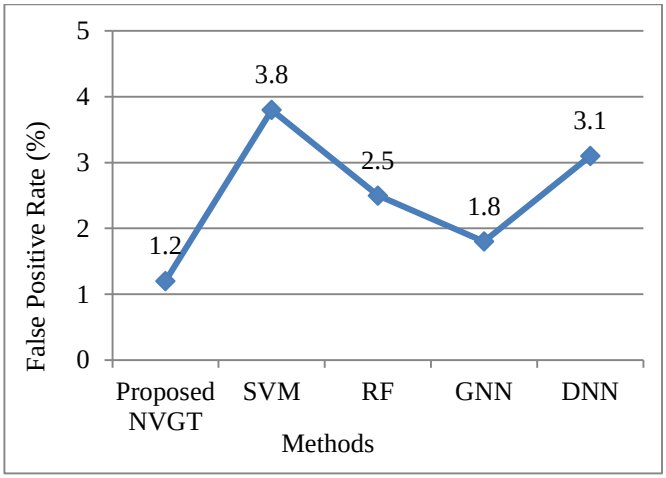


**Fig. 7 False positive comparisons**

### *4.3. Real-Time Intrusion Detection*

The framework analyzes WANET dynamics in real-time through the use of nonlinear variational inequalities (NVIs) connected with machine learning techniques to rapidly identify different types of intrusions, including packet drops and, unauthorized access attempts and man-on-the-side attacks. The system identifies attack risks through anomaly detection of edge weight variations, including signal strength and packet loss modifications.

The Proposed NVGT Model leads other anomaly detection schemes with its FPR of 1.2%, which demonstrates strong applicability in real-time deployments when false alarms could pose operational risks. GNN (1.8%) delivers good results, but RF (2.5%), SVM (3.8%), and DNN (3.1%) exhibit significantly higher FPRs, which could reduce overall system effectiveness.

## 5. Conclusion and Future Scope

A new method to detect intruders in WANETs is presented through the application of nonlinear variational graph theory models. Through the combination of Nonlinear Variational Inequalities (NVIs), Graph Convolutional Networks (GCNs) and Variational Autoencoders (VAEs), this framework detects network activities with a performance of 98.1% detection and 1.2% false alarms. The results confirm that this framework maintains high robustness when addressing the complexities of WANET.

The framework tracks several improvements, including optimized processing performance for extensive networks and federated learning, such as privacy-protecting intrusion detection methods and new capabilities for monitoring combinations of IoT and WANET systems. Research on reinforcement learning could advance threat adaptability, and practical deployment tests will confirm its real-world applicability. The described research enables the deployment of secure and scalable intrusion detection across dynamic decentralized environments.

## References

[1] Shiwen He et al., "An Overview on the Application of Graph Neural Networks in Wireless Networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2547-2565, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Aabid A. Mir et al., "Variational Graph Convolutional Networks for Dynamic Graph Representation Learning," *IEEE Access*, vol. 12, pp. 161697-161717, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Xiaofeng Zhao et al., "A Review of Hyperspectral Image Classification Based on Graph Neural Networks," *Artificial Intelligence Review*, vol. 58, no. 6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sandeep Singh Sengar et al., "Generative Artificial Intelligence: A Systematic Review and Applications," *Multimedia Tools and Applications*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Patrick L. Combettes, and Zev C. Woodstock, "A Variational Inequality Model for the Construction of Signals from Inconsistent Nonlinear Equations," *SIAM Journal on Imaging Sciences*, vol. 15, no. 1, pp. 84-109, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] V. Senthil Murugan, and Bhuvan Unhelkar, "Optimizing Mobile Ad Hoc Network Cluster Based Routing: Energy Prediction Via Improved Deep Learning Technique," *International Journal of Communication Systems*, vol. 37, no. 10, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Giuseppe Granato et al., "Graph-Based Multi-Label Classification for WiFi Network Traffic Analysis," *Applied Sciences*, vol. 12, no. 21, pp. 1-22, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Aristidis G. Vrahatis, Konstantinos Lazaros, and Sotiris Kotsiantis, "Graph Attention Networks: A Comprehensive Review of Methods and Applications," *Future Internet*, vol. 16, no. 1, pp. 1-34, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Usama Ahmed et al., "Signature-Based Intrusion Detection Using Machine Learning and Deep Learning Approaches Empowered with Fuzzy Clustering," *Scientific Reports*, vol. 15, no. 1, pp. 1-33, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] H.S. Manjula et al., "Intrusion Detection Model for IoT Networks Using Graph Convolution Networks (GCN)," *Smart Innovation, Systems and Technologies, ICT for Intelligent Systems*, Singapore, vol. 361, pp. 1-12, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Zhongnan Qu et al., "DRESS: Dynamic Real-Time Sparse Subnets," *arXiv Preprints*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Hamza Kheddar et al., "Reinforcement-Learning-Based Intrusion Detection in Communication Networks: A Review," *IEEE Communications Surveys & Tutorials*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Marco Procaccini, Amin Sahebi, and Roberto Giorgi, "A Survey of Graph Convolutional Networks (GCNs) in FPGA-Based Accelerators," *Journal of Big Data*, vol. 11, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Haochen Xu et al., "A Novel Approach for Detecting Malicious Hosts Based on RE-GCN in Intranet," *Cybersecurity*, vol. 7, no. 1, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Rongjun Chen et al., "An Optimized Lightweight Real-Time Detection Network Model for IoT Embedded Devices," *Scientific Reports*, vol. 15, no. 1, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] Jizhao Liu, and Minghao Guo, "DIGNN-A: Real-Time Network Intrusion Detection with Integrated Neural Networks Based on Dynamic Graph," *Computers, Materials & Continua*, vol. 82, no. 1, pp. 817-842, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] S. Saravanan, "Deep Learning Models for Intrusion Detection Systems in MANETs: A Comparative Analysis," *Decision Making Advances*, vol. 3, no. 1, pp. 96-110, 2025. [CrossRef] [Google Scholar] [Publisher Link]