Intelligent Network Traffic Prediction Using Graph Neural Networks

Mr.T.Dineshkumar[1], Ranjithkumar P[2], Vishak P M[3], Yukendran S[4]
[1, 2, 3, 4] Dept of Electronics and Communication Engineering
[1, 2, 3, 4] kongunadu College of Engineering and Technology, Tiruchirapalli,Tamilnadu,India.

Abstract- *The widespread deployment of wireless communication technology has made the Wi-Fi network more susceptible to sophisticated cyber-attacks, which include de-authentication attacks, rogue access points, traffic flooding, and protocol misuse. The limitation of the traditional intrusion detection system in detecting unknown attacks in real-time has led to the development of this paper, which presents an intelligent real-time detection system for Wi-Fi network attacks using machine learning and Graph Neural Networks (GNNs) technology. The proposed system monitors the Wi-Fi network traffic in real-time and extracts essential features from the IEEE 802.11 protocol frames, which include packet rates, signal strength, protocol behaviour, and time-based features.*

The proposed system uses the extracted features to classify the network behaviour as normal or abnormal using the trained machine learning models. The proposed system effectively uses the GNN technology to detect the complex relationships between the network entities, which makes it more efficient in detecting network intrusions.

The proposed system has been tested and found effective in terms of accuracy, reducing false positives, and ensuring real-time detection of network intrusions, which makes it more suitable for modern enterprise and public network environments.

Keywords: Wi-Fi Security, Intrusion Detection System, Machine Learning, Graph Neural Networks, Network Traffic Analysis, Wireless Attacks.

I. INTRODUCTION

Wireless networks are the foundation of digital communication in the modern world. Various applications of wireless networks range from personal usage to organisational needs. Even though wireless networks provide a number of advantages, they are still vulnerable to attacks due to their open medium of transmission. Various attacks on a Wi-Fi network include de-authentication attacks, evil twin access point attacks, packet injection attacks, and denial of service attacks.

Conventional intrusion detection systems utiliseseveral techniques, namely, predefined rules and signature-based techniques. These techniques are only effective in detecting known attacks. However, the detection of unknown attacks is difficult using this method, and the system may produce a high number of false alarms in response to changes in traffic patterns. The need for the development of more efficient intrusion detection systems is increasing in response to the increasing complexity of attacks on a Wi-Fi network.

Our project discusses a real-time Wi-Fi network attack detection system based on machine learning and Graph Neural Networks. The system is effective in detecting attacks on a Wi-Fi network in real time.

Recent advancements in machine learning have made it possible for data-driven intrusion detection systems, which can be trained to recognise complex patterns of network traffic.

However, most conventional ML-based intrusion detection system approaches treat network traffic as isolated data points, failing to recognise its inherent relationships. Graph Neural Networks offer a promising solution by modelling a wireless network as a graph, allowing for learning relational and structural dependencies. This paper presents a study of using GNNs in real-time analysis of Wi-Fi network traffic.

II. SYSTEM ARCHITECTURE FOR INTELLIGENT NETWORK TRAFFIC PREDICTION USING GRAPH NEURAL NETWORKS

The proposed system architecture is designed to provide continuous monitoring, intelligent analysis, and rapid response to Wi-Fi attacks. It consists of three interconnected layers that work together to ensure reliable and real-time intrusion detection.

A] Traffic Capture and Monitoring Layer

This layer is in charge of the real-time acquisition of the Wi-Fi traffic through packet sniffing techniques. The management, control, and data frames specified in the IEEE 802.11 protocol are acquired in this layer. The parameters of interest include the RSSI, packet transmission rate, subtype, source, and destination identifiers. The monitoring of the traffic is crucial in allowing the system to detect not only the expected behaviour of the traffic but also any unusual changes in the traffic, which may be a result of a cyber attack.

B] Feature Processing and Learning Layer

The traffic features that are extracted are processed and arranged into a structured form as graphs. Each node in the graphs represents a wireless device or an access point.

The edges represent the interactions between the devices. The feature vectors of the nodes and edges contain information regarding the characteristics of the traffic flows. The machine learning classifiers that are associated with Graph Neural Networks are used to analyse the graphs to identify abnormal patterns that are associated with the attacks.

C] Alert and Response Layer

When malicious activities are detected, the system sends real-time alerts to the network administrators. The alert system facilitates the visualisation of the type of attack, nodes, and the severity of the attack. The alert and response layer facilitates quick response mechanisms, for instance, isolating the nodes, blocking the access points, etc.

D] SystemOverview

The proposed system will be called the "Real-Time Wi-Fi Attack Detection System," and its primary function will be the detection of malicious activities in the wireless network with the help of intelligent machine learning approaches.

III.WI-FI ATTACK DETECTION MODEL

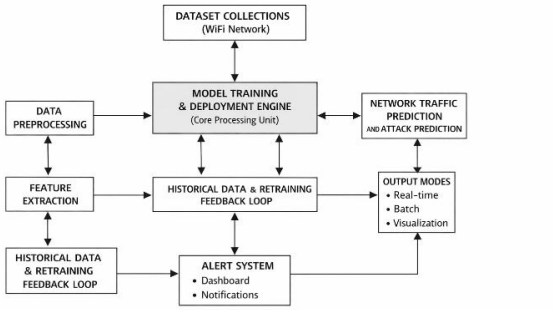
The Wi-Fi attack detection model is a behaviour-based intrusion detection system designed to continuously observe, analyse, and learn from wireless network traffic. The model focuses on identifying deviations from normal communication patterns rather than relying on predefined attack signatures. This adaptive approach allows the system to remain effective even when facing novel or evolving Wi-Fi attack techniques.

A. Traffic Monitoring and Data Collection

The model works by passively monitoring the Wi-Fi traffic at the access point or network gateway level.

It collects important information like the header of the packets, types of frames, transmission speeds, RSSI, authentication requests, and other fields specific to the protocol used.

These details are collected over time, creating a holistic view of normal and abnormal network behaviour.In a graph representation, each node will be a device, and each edge will be a relationship or interaction of some sort. This will enable the system to analyse the relationship of different devices in a network.



The system continuously monitors Wi-Fi traffic by capturing IEEE 802.11 frames via packet sniffing techniques. Raw Wi-Fi traffic is preprocessed to eliminate noise and extract relevant features, such as packet rate, frame type distribution, signal strength, protocol, MAC address, and temporal characteristics.

The classifier, after being trained, evaluates the features and determines if the network behaviour is normal or malicious. The system is capable of detecting various types of Wi-Fi attacks, including de-authentication attacks, denial of service flooding, rogue access points, MAC address spoofing, and packet injection attacks.

B. Feature Extraction and Temporal Analysis

The traffic features that are extracted are subjected to temporal analysis to identify the patterns of behaviour. The model will analyse the arrival rates of packets, the pattern of bursts, session times, retransmission rates, and signal strength. Sudden surges in the volume of traffic, authentication failures, abnormal sequencing of frames, or variations in timing are treated as suspicious behaviour.

Temporal modelling helps in the detection of attacks like flooding and denial of service, where unusual bursts of

packets are sent within a small time frame, as well as slow and stealthy attacks, where the attacks occur gradually over a period of time.

C. Graph-Based Network Representation

To effectively represent the interaction of multiple devices, the system will use a graph representation of the Wi-Fi environment. In a graph representation, each node will be a device, and each edge will be a relationship or interaction of some sort. This will enable the system to analyse the relationship of different devices in a network.

This representation will be highly effective at detecting coordinated attacks involving multiple nodes, such as an evil twin or a distributed flooding attack, that aim to mislead legitimate users or overwhelm the network.

D. Learning and Anomaly Detection Mechanism

In the detection model, a learning process takes place to establish a standard representation of normal Wi-Fi activity using past traffic patterns. By using a machine learning or graph neural network approach, the system is able to encode the spatial and temporal patterns of the traffic graph. Any major deviation in the learned representation is considered abnormal.In the anomaly detection process, a risk score is provided to the traffic flow, device, or session.

Depending on the thresholds set, the system categorises the activity as normal, suspicious, or malicious. This adaptive learning approach helps the system to be effective against zero-day attacks and minimises false positives due to normal variations.

E. Response and Alert Generation

Once the attack is detected, the system can generate alerts in real-time to notify the network administrators about the attack. The alerts can include details about the type of attack, devices involved, severity, and time of occurrence.

The model can also include a feature to respond to the attack automatically, such as isolating the attacking node, blocking suspicious traffic, or re-authenticating the nodes to ensure the security of the network.

F. Advantages of the Proposed Model

The Wi-Fi attack detection model has the following advantages:

Its adaptability to the dynamic nature of the wireless environment, its effectiveness in identifying unknown and zero-day attacks, its effectiveness in identifying coordinated and distributed attacks, and its reduced dependency on manually crafted signatures. Its scalability in dealing with dense heterogeneous Wi-Fi networks.

IV. METHODOLOGY

A] INTRODUCTION

The proposed Wi-Fi attack detection system follows a systematic methodology consisting of data collection, preprocessing, feature extraction, graph construction, learning, and classification. This structured approach ensures accurate modelling of network behaviour and effective detection of malicious activities in dynamic wireless environments.

B] Data Collection and Preprocessing

In the data collection phase, the data is collected using tools that perform packet sniffing and monitoring of the Wi-Fi traffic.

This data is monitored and collected when the Wi-Fi is under normal conditions and when attacks such as flooding attacks, unauthorised access, evil twin access points, and protocol misuse are launched. In the data preprocessing phase, the data is filtered to eliminate duplicate data, invalid data, and broadcasting noise. Additionally, the data is synchronised to ensure that it has a consistent timestamp.

This helps to prevent any inconsistencies during the training of the data. Furthermore, the data is normalised using the min-max normalisation method to prevent any biases during the training of the data.

C] Feature Extraction

From the preprocessed traffic data, a set of discriminative features is derived to describe normal and malicious network behaviour. The features include the rate of packet arrival, frame types, authentication request rates, retransmission counts, signal strength variation, protocol compliance features, and session duration features.

Temporal correlations between packets are also examined to detect short-term bursts in traffic and long-term trends in behaviour. For example, sudden spikes in the rate of transmission of packets can point to a possible flooding attack, or unusual signal strength changes can point to the presence of rogue or evil twin access points. By using these features, the

model achieves a complete understanding of Wi-Fi traffic under varied conditions.

D] Graph Construction and Representation

For the purpose of understanding the complex relationships involved in the wireless network, the features are represented using a graph-based representation. In the graph representation, the individual elements of the network, such as the access point or the devices, are represented as nodes. The relationships between the devices or the communication signals exchanged between the devices and the access point are represented using the edges. The weights associated with the edges may represent the communication frequency or the similarity in the signal strength.

Such a representation is useful for understanding the spatial and temporal relationships involved in the wireless network. The graph is updated dynamically using a time window to represent the changes in the behaviour of the devices. This representation is useful for identifying the distributed attacks that cannot be understood using individual communication patterns.

E] Graph-Based Learning with GNN

The graphs are further utilised with Graph Neural Networks (GNN), which learn meaningful representations of the behaviour of the devices. The GNNs are capable of gathering information from neighbouring nodes as well as edges. This helps the model learn the local traffic patterns as well as the overall network. The message-passing property of the GNN helps in learning the relational properties of the Wi-Fi network.

The GNN is further capable of learning to differentiate between normal communication patterns and anomalous communication patterns through iterative training. The learned representations gather information about temporal patterns, relationships, and protocol compliance.

F] Classification and Decision Making

Finally, the output embeddings from the GNN are input into a classification layer for the purpose of classifying the activity on the network as normal or malicious. In the case of a multi-class problem, the network traffic can be classified into a variety of attack categories, such as flooding attacks, unauthorised access attacks, evil twin attacks, or protocol misuse attacks.

The decision-making module is the final stage of the GNN-based IDS/IPS architecture. This module is responsible for the generation of alerts for the identified attacks.

G] Performance Evaluation

The performance of the proposed methodology is evaluated using various performance metrics such as accuracy, precision, recall, F1-score, and false positive rate. The performance of the model is examined with respect to various types of attacks and traffic loads to assess the robustness and adaptability of the model with respect to real-world Wi-Fi networks.

V. IMPLEMENTATION

The deployment of the proposed Intelligent Real-Time Wi-Fi Attack Detection System is centred on the real-world application of machine learning and Graph Neural Network (GNN) approaches for the constant monitoring of wireless security. The proposed system is capable of functioning in real-time, thereby allowing for instant detection of any malicious events with little delay. The entire deployment process is broken down into several stages.

A] Traffic Monitoring Module

This module has the responsibility of monitoring wireless network traffic in real-time. The module is charged with the responsibility of capturing traffic in the form of packets that are received and sent through access points and other devices without interrupting the communication process. The module is concerned with the monitoring of raw traffic information such as transmission rate, connection attempts, and communication patterns. The module is designed to ensure that the monitoring process is passive and scalable to accommodate different levels of traffic.

B] Data Preprocessing Module

The Data Preprocessing Module refines the captured traffic by removing redundant, inconsistent, or incomplete data. It normalises data formats, manages missing data, and removes unnecessary attributes to enhance analytical insights. Noise removal methods are employed to ensure that only relevant information is passed to the succeeding phase. This module optimises computational speed by simplifying data complexity without compromising key characteristics. Organising and cleaning data sets produced in this stage facilitates precise feature extraction and correct classification, ultimately improving the efficiency of the detection system.

C] Feature Engineering Module

This module extracts analytical features from organised network data. It extracts behavioural, statistical, and temporal patterns like traffic volume, signal variation, frame ratio, and protocol anomalies. By translating raw packet data into quantifiable features, it optimises the learning capacity of predictive models. Feature extraction methods are used to select only the most relevant parameters, thus optimising processing speed. Successful feature engineering has a direct impact on the accuracy of the detection system and ensures the correct interpretation of wireless activity patterns.

D] Machine Learning Classification Module

The Machine Learning Classification Module is responsible for the classification of extracted features based on trained predictive models. The module is able to identify patterns of legitimate communication and malicious activities via supervised or unsupervised learning models. After training the model, it is able to classify new data with minimal latency. This module is focused on accuracy, efficiency, and adaptability to changing traffic patterns. The module uses intelligence from data instead of rules to improve the system's ability to identify complex attack patterns that have never been seen before.

VI. RESULT AND DISCUSSION

The deployment of the Intelligent Real-Time WiFi Attack Detection System has proved the effectiveness of the system in detecting malicious wireless activities with improved accuracy and faster response times. The system was tested using various network traffic patterns that included both normal and attack traffic. The system was able to accurately capture real-time traffic and classify it based on its attributes.

The feature engineering phase played a critical role in improving the detection accuracy of the system by filtering out relevant attributes from raw packet data. The classification module of the system was able to distinguish between normal and attack traffic with high accuracy.

False positives were eliminated through improved preprocessing and strategic feature optimisation, which ensured that the system did not confuse normal traffic patterns with attack traffic.

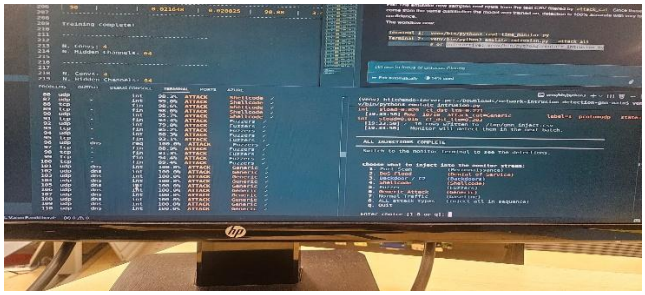
Real-time alerting was done effectively to enable the system to quickly point out any malicious activity without any delay. The adaptive learning component of the system further enhanced the system's resilience by adding new traffic patterns to the analytical model. This ensured that the system performed well even when faced with new or modified attack behaviours.

In general, the experimental results have confirmed that the integration of machine learning with continuous wireless monitoring is an effective approach to improve the detection precision and operational reliability. The proposed framework has successfully fulfilled its purpose of providing proactive, intelligent, and scalable security protection for Wi-Fi networks.

The results of the proposed system emphasise the need to move from static security systems to adaptive and data-driven systems in wireless networks. This is because traditional systems have difficulty adapting to changing strategies used by intruders, as they are highly dependent on signatures. However, the intelligent system used in this project showed greater adaptability as it was able to learn patterns of traffic behaviour instead of depending on predefined rules.

The efficiency of the system can be attributed to the fact that it used comprehensive feature extraction and real-time analytical processing. The behavioural and temporal features used in the system provided greater insight into network behaviour, allowing for more precise classification decisions. The decrease in false positives also suggests that the system uses contextual pattern recognition to identify legitimate variations from actual threats.

Another important point to note is the role of adaptive learning in maintaining the efficiency of the system over time. This is because wireless networks often experience fluctuations in usage patterns and device behaviour.



Therefore, the continuous adaptation of the system ensures that it remains relevant and effective.

The scalability factor further reinforces the applicability of the framework. The framework's ability to perform analysis even under heavy traffic conditions makes it suitable for use in enterprise and public WiFi networks. The

efficient processing of data also ensures that the framework does not affect the network resources.

VII. CONCLUSION

The Intelligent Real-Time Wi-Fi Attack Detection System is proof of the importance of adaptive and data-driven security solutions in securing contemporary wireless networks. With the continued use of WiFi networks to facilitate critical digital services, the need for securing these networks against emerging cyber threats has become more pressing than ever before. This research work aimed at the limitations of traditional security solutions by combining continuous traffic monitoring, systematic feature development, and machine learning-based classification in a single platform.

The system was able to create a proactive detection platform that can detect malicious activities with a higher degree of accuracy and in real time.

By concentrating on behavioural and temporal aspects of traffic patterns, the system improved its capacity to detect actual network anomalies from legitimate network fluctuations. The addition of adaptive learning further improved the long-term accuracy of the system by allowing the system to adapt to emerging attack patterns.

Scalability and efficiency were ensured through optimised data processing and intelligent classification systems.

On the whole, the proposed framework is a concept-based innovation in wireless cybersecurity, proving that intelligent monitoring and predictive modelling can greatly improve the detection capability and enhance service continuity in a dynamic Wi-Fi environment.

VIII. ACKNOWLEDGMENT

The authors would like to extend their sincere thanks to the management of Kongunadu College of Engineering and Technology (Autonomous), Trichy, for providing a conducive academic environment and necessary infrastructure to successfully complete this research work. The support and encouragement provided by the institution have played a crucial role in the successful completion of this project.

The authors would like to extend their sincere thanks to the Department of Electronics and Communication Engineering for their constant guidance, support, and provision of laboratory facilities throughout the course of this project. The collaborative academic environment provided by the department has significantly contributed to the development and implementation of the proposed system.

Special thanks are due to the project guide, Mr. T. Dinesh Kumar, M.E., (Ph.D.)., Assistant Professor, Department of ECE, for his constant guidance, motivation, and valuable suggestions throughout the course of this project. His expertise and contributions have significantly contributed to the development of this research.

REFERENCES

[1] D. Koutras, P. Dimitrellos, P. Kotzanikolaou and C. Douligeris, "Automated WiFi Incident Detection Attack Tool on 802.11 Networks," 2023 IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 2023, pp. 464-469, doi: 10.1109/ISCC58397.2023.10218077.

[2] P. Škrak, P. Lehoczký, R. Bencel, M. Galinski and I. Kotuliak, "Improved Preprocessing for Machine Learning Intrusion Detection in IEEE 802.11," 2022 14th IFIP Wireless and Mobile Networking Conference (WMNC), Sousse, Tunisia, 2022, pp. 118-122, doi: 10.23919/WMNC56391.2022.9954288.

[3] R. Saini, D. Halder and A. M. Baswade, "RIDS: Real-time Intrusion Detection System for WPA3 enabled Enterprise Networks," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 43-48, doi: 10.1109/GLOBECOM48099.2022.10001501.

[4] X. Li, S. Lahoud and N. Zincir-Heywood, "Unsupervised Anomaly Detection for Wi-Fi Networks using RFFI," 2025 21st International Conference on Network and Service Management (CNSM), Bologna, Italy, 2025, pp. 1-5, doi: 10.23919/CNSM67658.2025.11297558.

[5] B. T. Alemu and A. J. Muhammed, "Controller-Targeted DDoS Attack Detection and Mitigation in Software-Defined Internet of Vehicles (SD-IoV)," 2023 International Conference on Information and Communication Technology for Development for Africa (ICT4DA), Bahir Dar, Ethiopia, 2023, pp. 138-143, doi: 10.1109/ICT4DA59526.2023.10302231.

[6] Y. Huang, X. Li, W. Wang, T. Jiang and Q. Zhang, "Forgery Attack Detection in Surveillance Video Streams Using Wi-Fi Channel State Information," in IEEE Transactions on Wireless Communications, vol. 21, no. 6, pp. 4340-4349, June 2022, doi: 10.1109/TWC.2021.3129188.

[7] M. Agarwal, "DES Based IDS for detection Minimal De-authentication DoS Attack in 802.11 Wi-Fi Networks," 2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS),

Hyderabad, India, 2021, pp. 143-148, doi: 10.1109/ANTS52808.2021.9936939.

[8] M. Zang and Y. Yan, "Machine Learning-Based Intrusion Detection System for Big Data Analytics in VANET," 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 2021, pp. 1-5, doi: 10.1109/VTC2021Spring51267.2021.9448878.

[9] N. Xhemajli and Z. Tafa, "Mobile Proxy in Public WiFi Networks: A Tool Against MITM Attacks," 2024 13th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2024, pp. 1-5, doi: 10.1109/MECO62516.2024.10577803.

[10] Tiwari, P. Bafna, A. Baheti, A. Pareek and A. Ratnaparkhi, "Wireless Attack Simulation of WiFi Threats: A Real-Time Scenario," 2025 Third International Conference on Industry 4.0 Technology (I4Tech), Pune, India, 2025, pp. 1-5, doi: 10.1109/I4Tech64670.2025.11277543.