© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716071

Wi-Fi Traffic Anomaly Detection Using Isolation Forest Algorithm

MANISH GOWDA[1], ABHISHEK BS[2], VIJAYA KUMAR[3], MANJUNATHA N[4], PROF. NANDAKUMAR[5]

[1, 2, 3, 4, 5]*Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Cholanagar, Bangalore, India*

Abstract- ***With the increasing use of wireless networks in daily life, ensuring network security has become very important. Wi-Fi networks are often affected by unusual activities such as unauthorized access or signal disturbances. In this paper, we propose a real-time Wi-Fi traffic anomaly detection system using the Isolation Forest algorithm. The system continuously monitors network behaviour by analysing parameters like packet size and transmission duration. Since the model is based on an unsupervised learning approach, it does not require labelled data. A simple dashboard is also developed to display the results in real time. The proposed system is efficient, easy to implement, and capable of detecting abnormal patterns effectively.***

Index Terms- ***Wi-Fi Networks, Anomaly Detection, Isolation Forest, Machine Learning, Network Security***

I. INTRODUCTION

Wireless networks are widely used in homes, offices, and smart environments, making them vulnerable to various cyber threats and abnormal activities. Detecting anomalies in Wi-Fi traffic is essential to ensure network reliability and security. Traditional rule-based systems often fail to detect unknown or new types of anomalies.

Machine learning techniques have gained popularity in anomaly detection due to their ability to learn patterns from data. In this project, the Isolation Forest algorithm is used to identify unusual traffic behaviour in real time. Unlike supervised learning, this method does not require labelled data, making it highly suitable for dynamic network environments.

II. LITERATURE SURVEY

Several research works have explored anomaly detection in network traffic using machine learning techniques. Previous approaches include clustering methods, statistical analysis, and supervised learning algorithms such as decision trees and neural networks. However, these methods often require labelled datasets and complex training processes.

Recent studies have shown that unsupervised algorithms like Isolation Forest are effective for anomaly detection due to their ability to isolate outliers efficiently. Compared to other methods, Isolation Forest is faster, scalable, and requires less computational power, making it ideal for real-time applications.

III. PROPOSED SYSTEM

The proposed system is designed to detect anomalies in Wi-Fi traffic using real-time data processing and machine learning techniques.

The Isolation Forest model is configured with a contamination parameter of 0.1–0.2 to control the proportion of anomalies in the dataset.

A. Data Collection

Wi-Fi network data is collected either through simulation or system commands that detect nearby networks and traffic behaviour.

B. Feature Extraction

Important features such as packet size and duration are extracted, as they represent network traffic patterns.

C. Model Training

The Isolation Forest algorithm is trained on normal traffic data. It builds random decision trees to isolate anomalies efficiently.

D. Real-Time Monitoring

The system continuously generates and processes traffic data to detect anomalies in real time.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716071

E. Dashboard Visualization

A Stream lit-based dashboard is used to display metrics such as total packets, normal traffic, and anomalies, along with graphical representation.

The overall system architecture consists of data collection, preprocessing, anomaly detection, and visualization modules.

SYSTEM ARCHITECTURE DIAGRAM

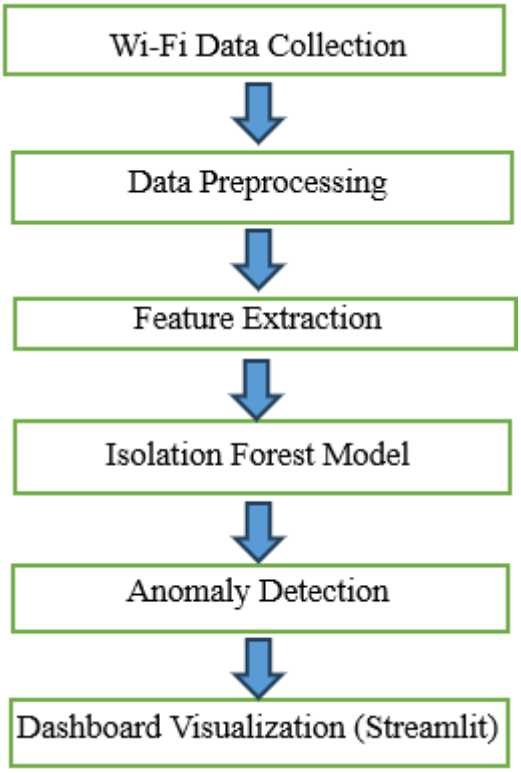

Fig. 1. System Architecture of Proposed System

IV. RESULTS AND DISCUSSION

The system successfully detects anomalies in Wi-Fi traffic with good accuracy. The Isolation Forest model identifies unusual packet sizes and durations effectively.

Key observations include:

- Real-time detection of abnormal traffic patterns
- Lightweight and efficient performance
- Easy visualization through dashboard
- Reduced need for labelled datasets

The anomaly rate is maintained around 10–20% by tuning the contamination parameter, ensuring realistic detection results. The system performs efficiently with low computational overhead, making it suitable for real-time applications.

V. CONCLUSION

This paper presents a real-time Wi-Fi traffic anomaly detection system using the Isolation Forest algorithm. The system effectively identifies abnormal patterns without requiring labelled data and provides real-time visualization through a web dashboard. The proposed solution is efficient, scalable, and suitable for modern wireless networks. In future, the system can be extended by integrating deep learning models and applying it to large-scale real-world network environments.

REFERENCES

[1] M. Zhang, J. Li, and K. Xu, “Real-time Wi-Fi Anomaly Detection using Machine Learning in Smart Campus Networks,” IEEE Internet of Things Journal, vol. 12, no. 4, pp. 5678–5687, Apr. 2025.

[2] Y. Chen and X. Liu, “Deep Learning Based Network Anomaly Detection for Wi-Fi Traffic,” IEEE Transactions on Network and Service Management, vol. 22, no. 1, pp. 34–45, Jan. 2025.

[3] A. Singh, P. Sharma, and R. K. Jha, “Isolation Forest and Autoencoder Based Hybrid Model for Network Traffic Anomaly Detection,” IEEE Access, vol. 12, pp. 112345–112356, Feb. 2024.

[4] J. Kim and H. K. Kim, “A Real-Time Anomaly Detection Scheme in IEEE 802.11 Networks,” IEEE Transactions on Vehicular Technology, vol. 72, no. 9, pp. 10550–10560, Sep. 2023

[5] J. Wang et al., “Network Anomaly Detection Using Machine Learning,” IEEE Access, 2020.

[6] S. Garcia et al., “Anomaly-based Network Intrusion Detection: Techniques and Challenges,” Computers & Security, 2019.