APPLICATION FOR MODELING ATTACKS IN WIRELESS NETWORKS AND DEVELOPING DETECTION METHODS

Yuan Zhiyong, Zhou Zhihua, Voronets V.
National Technical University «Kharkiv Polytechnic Institute», Kharkiv

With the growing complexity of wireless communication systems, ensuring their security against cyberattacks has become a top priority. This study presents an application developed for modeling various types of attacks in wireless networks and for testing the effectiveness of detection algorithms under different network conditions.

The application simulates popular attack types such as jamming, spoofing, Sybil, and wormhole attacks [1]. It allows users to configure network topology, mobility patterns, and traffic characteristics while injecting malicious behavior at defined time intervals. This setup provides a realistic testbed for evaluating detection techniques in controlled but diverse scenarios.

Detection methods based on statistical analysis, anomaly detection, and machine learning algorithms are integrated into the platform. These include threshold-based detectors, support vector machines (SVM), and deep learning models [2] trained on behavioral patterns of legitimate versus malicious nodes.

Implemented in Python with support for integration with NS-3 and Wireshark [3], the application provides comprehensive logging and visualization tools. Performance metrics such as detection accuracy, false alarm rate, and detection delay are automatically calculated.

The tool serves as a practical environment for cybersecurity research in wireless networks. It enables rapid prototyping and validation of intrusion detection systems (IDS), making it suitable for academic and industrial use.

The developed application provides a flexible and effective platform for simulating attacks in wireless networks and evaluating detection methods. It supports realistic testing, accelerates IDS development, and enhances cybersecurity research through integrated analytics and visualization tools.

References

1. Meleshko A., Desnitsky V. The Modeling and Detection of Attacks in Role-Based Self-Organized Decentralized Wireless Sensor Networks // Telecom. – 2024. – Vol. 5, No. 1. – pp. 145–175.

2. Manivannan R., Senthilkumar S. Intrusion Detection System for Network Security Using Novel Adaptive Recurrent Neural Network-Based Fox Optimizer Concept // International Journal of Computational Intelligence Systems. – 2025. – Vol. 18, Article 37.

3. MT S., Aminanto A.E., Aminanto M.E. Empowering Digital Resilience: Machine Learning-Based Policing Models for Cyber-Attack Detection in Wi-Fi Networks // Electronics. – 2024. – Vol. 13, No. 13. – Article 2583.