ALGORITHM FOR DETECTING UNAUTHORIZED ACCESS AT THE ENVIRONMENT ACCESS CONTROL LEVEL

Kovda E.O., Sokol H.V.
National Technical University "Kharkiv Polytechnic Institute", Kharkiv

The growing number of devices in wireless networks, especially in IoT environments, requires lightweight, real-time security solutions that work under limited computing resources. Traditional authentication methods remain important but may lack responsiveness in decentralized or dynamic network configurations.

Deep neural networks offer high accuracy in detecting attacks and generalizing new anomalies in wireless sensor networks [1]. Machine learning methods such as decision trees, support vector machines, and random forests are widely used for traffic classification and anomaly detection [2]. Naive Bayes classifiers are also effective for identifying unauthorized nodes due to their simplicity and real-time capabilities [3].

In general, the analysis of literary sources indicates the presence of a wide range of approaches to detecting unauthorized elements in the network - from classical statistical methods to modern artificial intelligence algorithms, which have significant potential for integration into practical network solutions.

The study proposes an effective method for detecting unauthorized devices at the MAC level, which is based on detecting anomalous behavior of nodes without the need for additional hardware. The developed approach combines Bayesian modeling with adaptive filtering, which allows real-time monitoring and evaluation of the activity of each device in the network.

The method is characterized by flexibility due to the ability to self-learn based on accumulated data and constantly update estimates when network conditions change. This makes it effective in situations with unstable traffic or variable topology. The selected algorithmic solutions ensure compatibility with a wide range of link-layer standards, in particular IEEE 802.11 and IEEE 802.15.4, which allows implementing this approach in wireless networks of various scales - from local IoT networks to large corporate systems.

Thus, the proposed technique combines high detection efficiency with practical applicability in modern telecommunication environments with limited resources.

References:

1. Zhang Y., Wang X. Deep Learning-Based Intrusion Detection for Wireless Sensor Networks // IEEE Transactions on Network and Service Management. – 2021. – Vol. 18, No. 2. – P. 123–135.
2. Kim H., Lee J. Machine Learning Techniques for Anomaly Detection in IoT Networks // Journal of Communications and Networks. – 2021. – Vol. 23, No. 4. – P. 289–298.
3. Singh R., Kaur A. Naive Bayes Classifier for Unauthorized Access Detection in Wireless Networks // International Journal of Wireless Information Networks. – 2021. – Vol. 28, No. 1. – P. 15–25.