УДК 004.056:004.8

USING ARTIFICIAL INTELLIGENCE TO DETECT ANOMALIES AND CYBER THREATS IN NETWORK TRAFFIC

Victoria Domanska

Institute of Special Communications and Information Protection,
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

Abstract. This paper studies the potential for using artificial intelligence to detect anomalies and cyber threats in network traffic. It analyzes key information security threats, the operating principles of intelligent intrusion detection systems, machine learning methods, and the specifics of their application to network data analysis. The advantages of using artificial intelligence over traditional security methods are identified, as well as the challenges associated with implementing such technologies. Particular attention is paid to detecting atypical network activity, automating responses to cyber incidents, and enhancing the resilience of information systems against modern attacks.

Keywords: artificial intelligence, cybersecurity, network traffic, machine learning, anomalies, cyber threats, intrusion detection, information systems, network security.

Research Relevance: The modern evolution of information technology is accompanied by a continuous increase in network traffic volumes, the number of connected devices, and the complexity of information systems. Corporate networks, cloud platforms, Internet of Things (IoT) systems, and digital services exchange vast amounts of data daily. At the same time, there is a rising number of cyber threats aimed at gaining unauthorized access, disrupting the functionality of information resources, stealing confidential information, and covertly interfering with network infrastructure operations. The relevance of this research stems from the need to develop adaptive cyber-defense tools capable of timely detection of suspicious activity, reducing incident response times, and enhancing the operational reliability of modern information systems.

Research Objective: The aim of this study is to analyze the potential for applying artificial intelligence and machine learning methods to detect anomalies and potential cyber threats within network traffic, as well as to identify the advantages, limitations, and prospects of using intelligent systems in the field of cybersecurity.

Network traffic consists of the data transmitted between devices, servers, users, and other components of an information system. Analyzing this traffic makes it possible to assess the network status, monitor information exchange, detect violations of established rules, and identify signs of potentially malicious activity. Key metrics used for network traffic analysis include source and destination IP addresses, port numbers, data transmission protocols, connection durations, packet counts, data volumes, request frequencies, and time intervals between network events. By aggregating these characteristics, one can establish a baseline for the normal behavior of network nodes and identify deviations that require further investigation.

An anomaly in network traffic is defined as an event or a set of events with characteristics that differ significantly from the system expected behavior. For instance, if a workstation typically connects to a few internal servers but suddenly begins sending a large volume of requests to numerous unknown nodes, such activity could indicate a malware infection, network scanning, or other suspicious behavior. Common threats that may manifest in network traffic include distributed denial-of-service (DDoS) attacks, port scanning, password-guessing attempts, malware propagation, unauthorized data transmission, and suspicious connections to remote command-and-control servers. Attacks where the adversary attempts to remain undetected by gradually altering the intensity and nature of network activity pose a particular risk.

However, not every deviation from normal behavior signifies a cyberattack. For example, an increase in request volume could result from data backups, software updates, or a surge in server load. Therefore, an effective anomaly detection system must take into account the context of events, the specific operational characteristics of the network, and the interrelationships between various metrics. It is precisely the need to analyze a vast array of interconnected parameters that makes artificial intelligence a promising tool for

ensuring network security. In the realm of cybersecurity, artificial intelligence encompasses methods that enable information systems to analyze data, identify patterns, classify events, and support decision-making. One of its key areas is machine learning, through which algorithms build models based on examples or characteristics of the data under analysis.

Unlike systems that merely check whether traffic complies with predefined rules, machine learning models can take multiple parameters into account simultaneously. This enables the detection of complex relationships between network events that are difficult to describe using a set of simple conditions. Several main approaches can be identified, depending on the learning method and the nature of the task at hand. Supervised learning involves the use of a dataset in which a network exists. Events are pre-labeled as either normal or malicious. The algorithm analyzes examples and learns to distinguish between these categories. Techniques such as decision trees, random forests, support vector machines, and neural networks can be employed for this purpose. The advantage of this approach is the ability to directly classify known threat types; however, the quality of the results depends on the completeness, reliability, and currency of the training data.

Unsupervised learning is used when the data lacks predefined labels. The algorithm explores the data structure, identifies groups of similar events, and detects objects that differ significantly from the majority. Methods such as clustering (e.g., DBSCAN) and the Isolation Forest algorithm can be applied to detect anomalies. This approach is useful when the full list of potential attacks is unknown, though it requires further analysis of the detected deviations. Semi-supervised learning combines a limited amount of labeled data with a larger dataset of unlabeled data. This is particularly relevant for organizations that lack a sufficient number of confirmed cyber-incident examples but possess vast amounts of network event logs. Deep learning methods occupy a distinct place, utilizing multilayer neural networks to detect complex patterns. For instance, recurrent neural networks and architectures incorporating attention mechanisms can be used to analyze sequences of network events and temporal dependencies. Autoencoders, in turn, can learn to reproduce the characteristics of normal traffic, and a significant reconstruction error can be viewed as a signal of a potential anomaly.

The choice of a specific method depends on network size, computational resources, the availability of training data, detection speed requirements, and the acceptable level of false positives. Relatively simple models may be suitable for small networks, whereas large distributed infrastructures might employ hybrid systems that combine multiple analysis algorithms. An intelligent cyber-threat detection system consists of several interconnected stages. First, data is collected from network devices, servers, firewalls, and monitoring systems. Information sources may include connection records, event logs, flow statistics, and network packet analysis results.

In the next stage, the data is cleaned of errors, standardized into a consistent format, and transformed into features used by the model. For instance, the system might calculate the average number of connections over a specific period, the frequency of failed requests, the volume of data transmitted, or the number of distinct ports accessed by a device. After data preparation, the model analyzes the data to determine the extent to which current activity aligns with the established profile of normal behavior. If metrics exceed a defined threshold or the combination of characteristics matches signs of suspicious activity, the system generates an alert. In more sophisticated solutions, events are further classified by risk level, and the findings are relayed to specialists at the security monitoring center.

The final stage involves verifying the detected event and responding to it. Depending on the security policy, the system may recommend blocking a suspicious connection, restricting network access, isolating a device, or intensifying monitoring. Automated execution of such actions must incorporate appropriate control mechanisms, as erroneously blocking a legitimate node could disrupt critical services. Thus, the use of artificial intelligence extends beyond the mere detection of anomalies. Its practical value lies in the ability to integrate data collection, analytical processing, risk assessment, and response support into a unified process.

One example of machine learning application is the detection of distributed denial-of-service (DDoS) attacks. During such attacks, malicious actors flood a target system with a large volume of requests, potentially overloading communications channels or server resources. An intelligent model can analyze

connection intensity, the distribution of traffic sources, request frequency, and the nature of server responses. A combination of atypical indicators can trigger an alert; however, confirming an attack requires accounting for the possibility of a legitimate surge in load.

Another important area is the detection of port scanning. During network infrastructure reconnaissance, an attacker might sequentially access various ports on a single node or check the availability of multiple devices. A machine learning model can detect an atypical increase in the number of such requests, unusual connection sequences, and a high rate of failed connection attempts. Artificial intelligence can also be used to detect signs of data exfiltration. For example, a workstation that typically transmits small amounts of information might suddenly start sending large volumes of data to an external server at an unusual time. The system can identify such an anomaly based on data transmission volume, connection duration, and the device network activity history. However, confirming a data leak requires further verification of the connection destination, access rights, and the nature of the transmitted data. One more example is the detection of infected devices establishing regular connections with external command-and-control nodes. Even if individual connections show no obvious signs of danger, their frequency, unusual duration, or combination with other suspicious events may indicate the presence of malware.

Protecting Internet of Things (IoT) devices is a critical area of focus. Such devices often have limited computing resources, utilize standard network protocol sets, and do not always support robust security measures. Consequently, they can become targets for attacks or be used to form botnets. Network behavior analysis makes it possible to identify devices that suddenly alter their communications patterns, connect to unknown servers, or generate atypical traffic volumes. In cloud-based and distributed information systems, intelligent analysis can be performed simultaneously across multiple layers: network, server, and application. Aggregating information from various sources enables a better understanding of the interrelationships between events and the detection of attacks that might otherwise go unnoticed if analyzed at individual nodes in isolation.

References

1. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg: NIST, 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1.

2. National Institute of Standards and Technology. Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. Gaithersburg: NIST, 2022. DOI: https://doi.org/10.6028/NIST.SP.1270.

3. National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

4. MITRE. MITRE ATT&CK: Enterprise Matrix. URL: https://attack.mitre.org/ (дата звернення: 13.10.2026).

5. Scikit-learn developers. Novelty and Outlier Detection. Scikit-learn User Guide. URL: https://scikit-learn.org/stable/modules/outlier_detection.html (дата звернення: 13.10.2026).

6. National Institute of Standards and Technology. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2023. Gaithersburg: NIST, 2024. DOI: https://doi.org/10.6028/NIST.AI.100-2e2023.

УДК 004.056:004.7

DEVELOPMENT OF ADAPTIVE ACCESS CONTROL POLICIES FOR MULTI-CLOUD ENVIRONMENTS IN DISTRIBUTED INFORMATION SYSTEMS

Dmytro Hleba

Institute of Special Communications and Information Protection,
National Technical University of Ukraine
«Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, Ukraine

Abstract. This paper investigates the challenges and prospects of developing adaptive access control policies for distributed information systems operating in multi-cloud environments. It analyzes key