https://www.proconference.org/index.php/usc/article/view/usc33-00-033
DOI: 10.30888/2709-2267.2025-33-00-033

UDC 004.4:005.8

INCREASING THE EFFICIENCY OF CYBER ATTACK DETECTION BY DESIGNING A NETWORK ANOMALIES ANALYSIS SYSTEM

Zamikhovska O. L.
Ph.D., Assoc.
ORCID:0000-0003-0775-0472
Ivano-Frankivsk National Technical University of Oil and Gas
Ivano-Frankivsk, Karpatska, 15

Abstract. *The article presents the design of a system for detecting and analyzing network anomalies. A modular architecture is proposed with data collection, preprocessing, analysis, and visualization modules. Experimental testing was performed in Cisco Packet Tracer with traffic analysis in Wireshark. Simulated DoS, port scanning, and IP spoofing attacks demonstrated the effectiveness of combining statistical/visual methods with filtering. The proposed system architecture is scalable and can be further implemented with Suricata, Zeek, and ELK Stack, integrating machine learning for automated detection.*

Key words: *network anomalies, cybersecurity, intrusion detection, machine learning, network traffic, system architecture, data analysis.*

Introduction.

The rapid development of digital technologies and the growth of cyber threats are rendering traditional security measures, such as firewalls and antivirus software, ineffective. Attackers actively use artificial intelligence, machine learning, and generative technologies to automate attacks, create phishing messages, or spoof voices, making their actions less predictable and difficult to detect [1]. An additional risk factor is the rapid growth in the number of IoT devices, which often have limited protection mechanisms.

In the absence of known signatures, the most promising approach is to detect anomalous behavior in traffic. The signature-based approach (Snort) is effective against known attacks but cannot recognize new (zero-day) ones. The anomaly approach (Zeek) allows unknown threats to be detected, but suffers from a significant number of false positives. Recent studies prove the effectiveness of hybrid methods that combine statistical analysis with machine learning, in particular autoencoder and LSTM models [2].

Anomaly detection is particularly important for protecting cyber-physical systems and critical infrastructure (SCADA, telecommunications, and financial networks).

IDS, IPS, and SIEM systems are already standard security measures, but their effectiveness can be improved by integrating architectures focused on behavioral traffic analysis.

The goal of this work is to improve the effectiveness of cyberattack detection by designing a network anomaly analysis system architecture based on modern data processing and analysis methods.

Theoretical foundations and analysis of modern approaches to anomaly detection

A network threat is a potentially harmful event or action that can lead to a breach of confidentiality, integrity, or availability of information resources. By origin, they are divided into external (initiated from outside the network, for example, by hackers) and internal (intentional or unintentional actions of employees). In terms of form, threats can be active (aimed at changing or destroying data, such as SQL injections) and passive (unauthorized collection of information without direct impact on the system, such as traffic interception) [3].

Anomalies in network traffic are deviations from the normal, expected behavior of the system or users. They can occur as a result of technical failures or malicious activity. The most common types of anomalies that may indicate cyberattacks are: in traffic volume (e.g., DDoS attacks); in protocols (atypical or prohibited protocols); behavioral (port scanning, unauthorized access attempts); temporal (connections outside working hours). Anomaly detection methods are broadly divided into three categories: statistical, machine learning (ML), and hybrid.

System design and implementation

The design of an effective network anomaly detection system (NADS) involves a modular approach. The general logical model of NADS consists of several interrelated components that perform specific functions.

A wide range of software tools are used to implement anomaly detection systems, which can be classified according to their purpose (Table 1) [4].

Network traffic collection module: This component is responsible for intercepting traffic in real time. Its task is to ensure continuous and complete capture control over

the data stream without packet loss, which can be implemented using software (tcpdump, pcap) or hardware tools.

Table 1.1 – Comparative characteristics of network traffic analysis tools

Tool	Main purpose	Anomaly detection support	Features
Wireshark	Network packet analysis (packet sniffer)	Partially (manual analysis)	Supports deep traffic inspection, graphical interface
Snort	Intrusion detection system (IDS)	Yes (signature-based approach)	Works in real time, requires signature updates
Suricata	Next-generation IDS/IPS	Yes (signature-based + statistical)	Supports multi-threaded processing, integration with SIEM
Bro/Zeek	Network protocol behavior analysis	Yes (behavioral approach)	High flexibility, powerful scripts for customization
NetFlow/nfdump	Streaming traffic analysis	Partially (through statistics)	Works with aggregated data, does not store the full contents of packets
ELK Stack	Data logging and visualization	Yes (using filters)	Requires prior integration with traffic sources
TensorFlow + Scikit-learn	Machine learning (ML) for anomaly detection	Yes (classification/clustering models)	Requires prior data processing and model training

Authoring Zamikhovska O. L.

Preprocessing module: Collected packets undergo filtering, normalization, and aggregation to prepare the data for analysis. This module performs session desegmentation, feature extraction, and data transformation into a convenient format.

Analysis module: performs the main function of anomaly detection. It can operate based on statistical analysis, rules, signatures, or machine learning methods, as well as use a hybrid approach.

Knowledge base and behavior profiles: stores a reference model of the normal state of the network, which can be updated automatically or manually.

Response and alert module: when an anomaly is detected, it initiates certain actions, such as generating a message to the administrator, creating an entry in the event log, or blocking an IP address.

The user interface provides data visualization and system management.

The presented architecture corresponds to modern approaches used in professional SIEM systems, where data from various sources (sensors) are correlated to obtain a comprehensive picture of security. This allows the project to be considered a scalable model that meets industry standards, rather than just an abstract academic task.

To test the system, a hierarchical network topology was developed that simulates a corporate environment. Its structure includes:

- access level: user workstations that generate typical traffic;
- distribution level: a switch that segments traffic between subnets using VLANs;
- core level: a router that acts as a gateway between local subnets and the external environment.

For testing the system, normal and abnormal traffic were clearly distinguished.

This distinction allows you to create a baseline profile of normal behavior for further detection of deviations. A number of services were set up in the test environment to serve as a source of traffic for analysis. All of them corresponded to real protocols and were configured on a separate server. These services created full-fledged background traffic, which could be used to test the system's response to simulated anomalies.

Within the experiment, three types of attacks were successfully simulated, which are typical examples of network anomalies:

1. A DoS attack simulated using continuous ICMP requests to the target server;

2. Port scanning initiated attempts to connect to different server ports. This allows you to test how the system responds to network reconnaissance, which usually precedes an intrusion;

3. IP spoofing is an attempt to forge the sender's IP address. This shows how the system can identify anomalies by analyzing discrepancies between IP and MAC addresses.

Wireshark was used to collect traffic, which allowed us to obtain a complete dataset for further analysis. Figure 1 shows the properties of the capture file: key

metadata and statistics. A total of 3,646 packets were recorded without loss, ensuring the completeness of the data for further analysis.

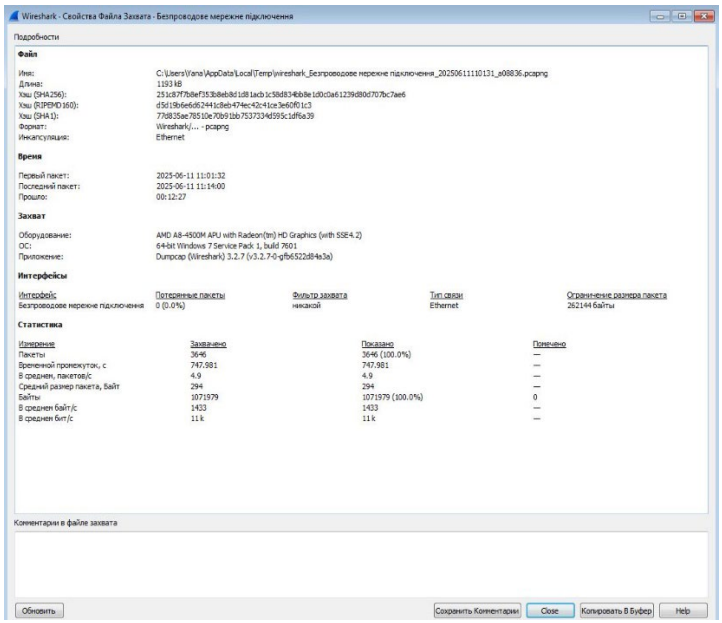

Figure 1 – Properties of a traffic capture file in Wireshark

Figure 2 shows a graph of packet input/output per second, which reflects traffic intensity.

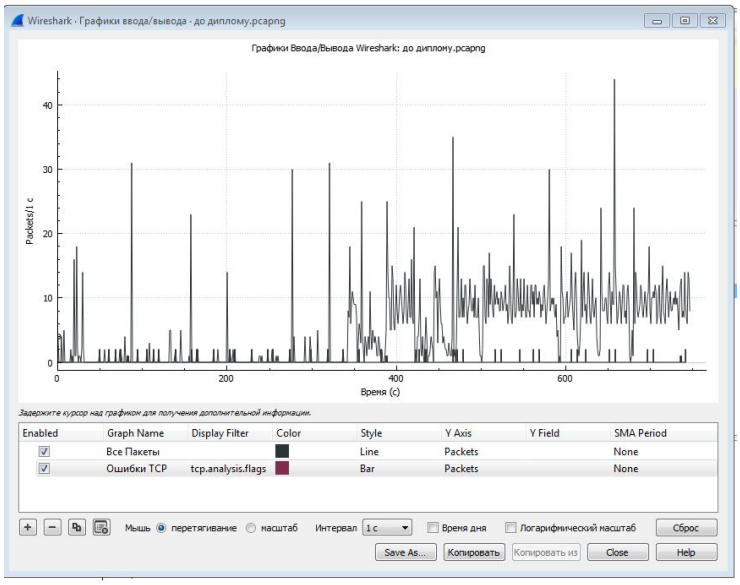

Figure 2 – Graph of packet input/output per second

Figure 3 shows the traffic protocol hierarchy, which indicates that a significant

portion of traffic belongs to UDP protocols, specifically SSDP and mDNS. This ratio may be abnormal for a typical corporate network and may indicate the presence of a large number of Internet of Things (IoT) devices generating background traffic.

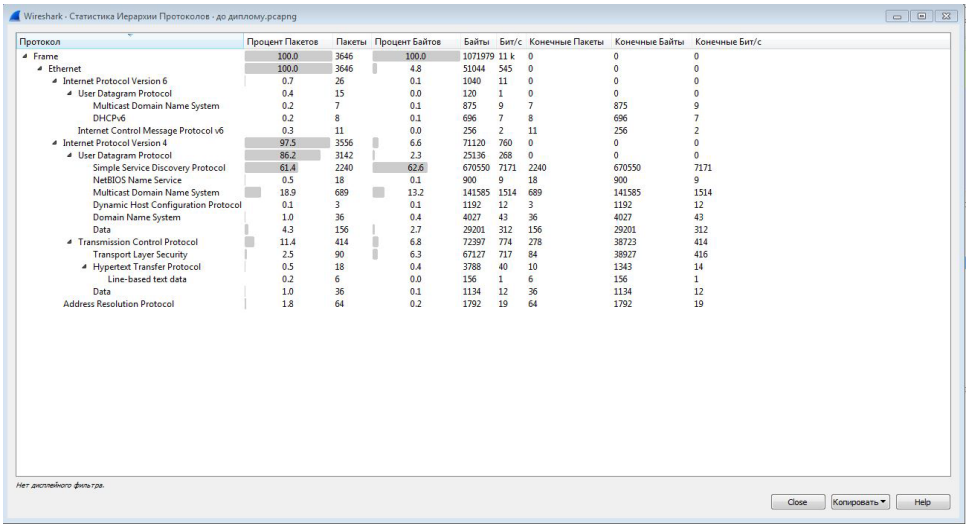

Figure 3 – Traffic protocol hierarchy

Figure 4, which shows IPv4 endpoints, reveals active interaction with numerous external IP addresses. For some of them, in particular 23.64.12.187, there is a significant imbalance between sent (Tx) and received (Rx) bytes. This may indicate attempts to exfiltrate data or the host's participation in a DoS attack.

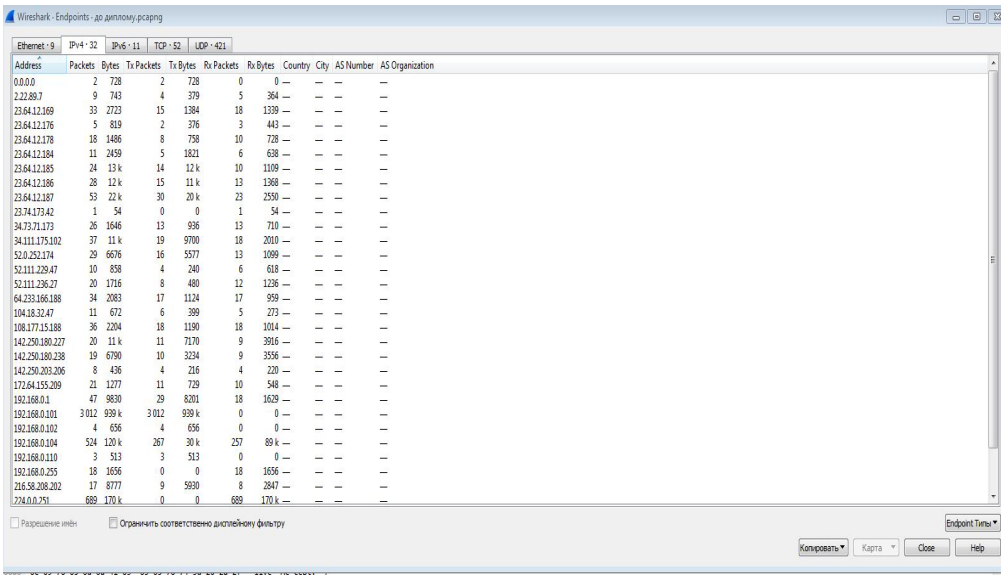

Figure 4 – IPv4 endpoints

Based on the results obtained, a comparative analysis of the effectiveness of visual and filtration approaches was conducted, confirming the advantages of combining them.

Visual-statistical analysis (I/O Graph, Protocol Hierarchy) allows you to quickly form a general idea of the nature of traffic and identify typical anomalies, such as activity peaks or atypical protocol distribution. This method is convenient for initial assessment, but it is subjective and not accurate enough for hidden attacks: it only indicates the problem, but does not explain its essence.

Filtering analysis provides high accuracy and allows you to isolate traffic that matches known attack patterns (for example, tcp.flags.syn==1 for SYN flood). It is useful for confirming hypotheses, but requires knowledge of threat signs and is not capable of detecting new anomalies.

Experiments have confirmed that a hybrid approach is best: visual analysis quickly identifies suspicious traffic segments, while filtering allows their causes (e.g., DoS attack) to be accurately identified. This combination of breadth and accuracy is critical for practical threat detection.

Traffic research has also revealed several characteristic patterns:

1) The dominance of multicast protocols (SSDP, mDNS) may indicate the presence of numerous IoT devices that create background “noise” and are potentially used in amplification attacks.
2) Atypical peaks of activity on input/output graphs require deeper analysis, in particular with the use of ML.
3) A significant imbalance of Tx/Rx bytes for individual external IP addresses is a sign of data exfiltration or host participation in a DDoS attack.

These results confirm the need for comprehensive systems capable of combining behavioral and content analysis for accurate threat detection.

Summary and conclusions.

Modern approaches to anomaly detection were analyzed, which became the basis for the development of a modular system architecture. The designed system, which includes modules for collection, processing, analysis, and notification, meets modern requirements for complex security systems.

The experimental part of the work, conducted in the Cisco Packet Tracer environment using Wireshark, confirmed the effectiveness of the proposed approach. During the simulation of DoS attacks, port scanning, and IP spoofing, abnormal activity was successfully detected and identified. Interpretation of visual and statistical data allowed us to identify potential threats, including excessive multicast traffic and atypical imbalances in transmitted and received data. This demonstrates that even manual analysis combined with the appropriate tools can be effective.

The results confirm that combining different analysis methods (visual, statistical, and filtering) is the most reliable approach to detecting anomalies, as it allows for the detection of both general and specific threats.

References:

1. Cybersecurity trends for 2025: how to protect your business / Kyivstar Business Hub [Electronic resource]. – 2025. – Access mode: https://hub.kyivstar.ua/articles/ostanni-trendy-kiberbezpeky

2. FoSDeT: a hybrid machine learning model for detecting Internet of Things botnets [Electronic resource] // Scientific Bulletin of the National University of Oil and Gas. – 2025. – No. 1. – Access mode: https://www.nvngu.in.ua/index.php/uk/vidavnitstvo/pro-zhurnal/1920-ukrcat/arkhiv-zhurnalu/2025/zmist-1-2025/7160-104

3. Sytnik, P. Y. Analysis of threats to data security in a network environment / P. Y. Sytnik // Information Security. – 2022. – No. 1. – P. 18–23.

4. Reis, M.J.C.S. AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. Electronics 2025, 14, 2492. https://doi.org/10.3390/electronics14122492

5. Furikata, D. V., & Vakalyuk, T. A. (2025). Theoretical approaches to detecting anomalies in meter readings in scientific literature. Technical Engineering, (1(95), 325–331. https://doi.org/10.26642/ten-2025-1 (95)-325-331.

Article sent: 19.09.2025