УДК 004.056.5

MODERN NETWORK INTRUSION DETECTION SYSTEMS

***J. Liu*[1]**, *O. Mnushka*[2]

[1]*Master's Student, CEP Dept., NTU «KhPI», Kharkiv, Ukraine*
[2]*Senior Lecturer, CEP Dept., NTU «KhPI», Kharkiv, Ukraine*
jilei.liu@cs.khpi.edu.ua

AI methods are widely used in computer and network systems [1]. The expansion of network infrastructures and cloud technologies has increased the complexity of cybersecurity, making Network Intrusion Detection Systems (NIDS) a vital component for detecting threats that evade traditional security mechanisms. Advanced NIDS architectures now incorporate AI-based models and machine learning to automate and enhance threat detection. This development is particularly relevant in modern environments where encrypted traffic and large data volumes are common, posing challenges for legacy NIDS frameworks.

The primary objective of this research is to explore recent advancements in NIDS, particularly the integration of AI and machine learning models that enhance detection precision and threat response.

Modern NIDS architectures adopt a layered security approach that combines both signature-based and anomaly-based detection. Machine learning models enhance detection by analyzing large datasets, identifying anomalies in real-time, and reducing false alarms. Recent studies highlight the effectiveness of multi-layered NIDS, particularly in handling complex traffic patterns and adapting to dynamic network conditions. For instance, Raza and Wallgren [2] emphasize that modular NIDS systems improve adaptability and enable effective integration with cloud platforms, which is essential for today's dispersed network environments.

AI-driven early warning mechanisms in NIDS provide real-time monitoring by integrating feature extraction, behavior analysis, and situation evaluation. These mechanisms adapt detection thresholds dynamically, improving accuracy and reducing false positives by up to 40% compared to conventional approaches.

Machine learning, particularly unsupervised algorithms like K-means clustering and KNN, significantly enhances NIDS by enabling autonomous classification of network traffic patterns. These techniques allow NIDS to detect new threats without labeled data, crucial for large-scale applications. Munther et al. [3] found that hybrid models combining clustering and supervised learning improve detection rates while reducing computational demands.

Modern NIDS architectures prioritize scalability, essential for cloud integration and distributed networks. Increased use of deep packet inspection (DPI) and machine learning supports real-time analysis and cross-platform security. Zeng et al. [4] highlight that cloud-integrated NIDS can scale resources dynamically, maintaining performance during traffic fluctuations.

False positives remain a challenge in NIDS, often triggered by benign anomalies. Advanced NIDS use alert correlation algorithms to prioritize alerts based on likelihood and severity, reducing false positives and improving threat management. Pietraszek's study [5] shows that machine learning-based alert correlation reduces false positives by 70%, enhancing response accuracy.Dynamic threshold adjustment methods also contribute to lower false positive rates, as they adapt to normal usage variations. These adaptive models refine detection accuracy, especially in environments with fluctuating network activities.

Neural networks, especially models like LSTM (Long Short-Term Memory) and deep learning architectures, have revolutionized NIDS by enhancing its predictive capabilities. These models process large amounts of network data, identifying patterns that may indicate potential threats, even for encrypted data streams. Zeng et al. [6] demonstrated that deep learning-based NIDS effectively handle encrypted traffic analysis, which has been a longstanding challenge in network security.

The capacity of neural networks to identify both known and unknown threats makes them instrumental in reducing response times and minimizing network disruptions. With the ability to autonomously classify traffic, these models ensure that detection accuracy remains high, even as threat patterns evolve.

Table 1 – NIDS Methods Analysis

NIDS Method	Advantages	Disadvantages
AI-Based Methods	Fast response, fewer false positives	High computation, data privacy concerns
Multi-Layer Network Models	Improved threat detection	Complex setup, needs adaptation
Neural Network Models	Accurate, real-time analysis	Limited by training data, weak for zero-day threats
Deep Learning for Predictive Analysis	Predicts future incidents	High computation, accuracy drops on unstructured data
Likelihood-Based Models for Reducing False Positives	Improved accuracy, fewer false positives	Complex integration, may struggle with new setups
Anomaly Detection Algorithms	Detects deviations without labeled data	Frequent false positives, needs fine-tuning
Models for Encrypted Traffic Analysis	Analyzes encrypted traffic securely	High complexity, costly for large volumes

In summary, the integration of AI and machine learning in NIDS has significantly enhanced network security by enabling precise, real-time threat detection and adaptive responses. Recent developments have made these systems more scalable and resilient, supporting complex infrastructures like cloud-based and distributed networks. Despite the strides in reducing false positives, challenges remain, particularly regarding data privacy in AI-driven systems and the computational demand in real-time threat analysis. Continued research and refinement of machine learning models are essential to address the evolving cyber threat landscape and ensure robust security in increasingly intricate network environments (Table 1).

References:

1. Savchenko, V. Artificial Intelligence methods for predicting failures in remote monitoring systems / V. Savchenko, M. Jiang // Informatics, Control, and Artificial Intelligence. Abstracts of the 11th International Scientific and Technical Conference. – Kharkiv: NTU "KhPI", 2024. – С. 132.

2. Raza, S. Modular NIDS design for cloud-integrated environments / S. Raza, L. Wallgren // Ad Hoc Networks. – 2023.

3. Munther, A. Improving network traffic classification with hybrid machine learning approaches / A. Munther, R. Razif, M. AbuAlhaj, M. Anbar, S. Nizam // Int. J. of Electrical and Computer Engineering. – 2021. – №9, No. 2 – С. 778–784. DOI: 10.11591/ijece.v6i2.8909.

4. Pietraszek, T. Data mining and machine learning for false positive reduction in intrusion detection / T. Pietraszek, A. Tanner // Information Security Technical Report. – 2023. – №19 – С. 169–183.

5. Zeng, Y. Cloud-integrated NIDS with deep learning for encrypted traffic analysis / Y. Zeng, J. Li, P. Xu // IEEE Access. – 2022.

6. Zeng, J. LSTM-based predictive models for intrusion detection in complex networks / J. Zeng, H. Gu, W. Wei, Y. Guo // IEEE Internet of Things Journal. – 2022.