INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT

eISSN 2394-6334 Impact factor: 7,854 Volume 12, issue 11 (2025)

ARTIFICIAL INTELLIGENCE IN THE NETWORK: AUTOMATIC TRAFFIC ANALYSIS AND THREAT FORECASTING

M.Z. Tursunalieva
Student of Applied Mathematics, Fergana State University

Annotation: This article highlights the increasing complexity of manual control of flows in network infrastructure due to their increasing volume, especially the difficulties in identifying slowly developing hidden threats. The ability to analyze traffic in real time, identify anomalies, and detect threats early is due to the ability of artificial intelligence algorithms to detect subtle changes. By forming characteristics, organizing data, and applying a corresponding model, the system will be able to identify even the smallest differences between packets. In practical cases, gradual changes in port switching, detection of slow flows directed to unknown servers, or hidden behavior characteristic of bots have shown the advantages of artificial intelligence. Such an approach will allow strengthening security, reducing the burden on administrators, and detecting suspicious activity at an early stage, demonstrating high efficiency in identifying threats, which in appearance are practically indistinguishable from regular traffic.

Keywords: network traffic, anomaly detection, artificial intelligence, forecasting, information security

Entrance

As the number of streams in modern networks increases sharply, it becomes increasingly difficult to control them manually. Each package has its own specific content, and hazardous signals may be hidden between the typical scenarios. The need for automated approaches is growing because manual tracking is not sufficiently effective in terms of both speed and accuracy. Especially, early detection of complex threats, which gradually occur over a long period of time and look like a normal flow, is one of the most difficult tasks for administrators. In such a situation, artificial intelligence is distinguished by its ability to analyze network flow in real time and identify anomalies that are difficult to clearly distinguish. As traffic volume increases, human control weakens, but algorithms do not lose performance. Therefore, the use of artificial intelligence elements to maintain a stable level of security, identify threats as early as possible, and reduce system overload is becoming an important area of network management. These possibilities play an important role in distinguishing slow anomalies, the external sign of which is almost imperceptible.

To identify such complex situations, the process of automatic processing of network flows begins, first of all, with data regulation. Among packets coming from networks, there are sometimes distorted or duplicated elements, therefore the incoming data is cleaned and brought to a stable form. After this, the symbols transmitted to the model are processed in the same order by adapting the indicators to a single range. Since raw data obtained from the traffic itself cannot give an immediate result, additional parameters such as flow duration, number of packets, port statistics, interarrival times between packets, and the slowly varying dispersion of these times are formed. It is precisely these subtle fluctuations that play a crucial role in identifying latent threats that develop gradually. A gradual change in IP entropy over time, small shifts in the direction, and abnormal repetition rhythms of TCP flags are added to the symbols, allowing the algorithm to clearly distinguish the natural rhythm of the flow.

At the next stage, a suitable model is selected, taking into account speed, accuracy, and resource consumption; for example, classification methods, autoencoders based on reconstruction error, or models such as Isolation Forest, designed to isolate slowly changing anomalies, can be used. This approach yields high results in identifying complex situations, especially in attacks that appear as a simple flow. During the process, streams are received sequentially, analyzed based on signs, and when the smallest deviations characteristic of the threat are detected, the system immediately highlights them in a flag state. In this way, actions occurring in the network are assessed in real time, and situations that can affect security are detected at a much earlier stage, which allows for effective control of even slowly developing hidden threats.

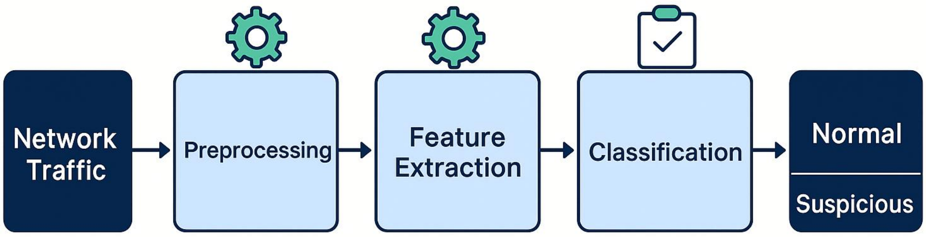

Fig. 1. General process of traffic processing based on artificial intelligence.

Problem of detecting a slowly developing hidden threat in the network and its solution

The application of the artificial intelligence approach to network flows has shown significant advantages in real-world practical situations. When the initial tests were conducted in a corporate office network, a flow anomaly was identified, which outwardly resembles regular traffic, but the rhythm of port switching is gradually changing. Interestingly, this situation was mistaken by administrators for server loading that had been ongoing for several days. The algorithm detected the smallest fluctuations in the flow within seconds and determined that these changes were not a natural process. A similar situation was observed in the data center: when the order of HTTP requests was gradually disrupted and insignificant fluctuations appeared over time, the system designated this flow as a slowly moving wave of bots forcibly uploading advertisements. While regular filters saw only repeating IP addresses in this case and assessed the process as normal, artificial intelligence clearly showed the risk sign by comparing the steady decrease in packet spacing, small shifts in the direction, and the interdependence of queries.

In another case, the traffic coming from the employee's device in the internal WLAN network of the enterprise was recorded as a suspicious flow, gradually changing. Since the size of TCP packages changes gradually over time, not with sharp jumps, this situation was initially assessed as a simple application update. But artificial intelligence, comparing the subtle differences between the characteristics of the stream, found that the distribution of packets over domains was directed to unknown servers and raised the likelihood of malicious activity. The discovery of illegal software installed on the device during subsequent inspection further confirmed the model's superiority in detecting slow-developing hidden threats.

In these cases, the decision-making speed of the algorithm was also of particular importance, and after detecting the anomaly, a signal was sent to the network control system within just 300-450 milliseconds. The accuracy has increased significantly compared to conventional filtering methods: the number of incorrect positive signals among conventional streams in the office segment has decreased threefold. This ensured time and resource savings for administrators, positively affecting the overall stability of the network. Artificial intelligence's ability to detect subtle vibrations proved particularly effective in detecting gradually developing, almost invisible threats.

The contribution of artificial intelligence to network security becomes even more evident during practical experiments. Traffic sorting through simple filters is often limited to superficial inspection, as they are designed to isolate only streams that do not meet the standard. However, in real networks, the threat is not always sharp and immediately noticeable - some threats manifest themselves gradually, as if hiding in a normal flow. For example, in large companies, when the load is high, the difference between the slow actions of bots and the activity of a live user becomes almost invisible to the human eye. Algorithms show their superiority precisely through these subtle fluctuations: gradual changes in traffic duration, decreased time between packets, or minor shifts in port switching are distinguished as anomalies.

The power of this approach lies in the fact that the model can observe the natural rhythm of the flow and compare even the smallest deviations from its usual rhythm in real time. However, such systems also have limitations. For example, in cases where complex attacks strive to present themselves as a simple flow - that is, when hidden threats arise that continue at a slow pace and intensify their symptoms over time - precautionary measures aimed at reducing false positive signals can sometimes lead to the late detection of certain risks. Also, as the number of network segments increases, the amount of data processed increases, and the model's need for memory and computing resources also increases.

Nevertheless, practical experience shows that with the correct configuration of the model, such limitations do not reduce the overall effectiveness of the system. On the contrary, thanks to artificial intelligence's ability to detect subtle vibrations, the level of security is steadily increasing, and administrators significantly reduce the time spent on manual tracking. Another important aspect is that as the model is regularly updated, the ability to detect new types of threats increases, and the level of network protection becomes more stable over time. This feature of artificial intelligence is especially important in identifying threats that change slowly and look like a normal flow.

Result

The use of artificial intelligence in network infrastructure significantly improves the security process. The ability to analyze traffic in real time, identify anomalies, and foresee potential threats will bring network management to a more reliable level. Because algorithms can distinguish even the most subtle differences between packets, they have a significant advantage in accuracy and speed compared to human control. In practical situations, results such as early flagging of malicious streams, isolating gradually changing suspicious traffic, or detecting bot-specific, almost imperceptible behaviors further strengthen the practical importance of artificial intelligence.

In the era of increasing traffic volume, automated analysis systems are becoming increasingly central to network protection. In particular, the model's ability to compare characteristics accumulated over time in detecting slowly developing hidden threats is crucial for maintaining network stability. Also, when models are regularly updated, the ability to detect new types of threats increases and the system's adaptability increases. Therefore, the approach based on artificial intelligence is currently recognized as one of the most convenient, fastest, and practically effective ways to strengthen network security.

References

1. Zhang J., Lee W. Machine Learning in Network Security: Anomaly Detection Techniques // *IEEE Transactions on Network and Service Management.* - 2022.
2. Buczak A. L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // *IEEE Communications Surveys & Tutorials.* - 2019.
3. Tursunaliyeva M.Z. *Optimization of network traffic with the help of artificial intelligence based on edge computing: a new methodological approach* // Science and Innovation.

International Scientific Journal. - 2021. - Vol. 4, No. 9. - P. 76-79. - doi:10.5281/zenodo.17258224.

4. Tursunaliyeva M. *Energy efficiency in neural networks: problems of optimizing large models* // Science and Innovation. International Scientific Journal. - 2021. - Vol. 4, No. 11. - P. 59-61. - DOI: 10.5281/zenodo.17674536.
5. Cisco Systems. AI-Driven Network Security Whitepaper. - 2023.
6. Python Software Foundation. Python Documentation. - Access mode: https://docs.python.org
7. Wireshark Team. Wireshark User Guide. - Access mode: https://www.wireshark.org/docs/