UDC 004.732.056

ADVANTAGES OF A NETWORK ATTACK DETECTION SYSTEM (NADS) USING WAVELET ANALYSIS

Hrynchenko P.V., postgraduate student, phrynchenko@ukr.net, NUZP

The current development of computer networks affects most areas of economic activity. In addition to the dependability of the hardware being used, maintaining the functioning of networks and the information systems running on them also requires the network's resilience against deliberate attempts to interfere with its normal operations. Networks becoming bigger, more sophisticated, and more intense every year. As a result, there is an increasing need to improve intrusion detection systems, the primary responsibility of which is to identify network assaults, or efforts at gaining unauthorized entry to the network and using its resources. The constant rapid development of methods and destructive software influence on information systems necessitates a comparative analysis of attack detection and intrusion prevention systems in order to determine the most effective information protection mechanisms.

It takes a lot of resources to create information systems that are guaranteed to be safe from malicious influences and computer assaults. Furthermore, there is a well-established inverse link between a system's security and ease of use: the more robust the security measures, the more challenging it is to effectively use the information system's primary functionality.

The main goal of this research is the problem of making a decision regarding the effectiveness of the developed network attack detection system (NADS) relative to already existing open systems.

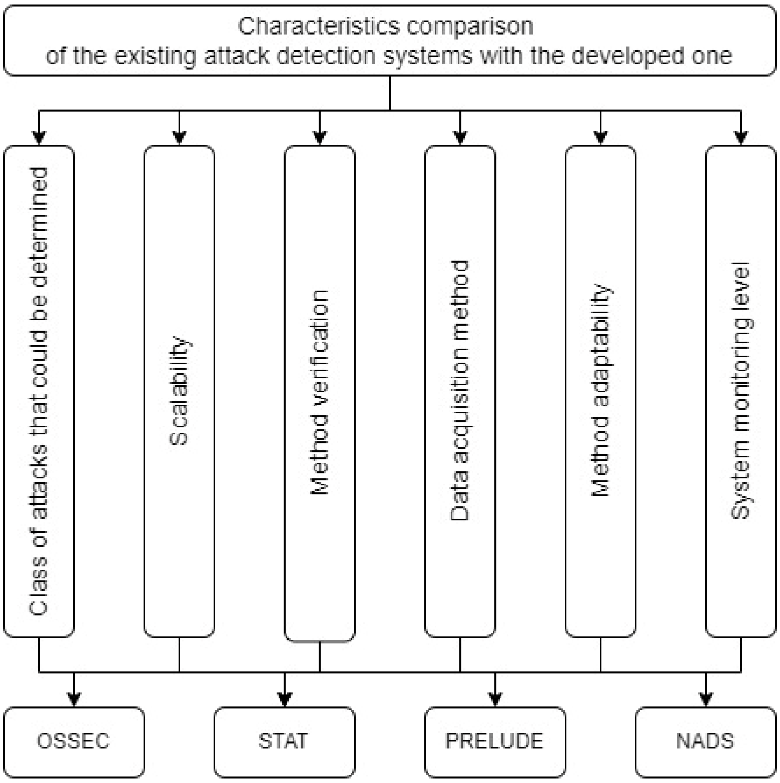
The wavelet transform is the foundation of NADS's suggested method for detecting network abnormalities. A 15-dimensional vector of attributes that is intended to describe the dynamics of network flows makes up the input signal. NADS present a model for prediction for normal traffic in which the wavelet coefficients are crucial since the ARX model uses them as external inputs to forecast the signal approximation coefficient. The output of the traffic prediction model calculates the deviation between typical and anomalous activity. Based on empirical data, the locations of the attacks consistently align with the maxima of the residuals. To identify peaks from a collection of residuals, an outlier identification technique based on GMM is used. Based on the output of the suggested emission detection algorithm, decisions are taken.

The system uses a discrete wavelet transformation, since the network signals under consideration have a cutoff frequency, the basis functions of which are used to transform the input signals into a set of approximation coefficients and detail coefficients, which can be used to reconstruct the input signal. Modeling of normal network traffic consists of two stages – wavelet decomposition/reconstruction and autoregression model generation. In practical situations, signals flow through both high-pass and low-pass filters at each level. Downsampling can be used to minimize the quantity of the data because, in this instance, only approximations of the values are significant. The remaining coefficients, which provide a high-level overview of the signal behavior after the low-level characteristics have been removed, can be utilized to build a signal profile that describes the typical patterns of network traffic. Since details are lost during filtering, the original signals are converted into a collection of wavelet approximation coefficients during wavelet decomposition/reconstruction. These coefficients estimate the approximate signal's sum. In order to create a prediction model and estimate the ARX parameters, the wavelet coefficients of various training data segments are utilized as input and model fitting data. The least squares approach is utilized to estimate the ideal parameters using the ARX fitting procedure. It is possible to distinguish anomalous signals from regular ones using a prediction model for typical network traffic after it has been received. When the model's inputs consist solely of normal traffic, its outputs, sometimes referred to as residuals, will approach zero, indicating that the model's projected value is in close proximity to the input of real normal behavior. Otherwise, the residuals will have several peaks where anomalies emerge when the model's input consists of both regular and aberrant traffic. The intrusion decision-making system receives the residuals and uses an outlier identification algorithm to determine whether an incursion may have occurred [1].

The work analyzes and considers a number of attack detection systems (OSSEC, NETSTAT, Prelude), whose main features are compared with the one developed to study its relevance (pic. 1).

Decomposition of the decision-making problem is made with the selection of the main goal and alternatives. Elements of the same levels are comparable to each other in terms of prioritization.

According to Saati's method, to solve this problem, a hierarchy of goals is defined. Based on this, the scheme of the current study is similarly constructed, the main goal of which is to prove the effectiveness of the developed network attack detection system among three existing alternatives according to six criteria.


Characteristics comparison
of the existing attack detection systems with the developed one
Class of attacks that could be determined
Scalability
Method verification
Data acquisition method
Method adaptability
System monitoring level
OSSEC
STAT
PRELUDE
NADS

Picture 1 – Hierarchy of choosing an attack detection system from a certain set of alternatives

Conclusion. Priorities are calculated for the entire hierarchy in total. There is a transition to the principle of priority synthesis. For each element, the local priorities of the alternatives are multiplied by the appropriate level criteria priorities and totaled in accordance with the criteria. Consequently, the global priorities of the alternatives are established while considering the criteria's preferences. The option with the highest global priority value will receive the highest rating.

By comparing the obtained values of global priorities, ratings of alternatives are determined. In the current research, the developed network attack detection system has the highest priority of 0.3, which indicates its advantages according to certain criteria in the overall ranking of compared systems, and therefore makes its further development and improvement appropriate.

References

1. Hrynchenko P. Detection of Unauthorized Actions in Networks Using Wavelet Analysis. Theoretical and Applied Cyber Security. 2023. Vol. 5. № 2. P. 40–46.