An Intelligent Network Traffic Analysis Module for Intrusion Detection Systems Using an Ensemble of Neural Networks

Mukhamadieva Kibriyo[1] and Mukhamadieva Zarina[2]
[1]*Applicant of the department of computer engineering, University of Tashkent for Applied Sciences, Gavhar Str. 1, 100149 Tashkent, Uzbekistan*
[2]*Bukhara Engineering Technological Institute, Q.Murtazoyev Str. 15, 200101 Bukhara, Uzbekistan*
kibriyo40@gmail.com, zarina21@gmail.com

Keywords: Neural Network, Network Traffic, Data Analysis, False Positive, Attack, Intrusion, Detection Accuracy, IDS, MLP, RBF, SOM.

Abstract: This paper presents a module for the intelligent analysis of network traffic for Intrusion Detection Systems (IDS), implemented as an ensemble of three artificial neural networks (ANNs): a Multi-Layer Perceptron (MLP), a Radial Basis Function (RBF) network, and a Self-Organizing Map (SOM). The problem is formalized as an optimization of two criteria: attack detection accuracy (Accuracy) and False Alarm Rate (FAR). An algorithm is proposed that allows for a flexible adjustment of the balance between these metrics depending on security policy priorities. Experiments on the UNSW-NB15 dataset demonstrated that the module achieves an accuracy of 97.2% with a FAR of 2.2% in a balanced mode, and an accuracy of 98.0% with a FAR of 3.6% in a maximum sensitivity mode. The results show the feasibility of adapting an IDS to specific operational conditions, which is particularly important for Security Operations Centers (SOCs), cloud service providers, and operators of critical infrastructure.

1 INTRODUCTION

Modern information communication networks, both corporate and public, impose high demands on information security. This security is provided by antivirus tools, firewalls, integrity control systems, cryptographic protection measures, and Intrusion Detection Systems (IDS). Currently, IDS are one of the most effective tools for identifying network attacks and other malicious activities in real time.

This research is of interest to a wide range of specialists, including:

- Network security administrators,
- Analysts at Security Operations Centers (SOC),
- Information security system developers, and IT managers responsible for network infrastructure security.

The approach proposed in this article can be applied to solve practical tasks such as protecting corporate networks, ensuring the security of cloud infrastructure, and monitoring traffic for internet service providers. It is effective against attacks like Denial of Service (DoS), Fuzzing, and Exploits, where intelligent real-time analysis of network activity is required.

1.1 Problem Statement

Despite the wide variety of existing IDS, none of them guarantees absolute information security [1]. The primary requirement for such systems is their ability to identify both known and new types of network attacks, including those distributed over time.

The main challenge lies in achieving a compromise between two critical performance metrics [2]:

1) Accuracy. The system's ability to correctly identify both malicious and legitimate traffic. Low accuracy can lead to successful cyberattacks, data breaches, financial losses, and business process disruptions.
2) False Alarm Rate (FAR). The proportion of legitimate activities that the system incorrectly flags as attacks. A high FAR lead to alert fatigue, causing analysts to overlook real threats.

Thus, there is a need to develop more effective methods that allow for flexible tuning of this balance according to specific tasks and security policies [3], [4].

1.2 Formalized Problem Statement

Let T, be a stream of network traffic, where each element $p \in T$, (e.g., a network packet or session) is described by a feature vector $x \in R^n$. Each vector x corresponds to a true class label $y \in Y$, where $Y = \{y_0, y_1, \dots y_k\}$, is a set of states, including the normal state (y_0) and k types of attacks $(y_0, y_1, \dots y_k)$.

The objective of this research is to construct a classification function $F(x) \to \hat{y}$, where $\hat{y}$, is the predicted class label, which solves the following optimization problem:

$$maximize\big(\omega_1 * Accuracy(F) - \omega_2 * FAR(F)\big),$$

where $Accuracy$ and FAR are the quality metrics defined in Section 4, and ω_1 and ω_2 are weighting coefficients that reflect the priorities of the security policy. The function $F(x)$ must be adaptive, allowing the balance between $Accuracy$ and FAR to be adjusted by tuning internal parameters.

Neural Network Models for Network Traffic Analysis

To address the stated problem, three types of artificial neural networks (ANNs), which have proven effective in classification tasks [5], were selected:

- Multilayer Perceptron (MLP). A classic architecture effective for a wide range of tasks.
- Radial Basis Function (RBF) Network. Well-suited for separating non-linear data.
- Self-Organizing Map (SOM). Effective for clustering and visualizing high-dimensional data.

The quality of an ANN's development is directly dependent on the training data [6]. The public attack database UNSW-NB15 was chosen as the dataset for training and testing. It includes approximately 2.5 million records of network connections, each described by 49 features [7]. After preprocessing and selecting the most significant features as described in [8], a sample of 80,000 records was used for training and 20,000 records for testing, with 32 features per record.

1.3 Evaluation Criteria

The effectiveness of the models is evaluated using standard performance metrics [9] derived from four basic indicators. True Positives refer to the number of attack instances that are correctly identified by the system, while True Negatives represent normal situations that are correctly classified. False Positives occur when normal situations are incorrectly classified as attacks, whereas False Negatives correspond to attack instances that are mistakenly identified as normal situations.

Based on these indicators, several evaluation criteria are used to assess model performance. Accuracy represents the overall proportion of correctly classified records, including both attack and normal cases, across the entire dataset. The False Positive Rate measures the proportion of normal situations that are incorrectly classified as attacks, indicating the tendency of the model to generate false alarms. The False Negative Rate reflects the proportion of attack instances that are missed by the system, which is particularly critical in security-related applications. Finally, the False Alarm Rate provides an overall measure of misclassification by averaging the false positive and false negative tendencies.

Together, these metrics provide a comprehensive assessment of the effectiveness and reliability of the proposed decision-making mechanism.

1.4 Proposed Module and Solution Algorithm

The performance of the intelligent analysis module can be enhanced by using an ensemble of several neural networks [10], [11]. This work proposes a modification that utilizes an ensemble of the three previously mentioned ANNs: MLP, RBF, and SOM.

The same network traffic feature vector is fed to the input of each neural network. The output of each network is a vector where each coordinate corresponds to a type of attack or the normal state. To combine the results and make a final decision, a resultant block is used, which considers the "opinion" of each network through configurable coefficients (Fig. 1).

Let *X* be a vector characterizing the situation. Its elements $x_i = 1,\ for\ i = 1, 2, 3, 4$ represent an attack of the corresponding type, while the element $x_i = 0$ represents the absence of an attack. The state detected by the j-th neural network is denoted by $NN_i^j,\ where\ i = 0 \dots 4,\ j = 1 \dots 3$. It takes a value of 1 or 0. Each element of the vector *X* is determined by the formula:

$$x_i = \sum_{j-1}^{3} NN_i^j. \quad (5)$$

In (5), x_i can take values of 0, 1, 2, or 3. A value of x_i=0 indicates that no neural network detected this state. $x_i = 1$ means that only one of the neural networks detected this state. $x_i = 2$ means that two out of three networks detected this state. $x_i = 3$ indicates that all three neural networks characterized the situation identically. The resulting decision is defined as $R = argmax_i(x_i)$, where $argmax_i$ is the index of the element with the maximum value in vector *X*.

Uncertainty arises when several elements have maximum values. Such a situation is possible only when all three neural networks have produced different results. That is, three of the five states will be characterized by $x_i = 1$.

To resolve this ambiguity, we introduce significance coefficients for the neural networks, A_i, which characterize the degree of confidence in the results produced by each network. Since the modeling experiment results show that the SOM network (with index j=3) performs best in terms of accuracy, we assign it the highest significance coefficient, $A_3 = 1.1$. The MLP network (with index j=1), having the lowest FAR, is assigned the smallest significance coefficient, $A_1 = 0.9$. Accordingly, the RBF network will receive an average significance coefficient, $A_2 = 1.0$. The formula then takes the form:

$$x_i = \sum_{j=1}^{3} A_j \cdot NN_i^j. \quad (6)$$

To account for the high-level requirements of a security policy, we introduce additional significance coefficients, B_i. The value of B_i is higher when it is more important to recognize a situation of type *i*. For example, if the security policy requires maximum recognition of DoS attacks, the coefficient B_2 could be set to 100. If it is less critical for the system to miss a DoS attack than to overload the administrator with false alarms, the coefficient for the normal state, B_2, could be set to 0. The final formula is:

$$x_i = B_i \sum_{j=1}^{3} A_j \cdot NN_i^j. \quad (7)$$

1.5 Module Operation Algorithm

Algorithm 1: Network Traffic Classification using an ANN Ensemble

1) Input. A feature vector of network traffic, x.
2) Parallel Processing. Feed the vector x simultaneously to the inputs of three pre-trained models: $F_{MLP}(x)$, $F_{RBF}(x)$, $F_{SOM}(x)$. Each model returns a prediction vector NN_j.
3) Result Aggregation. Calculate the final score vector *X* using formula (7), where NN_i^j is the prediction of the *j*-th network for the *i*-th class, A_j is the confidence coefficient for the *j*-th network, and B_i is the importance coefficient for the *i*-th class according to the security policy.
4) Decision Making. Determine the final classification $\hat{y}$ as the class corresponding to the maximum value in the vector *X*:

$$\hat{y} = argmax_i(x_i), \quad (8)$$

5) Output. The class label $\hat{y}$.
6) The introduction of coefficients A_j and B_i allows for flexible system tuning. For instance, by increasing the coefficient B_i for a particularly dangerous type of attack, the module's sensitivity to that threat can be increased, consciously accepting a potential rise in FAR.

2 RESULTS

A comparative analysis revealed the strengths and weaknesses of each model when operating individually (Table 1):

- SOM demonstrated the highest testing accuracy (99.2%) but also the highest FAR (7.5%).
- MLP showed the best (lowest) FAR (1.8%) with good accuracy (96.2%).
- RBF performed at an intermediate level.

The performance of the ensemble module is shown in Table 2.

The proposed modified module was tested in two configurations:

- Modification A (Balanced). All security policy coefficients B_i were set to a minimum.
- Modification B (Maximum Sensitivity). All security policy coefficients B_i were set to a maximum.

The results of the simulation in terms of anomaly detection accuracy and false alarm rate are shown in Figures 2 and 3, respectively.

Table 1: Comparison of single model performance.

Model	Accuracy, %	FAR, %
MLP	96,2	1,8
RBF	94,1	2,6
SOM	99,2	7,5

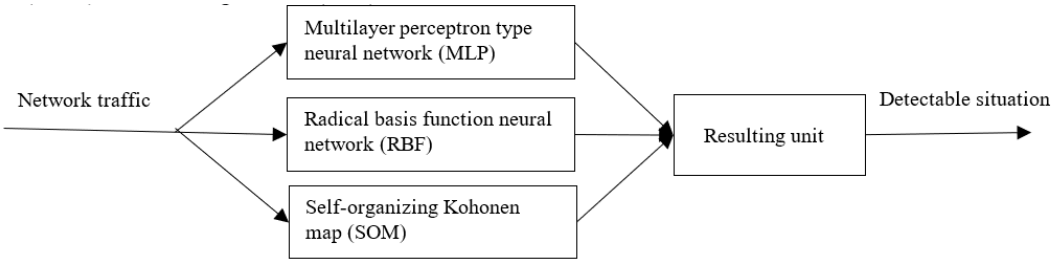

Figure 1: Schematic diagram of the intelligent network traffic analysis module.

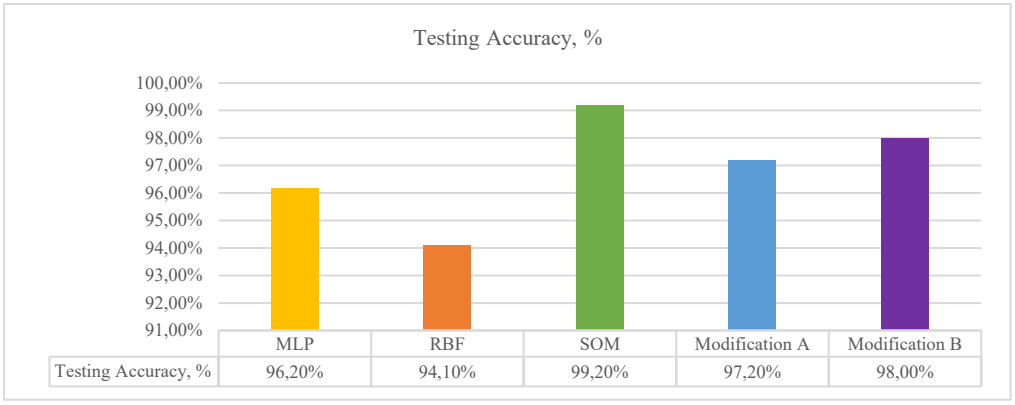

Figure 2: Results of the modeling study of the intelligent network traffic analysis module by the "anomaly detection accuracy" indicator.

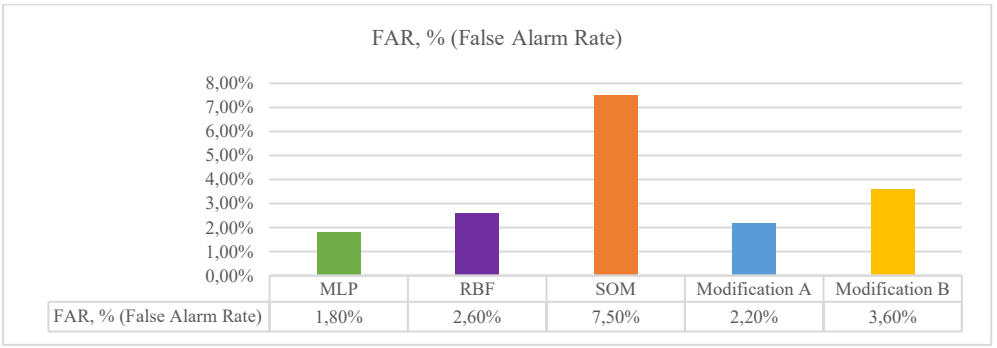

Figure 3: Results of the modeling study of the intelligent network traffic analysis module by the "false alarm rate" indicator.

Table 2: Performance of the ensemble module.

Configuration	Accuracy, %	FAR, %	Characteristics
Modification A (Balanced)	97.2	2.2	Optimal trade-off between accuracy and false alarms
Modification B (Max. Sensitivity)	98.0	3.6	Maximum attack detection with a moderate increase in FAR

The analysis shows that Modification A is an effective compromise: it increases accuracy compared to MLP (from 96.2% to 97.2%) at the cost of a slight increase in FAR (from 1.8% to 2.2%).

Modification B demonstrates how the system can be tuned for maximum threat sensitivity, achieving an accuracy of 98.0% while increasing the FAR to 3.6%, which is still significantly better than that of the most accurate single network, SOM.

3 CONCLUSIONS

This paper has proposed and investigated a modification of an intelligent network traffic analysis module based on an ensemble of three different neural networks.

1) The task was formalized, and a clear algorithm was developed that allows for combining the predictions of multiple models to enhance the quality and flexibility of an IDS.
2) The results of a modeling study on the UNSW-NB15 dataset showed that the proposed approach allows for effective management of the trade-off between detection accuracy and false alarm rate.
3) The ensemble successfully combines the strengths of the individual models:
   - In Modification A minimum sensitivity, the FAR increased by only 0.4 percentage points compared to MLP, while accuracy increased by 1 percentage point.
   - In Modification B maximum sensitivity, accuracy increased by 1.8 percentage points relative to MLP, while the FAR remained half that of SOM.
4) The developed module is a flexible tool that allows security administrators to adapt the behavior of an IDS according to the current security policy, choosing between a balanced mode and a maximum sensitivity mode.

Thus, the proposed modification proves its viability and can be used to enhance the reliability of security systems in modern information communication networks.

REFERENCES

[1] H. Holm, “Signature-based intrusion detection for zero-day attacks: (Not) a closed chapter?” in Proc. 47th Hawaii Int. Conf. System Sciences (HICSS), Jan. 2014, pp. 4895–4904.

[2] V. Jyothsna, V. V. Rama Prasad, and K. Munivara Prasad, “A review of anomaly-based intrusion detection systems,” Int. J. Comput. Appl., vol. 28, pp. 26–35, Aug. 2011.

[3] R. Braga, E. Mota, and A. Passito, “Lightweight DDoS flooding attack detection using NOX/OpenFlow,” in Proc. IEEE Conf., Oct. 2010, pp. 408–415.

[4] C. Chung, P. Khatkar, T. Xing, J. Lee, and D. Huang, “NICE: Network intrusion detection and countermeasure selection in virtual network systems,” IEEE Trans. Dependable Secure Comput., vol. 10, no. 4, pp. 198–211, Jul. 2013.

[5] N. Z. Bawany, J. A. Shamsi, and K. Salah, “DDoS attack detection and mitigation using SDN: Methods, practices, and solutions,” Arabian J. Sci. Eng., vol. 42, no. 2, pp. 425–441, Feb. 2017, doi: 10.1007/s13369-017-2414-5.

[6] S. Dotcenko, A. Vladyko, and I. Letenko, “A fuzzy logic-based information security management for software-defined networks,” in Proc. 16th Int. Conf. Advanced Communication Technology (ICACT), Feb. 2014, pp. 167–171.

[7] J. Wang, R. C. Phan, J. N. Whitley, and D. J. Parish, “Augmented attack tree modeling of distributed denial of service and tree-based attack detection method,” in Proc. 10th IEEE Int. Conf. Computer and Information Technology, Jun. 2010, pp. 1009–1014.

[8] E. Markakis, Y. Nikoloudakis, G. Mastorakis, C. X. Mavromoustakis, E. Pallis, A. Sideris, N. Zotos, J. Antic, A. Cernivec, D. Fejzic, J. Kulovic, A. Jara, A. Drosou, K. Giannoutakis, and D. Tzovaras, “Acceleration at the edge for supporting SMEs security: The Fortika paradigm,” IEEE Commun. Mag., vol. 57, no. 2, pp. 41–47, Feb. 2019.

[9] J. Jiang, Q. Yu, M. Yu, G. Li, J. Chen, K. Liu, C. Liu, and W. Huang, “ALDD: A hybrid traffic-user behavior detection method for application-layer DDoS,” in Proc. IEEE Conf., Aug. 2018, pp. 1565–1569.

[10] D. Aksu, S. Ustebay, M. Aydin, and T. Atmaca, “Intrusion detection with comparative analysis of supervised learning techniques and Fisher score feature selection algorithm,” in Proc. Int. Conf., Sep. 2018, pp. 141–149.

[11] K. Mukhamadieva, “Fuzzy artificial neural network for prediction and management tasks,” pp. 118–124, 2021.