ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIVE INFORMATION TECHNOLOGIES

UDC 004.056.5

Alguliyev R. M.[1], Aliguliyev R. M.[2], Imamverdiyev Y. N.[3], Sukhostat L. V.[4]

[1]Full member of Azerbaijan National Academy of Sciences, Dr.Sc, Professor, Director Institute of Information Technologies, Azerbaijan National Academy of Sciences, Baku, Azerbaijan
[2]Corresponding member of Azerbaijan National Academy of Sciences, Dr.Sc, Head of Department, Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan
[3]PhD, Associate Professor, Head of Department Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan
[4]PhD, Senior Researcher, Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

AN IMPROVED ENSEMBLE APPROACH FOR DOS ATTACKS DETECTION

Context. The task of using the ensemble of classifiers to detect DoS attacks in large arrays of network traffic data is solved to withstand attacks on the network.

Objective of this paper is to build an ensemble of classifiers that surpasses single classifiers in terms of accuracy.

Method. To achieve the formulated goal an algorithm, that indicates the probability of belonging to certain classes, which return a vector of classification scores for each point, is proposed. The peculiarity of the proposed approach is that for each point from the dataset, the predicted class label corresponds to the maximum value among all scores obtained by classification methods for a given point. As classifiers, decision trees, k-nearest neighbors algorithm, support vector machines with various kernel functions, and naпve Bayes are considered. A comparative analysis of the proposed approach with single classifiers is considered using the following metrics: accuracy, precision, recall, and F-measure.

Results. The experiments have been performed in R 3.4.1 on the NSL-KDD dataset of network attacks, which was divided into three classes (DoS, normal network behavior and other types of attack).

Conclusions. The conducted experiments have confirmed the efficiency of the proposed approach. The most accurate result showed an ensemble of five classifiers. The development of techniques for attacks detection based on an ensemble of classifiers avoids the problems inherent in most approaches since it is capable of detecting both known and new attacks with high accuracy. It can be concluded that the proposed approach for network attacks detection is of practical significance. In order to further study the attacks detection in network traffic, studies will be performed on real Big data sets.

Keywords: network security, network attacks, DoS, classification, ensemble of classifiers, Big data.

NOMENCLATURE

KDD – Knowledge Discovery and Data Mining;
DoS – Denial of Service Attack;
DDoS – Distributed Denial of Service Attack;
U2R – Users to Root Attack;
R2L – Remote to Local Attack;
Probe – Probing Attack;
TCP – Transmission Control Protocol;
IP – Internet Protocol;
TP – True Positive;
FP – False Positive;
TN – True Negative;
FN – False Negative;
BN – Naïve Bayes;
DT – decision tree;
SVM – support vector machines;
KNN – k-nearest neighbors algorithm;
ANN – artificial neural network;
WOAR-SVM – weighted one-against-rest SVM;
RBPBoost – Resilient Back Propagation Boosting;
MAP – maximum a posteriori probability;
RBF – radial based function kernel function;
Polynom – polynomial kernel function;
Linear – linear kernel function;
$X(t)$ – feature vector measured at time t;
w – normal vector perpendicular to the hyperplane;
b – offset of the hyperplane;
r – distance from the data point to the separating hyperplane;

DOI 10.15588/1607-3274-2018-2-8

$P(H)$ – a priori probability of each class without information on the variable x;

$P(H \mid x)$ – a posteriori probability of the variable x over the possible classes;

$P(x \mid H)$ – conditional probability of x at the likelihood H;

C – set of class labels;

x_i – dataset of points;

n – number of data points;

m – number of classifiers;

M – classification methods;

k – number of classes;

A – classification scores for each point of the dataset;

P – vector of ensemble scores.

INTRODUCTION

Big data analysis in intrusion detection and in solving network security problems is attracting increasing attention, as it facilitates the study of large amounts of complex and disparate data and detects network intrusions and contributes to the fight against cyber-attacks [1].

Network attacks are one of the causes of the abnormal phenomena observed in the work of the network equipment, as well as traffic transmission over the network. Anomalies of network traffic may result in incorrect operation of a single channel or entire network segments, lead to a denial of service in this network equipment. Network attacks are constantly changing because attackers use individual approaches. It is also affected by changes in software and hardware.

The solution of anomaly detection problem is not trivial since anomalies nature itself is changeable. Providing a comprehensive definition of abnormal or normal behavior in the context of a computer network is quite subtle [2, 3]. Another reason is that some anomaly detection methods require labels of normal and abnormal behaviors that are difficult to obtain [4, 5]. In addition, choose the right tool for anomalies detection is not easy. In [6], the study has shown that the intended tool may well be suitable for only one type of abnormality, but not for all. It is a very realistic assumption, that the selection of anomaly detection method is not simple when anomaly types are not known a priori. In addition, the network scale is the problem: when it detects anomalies it needs to consider the distribution of the tasks implementation process between multiple network servers in order to increase the overall performance and the system ability to work in case of failure of its individual elements, taking into account the size of the growing networks [7, 8].

Vulnerabilities in the communication protocol stack (TCP/IP) result in intentional or unintentional distributed denial of service (DDoS) attacks. DDoS attacks can be detected using existing machine learning methods.

The latest research works have been based on binary classification methods, which can distinguish between two states (“normal” or “abnormal”). In the event of a conflict between binary classifiers, the final solution is achieved by comparing their accuracy. An alternative solution is possible by developing an ensemble of classifiers. A new approach is required to combine such classifiers in the ensemble.

The research objective is to construct an ensemble of classifiers that surpasses single classifiers in terms of accuracy in order to detect DoS attacks.

1 PROBLEM STATEMENT

To solve the task of DoS attacks detection in network traffic, an ensemble of classifiers that surpasses single classifiers in terms of accuracy is suggested in this paper.

Let us denote the following notations (Table 1): $x_i \in R^n \ (i = \overline{1,n})$ is the point from the dataset, where n is the total number of points in the input dataset, $M = \{M_1, M_2, ..., M_m\}$ is the set of classification methods, subsequently combined into an ensemble, m is the number of classification methods, a_{ij} is the classification score for the point x_i, k is the number of classes.

Table 1 – Evaluation of classifiers for each point

Data point	Classifiers	Ensemble score
X	$M_1 \ \dots \ M_m$	
x_1	$a_{11} \ \dots \ a_{1m}$	$\max\limits_j(a_{1j})$
$\vdots$	$\vdots \ \ddots \ \vdots$	$\vdots$
x_n	$a_{n1} \ \dots \ a_{nm}$	$\max\limits_j(a_{nj})$

It is necessary to obtain a vector of ensemble scores on the basis of single classifiers to each data point in order to improve the classification accuracy.

2 REVIEW OF THE LITERATURE

A number of studies and review articles have been devoted to the intrusion detection technology [9, 10] or data mining for specific applications [11]. Since the introduction of intrusion detection principles by Denning in 1987, a large number of reactive protection systems have been developed [12–14].

Intrusion detection methods can be divided into three categories: single, hybrid, and assemblies [15]. Support vector machines (SVMs) and artificial neural networks (ANNs) are the most popular approaches among single classifiers. Several classifiers are combined to a higher goal of a significant increase in efficiency of the classifier known as an ensemble of classifiers [16]. The majority votes, bagging and boosting are some common strategies for combining classifiers [17]. Although it is known that the disadvantages of classifiers’ components accumulate in the ensemble of classifiers, but it works very effectively in varying combinations. Thus, the researchers become more and more interested in the application of the ensemble of classifiers every day.

The important cybersecurity problems for mathematical and statistical solutions have been shown in [18]. A method to improve the detection accuracy by an ensemble of two-layer SVM based on rotation forest was presented in [19]. The experiments were conducted on the KDD CUP 1999 dataset. The output of ensemble network was made by majority voting. The second layer result is used to focus on two classes “normal” and “attack”.

Classification accuracy has been improved by combining opinions from multiple experts into one using an ensemble approach in [20]. The ensemble construction method uses PSO generated weights to create the ensemble of classifiers with better accuracy for intrusion detection. This work was based on binary classification methods, which can distinguish between two states. In case of conflict between binary classifiers final decision has been reached by comparing their accuracy.

In [21] a multistep framework based on machine learning techniques to create an efficient classifier was introduced. A novel fuzzy weighting method for ensemble classifiers was proposed. Thus, adding the fuzzy weighted combiner can tag weights to classifiers related to their cost and performance.

Architecture of intelligent false alarm filter by employing a method of voted ensemble selection aiming to maintain the accuracy of false alarm reduction was proposed in [22]. The experiment was conducted using SVM, decision tree, and k-nearest neighbor (KNN) machine learning algorithms. The proposed method was validated on a real dataset.

The paper [23] aims to identify multiclass SVM models best suited to the intrusion detection task. A new approach (WOAR-SVM) based on a set of optimal, or near-optimal, weight coefficients, which define the relationship between the decision rules of the binary SVM classifiers was developed.

A generic architecture for automated DDoS attack detection and response system for the collaborative environment using machine learning were proposed in [24]. The main objective of this paper was to minimize the cost of classification errors of the intrusion detection. The proposed classification algorithm, RBPBoost, was achieved by combining ensemble of classifier outputs and Neyman Pearson cost minimization strategy, for final classification decision.

3 MATERIALS AND METHODS

More information about intrusion detection can be obtained by data classification methods. Theoretically, classification algorithms can achieve high performance, i.e. they can minimize the number of false alarms and maximize detection accuracy. One of the most attractive features of the algorithms is the ability to distinguish normal from abnormal behavior [8]. In the context of the intrusion detection, the classification algorithm is typically a map which adapts to the network invisible abnormalities [25].

Formally, each data instance is a feature vector X measured at time t and denoted as $X(t)$.

The classification algorithm is aimed to train the function that maps all the samples to their own states. To achieve its purpose, they use a set of data instances within the network. This set is known as the training dataset. Some algorithms learn a mapping function by the use of labeled training sets, where each sample in the training set is marked as one of the states. These algorithms are called supervised learning algorithms. The purpose of the use of these algorithms is to achieve high classification accuracy.

The most popular supervised machine learning methods include SVM, decision trees, Bayesian networks, KNN algorithm, etc.

The aim of SVM is to classify data points X of an n-dimensional space using $(n-1)$-dimensional hyperplane. The hyperplane satisfies $w^T x + b = 0$, where X is a set of points, w is a normal vector perpendicular to the hyperplane and b is an offset of the hyperplane $w^T x + b = 0$ from the initial point along the direction of w.

The distance from the data point to the separating hyperplane $w^T x + b = 0$ can be calculated as $r = (w^T x + b)/\|w\|$. The closest to the hyperplane data points are called support vectors. The distance between support vectors is known as margin. Linear SVM can be achieved by quadratic optimization:

$$\arg\min_{w,b}\left(\frac{1}{2}\|w\|^2\right),$$
$$y(w^T x + b) \geq 1. \quad (1)$$

SVM can find accurately linear, nonlinear and complex classification boundaries, even with a small amount of training sample.

SVMs are widely used for transmission of various type of data by switching the kernel function. The most used kernel functions include linear, polynomial, radial based function and sigmoid.

However, choosing the kernel function and fit the relevant parameters by SVM are still in the procedure of trial and error. SVM is fast, but its duration is increased four times when the data size of the sample is doubled. Unfortunately, the root of SVM algorithms is in binary classification. To solve the problems of multi-class classification several SVM for binary classes can be combined by the classification of each class or classification of each class pair.

A decision tree (DT) is a tree-structure model, which has leaves that represent classes or solutions, and branches that represent conjunctions of features that lead to those classifications.

Tree-structure classification of an input vector is performed by bypassing the tree from the root node to the end with a leaf. Each tree node computes inequality on the basis of one of the input variables. Each leaf is assigned to a particular class. Each inequality, which is used to divide the input space is based only on one of the input variables. Linear DTs are like binary DTs, except for the fact that inequality calculated at each node has a random linear form, which may depend on several variables. DT depends on the rules of "if-then", but does not require any parameters and metrics. This simple and interpretable structure allows decision trees to solve the problem for different types of attributes. DTs can also manage the missing values or noisy data. However, they can not guarantee the optimal accuracy, unlike other machine learning techniques. Although decision trees are easy to learn and implement, they are not often used for intrusion detection. This is due to the fact that finding the smallest decision tree is NP-hard.

Bayesian network classifier is based on Bayes' rule, which gives the hypothesis H of classes and data x

$$P(H \mid x) = \frac{P(x \mid H)P(H)}{P(x)}, \quad (2)$$

where $P(H)$ represents the a priori probability of each class without information on the variable x, $P(H \mid x)$ is a posteriori probability of the variable over the possible classes, is the conditional probability of x at this likelihood H. Bayesian network nodes are represented with random variables and arcs representing probabilistic relationships between variables and conditional probabilities. Node always calculates the posterior probabilities, giving proof of inheritance for the selected nodes.

Naïve Bayes (NB) is a simple Bayesian network model, which assumes that all variables are independent. It is necessary to find the maximum likelihood hypothesis, which defines the class label for the test data x, for classification by NB.

NB classifier can be resolved by the hypothesis of maximum a posteriori probability (MAP) for data as follows:

$$\arg\max_{c_j \in C} P(x \mid c_j) P(c_j), \quad (3)$$

where x is an observable data, and $C = \{c_j\}$ is a set of class labels.

Naïve Bayes is effective for tasks with a logical conclusion. However, Naıve Bayes is based on the strong assumption of variables independence.

Numbers of nearest neighbors k and distances measures are key components of the KNN algorithm. Selection of the number k should be based on cross-validation. By increasing the number k, the effect of noise in the data during classification is reduced, and this can erase the difference between the classes. In practice, k have to be less than the square root of the total number of training samples.

In the case of multiclass classification, KNN method is based on measuring the distance from one data sample to each trained sample [26]. The k-smallest distances are calculated, and the most common class based on these KNNs is considered to be the label of the output class.

KNN does not require training parameters. It is easy to implement, but it requires a lot of memory and time.

The proposed algorithm, that indicates the probability of belonging to certain classes, returns a vector of classification scores for each data point.

The peculiarity of the proposed approach is that for each point from the dataset, the predicted class label corresponds to the maximum value among all scores obtained by clustering methods for a given point.

The algorithm of the proposed approach for network attacks detection based on an ensemble of classifiers is presented below:

Input: $x_i \in R^n$: dataset of points

n: number of data points

m: number of classifiers

$M = \{M_1, M_2, ..., M_m\}$: classification methods

k: number of classes

Output:

$A = \{a_{ij}\}_{n \times m}$: classification scores for each point of the dataset

P: vector of ensemble scores

for i=1 to n do

for j=1 to do

Calculate the value of a_{ij} for M_i

End

$$P_i = \max_j a_{ij}$$

End

It is required to increase the accuracy of DoS attacks detection by using an ensemble of classifiers.

4 EXPERIMENTS

For the experiments was considered NSL-KDD dataset of network attacks [27], built on the basis of KDD-99 database on the initiative of the American Association for the Defense Advanced Research Projects Agency (DARPA) [28]. A dataset of connections was collected to conduct the research in the field of intrusion detection, which covers a wide range of intrusions simulated in a medium that mimics the US Air Force network.

Statistical analysis showed that there are important issues in the databases that highly affect the performance of the systems, as well as lead to a very bad evaluation of anomaly detection approaches. The considered database NSL-KDD has the following advantages:

1. No redundant records in the training set, so that the classifier does not show any bias results.

2. Duplicate records are not present in the test set. It contains some of the attacks that are not present in the training set.

3. A number of records selected from each difficulty levels group are inversely proportional to the number of records in the original dataset KDD.

The training set consists of 21 different attacks of 37 present in the test set. In addition, the number of records in the training (125973 samples) set and test set (22544 samples) of NSL-KDD is acceptable. This advantage makes it accessible for experiments on comprehensive data without the need to randomly select a small portion of data. Consequently, the evaluation of the results of various research projects is consistent and comparable.

All attacks in NSL-KDD are divided into four groups:

– DoS attacks include: “neptun”, “back”, “smurf”, “pod”, “land”, and “teardrop”;

– U2R (Users to Root Attack) attacks include: “buffer_overflow”, “loadmodule”, “rootkit”, and “perl”;

– R2L (Remote to Local Attack) attacks include: “warezclient”, “multihop”, “ftp_write”, “imap”, “guess_passwd”, “warezmaster”, “spy”, and “phf”;

– Probe (Probing Attack) attacks include the following types of attack: “portsweep”, “satan”, “nmap”, and “ipsweep”.

The main objectives put forward in network intrusion detection include recognition of rare types attack, increasing the accuracy of suspicious activity detection, as well as increasing the efficiency of real-time intrusion detection models. Each record has 41 attributes, which describe various features.

To evaluate the performance of classifiers, the following metrics are used: Accuracy, Recall, Precision, and F-measure. For any classification algorithm, four classification cases are possible, and this helps to understand the difference between the following metrics: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) results.

Classification accuracy can be defined as the proportion of the correct results, which is achieved by the classifier:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}. \quad (4)$$

Precision shows how much of the objects identified by the classifier as positive are really positive:

$$precision = \frac{TP}{TP + FP}. \quad (5)$$

Recall shows which part of the positive objects was selected by the classifier:

$$recall = \frac{TP}{TP + FN}. \quad (6)$$

F-measure is a metric that combines the recall and precision:

$$F - measure = \frac{2 \times recall \times precision}{recall + precision}. \quad (7)$$

Error rate (or Misclassification error) measures the ratio of incorrectly classified samples over the total number of classified samples:

$$Error\ rate = \frac{FP + FN}{TP + TN + FP + FN}. \quad (8)$$

5 RESULTS

It is the experiments were conducted using Windows® 10–64 bits operating system platform with core i7 processor 2.5 GHz, 8.0 GB RAM. The proposed approach was evaluated on R 3.4.1. NSL-KDD dataset was divided into 3 classes (DoS, Normal and Other attacks (U2R, R2L, and Probe)).

A comparative analysis of the proposed approach with single classifiers has been carried out. The ensemble of classifiers consisted of combinations of DT, SVM with various kernel functions, NB and KNN.

Accuracy, Recall, Precision, and F-measure were considered as evaluation metrics. The classification results are shown in Tables 2–5. From these tables, ranks (shown in square brackets) were obtained for each metric of each class, the results of which are shown in Tables 6–8.

It can be concluded from Table 2 that the highest accuracy (92.33%) of DoS attacks detection was achieved for the ensemble of five classifiers (DT+KNN+SVM(Polynom)+ +NB+SVM(Linear)), which exceeded the result of the single classifier (KNN) by 4.12%.

Despite the fact that NB shows the lowest result (80.45%), when adding it to the ensemble of classifiers, the accuracy of the proposed approach increased and amounted to 92.19% for four classifiers (DT+KNN+SVM(Polynom)+NB), and for six classifiers (DT+KNN+SVM(Polynom)+NB+SVM(Linear)+ +SVM (RBF)) – 91.89%.

Comparison of the recall and precision values for DoS attacks detection is shown in Tables 3 and 4, respectively.

Table 5 presents the F-measure results, where the performance of classification methods in general, combining the Recall and Precision values, is evaluated.

For the DoS class, the ensemble DT+KNN+SVM(Polynom)+NB+SVM(Linear) showed the best rank [29] according to the three metrics Accuracy, Precision and F-measure, according to the metric Recall the ensemble DT+KNN+SVM(Polynom)+NB demonstrates the best result. From Table 6, the worst result showed the NB method under three metrics (out of four), and the DT method had the worst rank by one metric (Recall).

From Table 7, the ensemble DT+KNN+ +SVM(Polynom)+NB showed the best results for the Normal class under the three metrics, and the worst result showed the NB method according to Accuracy, Recall, and F-measure.

Table 2 – Comparison of the classification accuracy of the proposed algorithm with other classifiers

Class / Method	DoS	Normal	Other attacks
DT	86.32% [9]	77.19% [9]	64.25% [10]
KNN	88.21% [5]	79.67% [5]	65.80% [8]
SVM(Linear)	87.21% [7]	77.96% [8]	66.22% [7]
SVM(Polynom)	86.64% [8]	79.50% [6]	68.31% [5]
SVM(RBF)	87.25% [6]	78.84% [7]	65.38% [9]
NB	80.45% [10]	71.25% [10]	66.50% [6]
DT+KNN+SVM(Polynom)	90.74% [4]	84.77% [4]	74.53% [4]
DT+KNN+SVM(Polynom)+NB	92.19% [2]	88.63% [1]	82.76% [3]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	92.33% [1]	88.58% [3]	83.35% [1]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	91.89% [3]	88.60% [2]	82.93% [2]

Table 3 – Comparison of classification methods in terms of Precision

Class / Method	DoS	Normal	Other attacks
DT	95.94% [7]	63.17% [10]	88.15% [6]
KNN	95.88% [8]	65.87% [6]	86.05% [8]
SVM(Linear)	96.65% [5]	64.37% [9]	84.47% [9]
SVM(Polynom)	96.14% [6]	65.70% [7]	88.12% [7]
SVM(RBF)	85.07% [9]	64.92% [8]	96.17% [2]
NB	73.03% [10]	74.78% [4]	41.80% [10]
DT+KNN+SVM(Polynom)	96.74% [4]	71.95% [5]	94.41% [5]
DT+KNN+SVM(Polynom)+NB	97.94% [2]	77.74% [1]	95.76% [4]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	99.98% [1]	76.81% [3]	100% [1]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	97.91% [3]	77.60% [2]	96.06% [3]

Table 4 – Comparison of classification methods in terms of Recall

Class / Method	DoS	Normal	Other attacks
DT	74.19% [10]	97.33% [8]	29.75% [10]
KNN	78.08% [5]	97.62% [5]	33.28% [8]
SVM(Linear)	75.72% [7]	96.19% [9]	34.42% [7]
SVM(Polynom)	74.77% [8]	97.50% [7]	38.23% [6]
SVM(RBF)	76.00% [6]	97.57% [6]	32.54% [9]
NB	74.51% [9]	57.07% [10]	58.51% [4]
DT+KNN+SVM(Polynom)	82.86% [4]	98.62% [4]	49.99% [5]
DT+KNN+SVM(Polynom)+NB	85.28% [1]	98.63% [3]	66.44% [3]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	84.67% [2]	100% [1]	66.70% [2]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	84.66% [3]	98.77% [2]	66.72% [1]

Table 5 – Comparison of classification methods in terms of F-measure

Class / Method	DoS	Normal	Other attacks
DT	83.67% [9]	76.62% [9]	44.48% [10]
KNN	86.07% [5]	78.66% [5]	48.00% [8]
SVM(Linear)	84.91% [6]	77.13% [8]	48.91% [6]
SVM(Polynom)	84.12% [8]	78.50% [6]	53.33% [5]
SVM(RBF)	84.90% [7]	77.97% [7]	47.07% [9]
NB	73.76% [10]	64.74% [10]	48.76% [7]
DT+KNN+SVM(Polynom)	89.27% [4]	83.20% [4]	65.37% [4]
DT+KNN+SVM(Polynom)+NB	91.17% [2]	86.95% [1]	78.45% [3]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	91.69% [1]	86.88% [3]	80.02% [1]
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	90.81% [3]	86.92% [2]	78.74% [2]

The best rank for Other attacks class is obtained for ensemble DT+KNN+SVM(Polynom)+NB+SVM(Linear) according to the Accuracy, Precision, and F-measure metrics. The ensemble DT+KNN+SVM(Polynom)+NB+ +SVM(Linear)+SVM(RBF) showed the best result under one metric (Recall) (Table 8).

6 DISCUSSION

From Tables 6–8, we can conclude:

1) The best results among the methods for network attacks detection showed the ensemble DT+KNN+SVM(Polynom)+NB.

2) The methods KNN and DT (Table 6), NB and SVM (Linear) (Table 7) and SVM (RBF) and SVM (Linear) have the equal ranks (Table 8).

3) The proposed approach with different combinations of classifiers is superior to single classifiers.

To show a comparison of methods more clearly, we demonstrate this in Fig. 1, where the error rates for each classifier are shown. For each classifier, the error rates were computed. In the figure, the red color indicates the classification error rates for DoS attacks, the green color indicates the error rates for other types of attack and the blue color shows the error rates for "normal" state. Single classifiers (DT, NB, SVM, and KNN) were compared with various ensembles of classifiers using the proposed approach.

Table 6 – The resultant rank of the methods for DoS class

Method	The number of times the method is in the S^{th} rank S =										Resultant rank	
	1	2	3	4	5	6	7	8	9	10		
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	3	1	0	0	0	0	0	0	0	0	3.9	1
DT+KNN+SVM(Polynom)+NB	1	3	0	0	0	0	0	0	0	0	3.7	2
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	0	0	4	0	0	0	0	0	0	0	3.2	3
DT+KNN+SVM(Polynom)	0	0	0	4	0	0	0	0	0	0	2.8	4
SVM(Linear)	0	0	0	0	1	1	2	0	0	0	1.9	5
SVM(RBF)	0	0	0	0	0	2	1	0	1	0	1.6	6
SVM(Polynom)	0	0	0	0	0	1	0	3	0	0	1.4	7
KNN	0	0	0	0	3	0	0	1	0	0	0.9	8
DT	0	0	0	0	0	0	1	0	2	1	0.9	9
NB	0	0	0	0	0	0	0	0	1	3	0.5	10

Table 7 – The resultant rank of the methods for Normal class

Method	The number of times the method is in the S^{th} rank S =										Resultant rank	
	1	2	3	4	5	6	7	8	9	10		
DT+KNN+SVM(Polynom)+NB	3	0	1	0	0	0	0	0	0	0	3.8	1
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	0	4	0	0	0	0	0	0	0	0	3.6	2
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	1	0	3	0	0	0	0	0	0	0	3.4	3
DT+KNN+SVM(Polynom)	0	0	0	3	1	0	0	0	0	0	2.7	4
KNN	0	0	0	0	3	1	0	0	0	0	2.3	5
SVM(Polynom)	0	0	0	0	0	2	2	0	0	0	1.8	6
SVM(RBF)	0	0	0	0	0	1	2	1	0	0	1.6	7
NB	0	0	0	1	0	0	0	0	0	3	1.0	8
SVM(Linear)	0	0	0	0	0	0	0	2	2	0	1.0	9
DT	0	0	0	0	0	0	0	1	2	1	0.8	10

Table 8 – The resultant rank of the methods for Other attacks class

Method	The number of times the method is in the S^{th} rank S =										Resultant rank	
	1	2	3	4	5	6	7	8	9	10		
DT+KNN+SVM(Polynom)+NB+SVM (Linear)	3	1	0	0	0	0	0	0	0	0	3.9	1
DT+KNN+SVM(Polynom)+NB+SVM (Linear)+SVM(RBF)	1	2	1	0	0	0	0	0	0	0	3.6	2
DT+KNN+SVM(Polynom)+NB	0	0	3	1	0	0	0	0	0	0	3.1	3
DT+KNN+SVM(Polynom)	0	0	0	2	2	0	0	0	0	0	2.6	4
SVM(Polynom)	0	0	0	0	2	1	1	0	0	0	2.1	5
NB	0	0	0	1	0	1	1	0	0	1	1.7	6
SVM(RBF)	0	1	0	0	0	0	0	0	3	0	1.5	7
SVM(Linear)	0	0	0	0	0	1	2	0	1	0	1.5	8
KNN	0	0	0	0	0	0	0	4	0	0	1.2	9
DT	0	0	0	0	0	1	0	0	0	3	0.8	10

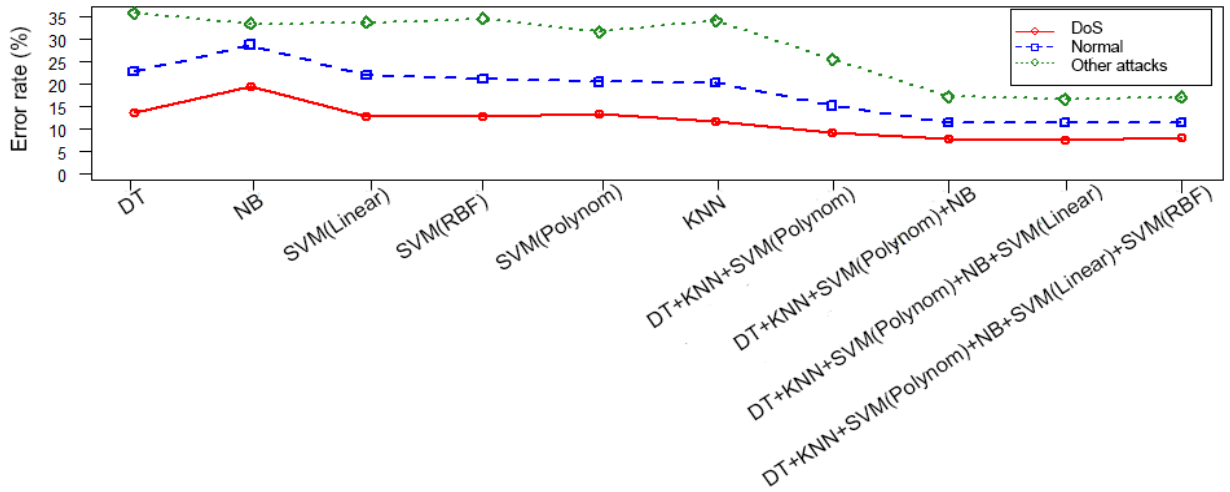

Figure 1 – Error rates for the classifiers on NSL-KDD dataset

KNN, SVM(Linear), and SVM(RBF) gave the lowest error rates among the single classifiers for DoS class (11.79%, 12.79%, and 12.75%, respectively). The lowest result for the DoS class showed the NB method and amounted to 19.55%. Despite the fact that the NB classifier has the highest error rate, in combination with other classifiers in the proposed approach, it showed a good result.

CONCLUSIONS

At present, the processing and analysis of Big data are important for ensuring information security. Intrusion detection is one of the serious problems in the field of network security. In this study, in order to resist attacks on the network, the ensemble of classifiers was successfully applied. The ensemble improves recognition accuracy by combining various single classifiers. The ensemble of classifiers consisted of combinations of DT, SVM with various kernel functions, NB and KNN algorithms.

In general, the considered classification methods showed high accuracy of DoS attacks detection. The most accurate result was shown by an ensemble of five classifiers (DT+KNN+SVM(Polynom)+NB+SVM(Linear)). It can be concluded that the proposed approach for network attacks detection is of practical significance.

ACKNOWLEDGEMENTS

This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan – Grant № EƏF-KETPL-2-2015-1(25)-56/05/1.

REFERENCES

1. Aliguliyev R. M. Multidisciplinary problems of big data in information security / R. M. Aliguliyev, Y. N. Imamverdiyev, M. S. Hajirahimova // Proceedings of the II International scientific and practical conference Information Security and Computer Technologies. – 2017. – P. 10-11.
2. Nallaivarothayan H. An evaluation of different features and learning models for anomalous event detection / H. Nallaivarothayan, D. Ryan, S. Denman, S. Sridharan, C. Fookes // Proceedings of the International Conference on Digital Image Computing: Techniques and Applications. – 2013. – P. 1–8. DOI: 10.1109/dicta.2013.6691480
3. Xie M. Anomaly detection in wireless sensor networks: a survey / M. Xie, S. Han, B. Tian, S. Parvin // Journal of Network and Computer Applications. – 2011. – Vol. 34. – P. 1302–1325. DOI: 10.1016/j.jnca.2011.03.004
4. Davis J. J. Data preprocessing for anomaly based network intrusion detection: a review / J. J. Davis, A. J. Clark // Computers & Security. – 2011. – Vol. 30. – P. 353–375. DOI: 10.1016/j.cose.2011.05.008
5. Fiorea U. Network anomaly detection with the restricted boltzmann machine / U. Fiorea, F. Palmierib, A. Castiglionec, A. D. Santis // Neurocomputing. – 2013. – Vol. 122. – P. 13–23. DOI: 10.1016/j.neucom.2012.11.050
6. Chandola V. Anomaly detection: a survey / V. Chandola, A. Banerjee, V. Kumar // ACM Computing Surveys. – 2009. – Vol. 41, № 3. – P. 1–58. DOI: 10.1145/1541880.1541882
7. Anceaume E. Anomaly characterization in large scale networks / E. Anceaume, Y. Busnel, E. L. Merrer, R. Ludinard, J. Marchand, B. Sericola // Proceedings of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. – 2014. – P. 68–79. DOI: 10.1109/dsn.2014.23
8. Dua S. Data mining and machine learning in cybersecurity / S. Dua, X. Du. – Boca Raton, FL: CRC Press, 2011. – 256 p. DOI: 10.1201/b10867
9. Catania C. A. Automatic network intrusion detection: current techniques and open issues / C. A. Catania, C. G. Garino // Computers and Electrical Engineering. – 2012. – Vol. 38, № 5. – P. 1062–1072. DOI: 10.1016/j.compeleceng.2012.05.013
10. Ahmed M. A survey of network anomaly detection techniques / M. Ahmed, A. Mahmood, J. Hu // Journal of Network and Computer Applications. – 2016. – Vol. 60. – P. 19–31. DOI: 10.1016/j.jnca.2015.11.016
11. Wu S. X. The use of computational intelligence in intrusion detection systems: a review / S. X. Wu, W. Banzhaf // Applied Soft Computing. – 2010. – Vol. 10, № 1. – P. 1–35. DOI: 10.1016/j.asoc.2009.06.019
12. Chandola V. Data mining for cyber security / V. Chandola, E. Eilertson, L. Ertoz, G. Simon, V. Kumar. – New York: Springer, 2006. – 159 p. – (Data Warehousing and Data Mining Techniques for Computer Security.). DOI: 10.1007/978-0-387-47653-7
13. Lee W. A framework for constructing features and models for intrusion detection systems / W. Lee, S. J. Stolfo // ACM Transactions on Information and System Security. – 2000. – Vol. 3, № 4. – P. 227–261. DOI: 10.1145/382912.382914
14. Mahoney M. V. Learning nonstationary models of normal network traffic for detecting novel attacks / M. V. Mahoney, P. K. Chan / / Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining. – 2002. – P. 376–386. DOI: 10.1145/775047.775102
15. Hodge V. A survey of outlier detection methodologies / V. Hodge, J. Austin // Artificial Intelligence Review. – 2004. – Vol. 22, № 2. – P. 85–126. DOI: 10.1023/b:aire.0000045502.10941.a9
16. Farid D. M. Adaptive intrusion detection based on boosting and naive bayesian classifier / D. M. Farid, M. Z. Rahman, C. M. Rahman // International Journal of Computer Applications. – 2011. – Vol. 24, № 3. – P. 12–19. DOI: 10.5120/2932-3883

17. Laurentys C. A. A novel artificial immune system for fault behavior detection / C. A. Laurentys, R. M. Palhares, W. M. Caminhas // Expert Systems with Applications. – 2011. – Vol. 38. – P. 6957–6966. DOI: 10.1016/j.eswa.2010.12.019
18. Meza J. Mathematical and statistical opportunities in cybersecurity / J. Meza, S. Campbell, D. Bailey // Paper LBNL-1667E, Lawrence Berkeley National Laboratory, Berkeley, CA. – 2009. – P. 1–11. DOI: 10.2172/950976
19. Lin L. SVM ensemble for anomaly detection based on rotation forest / L. Lin, R. Zuo, S. Yang, Z. Zhang // Proceedings of the 3rd International Conference on Intelligent Control and Information Processing. – 2012. – P. 150–153. DOI: 10.1109/icicip.2012.6391455
20. Aburomman A. A novel SVM-kNN-PSO ensemble method for intrusion detection system / A. A. Aburomman, M. B. I. Reaz // Applied Soft Computing. – 2016. – Vol. 38. – P. 360–372. DOI: 10.1016/j.asoc.2015.10.011
21. Masarat S. A novel framework, based on fuzzy ensemble of classifiers for intrusion detection systems / S. Masarat, H. Taheri, S. Sharifian // Proceedings of the 4th International Conference on Computer and Knowledge Engineering. – 2014. – P. 165–170. DOI: 10.1109/iccke.2014.6993345
22. Meng Y. Enhancing false alarm reduction using voted ensemble selection in intrusion detection / Y. Meng, L. F. Kwok, W. Li // International Journal of Computational Intelligence Systems. – 2013. – Vol. 6, № 4. – P. 626–638. DOI: 10.1080/18756891.2013.802114
23. Aburomman A. A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems / A. A. Aburomman, M. B. I. Reaz // Information Sciences. – 2017. – Vol. 414. – P. 225–246. DOI: 10.1016/j.ins.2017.06.007
24. Kumar P. A. R. Distributed denial of service attack detection using an ensemble of neural classifier / P. A. R. Kumar, S. Selvakumar // Computer Communications. – 2011. – Vol. 34, № 11. – P. 1328–1341. DOI: 10.1016/j.comcom.2011.01.012
25. Nguyen N.T. Advances in multimedia and network information system technologies / N. T. Nguyen, A. Zgrzywa, A. Czyzewski. – Berlin: Springer-Verlag, 2010. – 318 p. DOI: 10.1007/978-3-642-14989-4
26. Zhang M.-L. A k-nearest neighbor based algorithm for multi-label classification / M.-L. Zhang, Z.-H. Zhou // Proceedings of IEEE International Conference on Granular Computing. – 2005. – P. 718–721. DOI: 10.1109/grc.2005.1547385
27. Aggarwal P. Analysis of KDD dataset attributes-class wise for intrusion detection / P. Aggarwal, S. K. Sharma // Procedia Computer Science. – 2015. – Vol. 57. – P. 842–851. DOI: 10.1016/j.procs.2015.07.490
28. McHugh J. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by Lincoln laboratory / J. McHugh // ACM Transactions on Information and System Security. – 2000. – Vol. 3, № 4. – P. 262–294. DOI: 10.1145/382912.382923
29. Aliguliyev R. M. Performance evaluation of density-based clustering methods / R. M. Aliguliyev // Information Sciences. – 2009. – Vol. 179. – P. 3583–3602. DOI: 10.1016/j.ins.2009.06.012

Article was submitted 29.12.2017.
After revision 15.01.2018.

Алгуліев Р. М.[1], Алигуліев Р. М.[2], Імамвердієв Я. Н.[3], Сухостат Л. В.[4]

[1]Академік Національної Академії Наук Азербайджану, д-р техн. наук, проф., директор Інституту Інформаційних Технологій Національної Академії Наук Азербайджану, Баку, Азербайджан

[2]Член-кореспондент Національної Академії Наук Азербайджану, д-р техн. наук, зав. відділом, Інститут Інформаційних Технологій Національної Академії Наук Азербайджану, Баку, Азербайджан

[3]Канд. техн. наук, доцент, зав. відділом, Інститут інформаційних технологій Національної Академії Наук Азербайджану, Баку, Азербайджан

[4]Канд. техн. наук, старший науковий співробітник, Інститут інформаційних технологій Національної Академії Наук Азербайджану, Баку, Азербайджан

ПОКРАЩЕНИЙ ПІДХІД ВИЯВЛЕННЯ DOS АТАК З ВИКОРИСТАННЯМ АНСАМБЛЮ

Актуальність. Розв'язана задача застосування ансамблю класифікаторів для виявлення DoS атак у великих масивах даних мережевого трафіку, щоб протистояти атакам в мережі.

Мета роботи полягає в побудові ансамблю класифікаторів, що перевершує поодинокі класифікатори з точки зору точності.

Метод. Для досягнення поставленої мети в роботі запропоновано алгоритм, який вказує на ймовірність приналежності до певних класів, який повертає вектор оцінок класифікаторів для кожної точки. Особливість запропонованого підходу полягає в тому, що для кожної точки з набору даних передбачена мітка класу відповідає максимальному значенню серед всіх оцінок, отриманих методами класифікації для даної точки. Як класифікаторів були розглянуті дерева рішень, алгоритм *k*-найближчих сусідів, машини опорних векторів з різними ядерними функціями і наївний байесовский класифікатор. Порівняльний аналіз запропонованого підходу з розглянутими одиничними класифікаторами проводиться за наступними метрик: точність, повнота, «влучність» і *F*-міра.

Результати. Експерименти були проведені на мові R 3.4.1 на наборі даних мережевих атак NSL-KDD, який був розбитий на три класи (DoS, «нормальну» поведінку мережі та інші типи атак).

Висновки. Проведені експерименти підтвердили працездатність запропонованого підходу. Найбільш точний результат показав ансамбль з п'яти класифікаторів. Розробка техніки виявлення атак, заснованої на застосуванні ансамблю класифікаторів, дозволяє уникнути проблем, характерних для більшості підходів, оскільки він здатний з високою точністю виявити як відомі, так і нові атаки. Можна зробити висновок про практичну значимість запропонованого підходу до виявлення атак в мережі. З метою подальшого вивчення виявлення атак в мережевому трафіку будуть проведені дослідження на реальних наборах даних великої розмірності.

Ключові слова: інформаційна безпека, мережеві атаки, DoS, класифікація, ансамбль класифікаторів, Big data.

Алгулиев Р. М.[1], Алыгулиев Р. М.[2], Имамвердиев Я. Н.[3], Сухостат Л. В.[4]

[1]Академик Национальной Академии Наук Азербайджана, д-р техн. наук, проф., директор Института Информационных Технологий Национальной Академии Наук Азербайджана, Баку, Азербайджан

[2]Член-корреспондент Национальной Академии Наук Азербайджана, д-р техн. наук, зав. отделом, Институт Информационных Технологий Национальной Академии Наук Азербайджана, Баку, Азербайджан

[3]Канд. техн. наук, доцент, зав. отделом, Институт информационных технологий Национальной Академии Наук Азербайджана, Баку, Азербайджан

[4]Канд. техн. наук, старший научный сотрудник, Институт информационных технологий Национальной Академии Наук Азербайджана, Баку, Азербайджан

УЛУЧШЕННЫЙ ПОДХОД ОБНАРУЖЕНИЯ DOS АТАК С ПРИМЕНЕНИЕМ АНСАМБЛЯ

Актуальность. Решена задача применения ансамбля классификаторов к обнаружению DoS атак в больших массивах данных сетевого трафика, чтобы противостоять атакам в сети.

Цель работы заключается в построении ансамбля классификаторов, превосходящего единичные классификаторы с точки зрения точности.

Метод. Для достижения поставленной цели в работе предложен алгоритм, указывающий на вероятности принадлежности к определенным классам, возвращающий вектор оценок классификаторов для каждой точки. Особенность предложенного подхода состоит в том, что для каждой точки из набора данных предсказанная метка класса соответствует максимальному значению среди всех оценок, полученных методами классификации для данной точки. В качестве классификаторов были рассмотрены деревья решений, алгоритм *k*-ближайших соседей, машины опорных векторов с различными ядерными функциями и наивный байесовский классификатор. Сравнительный анализ предложенного подхода с рассмотренными единичными классификаторами проводится по следующим метрикам: точность, полнота, «меткость» и *F*-мера.

Результаты. Эксперименты были проведены на языке R 3.4.1 на наборе данных сетевых атак NSL-KDD, который был разбит на три класса (DoS, «нормальное» поведение сети и другие типы атак).

Выводы. Проведенные эксперименты подтвердили работоспособность предложенного подхода. Наиболее точный результат показал ансамбль из пяти классификаторов. Разработка техники обнаружения атак, основанной на применении ансамбля классификаторов, позволяет избежать проблем, характерных для большинства подходов, поскольку он способен с высокой точностью обнаружить как известные, так и новые атаки. Можно сделать вывод о практической значимости предложенного подхода к обнаружению атак в сети. В целях дальнейшего изучения обнаружения атак в сетевом трафике будут проведены исследования на реальных наборах данных большой размерности.

Ключевые слова: информационная безопасность, сетевые атаки, DoS, классификация, ансамбль классификаторов, Big data.

REFERENCES

1. Aliguliyev R. M., Imamverdiyev Y. N., Hajirahimova M. S. Multidisciplinary problems of big data in information security, *Proceedings of the II International scientific and practical conference Information Security and Computer Technologies*, 2017, pp. 10–11.
2. Nallaivarothayan H. Ryan D., Denman S., S. Sridharan, C. Fookes An evaluation of different features and learning models for anomalous event detection, *Proceedings of the International Conference on Digital Image Computing: Techniques and Applications*, 2013, pp. 1–8. DOI: 10.1109/dicta.2013.6691480
3. Xie M., Han S., Tian B., Parvin S. Anomaly detection in wireless sensor networks: a survey, *Journal of Network and Computer Applications*, 2011, Vol. 34, pp. 1302–1325. DOI: 10.1016/j.jnca.2011.03.004
4. Davis J. J., Clark A. J. Data preprocessing for anomaly based network intrusion detection: a review, *Computers & Security*, 2011, Vol. 30, pp. 353–375. DOI: 10.1016/j.cose.2011.05.008
5. Fiorea U., Palmierib F., Castiglionec A., Santis A. D. Network anomaly detection with the restricted boltzmann machine, *Neurocomputing*, 2013, Vol. 122, pp. 13–23. DOI: 10.1016/j.neucom.2012.11.050
6. Chandola V., Banerjee A., Kumar V. Anomaly detection: a survey, *ACM Computing Surveys*, 2009, Vol. 41, No. 3, pp. 1–58. DOI: 10.1145/1541880.1541882
7. Anceaume E., Busnel Y., Merrer E. L., Ludinard R., Marchand J., Sericola B. Anomaly characterization in large scale networks, *Proceedings of the 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2014, pp. 68–79. DOI: 10.1109/dsn.2014.23
8. Dua S., Du X. Data mining and machine learning in cybersecurity. Boca Raton, FL, CRC Press, 2011, 256 p. DOI: 10.1201/b10867
9. Catania C. A., Garino C. G. Automatic network intrusion detection: current techniques and open issues, *Computers and Electrical Engineering*, 2012, Vol. 38, No. 5, pp. 1062–1072. DOI: 10.1016/j.compeleceng.2012.05.013
10. Ahmed M., Mahmood A., Hu J. A survey of network anomaly detection techniques, *Journal of Network and Computer Applications*, 2016, Vol. 60, pp. 19–31. DOI: 10.1016/j.jnca.2015.11.016
11. Wu S. X., Banzhaf W. The use of computational intelligence in intrusion detection systems: a review, *Applied Soft Computing*, 2010, Vol. 10, No. 1, pp. 1–35. DOI: 10.1016/j.asoc.2009.06.019
12. Chandola V., Eilertson E., Ertoz L., Simon G., Kumar V. Data mining for cyber security. New York: Springer, 2006, 159 p. (Data Warehousing and Data Mining Techniques for Computer Security.). DOI: 10.1007/978-0-387-47653-7
13. Lee W., Stolfo S. J. A framework for constructing features and models for intrusion detection systems, *ACM Transactions on Information and System Security*, 2000, Vol. 3, No. 4, pp. 227–261. DOI: 10.1145/382912.382914
14. Mahoney M. V., Chan P. K. Learning nonstationary models of normal network traffic for detecting novel attacks, *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2002, pp. 376–386. DOI: 10.1145/775047.775102
15. Hodge V., Austin J. A survey of outlier detection methodologies, *Artificial Intelligence Review*, 2004, Vol. 22, No. 2, pp. 85–126. DOI: 10.1023/b:aire.0000045502.10941.a9
16. Farid D. M., Rahman M. Z., Rahman C. M. Adaptive intrusion detection based on boosting and naive bayesian classifier, *International Journal of Computer Applications*, 2011, Vol. 24, No. 3, pp. 12–19. DOI: 10.5120/2932-3883
17. Laurentys C. A., Palhares R. M., Caminhas W. M. A novel artificial immune system for fault behavior detection, *Expert Systems with Applications*, 2011, Vol. 38, pp. 6957–6966. DOI: 10.1016/j.eswa.2010.12.019
18. Meza J., Campbell S., Bailey D. Mathematical and statistical opportunities in cybersecurity, *Paper LBNL-1667E, Lawrence Berkeley National Laboratory, Berkeley, CA*, 2009, pp. 1–11. DOI: 10.2172/950976
19. Lin L. Zuo R., Yang S., Zhang Z. SVM ensemble for anomaly detection based on rotation forest, *Proceedings of the 3rd International Conference on Intelligent Control and Information Processing*, 2012, pp. 150–153. DOI: 10.1109/icicip.2012.6391455
20. Aburomman A., Reaz M. B. I. A novel SVM-kNN-PSO ensemble method for intrusion detection system, *Applied Soft Computing*, 2016, Vol. 38, pp. 360–372. DOI: 10.1016/j.asoc.2015.10.011
21. Masarat S., Taheri H., Sharifian S. A novel framework, based on fuzzy ensemble of classifiers for intrusion detection systems, *Proceedings of the 4th International Conference on Computer and Knowledge Engineering*, 2014, pp. 165–170. DOI: 10.1109/iccke.2014.6993345
22. Meng Y., Kwok L. F., Li W. Enhancing false alarm reduction using voted ensemble selection in intrusion detection, *International Journal of Computational Intelligence Systems*, 2013, Vol. 6, No. 4, pp. 626-638. DOI: 10.1080/18756891.2013.802114
23. Aburomman A. A., Reaz M. B. I. A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems, *Information Sciences,* 2017, Vol. 414, pp. 225–246. DOI: 10.1016/j.ins.2017.06.007
24. Kumar P. A. R., Selvakumar S. Distributed denial of service attack detection using an ensemble of neural classifier, *Computer Communications*, 2011, Vol. 34, No. 11, pp. 1328–1341. DOI: 10.1016/j.comcom.2011.01.012
25. Nguyen N. T., Zgrzywa A., Czyzewski A. Advances in multimedia and network information system technologies. Berlin, Springer-Verlag, 2010, 318 p. DOI: 10.1007/978-3-642-14989-4
26. Zhang M.-L., Zhou Z.-H. A k-nearest neighbor based algorithm for multi-label classification, *Proceedings of IEEE International Conference on Granular Computing,* 2005, pp. 718–721. DOI: 10.1109/grc.2005.1547385
27. Aggarwal P., Sharma S. K. Analysis of KDD dataset attributes-class wise for intrusion detection, *Procedia Computer Science*, 2015, Vol. 57, pp. 842–851. DOI: 10.1016/j.procs.2015.07.490
28. McHugh J. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory, *ACM Transactions on Information and System Security*, 2000, Vol. 3, No. 4, pp. 262–294. DOI: 10.1145/382912.382923
29. Aliguliyev R. M. Performance evaluation of density-based clustering methods, *Information Sciences*, 2009, Vol. 179, pp. 3583–3602. DOI: 10.1016/j.ins.2009.06.012