Computers, Materials & Continua
DOI:10.32604/cmc.2022.018773
Article

Tech Science Press

Deep Semisupervised Learning-Based Network Anomaly Detection in Heterogeneous Information Systems

Nazarii Lutsiv[1], Taras Maksymyuk[1,*], Mykola Beshley[1], Orest Lavriv[1], Volodymyr Andrushchak[1], Anatoliy Sachenko[2], Liberios Vokorokos[3] and Juraj Gazda[3]

[1]Lviv Polytechnic National University, Lviv, 79013, Ukraine
[2]West Ukrainian National University, Ternopil, 46009, Ukraine
[3]Technical University of Kosice, Kosice, 04200, Slovakia
[*]Corresponding Author: Taras Maksymyuk. Email: taras.maksymyuk@gmail.com
Received: 21 March 2021; Accepted: 23 April 2021

Abstract: The extensive proliferation of modern information services and ubiquitous digitization of society have raised cybersecurity challenges to new levels. With the massive number of connected devices, opportunities for potential network attacks are nearly unlimited. An additional problem is that many low-cost devices are not equipped with effective security protection so that they are easily hacked and applied within a network of bots (botnet) to perform distributed denial of service (DDoS) attacks. In this paper, we propose a novel intrusion detection system (IDS) based on deep learning that aims to identify suspicious behavior in modern heterogeneous information systems. The proposed approach is based on a deep recurrent autoencoder that learns time series of normal network behavior and detects notable network anomalies. An additional feature of the proposed IDS is that it is trained with an optimized dataset, where the number of features is reduced by 94% without classification accuracy loss. Thus, the proposed IDS remains stable in response to slight system perturbations, which do not represent network anomalies. The proposed approach is evaluated under different simulation scenarios and provides a 99% detection accuracy over known datasets while reducing the training time by an order of magnitude.

Keywords: DDoS; deep semisupervised learning; cybersecurity; anomaly detection

1 Introduction

Cybersecurity has always been a key part since the very beginning of the development of information and communication technologies. With the rapid proliferation of the Internet of Things (IoT), cybersecurity is becoming increasingly important because large volumes of personal data widely circulate in modern information systems. To this end, there are many technical solutions that aim to detect malicious behavior within a network. However, the continuous improvement on the attacker side has encouraged researchers and network equipment manufacturers to develop new advanced solutions, which handle new potential threats. Modern network

attacks occur when malicious traffic is masqueraded as typical network traffic, which remains undetected via a brief overview of packet headers. Therefore, most current intrusion detection systems (IDSs) are based on deep packet inspection (DPI), which allows deep examination of the packet payload and identification of the corresponding application layer service [1–3]. Despite the widespread use and great potential of DPI, this approach exhibits certain important limitations. First, DPI effectively detects known intrusions but easily fails to detect new intrusions. Second, attackers may even exploit DPI as a tool to perform malicious actions. Third, DPI adds more complexity to existing firewalls, which requires continuous updates to maintain a good performance. Finally, DPI is very slow in modern networks due to the limitation of the packet processing time. Recent studies have indicated that DPI works well if the data rate of incoming traffic reaches up to 1 Gbps. At higher data rates, modern DPI tools start to discard packets. For example, at a data rate of 10 Gbps, DPI discards approximately 20% of packets. Studies have shown that hardware acceleration through parallel DPI processing may provide a data rate up to 4 Gbps without any loss via field programmable gate arrays and up to 7.2 Gbps via application-specific integrated circuits [4,5].

Nevertheless, with the widespread deployment of 5G networks, 10-Gbps data rates can be expected for single small cells, which indicates data rates of several terabits per second via the transport network [6–8]. At these data rates, even the most effective DPI solutions cannot be effectively scaled to provide the required tradeoff between service quality and security. Therefore, most recent studies have focused more on artificial intelligence (AI)-based techniques, which detect certain anomalies of data flows and prevent attacks without deep inspection of each packet. Among all AI-based solutions, the most promising are those based on deep learning, or more specifically deep neural networks [9–12]. A detailed survey of existing solutions based on deep learning was reported in [13]. Most modern solutions based on deep learning attain an accuracy higher than 90% in the detection of the most common network attacks. However, there is no simple solution among the various existing solutions that can be effectively applied under all network scenarios and types of attacks. Therefore, further research is needed to gain more insights into the proper selection of deep learning models for each particular cybersecurity problem. One of the main limitations of current systems is that they require extensive training over large datasets, which is not always feasible in real work applications.

In this paper, we propose a new IDS based on deep learning, which is founded on a deep recurrent autoencoder that allows learning adequate network behavior and detection of any anomalies without extensive training over large datasets. The key feature of the proposed IDS is optimal feature extraction to reduce the computational complexity and improve the detection of previously unknown attacks. The proposed model may be implemented either as a standalone solution or as a part of a more complex IDS with other deep learning and DPI models. The performance of the proposed model is tested on different datasets in terms of distributed denial of service (DDoS) attacks.

The remainder of this paper is organized as follows. Section 2 surveys the most recent AI-based IDS solutions. Section 3 describes the proposed IDS solution based on the deep recurrent autoencoder. Section 4 provides the simulation results and performance evaluation of the proposed model. Finally, we conclude the paper in Section 5.

2 Recent Related Research on Existing AI-Based IDS Solutions

2.1 Basic Requirements of DDoS Detection in Modern Information Systems

DDoS attacks occur when malicious users infect a massive number of network nodes and turn them into networks of bots (botnets), which send numerous packets to a target victim server [14]. DDoS attacks have been known for quite a long time, and we have observed tremendous growth in both the attack power and detection abilities of IDSs [15,16]. With the current development of the IoT and the corresponding exponential growth of the number of devices connected to the Internet, attackers have more opportunities to deploy massive botnets composed of IoT devices [17–19]. Considering that most of these devices are usually low-cost devices and not well protected, in the foreseen future, we can expect notable attacks from different IoT devices, such as smart kettles or home thermostats. Therefore, despite the many studies conducted over the last decade, IDS development against DDoS attacks remains of great interest.

Most existing IDSs exhibit a modular architecture that allows continuous updates and swift implementation of new features [20–24]. In a modular architecture, a separate module is created for each data-particular IDS task with corresponding methods and data structures. The major limitation of the modular architecture in the modern IDS is the problem of dependency between the different modules and compatibility issues. Any change in program code results in updates of all related modules. Therefore, most IDSs are designed in a way that allows the implementation of new features with a minimum change in the whole system.

The key challenge in the detection of modern DDoS attacks is that they usually do not contain common revealing attributes. The distributed nature of attacks does not allow their proper tracing nor determination of the identity of the attacker. Moreover, the large variety of connected devices with different types of connections and levels of security introduces an additional degree of uncertainty into the DDoS attack process.

Therefore, so far, we have observed a growing interest in machine learning-based solutions for DDoS attack detection and prevention purposes. In general, machine learning for attack detection can be implemented as follows:

- Supervised classification requires a training dataset with labeled classes of normal and anomalous system behaviors [25–27].
- Unsupervised or semisupervised clustering requires only a training dataset of normal system behavior to form a corresponding cluster. Then, any event sufficiently different from the previously learned cluster is considered anomalous system behavior [28,29].

In practical IDS applications, both aforementioned cases have usually been implemented to improve the detection capability. In the following section, we cover the recent related research on machine learning and AI approaches to DDoS attack detection.

2.2 Recent Related Research on AI-Based DDoS Detection

The advantage of AI-based detection systems is their ability to learn based on collected statistical information and accordingly modify detection rules without human input [30]. Many different AI-based methods for DDoS attack detection have been developed so far based on various machine learning models.

In [31], the authors proposed calculation of the packet score, upon which packets were discarded based on the Bayesian theoretic grade. In [32], a Bayesian inference prototype was applied in trust agreement among access routers to detect malicious routers. In [33], the authors

presented a real-time DDoS attack detection method based on a naive Bayesian classifier of legitimate and malicious network packets and a signature-based IDS for attack detection. In [34], a signature-based IDS was proposed to identify DDoS attacks on HTTP servers. The proposed system adopted a naive Bayesian classifier, which achieved a detection accuracy up to 98%. Nevertheless, the proposed approach was useful only against low-rate DDoS attacks.

Different models based on fuzzy logic function well when there is a need to analyze a large number of input parameters, such as the CPU load, traffic rate, and connection time [35]. In [36], the integration of fuzzy logic with cross-correlation was proposed to improve the detection precision. However, the proposed system failed in regard to real-time detection due to its time-consuming calculations. Real-time DDoS detection was achieved by Wang et al. via the application of fuzzy logic in Hurst factor analysis [37]. Another recent study has proposed a reliable DPI method for anomaly detection via Hurst factor calculation considering different time frames [38]. Authors have proposed threshold boundaries for the Hurst factor considering different timeframes to prevent false detection/misdetection of anomalous traffic.

In [39], the authors proposed a method for the advanced detection of DDoS attacks by using the K-nearest neighbor method of traffic classification. Their approach is suitable for the initial detection phase because it considers only traffic variation. In [40], a more comprehensive model was developed considering different types of DDoS attacks. The proposed model achieved an accuracy ranging from 40–70% depending on the attack type.

In [41], a new DDoS attack detection model based on several support vector machines (SVMs) was established. The authors analyzed the traffic attributes of attacks and achieved a high precision of early anomaly detection. Another SVM-based approach was proposed in [42] in regard to attack categorization. The authors adopted a two-step approach to initially recognize anomalous traffic and then performed a detailed classification of the attack type.

Over the last few years, deep learning methods for DDoS attack detection have gained attention due to their promising outputs in many other tasks. Deep learning models based on different types of neural networks provide better results than those yielded by basic signature testing methods [43]. In [44], the authors proposed a time delay neural network as an early DDoS detector. The proposed model employed a layered architecture to implement appropriate actions against DDoS attacks with an 82.7% accuracy.

In [45], the authors mapped attributes of the neural network to recognize DDoS attacks based on traffic monitoring with a software-defined network (SDN) controller. Another SDN-based approach was proposed in [46] via multivector deep learning-based DDoS detection. However, the major drawback of both methods is that they struggle in the detection of low-rate attacks, usually considered legitimate traffic.

A very promising research direction was reported in [30], where the authors developed a multilevel anti-DDoS framework for the IoT and cloud environment. The authors considered a typical state-of-the-art structure comprising intelligent IoT edges, fog computing and cloud computing levels. This framework was demonstrated to effectively neutralize DDoS attacks by exploiting early detection at IoT edges, local state analysis in the fog and powerful big data analytics in the cloud with deep learning tools.

2.3 Existing Challenges of AI-Based Network Anomaly Detection

The main advantage that drives the popularity of machine learning-based IDSs is their ability to quickly adapt to changes in the network environment. Modern heterogeneous information

systems contain numerous available degrees of freedom that they do not allow us to predict all potential vulnerabilities in DDoS attack deployment and manually hardcode required security mechanisms. Summarizing the abovementioned related research, we conclude that AI-based methods overcome the limits of statistical approaches, which are based only on statistical parameters. While smart attackers may easily adjust the statistical properties of DDoS traffic, thereby rendering them undistinguishable from legitimate traffic, they are still unable to determine how many other latent attributes can be learned by deep neural networks. Nevertheless, an important challenge remains involving the training time and data availability for AI-based IDSs [47].

Considering the real-time detection requirements and lack of time required for training over new possible attacks, it is important to extract the most important features of network traffic. By learning the most important features of network traffic, we can finely tune the deep learning model on normal system behavior so that potentially new attacks are easily detected by the IDS. Another advantage of optimal feature selection is that the computational complexity of detection is reduced and that the IDS is more compatible with real-time operation. To our knowledge, optimal feature extraction currently lacks attention in recent research of AI-based network anomaly detection. Therefore, further development of deep learning-based IDSs leveraging advanced feature extraction and optimization is of great interest for modern heterogeneous information systems.

3 Proposed Semisupervised Intrusion Detection System Based on a Deep Recurrent Autoencoder

3.1 System Model

Usually, deep learning-based solutions for DDoS attack detection are based on supervised learning over a large dataset of known attacks mixed with normal network traffic. These datasets consist of input parameters, which are passed to the deep neural network and output labels are targeted so that the model can learn any hidden dependencies between the input and output. During training, the neural network evaluates the input features and predicts the output values. The output values are then compared to target values, and the corresponding loss function is calculated. With each iteration of the training process (epoch), the weight between neurons is updated to reduce the loss function. This training process continues until the loss function is minimized to an acceptable threshold.

However, supervised learning alone is not feasible for modern IDSs because there are many possible attacks with different features, which renders the training process computationally expensive and time consuming. Therefore, most recent research works have applied autoencoders in IDSs and obtained promising outputs [48,49]. An autoencoder is an unsupervised learning technique that uses neural networks for the so-called task of representation learning [50]. The key function of the autoencoder is data dimensionality reduction so that hidden structures within the data can be discovered and represented as a compressed form. The important aspect of training an autoencoder for DDoS attack detection is to ensure that its learned compressed latent space representation comprises meaningful attributes of the input network traffic. The above compressed representation can be learned by limiting the number of neurons in the hidden layers so that the deep neural network is forced to reconstruct the original traffic from a much smaller number of features (Fig. 1).

3.2 Traffic Prediction Using a Long Short-Term Memory-Based Autoencoder

Since supervised anomaly detection systems are naturally limited only to known types of network attacks over which the AI model has been trained, in this paper, we focus mostly on semisupervised anomaly detection using the deep autoencoder. Recently, semisupervised IDSs have

gained attention from the industry as a promising solution to bridge the gap in supervised models. Instead of learning numerous patterns of different network attacks, semisupervised algorithms learn the features of legitimate network traffic and treat any traffic with notable differences as an anomaly. Nevertheless, the following unsolved problems of semisupervised anomaly detection based on autoencoders remain [51–53]:

- The complex training process of the autoencoder occurs due to the large number of traffic parameters and corresponding features, which vary over time.
- Frequent false detections of anomalous traffic behavior may occur when a notable variation in legitimate traffic is observed in the network.

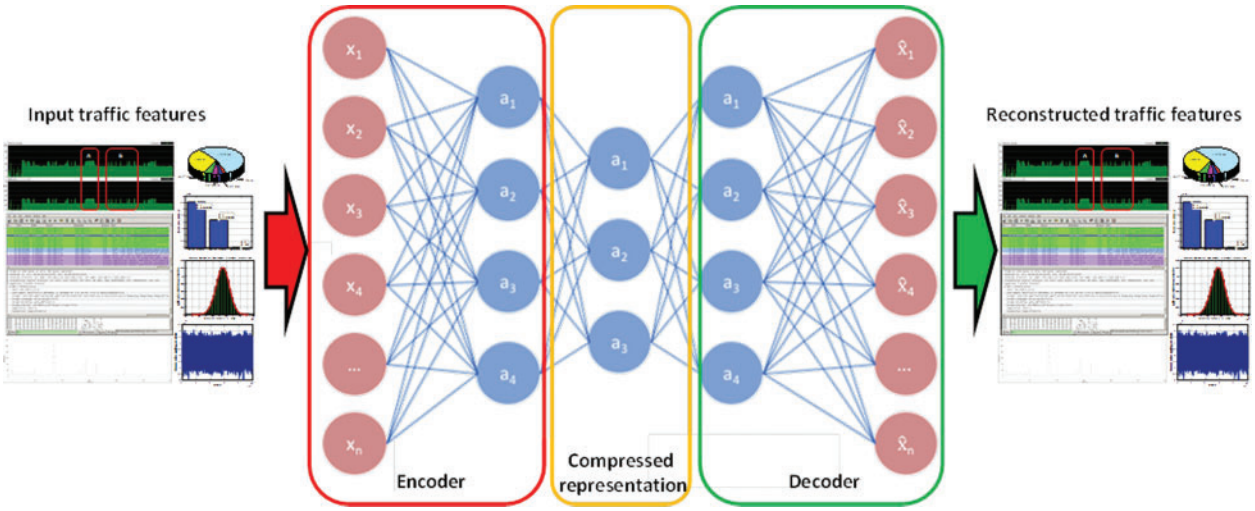

Figure 1: General architecture of autoencoder-based representation learning of traffic features

To tackle the aforementioned problems, we propose a preliminary feature selection approach to determine the most important parameters of network traffic and train the most fitted autoencoder model over normal network behavior within long and short timeframes.

We adopt an autoencoder structure based on the recurrent neural network (RNN). RNNs have been widely applied for time series prediction, analysis and classification, such as natural language processing [54], stock market prediction [55], and anomaly detection [56–58]. Therefore, RNNs are suitable for IDSs to learn the different features of network traffic and recognize attacks. In particular, we employ an advanced RNN model, namely, the long short-term memory (LSTM) model [59,60]. The LSTM model is composed of complex cells, which allows the learning of both long- and short-term dependencies. This feature is especially useful in network traffic analysis and important feature learning in different time frames. The LSTM cell contains four main blocks: input gate, forget gate, hidden state and output gate.

The data processing workflow with an LSTM cell is described as follows: initially, the LSTM cell filters out the less relevant features of network traffic and removes them from the cell state via the forget gate. The function of the forget gate can be expressed as follows:

$$f_t = \sigma(W_{xf} x_t + W_{hf} h_{t-1}), \tag{1}$$

where σ denotes the sigmoid activation function and W_{xf} and W_{hf} are the input and hidden state weight matrices, respectively. After the operation within the parentheses in Eq. (1), a value between 0 and 1 is determined for each feature in the previous cell state. This value is then passed through the sigmoid activation function, which outputs a value of 0 for less important information and a value of 1 for more important information. Thus, the LSTM cell forgets less important features of the traffic time series while retaining the most significant features, which reflect the currently learned network behavior.

After filtering out redundant information, the input gate decides what information should be memorized with the following function:

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-1}) \tag{2}$$

where σ denotes the sigmoid activation function and W_{xi} and W_{hi} are the input and hidden state weight matrices, respectively. The output of the input gate function is processed in the same way as that of the forget gate by the sigmoid activation function.

When the relevant traffic features have been determined, the cell state is updated with new values to replace those removed by the forget gate as follows:

$$c'_t = \tanh(W_{xc}x_t + W_{hc}h_{t-1}), \tag{3}$$

$$c_t = f_t \odot c_{t-1} + i_t \odot c'_t \tag{4}$$

Eqs. (3) and (4) reflect the LSTM cell state update process, which thus affects the learning process of neural networks. Thereafter, the LSTM cell calculates the output and transfers it to the next cell:

$$h_t = \sigma(W_{xo}x_t + W_{ho}h_{t-1}) \odot \tanh(c_t) \tag{5}$$

Finally, the LSTM neural network outputs the predicted traffic based on the most recently learned features.

Thus, with the LSTM-based autoencoder, we solve the uncertainty in network traffic variation over time because the IDS can now compare the predicted traffic with the LSTM to real network traffic and make a decision regarding potentially anomalous behavior. However, the most important task is to appropriately train the autoencoder and find the best generalized traffic representation, which must be robust to small fluctuations that are still distinguishable from anomalies. The uncertainty in this task is that we must attain a tradeoff between the number of features and model performance. While it may be intuitively expected that more features provide a better performance, in reality, this is not always the case. Too many features usually result in a more complex training process and high overhead of the model, while the elimination of redundant features makes the model vulnerable to specific target attacks.

3.3 Feature Extraction from Network Traffic via Principle Component Analysis

We describe the process of feature extraction in detail by using the CSE-CIC-IDS2018 dataset [61]. CSE-CIC-IDS2018 contains information on different attacks, such as brute-force, botnet, DDoS, web, and many other attacks on the cloud datacenters and other information systems [62]. The dataset is based on the logs of 80 features, which have been extracted from captured network traffic. To improve the efficiency of AI model training, we analyze the most important features, which are associated with the high variance in classification via the gradient boosting

model. As a result, we obtain the numerical output weights of features to better understand their impact on the overall classification performance. To estimate the minimal number of features required to achieve a total weight close to 1, we calculate the cumulative feature importance. According to the obtained results, the total number of required features can be reduced from 80 to 20, without a notable loss in the cumulative importance for AI-based classification.

However, considering highly heterogeneous network traffic, which is generated by the very large number of different personal, industrial and other IoT applications, there exists a high possibility that feature weights vary over time. Thus, straightforward elimination of redundant features could result in IDS vulnerability to new types of traffic anomalies in the future.

Therefore, in the proposed IDS model, we implement preliminary feature extraction from network traffic with the principal component analysis (PCA) algorithm [63]. Similar to gradient boosting, the key idea of PCA is to realize informative visualization of each input data feature to find those features more important to the correct classification between normal network traffic and network attacks. However, the key difference of PCA is that it applies an orthogonal linear transformation of the input data to obtain a new coordinate system as follows:

$$\mathbf{T} = \mathbf{XW} \tag{6}$$

where $\mathbf{W}$ is a matrix of the weights of size $K \times K$, K is the number of input traffic features, and $\mathbf{X}$ is a matrix of the input traffic features contained in the CSE-CIC-IDS2018 dataset. The columns of $\mathbf{W}$ are eigenvectors of $\mathbf{X}^T\mathbf{X}$, so that each feature in matrix $\mathbf{T}$ is related to all features in input matrix $\mathbf{X}$.

The cumulative contribution of the output features produced by PCA to the variance score of the features is shown in Fig. 2. According to the results, to maintain the total variance at 98.75%, it is enough to consider only 3 traffic features, while 5 features provide a total variance of 99.55%.

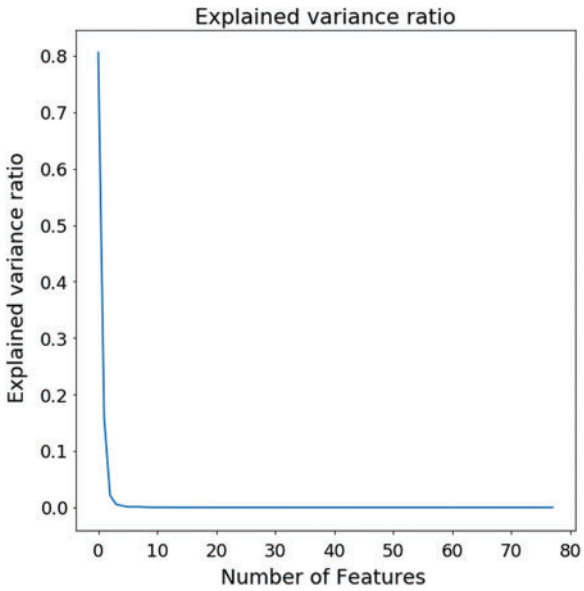

Figure 2: Cumulative variance score of the traffic features after PCA

The result of data clustering into benign and malicious traffic behaviors based on the 3 most important features of the CSE-CIC-IDS2018 dataset is shown in Fig. 4a. For a more detailed assessment of the data clustering representation, we also apply the t-distributed stochastic neighbor embedding (t-SNE) algorithm based on the 3 most important features (Fig. 3b) [64].

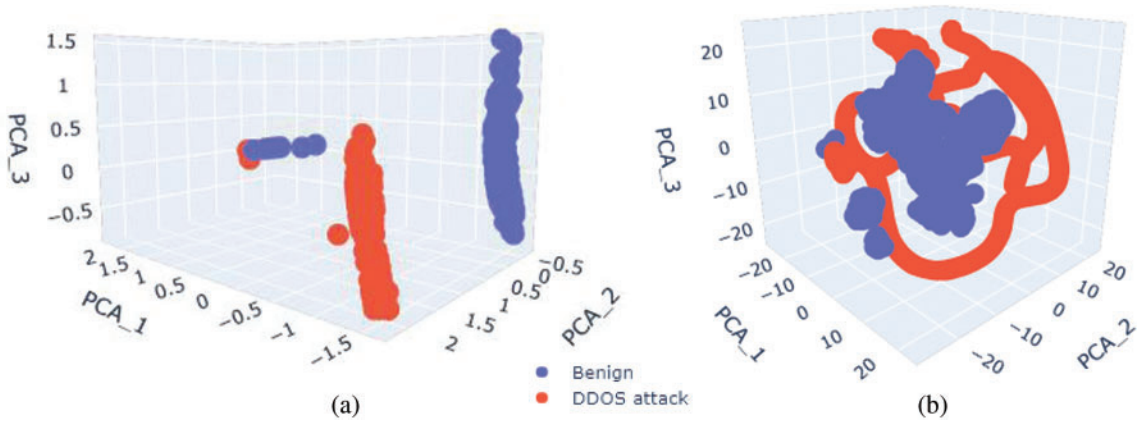

Figure 3: Distribution of the benign and malicious traffic clusters based on the 3 most important features before (a) and after (b) application of the t-SNE algorithm

As shown in Fig. 3b, the benign and malicious traffic clusters are easily distinguished by using only the 3 most important features. Therefore, we can assume that these 3 features sufficiently train a robust autoencoder for network anomaly detection. The interesting result, which is observed in Fig. 4, is that the benign class can be further classified into 3 different clusters. Hence, the obtained features allow us to train other AI-based traffic analyzers, which can be employed to classify different types of network services while applying the corresponding quality of service policies. However, these aspects are beyond the scope of the current paper.

To maximize the variance score of the training dataset, we consider the top 5 most important features, which account for 99.55% of the total variance score. Note that further increasing the number of features is inefficient because 0.45% is almost evenly distributed among 75 statistically insignificant features, while the computational complexity of training exponentially increases with each additional feature. A scatter matrix of the top 5 selected features for the training dataset is shown in Fig. 4.

4 Simulations and Performance Analysis of Anomaly Detection Based on the Deep Recurrent Autoencoder

In the previous section, we explained the key steps undertaken to prepare the dataset for training. In the current section, we describe the process of autoencoder training over the improved dataset. We train an LSTM-based autoencoder considering only the time series of benign traffic, which narrows our problem to regression instead of binary classification. Therefore, we choose a mean square error (MSE) loss function to minimize it during training [65]. The MSE calculates the squared differences between the true and predicted values as follows:

$$L(x, x') = \frac{1}{N}\sum_{i=0}^{N}(x_i - x'_i)^2 \tag{7}$$

where x is the real value and x' is the value predicted by the neural network.

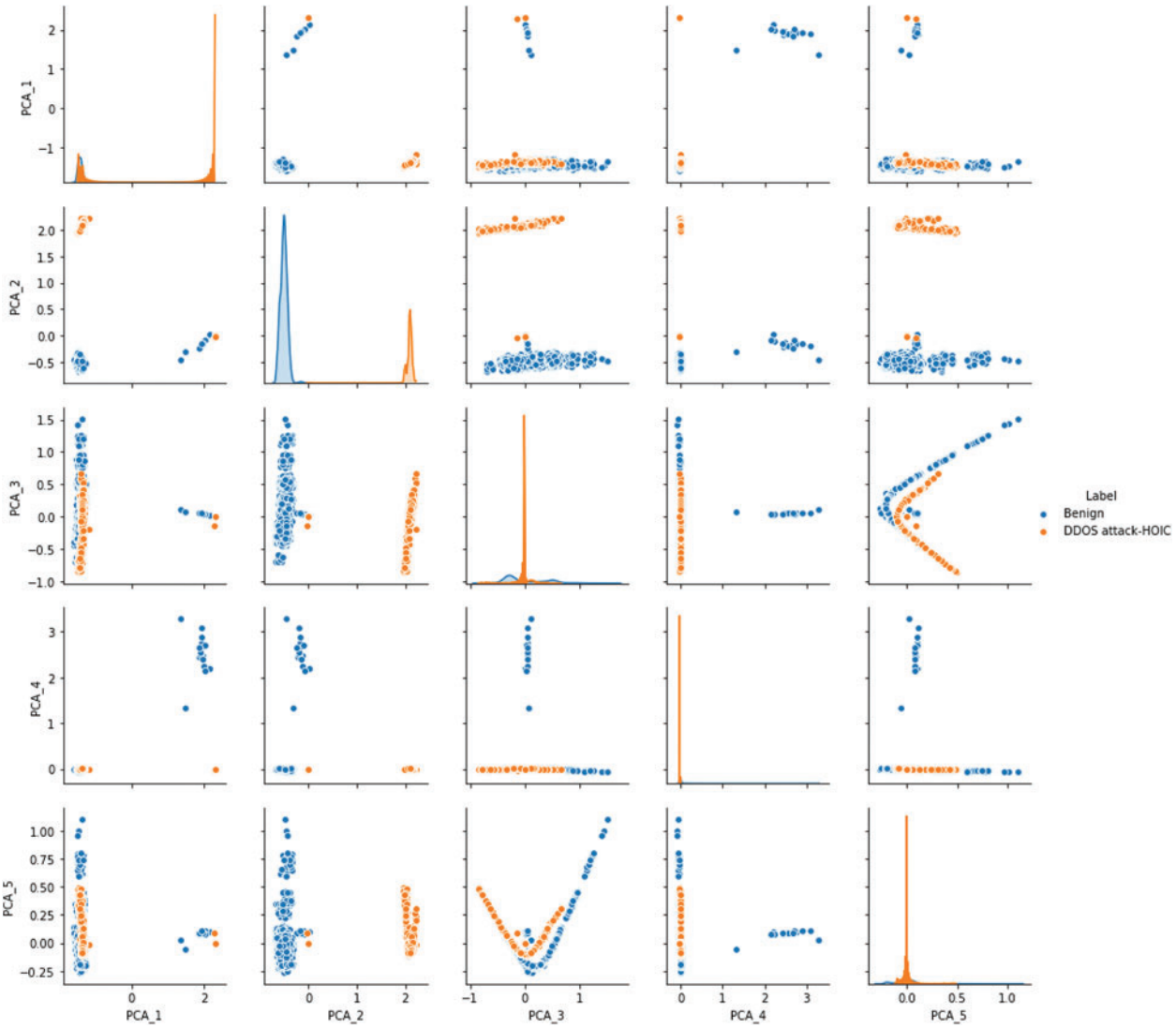

Figure 4: Scatter matrix of the top 5 selected features for the training dataset

The training objective is to minimize the MSE by iteratively updating the weights between the neurons (i.e., the LSTM cells). The training process is conducted by using an optimizer algorithm that updates the weights of the neural network until the MSE is minimized. In our system, we implement an Adam optimizer, which adjusts the learning rate based on the mean and uncentered variance moments of the gradient [66]. More specifically, the Adam optimizer calculates exponential moving average values of the gradient and the squared gradient and controls their decay rates by adjusting parameters β_1 and β_2.

During training, we selected 216800 samples of normal traffic behavior, while during testing, we considered 90033 samples of normal traffic behavior and 360833 samples of anomalous traffic behavior. An additional part, which contains 54001 samples, was adopted for validation to learn the model and avoid overfitting (see Tab. 1).

Table 1: Description of the training parameter distribution

Data type	Normal traffic behavior	Anomalous records
Training dataset	216800	-
Validation dataset	54001	-
Test dataset	90033	360833

The training process was conducted over 50 epochs. The batch size was set to 100, i.e., the weights of the neural network were updated once per 100 data samples. The result of autoencoder training over the training dataset is shown in Fig. 5. The level of the decision-making error is determined by the last error value for the validation dataset, which equals 0.005. Simulation results of the anomaly detection error for the testing dataset are shown in Fig. 6.

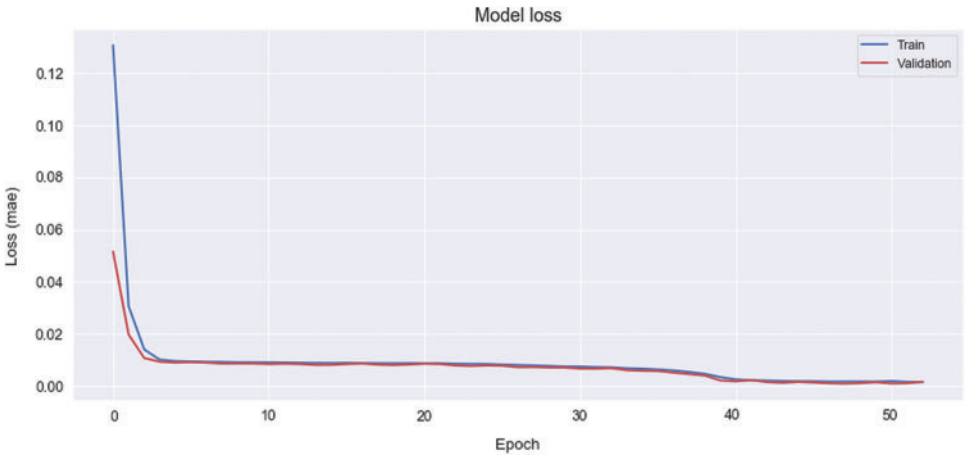

Figure 5: Result of autoencoder training over the dataset with the optimized features

Numerical results of the anomaly detection accuracy of the trained IDS are listed in Tab. 2. According to the results, the decision accuracy to recognize a DDoS attack is 100%. However, confusion remains when recognizing normal traffic.

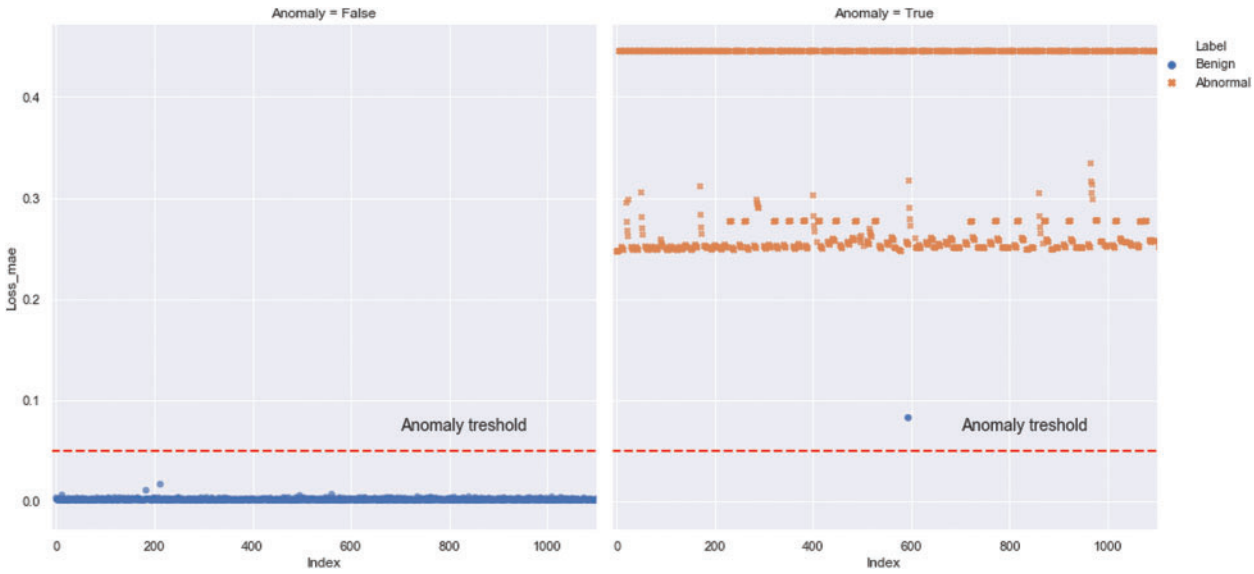

Figure 6: Simulation results of the anomaly detection error for the testing dataset

Table 2: Simulation results of the anomaly detection performance

Traffic behavior type	Normal traffic detected	Anomalous traffic detected
Normal traffic records	90012 (99.97%)	21 (0.023%)
Anomalous traffic records	0 (0%)	360833 (100%)

According to the results in Tab. 2, the accuracy of normal traffic recognition is 99.97%, i.e., 21 out of 90012 normal samples are recognized as an anomaly. To assess the efficiency of dataset decomposition with the PCA algorithm, we provide an additional training cycle of the deep neural network with all 80 available features. The dataset is split into training, validation and test parts at the same proportions as those defined in Tab. 1. Corresponding training results of the deep recurrent autoencoder without feature optimization are shown in Figs. 7 and 8.

According to the results shown in Fig. 8, we observe that the absolute accuracy of the autoencoder trained on the dataset with all 80 features is only 0.03% higher than that of the autoencoder trained on the dataset with the optimized features (Tab. 3). However, it is important to understand that this performance level is idealistic due to the limited dataset, and we should not expect a 100% accuracy in real-world deployment. However, the key advantage of the proposed approach of feature optimization is the much faster convergence and notably shorter training time. This result verifies that the proposed IDS solution achieves a better performance in real-world traffic testing. Therefore, in our further research, we will provide much deeper insights and experimental verification of the proposed solution under various scenarios of network deployment, such as fixed enterprise networks, 5G mobile networks, and massive IoT deployments. A generalized flow diagram of network anomaly detection with the proposed IDS based on feature optimization and a deep recurrent autoencoder is shown in Fig. 9.

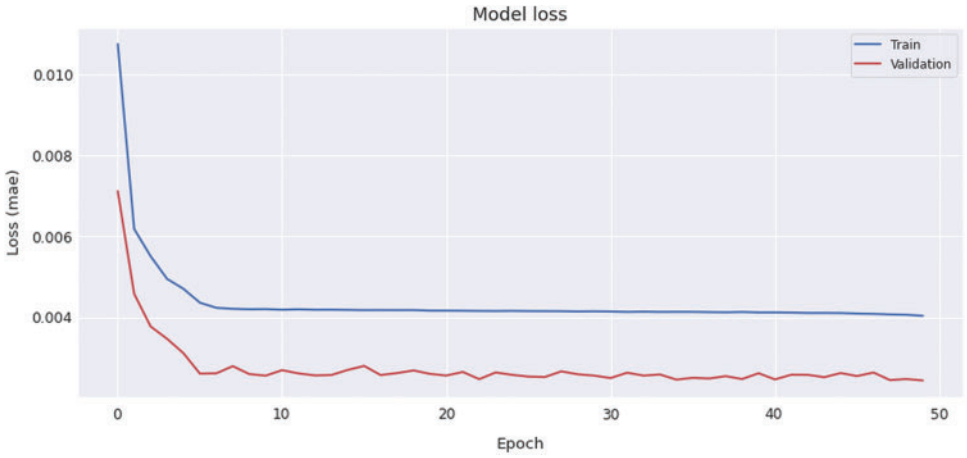

Figure 7: Result of autoencoder training over the dataset with all features

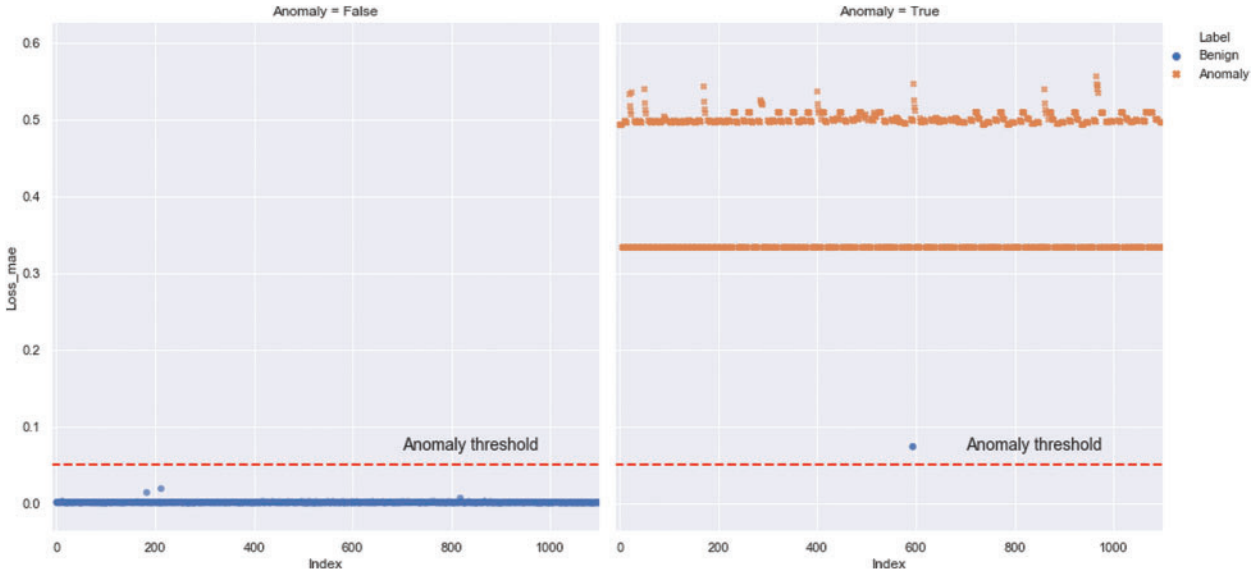

Figure 8: Simulation results of the anomaly detection error for the testing dataset

Table 3: Simulation results of the anomaly detection performance

Traffic behavior type	Normal traffic detected	Anomalous traffic detected
Normal traffic records	90033 (100%)	0 (0%)
Anomalous traffic records	0 (0%)	360833 (100%)

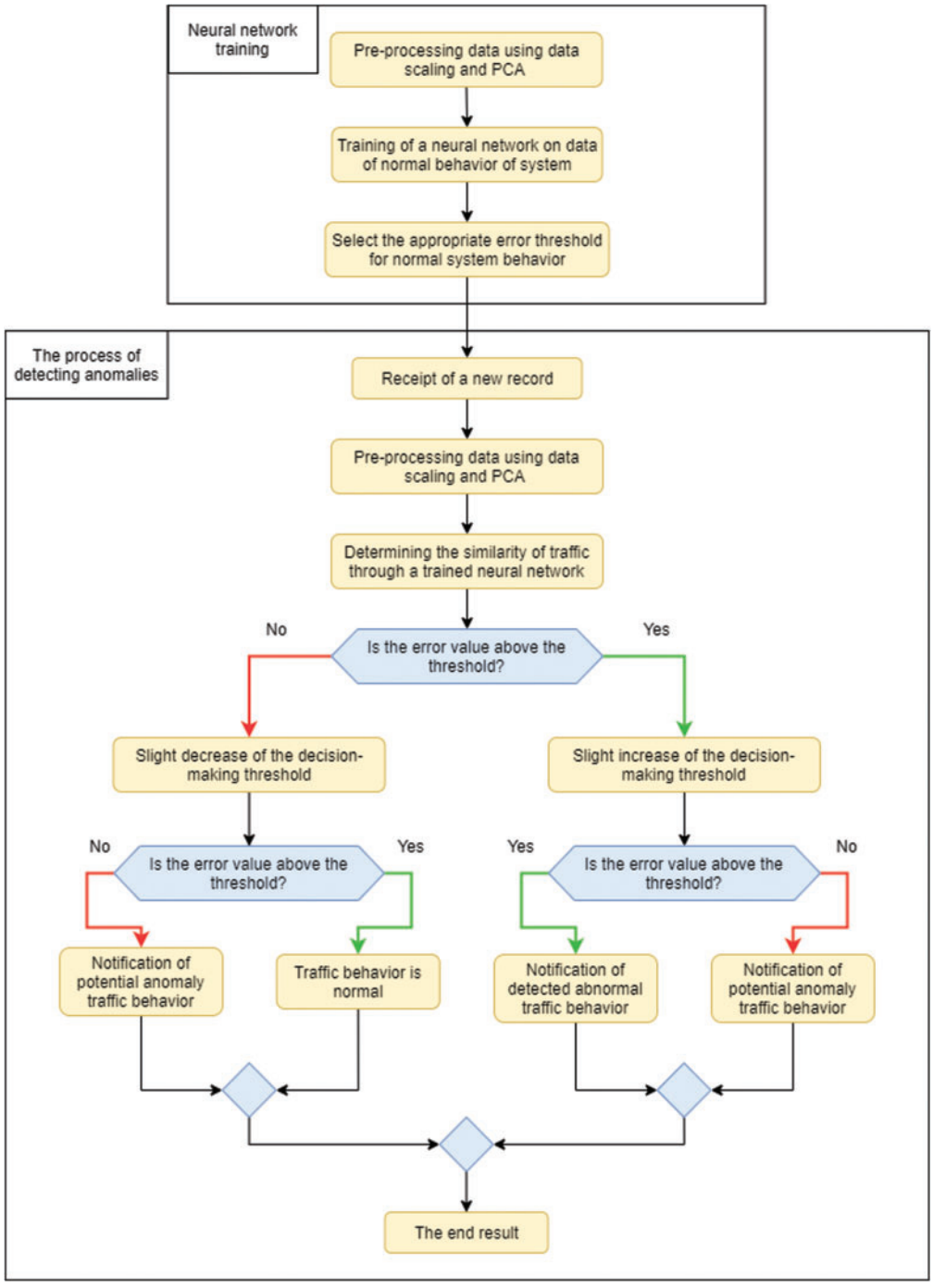

Figure 9: Flow diagram of the network anomaly detection procedure with the proposed IDS based on feature optimization and a deep recurrent autoencoder

5 Conclusions

In this paper, we have proposed a novel semi-supervised learning-based IDS system to detect traffic anomalies caused by DDoS attacks. The main novelty of the proposed system is in the preliminary feature extraction from the original network traffic to reduce the number of input features for the training dataset by 94%. Then, the optimized dataset is used to train the deep LSTM based autoencoder. Training has been conducted in the semi-supervised manner, i.e., only normal traffic behavior has been used for training. Then the trained autoencoder is used to detect any traffic, which is not recognized as the learned normal behavior as an anomaly. By combination of the dataset features optimization and LSTM regression capabilities to learn time series relations, we have reduced the training time by 10 times, while losing only 0.03% of accuracy. This advantage of the proposed IDS provides a wide range of possible use cases in the real world network deployment with highly dynamic environment, such as modern 5G networks with massive number of IoT devices.

Acknowledgement: The authors are thankful to the administration of the Lviv Polytechnic National University and the Technical University of Kosice for providing the necessary equipment to conduct this research.

Funding Statement: This work was supported by the Slovak Research and Development Agency, project number APVV-18-0214, by the Scientific Grant Agency of the Ministry of Education, science, research and sport of the Slovak Republic under the contract: 1/0268/19, and by the Ukrainian government projects No. 0120U102201 "Development the methods and unified software-hardware means for the deployment of the energy efficient intent-based multi-purpose information and communication networks," and No. 0120U100674, "Designing the novel decentralized mobile network based on blockchain architecture and artificial intelligence for 5G/6G development in Ukraine."

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. A. Ashraf, H. Jamal, S. A. Khan, Z. Ahmed and M. I. Baig, "A heterogeneous service-oriented deep packet inspection and analysis framework for traffic-aware network management and security systems," *IEEE Access*, vol. 4, pp. 5918–5936, 2016.

[2] C. Xu, S. Chen, J. Su, S. M. Yiu and L. C. K. Hui, "A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 4, pp. 2991–3029, 2016.

[3] Y. E. Yang and V. K. Prasanna, "Robust and scalable string pattern matching for deep packet inspection on multicore processors," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 11, pp. 2283–2292, 2013.

[4] J. Yu, B. Yang, R. Sun and Z. Chen, "FPGA-Based parallel pattern matching algorithm for network intrusion detection system," in *Proc. of Int. Conf. on Multimedia Information Networking and Security*, Wuhan, China, pp. 458–461, 2009.

[5] Y.-M. Hsiao, M.-J. Chen, Y.-S. Chu and C.-H. Huang, "High-throughput intrusion detection system with parallel pattern matching," *IEICE Electronics Express*, vol. 9, no. 18, pp. 1467–1472, 2012.

[6] T. Maksymyuk, M. Brych, M. Klymash and M. Jo, "Cooperative channels allocation in unlicensed spectrum for D2D assisted 5G cellular network," in *Proc. of 2nd Int. Conf. on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, pp. 197–200, 2017.

[7] M. Jaber, M. A. Imran, R. Tafazolli and A. Tukmanov, "5G backhaul challenges and emerging research directions: A survey," *IEEE Access*, vol. 4, pp. 1743–1766, 2016.

[8] T. Maksymyuk, J. Gazda, O. Yaremko and D. Nevinskiy, "Deep learning based massive MIMO beamforming for 5G mobile network," in *Proc. of IEEE 4th Int. Sym. on Wireless Systems Within the Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*, Lviv, pp. 241–244, 2018.

[9] L. Fernández Maimó, Á. L. Perales Gómez, F. J. García Clemente, M. Gil Pérez and G. Martínez Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5G networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018.

[10] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[11] V. Andrushchak, T. Maksymyuk, S. Dumych, M. Kaidan and O. Urikova, "Intelligent data flows management for performance improvement of optical label switched network," in *Proc. of IEEE 14th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Slavske, Ukraine, pp. 1143–1146, 2018.

[12] S. Haider, A. Akhunzada, I. Mustafa, T. Bharat Patel, A. Fernandez *et al.*, "A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53972–53983, 2020.

[13] M. A. Ferrag, L. Maglaras, S. Moschoyiannis and H. Janickeb, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, Article 102419, 2020.

[14] N. Hoque, D. K. Bhattacharyya and J. K. Kalita, "Botnet in DDoS attacks: Trends and challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.

[15] Q. Yan, F. R. Yu, Q. Gong and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[16] H. D. Trinh, E. Zeydan, L. Giupponi and P. Dini, "Detecting mobile traffic anomalies through physical control channel fingerprinting: A deep semi-supervised approach," *IEEE Access*, vol. 7, pp. 152187–152201, 2019.

[17] M. Roopak, G. Yun Tian and J. Chambers, "Deep learning models for cyber security in IoT networks," in *Proc. of IEEE 9th Annual Computing and Communication Workshop and Conf. (CCWC)*, Las Vegas, NV, USA, pp. 452–457, 2019.

[18] R. Vishwakarma and A. K. Jain, "A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks," in *Proc. of 3rd Int. Conf. on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, pp. 1019–1024, 2019.

[19] M. Roopak, G. Y. Tian and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," *IET Networks*, vol. 9, no. 3, pp. 120–127, 2020.

[20] I. Dutt, S. Borah and I. K. Maitra, "Immune system based intrusion detection system (IS-iDS): A proposed model," *IEEE Access*, vol. 8, pp. 34929–34941, 2020.

[21] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain and A. Nawaz, "HML-Ids: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89507–89521, 2019.

[22] J. Zhang, M. Zulkernine and A. Haque, "Random-forests-based network intrusion detection systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 649–659, 2008.

[23] S. Han, M. Xie, H. Chen and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1052–1062, 2014.

[24] C. Zhou, S. Huang, N. Xiong, S.-H. Yang, H. Li *et al.*, "Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 10, pp. 1345–1360, 2015.

[25] P. Casas, J. Mazel and P. Owezarski, "Coping with 0-day attacks through unsupervised network intrusion detection," in *Proc. of Int. Wireless Communications and Mobile Computing Conf. (IWCMC)*, Nicosia, pp. 24–29, 2014.

[26] W. Lu and I. Traore, "An unsupervised approach for detecting DDOS attacks based on traffic-based metrics," in *Proc. of IEEE Pacific Rim Conf. on Communications, Computers and Signal Processing*, Victoria, BC, Canada, pp. 462–465, 2005.

[27] P. V. Amoli and T. Hämäläinen, "A real time unsupervised NIDS for detecting unknown and encrypted network attacks in high speed network," in *Proc. of IEEE Int. Workshop on Measurements & Networking (M&N)*, Naples, pp. 149–154, 2013.

[28] Y. Gu, K. Li, Z. Guo and Y. Wang, "Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm," *IEEE Access*, vol. 7, pp. 64351–64365, 2019.

[29] G. Kaur, "A novel distributed machine learning framework for semi-supervised detection of botnet attacks," in *Proc. of Eleventh Int. Conf. on Contemporary Computing (IC3)*, Noida, pp. 1–7, 2018.

[30] Q. Yan, W. Huang, X. Luo, Q. Gong and F. R. Yu, "A multi-level DDoS mitigation framework for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 30–36, 2018.

[31] Y. Kim, W. C. Lau, M. C. Chuah and H. J. Chao, "Packetscore: A statistics-based packet filtering scheme against distributed denial-of-service attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 2, pp. 141–155, 2006.

[32] J. M. Gonzalez, M. Anwar and J. B. Joshi, "A trust-based approach against IP-spoofing attacks," in *Proc. of 9th Annual Int. Conf. on Privacy, Security and Trust*, Montreal, Quebec, Canada, pp. 63–70, 2011.

[33] R. Vijayasarathy, S. V. Raghavan and R. B. Ravindran, "A system approach to network modeling for DDoS detection using a naïve Bayesian classifier," in *Proc. on 3rd Int. Communication Systems and Networks and Workshops (COMSNETS)*, Bangalore, India, pp. 1–10, 2011.

[34] V. Katkar, A. Zinjade, S. Dalvi, T. Bafna and R. Mahajan, "Detection of DoS/DDoS attack against HTTP servers using naive Bayesian," in *Proc. on Int. Conf. on Computing Communication Control and Automation*, Pune, India, pp. 280–285, 2015.

[35] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," in *Proc. 19th Conf. of the North American Fuzzy Information Processing Society (NAFIPS)*, Atlanta, GA, USA, pp. 301–306, 2000.

[36] W. Wei, Y. Dong, D. Lu and G. Jin, "Combining cross-correlation and fuzzy classification to detect distributed denial-of-service attacks," in *Proc. of Int. Conf. on Computational Science*, Reading, UK, pp. 57–64, 2006.

[37] J. Wang and G. Yang, "An intelligent method for real-time detection of DDoS attack based on fuzzy logic," *Journal of Electronics*, vol. 25, no. 4, pp. 511–518, 2008.

[38] W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan *et al.*, "A software deep packet inspection system for network traffic analysis and anomaly detection," *Sensors*, vol. 20, no. 6, Article 1637, 2020.

[39] H. V. Nguyen and Y. Choi, "Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDoS framework," *International Journal of Electrical, Computer, and Systems Engineering*, vol. 4, no. 4, pp. 247–252, 2010.

[40] M. Barrionuevo, M. Lopresti, N. Miranda and F. Piccoli, "An anomaly detection model in a LAN using k-nN and high performance computing techniques," in *Computer Science-CACIC*, Cham, Switzerland, Springer, pp. 219–228, 2017.

[41] J. Seo, C. Lee, T. Shon, K. H. Cho and J. Moon, "A new DDoS detection model using multiple SVMs and TRA," in *Proc. of Int. Conf. on Embedded and Ubiquitous Computing*, Nagasaki, Japan, pp. 976–985, 2005.

[42] J. Yu, H. Lee, M. S. Kim and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Computer Communications*, vol. 31, no. 17, pp. 4212–4219, 2008.

[43] M. Gyanchandani, J. L. Rana and R. N. Yadav, "Taxonomy of anomaly based intrusion detection system: A review," *International Journal of Science and Research*, vol. 2, no. 12, pp. 1–13, 2012.

[44] C. L. Tsai, A. Y. Chang and M. S. Huang, "Early warning system for DDoS attacking based on multilayer deployment of time delay neural network," in *Proc. of 65th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*, Darmstadt, Germany, pp. 704–707, 2010.
[45] R. Braga, E. Mota and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. of IEEE Local Computer Network Conf.*, Denver, CO, USA, pp. 408–415, 2010.
[46] A. Javaid, Q. Niyaz, W. Sun and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. of 9th EAI Int. Conf. on Bio-Inspired Information and Communications Technologies*, New York, NY, US, pp. 21–26, 2016.
[47] B. A. Khalaf, S. A. Mostafa, A. Mustapha, M. A. Mohammed and W. M. Abduallah, "Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods," *IEEE Access*, vol. 7, pp. 51691–51713, 2019.
[48] M. Al-Qatf, Y. Lasheng, M. Al-Habib and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018.
[49] S. J. Lee, P. D. Yoo, A. Taufiq Asyhari, Y. Jhi, L. Chermak *et al.*, "IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction," *IEEE Access*, vol. 8, pp. 65520–65529, 2020.
[50] D. P. Kingma and M. Welling, "An introduction to variational autoencoders," *Foundations and Trends in Machine Learning*, vol. 12, no. 4, pp. 307–392, 2019.
[51] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," in *Proc. of 20th Int. Conf. on Advanced Communication Technology (ICACT)*, Chuncheon-si Gangwon-do, S. Korea, pp. 178–183, 2018.
[52] Y. Dong, R. Wang and J. He, "Real-time network intrusion detection system based on deep learning," in *Proc. of IEEE 10th Int. Conf. on Software Engineering and Service Science (ICSESS)*, Beijing, China, pp. 1–4, 2019.
[53] Y. N. Nguimbous, R. Ksantini and A. Bouhoula, "Anomaly-based intrusion detection using auto-encoder," in *Proc. of 2019 Int. Conf. on Software, Telecommunications and Computer Networks (SoftCOM)*, Split, Croatia, pp. 1–5, 2019.
[54] B. Zhang, D. Xiong, J. Su and H. Duan, "A context-aware recurrent encoder for neural machine translation," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 25, no. 12, pp. 2424–2432, 2017.
[55] R. Achkar, F. Elias-Sleiman, H. Ezzidine and N. Haidar, "Comparison of BPA-mLP and LSTM-rNN for stocks prediction," in *Proc. of 6th Int. Symp. on Computational and Business Intelligence (ISCBI)*, Basel, Switzerland, pp. 48–51, 2018.
[56] S. H. Park, H. J. Park and Y. Choi, "RNN-Based prediction for network intrusion detection," in *Proc. of Int. Conf. on Artificial Intelligence in Information and Communication (ICAIIC)*, Fukuoka, Japan, pp. 572–574, 2020.
[57] L. Bouzar-Benlabiod, L. Méziani, S. H. Rubin, K. Belaidi and N. E. Haddar, "Variational encoder-decoder recurrent neural network (VED-rNN) for anomaly prediction in a host environment," in *Proc. of IEEE 20th Int. Conf. on Information Reuse and Integration for Data Science (IRI)*, Los Angeles, CA, USA, pp. 75–82, 2019.
[58] W. Luo, W. Liu and S. Gao, "A revisit of sparse coding based anomaly detection in stacked RNN framework," in *Proc. of IEEE Int. Conf. on Computer Vision (ICCV)*, Venice, pp. 341–349, 2017.
[59] Y. Li and Y. Lu, "LSTM-Ba: DDoS detection approach combining LSTM and Bayes," in *Proc. of Seventh Int. Conf. on Advanced Cloud and Big Data (CBD)*, Suzhou, China, pp. 180–185, 2019.
[60] T. Maksymyuk, L. Han, S. Larionov, B. Shubyn, A. Luntovskyy *et al.*, "Intelligent spectrum management in 5G mobile networks based on recurrent neural networks," in *Proc. of IEEE 15th Int. Conf. on the Experience of Designing and Application of CAD Systems (CADSM)*, Polyana, Ukraine, pp. 1–4, 2019.
[61] I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. of 4th Int. Conf. on Information Systems Security and Privacy (ICISSP)*, Portugal, pp. 108–116, 2018.

[62] B. Fekade, T. Maksymyuk and M. Jo, "Clustering hypervisors to minimize failures in mobile cloud computing," *Wireless Communications and Mobile Computing*, vol. 16, no. 18, pp. 3455–3465, 2016.

[63] A. Seghouane, N. Shokouhi and I. Koch, "Sparse principal component analysis with preserved sparsity pattern," *IEEE Transactions on Image Processing*, vol. 28, no. 7, pp. 3274–3285, 2019.

[64] N. Rogovschi, J. Kitazono, N. Grozavu, T. Omori and S. Ozawa, "T-Distributed stochastic neighbor embedding spectral clustering," in *Proc. of Int. Joint Conf. on Neural Networks (IJCNN)*, Anchorage, AK, 2017, pp. 1628–1632, 2017.

[65] Y. Sai, R. Jinxia and L. Zhongxia, "Learning of neural networks based on weighted mean squares error function," in *Proc. of Second Int. Symp. on Computational Intelligence and Design*, Changsha, pp. 241–244, 2009.

[66] Z. Zhang, "Improved adam optimizer for deep neural networks," in *Proc. of IEEE/ACM 26th Int. Symp. on Quality of Service (IWQoS)*, Banff, AB, Canada, pp. 1–2, 2018.