International Journal of Engineering & Technology, 7 (4) (2018) 5869-5873

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.18076
Research paper

Adopting genetic algorithm to develop a neural network for recognition of network intrusion

Shashank K [1] *, Mamatha Balachandra [1]

[1] *Department of Computer Science and Engineering, MIT, Manipal Academy of Higher Education, Manipal Karnataka, India-576104*
**Corresponding author E-mail: mamtha.bc@manipal.edu*

Abstract

Protecting the network from unapproved access and exposure is called network security. Machine learning has been significantly useful in detecting the attack patterns. Deep learning being one among them is the standard tool for feature extraction and transformation. Building a deep learning model becomes tedious due to the substantial computation involved. Ultimately it can be optimized by suitably selecting the hyper parameters to evolve a neural network that gives the best results. The genetic algorithm is one such algorithm that can be employed to optimize the training phase of a deep learning model by selection of the best parameters. In the paper, a genetic algorithm based deep learning model is proposed to build a network intrusion detection system. NSL KDD dataset with 41 feature attributes is used to train and test the model.

Keywords: *Deep Learning; Neural Network; Genetic Algorithm; Network Intrusion; Network Security.*

1. Introduction

Network Communication is of primary criticalness among the innovative headways in the cutting-edge time. An extensive variety of utilizations exploit the network communication. However, it is inclined to a vast number of attacks in the current circumstances. The absence of a practical framework in the network to deal with such attacks is one reason for the hindered and open communication. Tremendous information is produced each day, and the transmission of secret data using the network has ascended by a high order of magnitude. The security of classified information is critical for the associations that exclusively rely upon network communications for their working.

The enormous growth in the number of cyber-attacks has paved the way for the development of Intrusion Detection Systems (IDS) that can efficiently and significantly defend networks from anticipated and unanticipated attacks [1]. Common attacks observed today include phishing, malware, DDoS attacks, SQL injection, brute force attacks, etc. Such attacks might leak sensitive data of the organizations that depend on network communications resulting in a substantial financial loss.

An IDS will be installed on a network to monitor the incoming traffic. It also records, current attack patterns and detects new attacks. IDS can be network-based and host-based. In a network-based system, the IDS is placed in the network such that it gets a complete picture of the network. In a host-based system, the IDS is placed in each host to monitor the traffic corresponding to each host. But with a host-based IDS, it is difficult to analyze the intrusions on multiple computers. IDS can also be knowledge-based and anomaly based. A knowledge-based IDS keeps a record of the previous attack patterns and based on this predicts the attacks. An anomaly-based IDS learns the normal traffic patterns and identifies any unusual activity as an attack[2].

Deep learning is a significant tool for computations on large data. Scalability is one of the main reasons for the usage of deep neural networks for any computationally tedious job[1][2[,3]. Artificial Intelligence has been remarkable in tasks, for example, speech, text and image recognition, language translation and so forth. Improvement of the deep learning techniques has given a monster jump to the longstanding AI tasks. Deep Neural Networks(DNN) [2] is an approach obtained from deep learning for neural networks, which has advanced to be a capable machine learning model. DNN show significant qualification from regular grouping approaches. They can take in more intricate models than shallow ones. Their expressivity and hearty training algorithms consider learning efficient object representations without the need to hand design features.

Genetic Algorithms are based on the Charles Darwin's principle, "Survival of the Fittest." [4] [5] the competition for insufficient resources among individuals in nature always results in the fittest individuals dominating over the weaker ones. Based on the evolutionary concepts of natural selection and genetics, the adaptive heuristic search algorithm- Genetic algorithm was developed. It is extensively used in optimization problems. They are designed to simulate the processes necessary for evolution. To direct the search into a region of better performance, genetic algorithms make use of historical information.

Various methods have been proposed in the past to develop a network intrusion detection system. Deep neural network is an important tool to develop network intrusion detection system. The efficiency and versatility of the neural network primarily relies on the hyper parameters used in developing them. This paper proposes a novel approach, to develop intrusion detection system by making use of genetic algorithm- a feature extraction algorithm to evolve the best neural network.

2. Related work

Over the last decade, a lot of attention has been channeled towards the intrusion detection using machine learning techniques. Various approaches have been used to monitor the Network traffic and to find the abnormal activities in the network. These approaches are well documented in the existing literature. Researches have used unique methodology to focus on different segments of intrusion detection process. Some have contributed to the analysis of different machine learning techniques whereas some have worked on the intrusion detection through network appliance with NIC(Network Interface Card), knowledge-based or signature based, statistical anomaly based etc. The applications of deep learning model have proved to be useful in detection as well as prediction of attacks.

Deep neural networks are extensively used for classification problems due to its efficiency with large datasets. Jin Kim et al. [1] proposed a deep learning based method for network intrusion detection using the KDD Cup 99 dataset. Building a DNN model that consisted of four hidden layers and 100 hidden units, they classified the normal and attack patterns in the dataset. The Rectified Linear Unit(ReLU) was used as the activation function, with adaptive moment(Adam) optimizer for back-propagation. Sasanka Potluri and Christian Diedrich[2] proposes an accelerated deep neural network for enhanced intrusion detection system wherein the deep neural network methodology is implemented through CPU and GPU, and the comparison is made on the computation time required to develop the learning model.

Sharmila Kishore Wagh, Vinod K Pachghare and Satish R Kolhe[3] surveyed on Intrusion Detection System using Machine Learning Techniques. The paper presents the different machine learning techniques adopted in the intrusion detection system. Bayesian network, Markov models, neural networks, genetic algorithms, fuzzy logic techniques, clustering and outlier detection, and data mining, are the different approaches used in machine learning for the detection of intrusion in the networks.

Nathan Shone et al. [4] presented a novel approach to building a deep learning classification model using stacked nonsymmetric deep autoencoder(NDAE). NDAE is an unsupervised learning approach to extract features, learning the best parameters needed to rebuild the output closer to input. The target values were set closer to input values using the back-propagation algorithm.

Rowayda A. Sadek, M. Sami Soliman and Hagar S. Elsayed[5] present an active anomaly intrusion detection system based on a neural network. It consisted of an indicator variable and rough set reduction. Rough Set Theory, which is applied to select out feature reducts. Indicator Variable is used to represent dataset productively. A hybrid algorithm is used to reduce computation time.

S.K. Sahu et al. [6] makes a detailed analysis on datasets used for network intrusion detection. KDDCup 99, GureKDDCup, NSLKDD are the different datasets discussed in the paper. The paper talks about the advantages and disadvantages of the datasets and also the preprocessing of the datasets.

Giorgis Vasiliadis et al. [7] proposes a method named 'GNORT' which makes use of enormous computational power of graphics processors. The implementation was done on Nvidia GPU programmed on CUDA.

Zhenghong Xiao et al. [8] proposed a Bayesian network based network intrusion detection system for wireless sensor networks. The implementation was made employing the NS2 tool. The results were much better than the methods that existed.

Wenjie Tian et al. [9] proposed a network intrusion detection system based on neural network and particle swarm optimization. KDDCup99 dataset was used for implementation and the results were quite effective.

Yichi Zhang et al. [10] presents a distributed network intrusion detection system for smart grids by developing and deploying an intelligent module that analyzes traffic in multiple layers of grid.

M Stampar et al. [11] made a review on different approaches that can be used for network intrusion detection systems based on artificial intelligence.

A review on semi-supervised method for network intrusion detection is made by Sofy Fitriani et al. [12]. Graph based, semi supervised clustering based method, constraint based, distant based, constraint and distance based methods are described in the paper.

Hatungimana Girvais et al. [13] used quality threshold distance for detecting intrusions in the network. The paper proposes a quality clusters based method for network intrusion detection. Also, it proposes a attribute selection method.

Deepika Venchurkar et al. [14] describes various methods of intrusion detection using machine learning. The paper talks about challenges in developing intrusion detection systems.

An extreme learning machine was developed by Yadigar Imamverdiyev et al. [15] for anomaly detection. A neural network was developed with non linear piecewise function as the activation function.

Anna L. Buzack et al. [16] surveyed different data mining and machine learning methods for cyber security intrusion detection. The paper talks about the challenges with different methods and also suggests the method which can be employed at different contexts.

A machine learning classification model for network base intrusion detection system was proposed by Sanjay Kumar et al. [17]. Different Machine learning classifiers were used to build the intrusion detection system to find the suitable.

Zhao Jian-hua et al. [18] proposed an intrusion detection system based on back propagation neural network and genetic algorithm. Genetic algorithm was used to optimize the classification rate of the BP network.

Genetic algorithms and Particle Swarm Optimization algorithms are used techniques used for optimization. Andrey Ferriyan et al. [19] presented feature selection optimization using genetic algorithms. Using one-point crossover for genetic algorithm parameters, they evaluated the NSL KDD dataset. The authors used Correlation-based Feature selection for the fitness value. They also modified the dataset considering only those attacks which are prevalent today. Various machine learning algorithms were used, and random forest classifier with genetic algorithm for feature selection gave the best results. Yann Carbonne et. Al [20] used the genetic algorithm as a supervised learning algorithm to train a computer to determine how much two profiles are similar. In the paper, the authors elucidated the steps involved in genetic algorithms such as genetic representation, population initialization, fitness function, crossover, mutation, and reproduction.

Yu Wang et al. [21] used a Genetic algorithm for feature selection in the fast feature fusion algorithm in image classification for cyber-physical systems.

Chih-Han Chen et al. [22] proposed a personalized expert recommendation system for optimized nutrition. Data categorization was done using a deep neural network model. The recommendation was optimized by using genetic algorithm. A self-improving convolution neural network to classify hyperspectral data was developed by Pedram Ghamisi et al. [23] using fractional order Darwinian Particle Swarm Optimization. Chen Huang et al. [24] also employed particle swarm optimization technique for part localization of fine-grained object recognition.

An optimized generation of test sequences for an interface between the high-speed train and ATP onboard equipment was proposed by Kaicheng Li et al. [25]. Genetic algorithm and deep learning made the generation more significant.

3. Methodology

Different hyper-parameters are involved in building a deep neural network. Hyperparameters determine the structure of and the training process of the neural network. Different combination of these variables can give results with varying accuracy. One way of finding the best parameters for the best deep neural network could be brute force trial and error, where each combination of the parameters are chosen, and a deep neural network is built. This ap-

proach is cumbersome due to the amount of computation involved in developing a neural network for each possible combination.
Four hyperparameters are considered in this paper,

a) Number of hidden layers: The number of layers between input and output layer. Neural Networks with 1 to 4 hidden layers are considered.
b) Number of neurons per layer: The number of neurons per hidden layer can be 64, 128, 256, 512, 768, 1024.
c) Activation function: Given an input or set of inputs the activation function defines the output of a node, which is later ugiven as input to the next layer. The activation functions can be ReLU- Rectified Linear Unit, Elu- exponential linear unit, tanh and sigmoid [1], [2].
d) Optimizer: Optimizer algorithms are used to minimize (or maximize) an error function. RMSprop, Adam, Stochastic gradient descent, Gradient descent, Adaptive gradient, adadelta, AdaMax, nadam.

These hyperparameters are chosen for the experiment and the combinations of them are chosen varyingly, to obtain different neural networks, evolving a deep neural network that gives the best accuracy rate.
The Genetic algorithm involves the following phases [18], [19]:

i) Initializing population
ii) Calculating fitness value
iii) Selection
iv) Crossover
v) Mutation

All title and author details must be in single-column format and must be centred.
Only the first word in a title must be capital and other word should be in small case. Author details must not show any professional title (e.g. Managing Director), any academic title (e.g. Dr.) or any membership of any professional organization (e.g. Senior Member IEEE).
To avoid confusion, the family name must be written as the last part of each author name (e.g. John A.K. Smith).
Each affiliation must include, at the very least, the name of the company and the name of the country where the author is based (e.g. Causal Productions Pty Ltd, Australia). Email address is compulsory for the corresponding author.
Algorithm
Input: Set of hyperparameters, Preprocessed NSL KDD Dataset
Output: Neural Network for Intrusion detection with the best accuracy

1) Start- Generate population of N neural networks making use of random hyperparameters from the selected set for each network. Each network evaluates with different accuracy. This variation is due to the different combination of hyperparameters used.
2) Fitness- Evaluate the fitness value of each neural network in the population. Sort the networks based on accuracy.
3) New population- Repeat the following steps until the new population is complete- To create new population

a) Selection- Select two parent networks from a population based on their accuracy rates- fitness value (Networks with better accuracy have a better chance of selection). Also randomly keep few of the non-top networks.
b) Crossover- Cross over the parents to form a new offspring (children) with a crossover probability. If crossover is not performed, offspring will be identical to parents
c) Mutation- Mutate new offspring at each locus with a mutation probability, to maintain genetic diversity between generations. The child generated represents a combination of its parents, i.e., the parameters used for creating the child is derived from its parent networks.
d) Accept- Place the new offspring in the new population

4) Replace- Use newly generated population for the further run
5) Test- Stop if the end condition is satisfied, and return the best solution in the current population
6) Loop- Go to step 2

The repetition of such a selection and mutation in the breeding process will produce the best offsprings with the best characteristics chosen from the previous generation. Similarly, multiple generations are evolved with a given population ultimately eveolving the best neural network for network intrusion detection with the best hyperparameters which gives the best accuracy score. Figure 1 pictorially represents the activities involved in evolving the best neural network for intrusion detection system using genetic algorithm.

4. Results and discussions

The models were built using the NSL KDD dataset which is a popular dataset used in Network intrusion detection problems. It is derived from the KDD DataCup 1999 dataset, by removal of redundant and unwanted data. The dataset consists of 148516 instances and 41 attributes. The dataset contains four attack classes- DoS, Probe, R2L, and U2R. 80% of the dataset (118812 instances) was chosen for training neural networks and the remaining for testing (29704 instances). Some of the attributes from the dataset include, duration of the network packet, protocol type, service type, source bytes, destination bytes, no. of failed logins, number of logins compromised, root access attempt, no. of file creations etc. The identical patterns among various instances are analyzed to detect if a particular instance is an attack or normal.

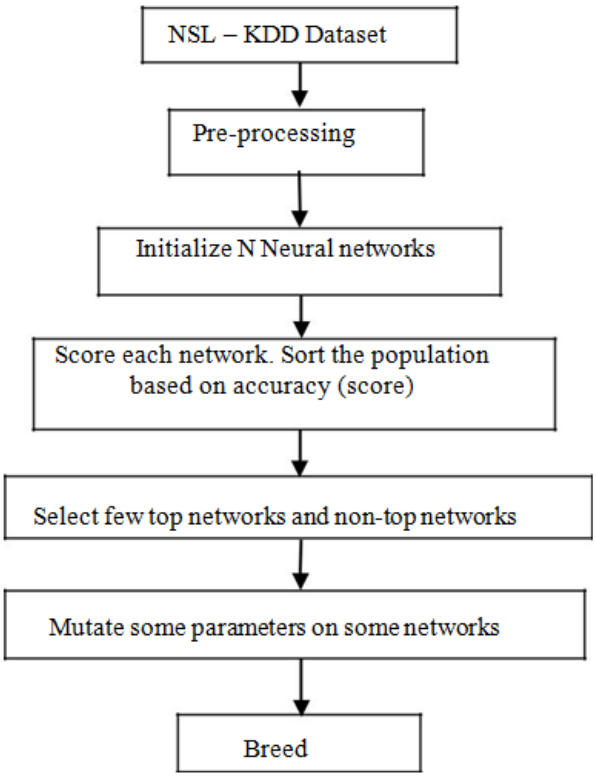

Fig. 1: The Activities Involved in Evolving A Neural Network for Intrusion Detection Using A Genetic Algorithm.

The proposed method was implemented on a Nvidia GPU using the keras deep learning framework. The Nvidia CUDA deep neural network library (cuDNN) was used for accelerated computing. Table 1 gives the complete specification of the system used for execution of the proposed method. Three experiments were conducted with the same setup.

Table 1: System Specification

GPU-	Nvidia	No. of	Memory	Maximum
GeForce 940MX		cores	capacity	frequency
		384	2 GB	1242 MHz
CPU-	Intel	No. of	RAM	Base processor

Core Gen	i5 7th	cores		frequency
		2	8 GB	2.5 GHz

Table 2: Experiment Details

Sl. No	No. of generations	Population	Time taken (Hours)
1	10	10	22
2	10	12	21
3	10	15	21

The number of generations involved in each experiment, the number of neural networks chosen as a subset of the neural networks in a generation for evolving the next generation and the number of hours taken for complete execution are given by the table 2. The no. of hours taken for execution is affected by other workload handled by the system. Also, it can be minimized with a greater number of cores in the GPU. More the number of cores, more the computations handled parallelly by the GPU.

Table 3 shows the average accuracy recorded in each generation of neural networks. As observed from the table, the accuracy increases gradually across generations and is almost constant in the last few generations. However, it is observed in the 4th generation of experiment 1 (Population = 10 neural networks), the accuracy falls abruptly. A bad combination of hyperparameters employed for building the networks in the generation can be a reason for such abrupt drop in accuracy. Therefore, having the appropriate combination of hyperparameters is necessary to derive a neural network giving the best output.

Table 3: The Average Accuracy of Each Generation

Gen	Average Accuracy (%)		
	Population=10	Population=12	Population=15
1	98.11	98.53	98.67
2	98.88	98.96	98.94
3	98.94	99.00	98.93
4	94.33	99.04	98.97
5	99.06	99.03	98.92
6	99.14	99.09	99.09
7	99.15	99.10	99.11
8	99.16	99.11	99.13
9	99.15	99.12	99.13
10	99.13	99.13	99.14

The selection of the best neural networks in each generation, by picking the best parameters from their parents has resulted in a gradual increase in the average accuracy rate of each generation. Also, it can be seen that the final average accuracy score at the end of execution in each experiment is approximately the same. Each neural network was 99% accurate in detecting the abnormal data. Figure 2 graphically represents the variation of average accuracy at various generations.

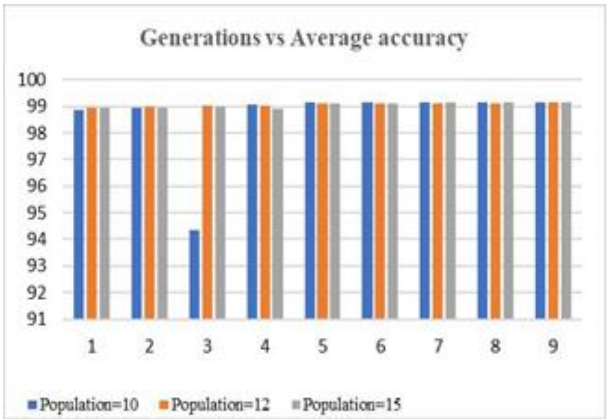

Fig. 2: Graphical Representation (Generations vs. Average Accuracy).

Table 4: Combination of Hyper parameters with The Best Accuracy Score

Population	10	12	15
Number of Layers	3	3	4
Number of Neurons	1024	768	1024
Activation Function	ReLu	ReLu	ReLu
Optimizer	Adamax	Adamax	Adamax
Accuracy	99.21	99.25	99.24

The top 5 neural networks from the final generation were chosen based on accuracy rate and the best hyperparameters are found. Table 4 gives the combination of hyperparameters that gave the best results among all. The results are listed for each experiment.

5. Conclusion and future work

Network security is of utmost importance in the current internet-driven world. Most networks are vulnerable to attacks, and it is necessary to detect the network intrusions to avoid loss of information. Deep learning is one among the various methods available to build a Network intrusion detection system. Different hyperparameters are considered in developing a deep neural network. The most suitable deep neural network for network intrusion detection can be designed by selection of the best hyperparameters using genetic algorithm. The selected hyperparameters can be used to develop a network intrusion detection system that detects the attacks accurately.

Over hundred neural networks are built in the complete execution of a single experiment, which requires high computational power. Hence the whole experiment requires a system with high computing capacity, preferably with a greater number of cores. It is necessary for real time implementation of such a network intrusion detection system.

References

[1] Jin Kim, Nara Shin, Seung Yeon Jo and Sang Hyun Kim, "Method of Intrusion Detection using Deep Neural Network," International Conference on Big Data and Smart Computing (BigComp), Jeju, Korea, IEEE, 2017. https://doi.org/10.1109/BIGCOMP.2017.7881684.

[2] Sasanka Potluri, Christian Diedrich, "Accelerated Deep Neural Networks for Enhanced Intrusion Detection System," IEEE Emerging Technologies and Factory Automation (ETFA), 2016. https://doi.org/10.1109/ETFA.2016.7733515.

[3] S. K. Wagh, Vinod K Pachghare, and Satish R Kolhe, "Survey on Intrusion Detection System using Machine Learning Techniques," Int. J. Comput. Appl., vol. 78, no. 16, pp. 30–37, 2013. https://doi.org/10.5120/13608-1412.

[4] Nathan Shone, Tran Nguyen Ngoc, Vu Dinh Phai and Qi Shi, "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, Vol 2., No.1, pp. 41-50, February 2018. https://doi.org/10.1109/TETCI.2017.2772792.

[5] Rowayda A. Sadek, M. Sami Soliman and Hagar S. Elsayed, "Effective anomaly detection system based on Neural Network with Indicator variable and Rough set Reduction,"International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2,pp.227-233, November 2013.

[6] Santosh Kumar Sahu, Sauravranjan Sarangi and Sanjaya Kumar Jena "A detail analysis on intrusion detection datasets",IEEE International Advance Computing Conference (IACC), Gurgaon, New Delhi, 2014.

[7] Giorgos Vasiliadis, Spiros Antonatos and Evangelos P. Markatos, "GNORT: High performance newtork intrusion detection using graphics processors," Advanced Network Fingerprinting,pp. 116-134, September 2008. https://doi.org/10.1007/978-3-540-87403-4_7.

[8] Zhenghong Xiao, Chuling Liu and Chaotian Chen,"An Anomaly Detection Scheme Based on Machine Learning for WSN", 1st Interna-

tional Conference on Information Science and Engineering (ICISE), Nanjing, China, 2009.
[9] WenJie Tian and JiCheng Liu,"A New Network Intrusion Detection Identification Model Research", 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR),Wuhan, China, 2010. https://doi.org/10.1109/CAR.2010.5456628.
[10] Yichi Zhang, Lingfeng Wang, Weiqing Sun, Robert C. Green II and Mansoor Alam,"Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids", IEEE Transactions on Smart Grid, 2011, pp.796-808. https://doi.org/10.1109/TSG.2011.2159818.
[11] M. Stampar and K. Fertalj "Artificial Intelligence in Network Intrusion Detection", 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2015. https://doi.org/10.1109/MIPRO.2015.7160479.
[12] Sofy Fitriani, Satria Mandala and Muhammad Ary Murti "Review of Semi-Supervised Method for Intrusion Detection System", Asia Pacific Conference on Multimedia and Broadcasting (APMediaCast), Bali, Indonesia, 2016. https://doi.org/10.1109/APMediaCast.2016.7878168.
[13] Hatungimana Girvais, Abdul Munif and Tohari Ahmad, "Using quality threshold distance to detect intrusion in TCP/IP Network," IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Surabaya, Indonesia, December, 2016. https://doi.org/10.1109/COMNETSAT.2016.7907421.
[14] Deepika Venchurkar and Alpa Reshamwala, "A review of intrusion detection system using neural network and machine learning technique," International Journal of Engineering Science and Innovative Technology,Vol. 1, Issue 2, pp. 54-63, November 2012.
[15] Yadigar Imamverdiyev and Lyudmila Sukhostat,"Anomaly detection in network traffic using extreme learning machine", IEEE 10th International Conference on Application of Information and Communication Technologies (AICT),Azerbaijan, Baku, 2016. https://doi.org/10.1109/ICAICT.2016.7991732.
[16] Anna L. Buczak and Erhan Guven,"A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", IEEE Communications Surveys & Tutorials,2015, pp. 1153 – 1176. https://doi.org/10.1109/COMST.2015.2494502.
[17] Sanjay Kumar, Ari Viinikainen and Timo Hamalainen, "Machine Learning Classification Model For Network Based Intrusion Detection System", 11th International Conference for Internet Technology and Secured Transactions (ICITST), University of Cambridge, UK, 2016. https://doi.org/10.1109/ICITST.2016.7856705.
[18] Zhao Jian-hua and Li Wei-hua,"Intrusion detection based on BP Neural network and genetic algorithm," International Conference on Information Computing and Applications, Chengde, China, September 2012. https://doi.org/10.1007/978-3-642-34041-3_61.
[19] Andrey Ferriyan, Achmad Husni Thamrin, Keiji Takeda and Jun Murai, "Feature Selection Using Genetic Algorithm to Improve Classification in Network Intrusion Detection System," International Electronics Symposium on Knowledge Creation and Intelligent Computing, December 2017. https://doi.org/10.1109/KCIC.2017.8228458.
[20] Yann Carbonne and Christelle Jacob, "Genetic algorithm as machine learning for profiles recognition," 7th International Joint Conference on Computational Intelligence, November 2015. https://doi.org/10.5220/0005590501570166.
[21] Yu Wang, Bin Song, Peng Zhang, Ning Xin and Guixing CAO, "A fast feature fusion algorithm in image classification for cyber-physical systems," IEEE Access, pp. 9089-9098, May 2017. https://doi.org/10.1109/ACCESS.2017.2705798.
[22] Chih-Han Chen, Maria Karvela, Mohammadreza Sohbati, Thaksin Shinawatra and Christofer Toumazou, "PERSON- Personalized expert recommendation system for optimized nutrition,"IEEE transactions on biomedical circuits and systems, Vol 12, No 1, pp.151-160, February 2018. https://doi.org/10.1109/TBCAS.2017.2760504.
[23] Pedram Ghamisi, Yushi Chen, Xiao Xiang Zhu, "A Self-Improving Convolution Network for the Classification of Hyperspectral Data,"IEEE Geoscience and Remote sensing letters, Vol 13, No 10, pp. 1537-1541, August 2016. https://doi.org/10.1109/LGRS.2016.2595108.
[24] Chen Huang, Zhihai He, Guitao Cao and Wenming Cao, "Task-Driven Progressive Part Part Localization for Fine-Grained Object Recognition,"IEEE Transactions on multimedia, Vol 18, No 12, December 2016. https://doi.org/10.1109/TMM.2016.2602060.
[25] Kaicheng Li, Qingpeng Gan, Lei Yuan and Qiang Fu, "Optimized Generatio of Test Sequences for High-speed Train using Deep Learning and Genetic Algorithm," IEEE Conference on Intelligent Transportation Systems, Brazil,2016. https://doi.org/10.1109/ITSC.2016.7795644.