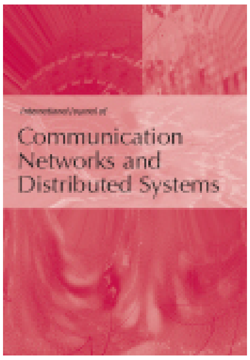


International Journal of Communication Networks and Distributed Systems

ISSN online: 1754-3924 - ISSN print: 1754-3916
https://www.inderscience.com/ijcnds

Research on the optimisation of whitelisting technology for network firewall in industrial control system using genetic algorithm

Xiuhong Zhou, Wenbing Shi

DOI: 10.1504/IJCNDS.2024.10060170

Article History:

Received:	23 November 2022
Accepted:	06 December 2022
Published online:	30 November 2023

Research on the optimisation of whitelisting technology for network firewall in industrial control system using genetic algorithm

Xiuhong Zhou*

Zhumadian Institute of Technology,
Zhumadian, Henan 463000, China
Email: rb57xz@yeah.net
*Corresponding author

Wenbing Shi

Zhumadian Agricultural School,
Zhumadian, Henan 463000, China
Email: isw394244@yeah.net

Abstract: Industrial control systems improve the efficiency of industrial production management but also bring network risks. This paper briefly introduced the industrial control system and the industrial firewall adopting whitelist policy and proposed to optimise the whitelist of industrial firewall with the genetic algorithm-support vector machine (GA-SVM) algorithm to make it learn the rules independently. Finally, simulation experiments were performed using industrial control data collected from light-emitting diode (LED) lamp production enterprises to compare the GA-SVM algorithm with K-means and traditional SVM algorithms. The results demonstrated that the GA-SVM algorithm had better detection accuracy and shorter detection time for abnormal industrial control data; the industrial firewall adopting the GA-SVM-optimised whitelist had lower false blocking rate.

Keywords: industrial firewall; industrial control system; whitelist; genetic algorithm.

Reference to this paper should be made as follows: Zhou, X. and Shi, W. (2024) 'Research on the optimisation of whitelisting technology for network firewall in industrial control system using genetic algorithm', *Int. J. Communication Networks and Distributed Systems*, Vol. 30, No. 1, pp.30–41.

Biographical notes: Xiuhong Zhou received her Master's degree from the Tianjin Vocational and Technical Normal University Major in Computer Application Technology in June 2017. She is working in the Zhumadian Technician College as a Senior Lecturer and is also interested in computer applications technology.

Wenbing Shi received her Bachelor's degree from the Jiangsu University of Science and Technology in June 1997. She is working in the Henan Zhumadian Agricultural School as a Senior Lecturer and is also interested in artificial intelligence.

1 Introduction

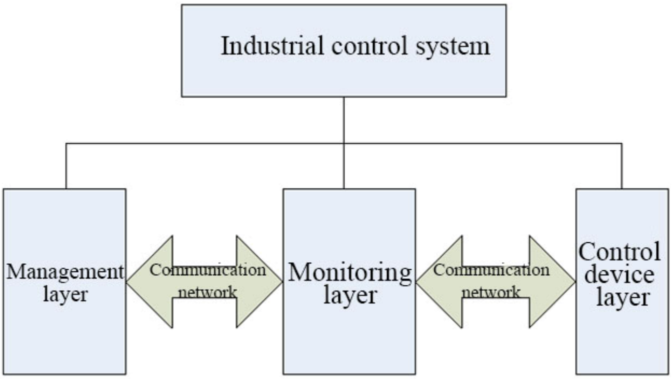
With the advancement of industrialisation, the scale and efficiency of industrial production has increased, and at the same time, the number of links that need to be managed and controlled in the industrial production process has also increased (Li et al., 2021a). The amount of information generated in this process has grown tremendously. In order to reduce the management difficulties caused by the increased amount of management and control information, information technology is combined with industrial production to form an industrial control network. By using the Internet, production personnel can realise centralised management of production facilities, which greatly enhances production efficiency. Industrial control systems are generally used in large-scale production activities, which are closely related to people's livelihoods; incalculable losses may generate if problems occur in the production process (Ahmed et al., 2019; Kumari et al., 2019; Abdulkadhim and Hasan, 2021; Solanki and Khatarkar, 2019). However, although industrial control systems achieve efficient management of industrial production with the help of the Internet, they also bear the risks that the Internet has. The openness of the Internet makes it possible for criminals to invade the industrial control system through the Internet and cause damages to the production activities. Therefore, in order to improve the security of industrial control systems, it is necessary to provide protection measures for industrial control systems. Firewall is a common protection technology. The traditional firewall protection policy for abnormal data is usually set by the firewall operator according to experience (Rideout, 2018; Fakiha, 2022; Li et al., 2021b), and it is difficult to adapt in the face of unknown intrusion attacks. In order to improve the security of firewalls, whitelisting technology that can adjust the protection rules by machine learning algorithms has been added to the traditional firewall technology, which makes the firewall more flexible in using protection policies in the face of various attacks. Al-Abassi et al. (2020) proposed a scalable deep joint learning-based approach for solving security problems in industrial control networks and verified the effectiveness of the approach through experiments. Kim et al. (2020a) proposed an anomaly detection technique using supervised and unsupervised machine learning algorithms in industrial control systems and verified the effectiveness of the technique through experiments. Tippenhauer et al. (2021) proposed a virtual bump solution for restricting traffic to whitelisted destinations. They found that the solution did not require any changes to the physical network topology and allowed for smarter decisions with fewer computational constraints. Lu and Yang (2020) proposed a network threat model for virtual machines in a cloud environment based on the characteristics that virtual machines share network resources through kernel bridges and designed a packet filtering firewall scheme based on kernel bridges. The experimental results showed that the proposed optimisation strategy effectively reduced the average number of matching rules and improved the performance of the firewall. Ariyanto et al. (2020) used the open source Proxmox VE to construct a network firewall and found through experimental analysis that the firewall rules constructed by the open source Proxmox VE could be used for cloud servers. Shah et al. (2020) studied firewalls and virtual private networks based on average throughput, average packet loss rate, and average end-to-end latency in dense mode and found that through extensive investigation, firewalls and virtual private networks provided better security but had slightly degraded cloud performance. Cheng et al. (2019) proposed a firewall policy compression scheme and verified through experimental evaluation that the scheme outperformed existing methods in terms of compression ratio and efficiency while maintaining conflict-free firewall rules. Prabakaran and Ramar (2019) used a software-defined network to build a network stateful firewall and found by simulation experiments that the firewall enhanced the safety, reliability, usability, and overall performance of the network. This paper briefly introduced industrial control systems and industrial firewalls adopting whitelist policies. Then, the genetic algorithm-support vector machine (GA-SVM) algorithm was proposed to optimise the whitelist of industrial firewalls so that they can learn rules autonomously. Finally, simulation experiments were conducted using industrial control data collected from light-emitting diode (LED) lamp production companies to compare the GA-SVM algorithm with K-means and traditional SVM algorithms. The novelty of this paper lies in improving the classification performance of SVM by optimising the SVM parameters in training with the GA. This paper improved the classification performance the SVM algorithm by introducing the GA in the process of SVM training, which provides an effective reference for whitelist optimisation of industrial firewalls.

2 Industrial control system firewall

2.1 Industrial control system

The basic architecture of the industrial control system is shown in Figure 1, which is structurally divided into management layer, monitoring layer, and control device layer. The management layer belongs to the management network in the industrial control network, and its overall function is to receive the equipment operation information collected by the industrial control system and give management instructions; the monitoring layer and the control equipment layer belong to the production network in the industrial control network, and their overall function is to control the production equipment according to the instructions given by the management network (Hoque et al., 2015).

Figure 1 Basic architecture of industrial control system (see online version for colours)



The management layer contains servers for production management and terminals for management personnel. The monitoring layer contains servers for supervisory control and data acquisition (SCADA) systems and database servers for a variety of operating data, which play a top-down connection role in the structure of the entire industrial control system. The monitoring layer receives commands from the management layer (Assis et al., 2017; Al-Haija and Ishtaiwi, 2021; Khairi et al., 2020; Kim et al., 2021) and stores the data collected by the control and equipment layers in the database. The control equipment layer contains a variety of sensors that collect operational data, controllers that execute commands, and other devices that are at the production site. The three structural layers in the industrial control system pass data via a communication network. In the working process of the industrial control system, various sensors in the control equipment layer will collect various operation data (Mahmood et al., 2021), which will be analyzed and judged in the monitoring layer; the useful data will be stored in the database and uploaded to the management layer; the management layer will give instructions according to the received data, and the instructions will be transmitted to the control equipment layer after being analyzing by the monitoring layer to realise remote control of the production equipment.

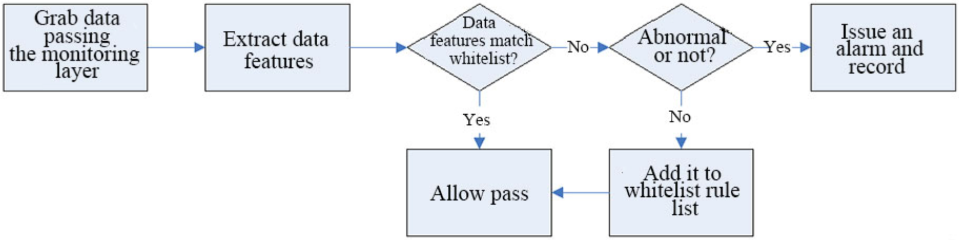
2.2 Firewall whitelisting technology

Industrial control systems enables large-scale remote control of industrial equipment and facilitates the efficient management of industrial production, but the risks associated with industrial control systems can affect conventional industrial production control (Ujjan et al., 2021; Dunn, 2019; Tekerek and Bay, 2019; Kim et al., 2020b). The risks include:

1 the risk of the industrial control system platform itself (the hardware and software used in the industrial control system ignore security at the beginning of production, leading to an increase in the possibility of malicious software installation)

2 the risk of the communication network used between different layers of the industrial control system (the interface of the Internet constituted by the communication network can be used by attackers).

Figure 2 Basic workflow of industrial firewall (see online version for colours)


Grab data passing the monitoring layer
Extract data features
Data features match whitelist?
No
Abnormal or not?
Yes
Issue an alarm and record
Yes
No
Allow pass
Add it to whitelist rule list

In order to improve the security of industrial control systems, corresponding protective measures need to be taken. Among the risks of the industrial control system described in the previous section, the risks of the industrial control system platform itself can be prevented by Trojan and virus detection, while the risk of the communication network can be prevented by isolating the management network and the production network with a firewall. Firewall is the main research subject of this study (Kang and Kim, 2016) Industrial firewalls used in industrial control systems are setup in the monitoring layer to monitor the data transmitted between the management and control device layers and to isolate abnormal data. Traditional firewalls use a blacklist policy, i.e., the data types on the blacklist are not allowed to pass, and the standard of passing is relatively low;

however, industrial firewalls have a higher standard of system security protection, so they use a whitelist policy, i.e., only the data verified by the whitelist are allowed to pass. In addition, in order to improve the reliability and applicability of the whitelist policy, an intelligent algorithm (Hao and Zhang, 2018; Hu et al., 2019; Kamoun-Abid et al., 2019) is introduced so that the whitelist of the industrial firewall can learn the rule table autonomously and thus achieve automatic whitelist adjustment. The workflow is shown in Figure 2.

1 Devices such as sensors in the control device layer collect equipment operation data and upload them to the monitoring layer, and the data to be transmitted are grabbed at the monitoring layer.

2 Features are extracted from the captured data, including the communication address in the packet, the port number of the transmission target, and the function code of the data.

3 The extracted data features are compared with the features recorded in the whitelist. If the features of the packet match the data features recorded in the whitelist, then the packet is directly allowed to pass; otherwise, it goes to the next step.

4 Whether the packet is abnormal or not is determined by the anomaly detection algorithm and the extracted packet features. If it is abnormal, an alert is issued, and it is recorded; if it is normal, the packet is allowed to pass after adding its features to the whitelist rule table.

3 Genetic algorithm-based firewall whitelist optimisation

The industrial firewall introduced with whitelist policy will judge whether the packet can continue transmission according to the data features recorded in the whitelist when facing unknown packets. Compared with the traditional firewall's blacklist policy, whitelist policy has stricter requirements for data communication. In addition, intelligent algorithms are added to the industrial firewall to adjust the whitelist rule table independently, which not only improves the interception flexibility of the industrial firewall but also reduces the maintenance difficulty of the management staff.

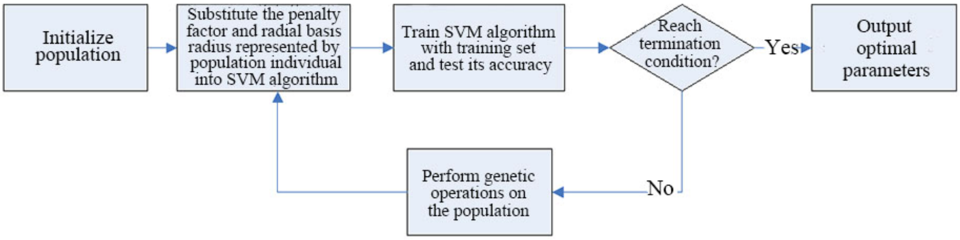
The role of the intelligent algorithm that can be used for autonomous learning of industrial firewall whitelist is further judging the unknown data that cannot be judged by the whitelist and recording the detected data features into the whitelist for autonomous learning of rules. SVM (Laftah Alyaseen et al., 2015; Upadhyay and Singh, 2019; Song, 2020) is used as the method for judging unknown data. Determining whether the unknown data are anomalous can be said to be a binary classification problem. SVM can search a hyperplane from the feature space of data to divide the dataset in the feature space into two parts. The decision function of classifying data with SVM is:

$$\begin{cases} f(x) = \operatorname{sgn}\left(\sum_{i=1}^{n} \alpha_i^* y_i K(x_i, x) + b^*\right) \\ 0 \le \alpha_i^* \le C \\ \sum_{i=1}^{n} \alpha_i^* y_i = 0 \\ b^* = y_i - \sum_{i=1}^{n} \alpha_i^* y_i (x_i, x) \\ K(x_i, x) = \exp\left(-\frac{\|x - x_i\|^2}{\sigma^2}\right) \end{cases} \tag{1}$$

where *f*(*x*) is the decision function used for classification, x_i is the input feature vector of the ith training sample, y_i is the judgment label of the ith training sample, which is 1 if it is normal and –1 if it is not, b^* is the bias term, α_i^* is the Lagrange multiplier of the ith training sample, *C* is the penalty factor, $K(x_i, x)$ is the kernel function, i.e., the Gaussian kernel function with good applicability, and σ is the radial base radius of the kernel function.

Before using SVM to classify unknown data, SVM needs to be trained using the training sample set. Parameters α_i^* and b^* are obtained after fitting when the values of *C* and σ are defined. For the SVM, *C* and σ directly affect its classification performance. Generally, the values of these two parameters are determined based on the user's experience and adjusted gradually in the testing process, which is time-consuming and may lead to the degradation of the classification performance. In order to improve the classification performance of SVM, the GA (Khan et al., 2020) is introduced to optimise *C* and σ. The training process of SVM after GA introduction is shown in Figure 3.

Figure 3 The training process of SVM combined with GA (see online version for colours)


Initialize population
Substitute the penalty factor and radial basis radius represented by population individual into SVM algorithm
Train SVM algorithm with training set and test its accuracy
Reach termination condition?
Yes
Output optimal parameters
No
Perform genetic operations on the population

1 The population is initialised to generate more than one chromosome. Two gene segments in a chromosome are the values of *C* and σ.

2 The values of *C* and σ represented by every chromosome within the population are taken as candidate parameter schemes and substituted into the SVM in turn.

3 The classification accuracy of the SVM under every candidate parameter scheme. The training set is randomly divided equally into *n* parts, and *n* – 1 parts are used to train the SVM under every candidate parameter scheme. The remaining one part is used to test the trained SVM. The classification accuracy of the SVM under every

candidate parameter scheme is used as the fitness value of the corresponding chromosome.

4 Whether the population of the GA meets the termination condition is determined. The termination conditions in the training process include the convergence of the fitness value to stability and reaching the maximum number of iterations. If the termination condition is reached, the scheme represented by the best individual in the population will be output; if the termination condition is not reached, it goes to the next step.

5 The genetic population that do not reach the termination condition are processed by genetic operations, including selection, crossover, and mutation (Wang et al., 2017; Arthur et al., 2019; Michalos et al., 2019). The selection operation is to keep the best chromosomes in the population and use them directly as offspring chromosomes, and the remaining chromosomes are processed by crossover and mutation operations. The crossover operation is to exchange gene segments at the same position of two chromosomes to generate two new offspring chromosomes. The mutation operation is a random change of a gene segment in a single chromosome within the allowed value. Then, it returns to step 2.

4 Simulation experiments

4.1 Experimental data

The simulation experiments were carried out in a laboratory server using MATLAB software. The industrial control data required in the simulation experiments were collected from a company that produces LED lamps, and these data were used to control the automatic assembly line of LED lamps. In addition to the industrial control data collection, the function codes and register addresses of the communication protocol in the company's industrial control system were also collected.

The collected industrial control data were combined with function codes and register addresses to generate 20,000 industrial control data for the simulation experiment. When labelling the industrial control data, data were determined as normal if the combination of data content, function code, and register address was consistent; otherwise, they were abnormal. The label of normal industrial control data was 1, and the label of abnormal industrial control data was –1. After statistics, there were 15,000 normal industrial control data and 5,000 abnormal industrial control data among the generated data. Then, 10,000 normal industrial control data and 3,000 abnormal industrial control data were randomly selected as training samples, and the remaining data were used as testing samples.

4.2 Experimental setup

The relevant parameters of the GA-SVM algorithm used are as follows. The population size of the GA was set as 20, the crossover probability was set as 0.4, the mutation probability was set as 0.1, and the maximum number of iterations was set as 500; the kernel function of the SVM algorithm was the radial basis function (RBF), and C and σ were given by the GA.

In order to verify the performance of the proposed GA-SVM algorithm, it was compared with the traditional SVM algorithm and K-means algorithm. The parameters of the conventional SVM algorithm are as follows. The Gaussian kernel function was used. Penalty factor C was set as 1, and radial base radius σ was set as 0.5. The parameters of the K-means algorithm are as follows. K was set as 3, and the maximum number of iterations was set as 500.

After the algorithm was trained using the training set, the performance of the algorithm was tested using the data from the test set. The test set was divided into five groups, each with 1,000 normal industrial and control data. There were 200 abnormal industrial and control data in the first group, 300 abnormal industrial and control data in the second group, 400 abnormal industrial and control data in the third group, 500 abnormal industrial and control data in the fourth group, and 600 abnormal industrial and control data in the fifth group.

In addition to the above performance tests of the three anomaly data detection algorithms, this paper also tested the optimisation effect of the three anomaly detection algorithms on the industrial firewall whitelist. First, in order of increased anomaly data ratio, five test sets of data were transmitted to the industrial firewall with the fixed whitelist in turn, and the data passing rate of every test set was tested; then, five test sets of data were transmitted to the whitelisted industrial firewall optimised by anomaly data detection in turn, and the data passing rate of every test set was tested.

4.3 Experimental results

Figure 4 shows the detection accuracy of the three anomalous data detection algorithms for test sets with different proportions of anomalous data. From the first group to the fifth group, the amount of anomalous industrial control data in the test set gradually increased, and the detection accuracy of all three anomalous data decreased; when detecting the same test set, the GA-SVM algorithm had the highest detection accuracy, followed by the traditional SVM algorithm, and the K-means algorithm had the lowest accuracy. The reason is as follows. The penalty factor and radial basis radius were optimised by the genetic algorithm in the GA-SVM algorithm, making the classification performance of the SVM optimal, The traditional SVM algorithm set the penalty factor and radial base radius according to experience, so the classification accuracy was lower. The K-means algorithm classified data without learning, but it could not directly judge the kind of data to be classified but could determine whether the data were abnormal or not according to their proportion in the total data, so it had the worst classification performance.

Figure 5 shows the average time of the three anomaly data detection algorithms for detecting test sets with different percentages of anomalous data. It was seen from Figure 5 that the detection time of all three anomalous data detection algorithms tended to increase with the increase of anomalous data in the test set. When detecting the same test set, the detection time of the K-means algorithm was the longest, and the detection time of traditional SVM and GA-SVM algorithms was not much different. The reason is that the K-means algorithm needed to iterate for several times and calculate the cluster centres, but the traditional SVM and GA-SVM algorithms only needed to substitute the data feature vectors into the decision function to get the judgment result, so they consumed less time in detection.

Figure 4 Accuracy of three anomalous data detection algorithms (see online version for colours)

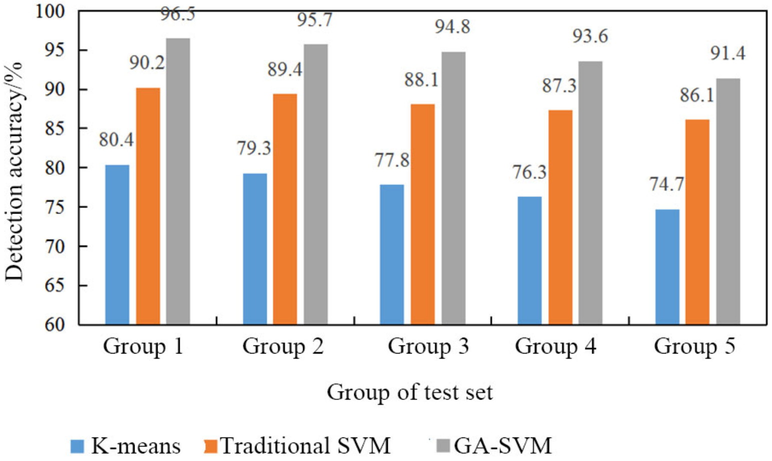


Figure 5 Detection time of three anomaly data detection algorithms (see online version for colours)

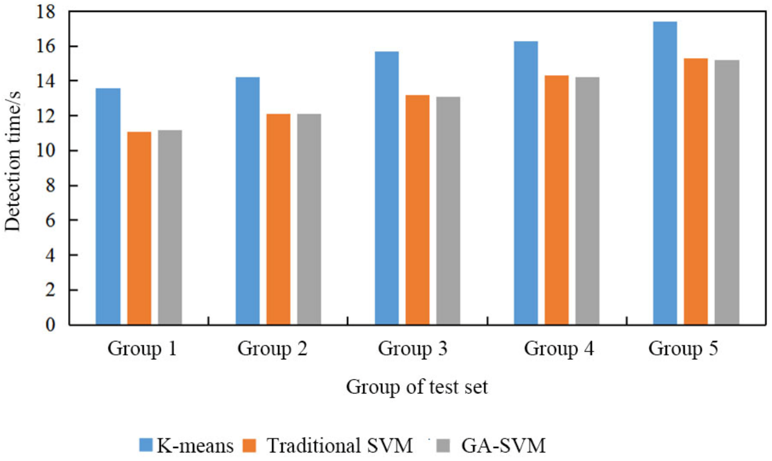


Table 1 False interception rate of the traditional industrial firewall and industrial firewalls optimised with three anomaly detection algorithms

	Traditional industrial firewall	*Industrial firewall optimised by the K-means algorithm*	*Industrial firewall optimised by the traditional SVM algorithm*	*Industrial firewall optimised by the GA-SVM algorithm*
Group 1	10.2%	9.4%	7.7%	4.1%
Group 2	10.9%	9.9%	8.3%	4.8%
Group 3	11.5%	10.3%	9.1%	5.2%
Group 4	12.8%	11.2%	9.9%	5.7%
Group 5	14.3%	12.4%	10.5%	6.1%

The false interception rates of the traditional industrial firewall and industrial firewalls whose whitelist policy was optimised by three anomaly detection algorithms for different percentages of anomalous data in the test set are shown in Table 1. It was seen from Table 1 that the traditional industrial firewall with the fixed whitelist had the highest false interception rate, followed by the industrial firewall whose whitelist policy was optimised by the K-means algorithm and the firewall whose whitelist policy was optimised by the traditional SVM algorithm, and the industrial firewall whose whitelist policy was optimised by the GA-SVM algorithm was the lowest. The false interception rate of every industrial firewall increased with the increase of abnormal industrial control data in the test set.

5 Conclusions

This paper briefly introduced the industrial control system and the industrial firewall adopting whitelist policy and proposed to optimise the industrial firewall's whitelist with the GA-SVM algorithm to make it learn the rules independently. Finally, simulation experiments were performed to compare the GA-SVM algorithm with the K-means algorithm and the traditional SM algorithm using the industrial control data collected from the LED lamp production company. The following results were obtained. With the increase of the proportion of abnormal industrial control data, the accuracy of all three abnormality detection algorithms decreased; when detecting the set with the same proportion of abnormal industrial control data, the GA-SVM algorithm had the highest accuracy, the traditional SVM algorithm was the second, and the K-means algorithm was the worst. As the proportion of anomalous industrial control data increased, the detection time of all three anomaly detection algorithms increased; when detecting the set with the same proportion of anomalous industrial control data, the K-means algorithm consumed the longest time, and the traditional SVM and GA-SVM algorithms consumed less time and had an insignificant difference. As the proportion of anomalous industrial control data increased, the false interception rate increased in the traditional industrial firewall with the fixed whitelist and industrial firewalls whose whitelist was optimised by three anomaly detection algorithms respectively, but the industrial firewall optimised by the GA-SVM algorithm always had a lower false interception rate.

References

Abdulkadhim, M. and Hasan, S. (2021) 'Boosting the network performance using two security measure scenarios for service provider network', *Iraqi Journal of Science*, pp.174–179.

Ahmed, O., Rehman, A. and Habib, A. (2019) 'Industrial control system cybersecurity best practices', *Control Engineering: Covering Control, Instrumentation, and Automation Systems Worldwide*, Vol. 66, No. 5, pp.24–26.

Al-Abassi, A., Karimipour, H., Dehghantanha, A. and Parizi, R.M. (2020) 'An ensemble deep learning-based cyber-attack detection in industrial control system', *IEEE Access*, Vol. 2020, pp.1–10.

Al-Haija, Q.A. and Ishtaiwi, A. (2021) 'Multi-class classification of firewall log files using shallow neural network for network security applications', *Advances in Intelligent Systems and Computing*, Vol. 1370, No. 1, pp.1–15.

Ariyanto, Y., Harijanto, B., Firdaus, V. and Arief, S. (2020) 'Performance analysis of Proxmox VE firewall for network security in cloud computing server implementation', *IOP Conference Series Materials Science and Engineering*, Vol. 732, No. 1, pp.1–6.

Arthur, J.K., Boahen, E.K., Doh, F. and Mantey, E.A. (2019) 'Firewall rule anomaly detection and resolution using particle swarm optimization algorithm', *International Journal of Computer Applications*, Vol. 178, No. 33, pp.975–8887.

Assis, M., Hamamoto, A.H., Abrão, T. and Proença, M.L. (2017) 'A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks', *IEEE Access*, Vol. 5, pp.9485–9496.

Cheng, Y., Wang, W., Wang, J. and Wang, H. (2019) 'FPC: a new approach to firewall policies compression', *Tsinghua Science & Technology*, Vol. 24, No. 1, pp.65–76.

Dunn, K. (2019) 'Sophos XG firewall', *SC Magazine*, Vol. 30, No. 3, pp.38–38.

Fakiha, B. (2022) 'Effectiveness of forensic firewall in protection of devices from cyberattacks', *International Journal of Safety and Security Engineering: An Interdisciplinary Journal for Research and Applications*, Vol. 12, No. 1, pp.77–82.

Hao, X. and Zhang, X. (2018) 'Research on abnormal detection based on improved combination of K-means and SVDD', *IOP Conference Series: Earth & Environmental Science*, Vol. 2018, pp.1–6.

Hoque, N., Bhattacharyya, D.K. and Kalita, J.K. (2015) 'BotNet in DDoS attacks: trends and challenges', *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 4, pp.2242–2270.

Hu, H., Han, W., Kyung, S., Wang, J., Ahn, G.J., Zhao, Z. and Li, H. (2019) 'Towards a reliable firewall for software-defined networks', *Computers & Security*, Vol. 87, No. 2, pp.1–17.

Kamoun-Abid, F., Meddeb-Makhlour, A., Zarai, F. and Guizani, M. (2019) 'DVF-fog: distributed virtual firewall in fog computing based on risk analysis', *International Journal of Sensor Networks*, Vol. 30, No. 4, pp.242–253.

Kang, S.H. and Kim, K.J. (2016) 'A feature selection approach to find optimal feature subsets for the network intrusion detection system', *Cluster Computing*, Vol. 19, No. 1, pp.1–9.

Khairi, H.H., Ariffin, S., Latiff, N., Kamaludin, M.Y., Yusof, M.K., Hassan, M.K., Rava, H.M. and Khairi, H. (2020) 'The impact of firewall on TCP and UDP throughput in an openflow software defined network', *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 20, No. 1, pp.256–263.

Khan, M.A., Rehman, A., Khan, K.M., Al Ghamdi, M.A. and Almotiri, S.H. (2020) 'Enhance intrusion detection in computer networks based on deep extreme learning machine', *Computers, Materials, & Continua*, Vol. 66, No. 1, pp.467–480.

Kim, J., Choi, H., Shin, J. and Seo, J.T. (2020a) 'Study on anomaly detection technique in an industrial control system based on machine learning', *ICEA '20: Proceedings of the 2020 ACM International Conference on Intelligent Computing and its Emerging Applications*, Vol. 2020, pp.1–5.

Kim, S., Yoon, S., Narantuya, J. and Lim, H. (2020b) 'Secure collecting, optimizing, and deploying of firewall rules in software-defined networks', *IEEE Access*, Vol. 8, pp.15166–15177.

Kim, T., Kwon, L.J. and Song, A.J. (2021) 'F/Wvis: hierarchical visual approach for effective optimization of firewall policy', *IEEE Access*, Vol. 9, pp.105989–106004.

Kumari, S., Singh, P. and Upadhyay, R.K. (2019) 'Virus dynamics of a distributed attack on a targeted network: effect of firewall and optimal control', *Communications in Nonlinear Science and Numerical Simulation*, July, Vol. 73, pp.74–91.

Laftah Alyaseen, W., Ali Othman, Z. and Ahmad Nazri, M.Z. (2015) 'Hybrid modified K-means with C4.5 for intrusion detection systems in multiagent systems', *Scientific World Journal*, Vol. 2015, No. 2, pp.1–14.

Li, J.S., Liu, C.G., Wu, C.J., Wu, C.C., Huang, C.W., Li, C.F. and Liu, I.H. (2021a) 'Design of industrial control system secure communication using moving target defense with legacy infrastructure', *Sensors and Materials: An International Journal on Sensor Technology*, Vol. 33, No. 10 Pt. 1, pp.3415–3424.

Li, Y., Zhang, X. and Jia, B. (2021b) 'The design of hardware firewall based on Acorn RISC machine', *IOP Conference Series: Earth and Environmental Science*, Vol. 692, No. 2, pp.1–5.

Lu, N. and Yang, Y. (2020) 'Application of evolutionary algorithm in performance optimization of embedded network firewall', *Microprocessors and Microsystems*, July, Vol. 76, pp.103087.1–103087.9.

Mahmood, H., Mahmood, D., Shaheen, Q., Akhtar, R. and Wang, C. (2021) 'S-DPS: an SDN-based DDoS protection system for smart grids', *Security and Communication Networks*, Vol. 2021, pp.1–19.

Michalos, M., Nalmpantis, S.L. and Ovaliadis, K. (2019) 'Design and implementation of firewall security policies using Linux Iptables', *Journal of Engineering Science and Technology Review*, Vol. 12, No. 1, pp.80–86.

Prabakaran, S. and Ramar, R. (2019) 'Stateful firewall-enabled software-defined network with distributed controllers: a network performance study', *International Journal of Communication Systems*, Vol. 32, No. 17, pp.1–17.

Rideout, J. (2018) 'Securing your industrial control system', *Manufacturing Automation: Machine Dessig, Systems, Technology*, Vol. 33, No. 3, p.14.

Shah, H., Din, A.U., Khalil, A., Khan, A. and Din, S. (2020) 'Enhancing the quality of service of cloud computing in big data using virtual private network and firewall in dense mode', *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 3, pp.402–412.

Solanki, P.S. and Khatarkar, P.R. (2019) 'Network security management and protection using UTM firewall', *International Journal of Computer Sciences and Engineering*, Vol. 7, No. 6, pp.1055–1058.

Song, X. (2020) 'Firewall technology in computer network security in 5G environment', *Journal of Physics Conference Series*, Vol. 1544, pp.1–5.

Tekerek, A. and Bay, O.F. (2019) 'Design and implementation of an artificial intelligence-based web application firewall model', *Neural Network World*, Vol. 29, No. 4, pp.189–206.

Tippenhauer, N.O., Chen, B., Mashima, D. et al. (2021) 'vBump: securing ethernet-based industrial control system networks with VLAN-based traffic aggregation', *CPSIoTSec '21: Proceedings of the 2nd Workshop on CPS&IoT Security and Privacy*, Vol. 2021, pp.3–14.

Ujjan, R.M.A., Pervez, Z., Dahal, K., Khan, W.A., Khattak, A.M. and Hayat, B. (2021) 'Entropy based features distribution for anti-DDoS model in SDN', *Sustainability*, Vol. 13, No. 3, pp.1–27.

Upadhyay, R.K. and Singh, P. (2019) 'Modeling and control of computer virus attack on a targeted network', *Physica A: Statistical Mechanics and its Applications*, Vol. 538, No. C, pp.1–16.

Wang, Y., Wang, A.N., Ai, Q. and Sun, H.J. (2017) 'An adaptive kernel-based weighted extreme learning machine approach for effective detection of Parkinson's disease', *Biomedical Signal Processing and Control*, September, Vol. 38, pp.400–410.