Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5031236, 10 pages
https://doi.org/10.1155/2022/5031236

*Research Article*

# Intrusion Detection System Based on Genetic Attribute Reduction Algorithm Based on Rough Set and Neural Network

**Jan Luo**,[1,2] **Huajun Wang**,[1] **Yanmei Li**,[3] **and Yuxi Lin**[4]

[1]*Geophysical Institute, Chengdu University of Technology, Chengdu, Sichuan 610059, China*
[2]*Computer School, China West Normal University, Nanchong, Sichuan 637009, China*
[3]*School of Artificial Intelligence, Chongqing University of Technology, Chongqing 401135, China*
[4]*Apartment Technology Department, 58. Com Inc., Beijing 100012, China*

Correspondence should be addressed to Huajun Wang; wanghuajun@mail.cdut.edu.cn

Received 12 January 2022; Revised 16 February 2022; Accepted 23 February 2022; Published 25 April 2022

Academic Editor: Kalidoss Rajakani



The development of computer network technology not only brings convenience to people's life but also has many information and data security problems and threats. The performance and problems of traditional intrusion detection system make it insufficient to resist intrusion attacks effectively and with high quality. Therefore, this paper proposes an intrusion detection system based on the combination of genetic attribute reduction algorithm based on rough set and neural network. Based on the traditional BP neural network, this paper combines the genetic attribute reduction algorithm based on rough set to optimize the structure and performance of the system. The experimental results show that the genetic attribute reduction algorithm based on rough set has faster convergence speed and can effectively shorten the running time of the system and improve the efficiency of the algorithm. At the same time, the intrusion detection system based on the combination of genetic attribute reduction algorithm based on rough set and neural network has significantly improved the detection rate of five intrusion attacks compared with the traditional algorithm and achieved the purpose of optimizing the real time and effectiveness of intrusion detection.

## 1. Introduction

The development of computer network technology and mobile intelligent terminal equipment and their wide application in various fields not only promote social progress and development but also change the way people work, live, study, and entertainment. The scale of network users is constantly expanding, and the connection between human and computer network has reached an unprecedented level. At present, with the support of computer network technology, people can make online shopping, order meals, buy train and air tickets, book hotels, etc., in life, which greatly saves people's time cost and provides great convenience [1]. At the same time, the development and application of computer network technology has also become an important prerequisite for the construction and development of modern society. It is one of the symbols to measure the strength of a country in all aspects. In addition to the various conveniences brought to people by the development of computer network technology, there are also various network security problems, such as the leakage of user information, the tampering of relevant information or the publication of personal private information, the disturbance of personal information in the database, and the destruction of user computer hardware, resulting in the paralysis of user network. These existing security problems seriously affect the confidentiality, controllability, availability, and auditability of network data and information, which is also a network problem that network users are increasingly concerned about [2]. Therefore, the research on various efficient security technologies and products to ensure the security of the Internet and computer system has become the focus of computer network security research. Common technologies in the field of network security include VPN technology, antivirus software technology, data secret key technology, firewall, and identity authentication technology. These network security technologies have played an important role in network security and personal privacy protection, but they are not perfect in themselves,

and there are many defects that cannot be ignored. For example, firewall technology cannot take effective measures against internal attacks. At the same time, with the update of attack methods, its resistance to new attack forms is relatively weak, and even some new attack methods can easily bypass the firewall [3]. VPN technology can statically protect the data in the transmission process, but it cannot actively detect and track the intrusion. Although the traditional intrusion detection system makes up for the problems of other network security technologies to a certain extent, its lack of effectiveness, adaptability, and scalability makes it unable to meet the continuous development of computer network technology and people's demand for security network.

Aiming at the problems of traditional intrusion detection system, many researchers propose to optimize its system and performance through rough set, particle swarm optimization, and other algorithms. Some researches have introduced rough set theory into intrusion detection technology to predict the prediction rule set in system sequence, but it can only be carried out in a small scale [4]. In addition, genetic algorithm and particle swarm optimization algorithm are introduced to optimize the rough set algorithm based on the rough set theory, but if its parameters are not set properly, it is easy to make the algorithm enter the local optimization, resulting in the stagnation of the algorithm [5]. With the development and application of machine learning technology, artificial intelligence, support vector machine, neural network, and other algorithms are introduced into intrusion detection technology to improve the performance of intrusion detection system and its degree of automation and systematization [6]. Some literatures have introduced support vector machine into intrusion detection and found a better solution to the problems such as the reduction of detection and classification accuracy in the case of small samples [7]. On the basis of this research result, other literatures compare the accuracy and effectiveness of real-time intrusion detection combined with neural network and further study the research on the sorting and selection of intrusion detection attribute features. The experimental results not only maintain the accuracy of intrusion detection but also reduce the time of intrusion detection [8]. In addition, the literature combines fuzzy clustering algorithm and immune theory to improve the recognition efficiency of intrusion detector [6].

This paper proposes an intrusion detection system based on genetic attribute reduction algorithm of rough set and neural network. The research and innovative contributions include the following: (1) introduce the genetic attribute reduction algorithm of rough set into neural network. Through the combination of various algorithms, the advantages complement each other, so as to improve the effect of intrusion detection. (2) The intrusion detection system has fast convergence speed, which can effectively shorten the time span of the system run time and improve the efficiency of the algorithm. (3) Compared with the traditional algorithm, it significantly improves the detection rate of five intrusion attacks and achieves the purpose of optimizing the real time and effectiveness of intrusion detection.

## 2. Principle and Classification of Intrusion Detection System

Intrusion detection is to detect the strategies and behaviors that can threaten the system security in the network. It is a dynamic security detection technology with detection, recording, alarm, and response. Intrusion detection mainly detects unauthorized activities from inside or outside by analyzing the computer system information and network behavior obtained from the security log audit data and identifies the threat of intrusion, so as to send corresponding alarms and take active protective measures before the network system is not endangered [9]. Intrusion detection is a real-time and active attack technology, which can strengthen the security of data information and ensure the integrity of the structure without affecting the network performance [10]. Therefore, the main tasks of intrusion detection are two aspects. One is to monitor and analyze the user's behavior activities, count, and analyze the characteristics of abnormal activities. The other is to carry out alert identification of various intrusion activities, timely convey the alarm information to relevant systems, complete audit tracking and management archiving, and facilitate subsequent analysis [11].

Intrusion detection has different classification results according to different classification standards, mainly from three standards: intrusion detection object, intrusion detection method, and real-time performance of intrusion detection system. According to the different objects of intrusion detection, it can be divided into network-based intrusion detection, host-based intrusion detection, and hybrid intrusion detection. Network-based intrusion detection is to obtain the required relevant data information by monitoring data packets at a key point and analyze the existing attacks in the current network with the help of statistical analysis, feature matching, and other methods. Host-based intrusion detection is based on log files and audit records in the host as abnormal data sources, combined with other information in the host to detect network attacks [12]. Hybrid intrusion detection system reduces the error rate of intrusion detection system by checking the host log file and network information in parallel.

According to the intrusion detection methods, it can be divided into anomaly detection and misuse detection. In anomaly detection, it is necessary to build an intrusion detection model that can be updated and normally active and compare the current activity behavior of network users with the model. If the difference between the user's current activity and normal activity does not exceed the preset threshold, it indicates that it is not a network attack; otherwise, it is a network attack [13]. Anomaly detection can detect new and unknown network attacks, but its intrusion detection accuracy is low. Misuse detection is to extract the possible attack characteristics of different attack behaviors based on the analysis results of different types of attack methods and then analyze and match the current network data with the extracted feature set. If the conditions of feature matching are met, it is an attack behavior; otherwise, it is not. Misuse detection has high detection accuracy for known attacks, but it cannot find unknown attacks.

According to the real-time performance of intrusion detection system, it can be divided into timing system and implementation system. The timing system processes the stored network data regularly and implements intrusion detection and alarm through post analysis method. It can reduce the resources occupied by intrusion detection system in CPU resources, but due to the lack of real-time performance of timing system, it does not have enough necessary preventive measures [14]. The real-time system can deal with abnormal activities and events in real time, which is also the way used by most intrusion detection systems. The speed of computer hardware is the guarantee for the implementation of intrusion detection system to deal with attacks in real time. The rapid development of computer hardware conditions has a great impact on the calculation speed and accuracy. The faster the real-time attack response of intrusion detection system, the faster the speed of computer hardware. If the hardware platform cannot keep up with the computing speed, there will be many loopholes in intrusion detection. In the actual operation, intrusion detection combines real-time processing and timing processing; that is, first analyze the relevant data with the real-time system and monitor the suspicious network attacks with intrusion signs, and then process and analyze the relevant data in detail through timing processing.

As shown in Figure 1, it is a hacker intrusion flow chart and a typical intrusion detection deployment diagram.

## 3. Construction of Intrusion Detection System Model Based on Rough Set Genetic Attribute Reduction Algorithm and Neural Network

*3.1. Intrusion Detection System Model Based on Rough Set Genetic Attribute Reduction Algorithm and Neural Network.* The importance of different knowledge attributes in rough set knowledge base is different, and the existing knowledge redundancy will affect the correctness and simplicity of decision-making. Attribute reduction is to delete irrelevant or unimportant attributes on the basis of ensuring that the classification and decision-making ability of knowledge base are not affected. Because the search for the minimum reduction of rough set has been proved to be a NP problem, the search direction or structure of genetic algorithm is diverse, taking multiple individuals as the possible solution, and its sampling range is in the global range of the search space, which improves the possibility of converging to the global optimal solution. The definition knowledge expression system is composed of four tuples, expressed as $S = (U, R, V, f)$, in which $U$ is the universe containing multiple data objects, $V = \bigcup_{r \in R} V_r$, the value domain of attribute $r$ is expressed as $V_r$, $f$ is the information function of $U \times R \longrightarrow V$, $R$ is all sets of attributes, and $R = C \cup D$, $C \cap D = \varnothing$, in which the conditional attribute set and decision attribute set are $C$ and $D$, respectively. There is a subset $B$ and $B \subseteq R$ in the attribute set $R$. Let the indiscernibility relationship be expressed as $IND(B)$, as shown in

$$IND(B) = \left\{(x, y) \middle| (x, y) \in U^2, \forall b \in B(b(x) = b(y))\right\}. \quad (1)$$

$S$ is the decision table, and the lower approximation and upper approximation of each subset $X \subseteq U$ in the equivalence relationship $R$ level are shown in

$$R\_(X) = \left\{x_i \in U \middle| [x_i]_R \subseteq X\right\}, \quad (2)$$

$$R^-(X) = \left\{x_i \in U \middle| [x_i]_R \cap X \neq \varnothing\right\}. \quad (3)$$

In practice, when $R$ is equivalent, its upper approximation and lower approximation will become as shown in

$$R\_(X) = \cup\{Y \in U/R | Y \subseteq X\}, \quad (4)$$

$$R^-(X) = \cup\{Y \in U/R\} | Y \cap X \neq \varnothing\}. \quad (5)$$

$P$ and $Q$ are defined as two equivalent relation clusters on the universe $U$, and the $P$ positive domain of $Q$ is expressed as $POS_P(Q)$ and $POS_P(Q) = \underset{r \in U/Q}{U} P(X)$. If the $Q$ independent subset $G \subseteq P$ of $P$ is $POS_G(Q) = POS_P(Q)$, then the $Q$ of $P$ is reduced to $G$.

The principle of genetic attribute reduction algorithm based on rough set is to encode the individuals in the algorithm through binary, and each individual corresponds to a conditional attribute in the decision table. Secondly, two principles are followed for attribute reduction. One is the condition reflecting the reduction degree. The less the attribute reduction, the better. The other is that the more the number of attribute classification ability distinguishes in the dye body, the better. Therefore, adding the attribute importance factor to the appropriate function can improve the classification ability on the basis of ensuring attribute reduction, as shown in

$$F(X) = 1 - \frac{1}{2}\left(\frac{n - \mathrm{Card}(X)}{n} + \frac{(x_1 p_1 + x_2 p_2 + \cdots + x_n p_n)}{\mathrm{Card}(X)}\right). \quad (6)$$

In the formula, the number of current condition attributes is $n$, the number of 1 in the current individual is $\mathrm{Card}(X)$, the value of the $n$ bit of the current individual is $x_n$ (0 or 1), and the ratio of the value equal to 1 after the $n$ attribute coding is $p_n$, and $p_n$ is as shown

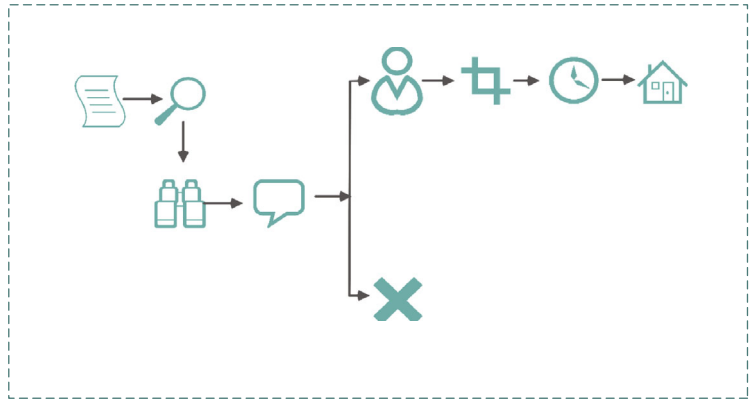
$$p_n = I_n / l. \quad (7)$$

The number of individuals in the current population is $l$, and $I_n$ is the number equal to 1 in the $n$ attribute.

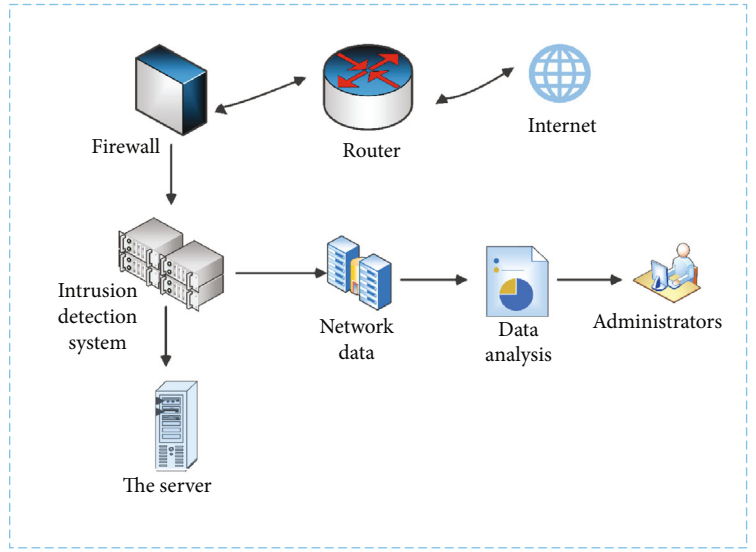
Third, genetic selection is carried out by roulette. The population with the scale of $l$ is expressed as $G = \{x_1, x_2, \cdots, x_l\}, x_k \in G$, and the individual fitness is expressed as $F(x_k)$. The probability of individual selection is shown in

$$g_k = 1 - F(x_k) / \sum_{k=1}^{l} F(x_i), \quad (8)$$

where $k = 1, 2, \cdots, l$; there is an inverse relationship between the value of fitness function and individual adaptability;



(a) Hacker intrusion flow chart




(b) Intrusion detection system deployment diagram

Figure 1: Hacker intrusion flow chart and typical intrusion detection deployment chart.

that is, the smaller the value, the better the adaptability. Formula (8) ensures that the individual with better fitness will have a greater probability of being selected.

Fourth, carry out crossover and mutation operations. The individuals in the middle group are randomly selected and paired for crossover operation. According to the crossover probability, that is, $p_c$, some genes of the two parents are exchanged at the exchange point, so as to produce two new individuals. Then, calculate the fitness of the new individual and compare it with the corresponding parent fitness. If its fitness is greater than the parent fitness, a new individual will replace the parent individual. The mutation operation first uses the integer randomly generated between [1, $n$] to specify the mutation location and then reverses the gene at the specified location according to the mutation probability, that is, $p_m$, so as to obtain a new individual. Since the crossover probability $p_c$ will become smaller and smaller in the whole evolution process of the population, and the mutation probability $p_m$ will gradually increase slightly with the decrease of population diversity in the algorithm, the crossover and mutation probabilities are shown in

$$p_c = \begin{cases} \dfrac{f' - f_{\text{avg}}}{(1 + e^{\alpha G}) e^{f_{\max} - f'}} + \beta, & f' \geq f_{\text{avg}}, \\ k_1, & f' < f_{\text{avg}}, \end{cases} \tag{9}$$

$$p_m = \begin{cases} \dfrac{f - f_{\text{avg}}}{1 + e^{-\alpha G}} + \beta, & f \geq f_{\text{avg}}, \\ k_2, & f < f_{\text{avg}}. \end{cases} \tag{10}$$

In the formula, $\beta$, $\alpha$, $k_1$, and $k_2$ are the constant coefficients, and $k_1 \in (0.5, 1)$, and $k_2 \in (0, 0.5)$; the evolutionary algebra is expressed as $G$, the average individual fitness value of the current population is expressed as $f_{\text{avg}}$, the individual with higher fitness in the two crossover individuals is expressed as $f'$, the maximum fitness value in the current population is expressed as $f_{\max}$, and the fitness value of variant individuals is expressed as $f$.

Fifth is the termination condition; that is, the evolution will stop automatically after the $T$ generation, or the fitness

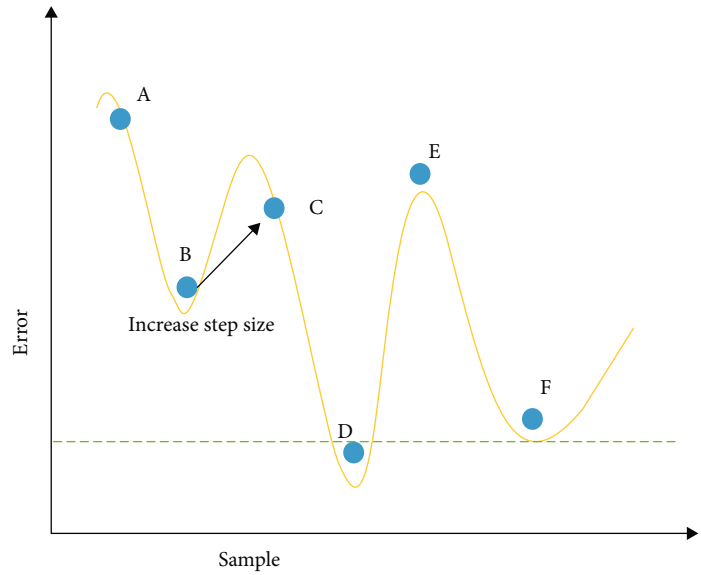



Figure 2: Global search diagram of genetic attribute reduction algorithm based on rough set and neural network.

of the optimal individual has been maintained $N$ times without improvement.

The traditional BP neural network algorithm back propagates through gradient descent and modifies the weight and threshold. Its excitation function may exist in the flat saturation interval of the surface. Due to the small gradient of the saturation interval, the number of iterations of the neural network increases, which affects the operation efficiency of the algorithm. At the same time, the surface of the error function is complex, and there are often many minimum points, which is easy to cause the gradient descent algorithm to fall into local minimum points and reduce the convergence accuracy of the algorithm. The combination of genetic attribute reduction algorithm based on rough set and neural network can avoid these problems. Figure 2 shows the global search diagram of the algorithm combining genetic attribute reduction algorithm based on rough set and neural network.

It can be seen from the figure that the combination of genetic attribute reduction algorithm based on rough set and neural network searches from point $a$, point $B$ is the local minimum point, and the algorithm gradually converges to this point, but the algorithm does not meet the stop condition at this time. Therefore, the algorithm increases the step size to make the search jump directly from point $B$ to point $C$ and finally converge to the global minimum point D. Let the average error of consecutive $m$ samples be $\bar{E}$ and $\bar{E} = (E_{n+1} + E_{n+2} + \cdots + E_{n+m})/m$; $s$ represent the number greater than $E_{n+1}$ in $E_{n+2} + E_{n+3}, \cdots, E_{n+m}$. The rules for determining local minimum points are shown in

$$\left|\bar{E} - E_{n+m+1}\right| < \varphi, \tag{11}$$

$$s \geq (m-1)/2 or E_{n+1} < E_{n+m+1}. \tag{12}$$

If and only if the above two conditions are met at the same time, it is considered that the algorithm has fallen into the local minimum. At this time, $E_{n+m+1}$ is the minimum point; increase the step size and jump out of the local minimum.

The combination of genetic attribute reduction algorithm based on rough set and neural network improves the structure and gradient descent method in traditional BP neural network. The weight and threshold of the network are optimized by genetic attribute reduction algorithm based on rough set, and then, the training samples are input into the optimized neural network. It carries out the secondary optimization of weight and threshold with the help of gradient descent method. This can not only give play to the advantages of good global search ability and fast convergence speed of genetic attribute reduction algorithm based on rough set but also overcome the problems of slow convergence speed and easy entry into local minimum through the strong generalization ability of neural network. As shown in Figure 3, it is the algorithm flow chart of the combination of genetic attribute reduction algorithm based on rough set and neural network.

*3.2. Evaluation Criteria of Intrusion Detection System.* There is no unified evaluation standard for intrusion detection system. According to the existing relevant literature, the evaluation standards of intrusion detection system in this paper are mainly four, namely, accuracy, completeness, fault tolerance, and processing performance. Accuracy is the ability of intrusion detection system to correctly distinguish attack behavior in various behaviors. It includes three indicators: alarm accuracy, false alarm rate, and detection reliability. The calculation of alarm accuracy is shown in

$$p_A = \frac{N_r}{N_t}. \tag{13}$$

The alarm accuracy is expressed as $p_A$, the number of correctly alarmed intrusions is expressed as $N_r$, and the total number of intrusions is expressed as $N_t$.

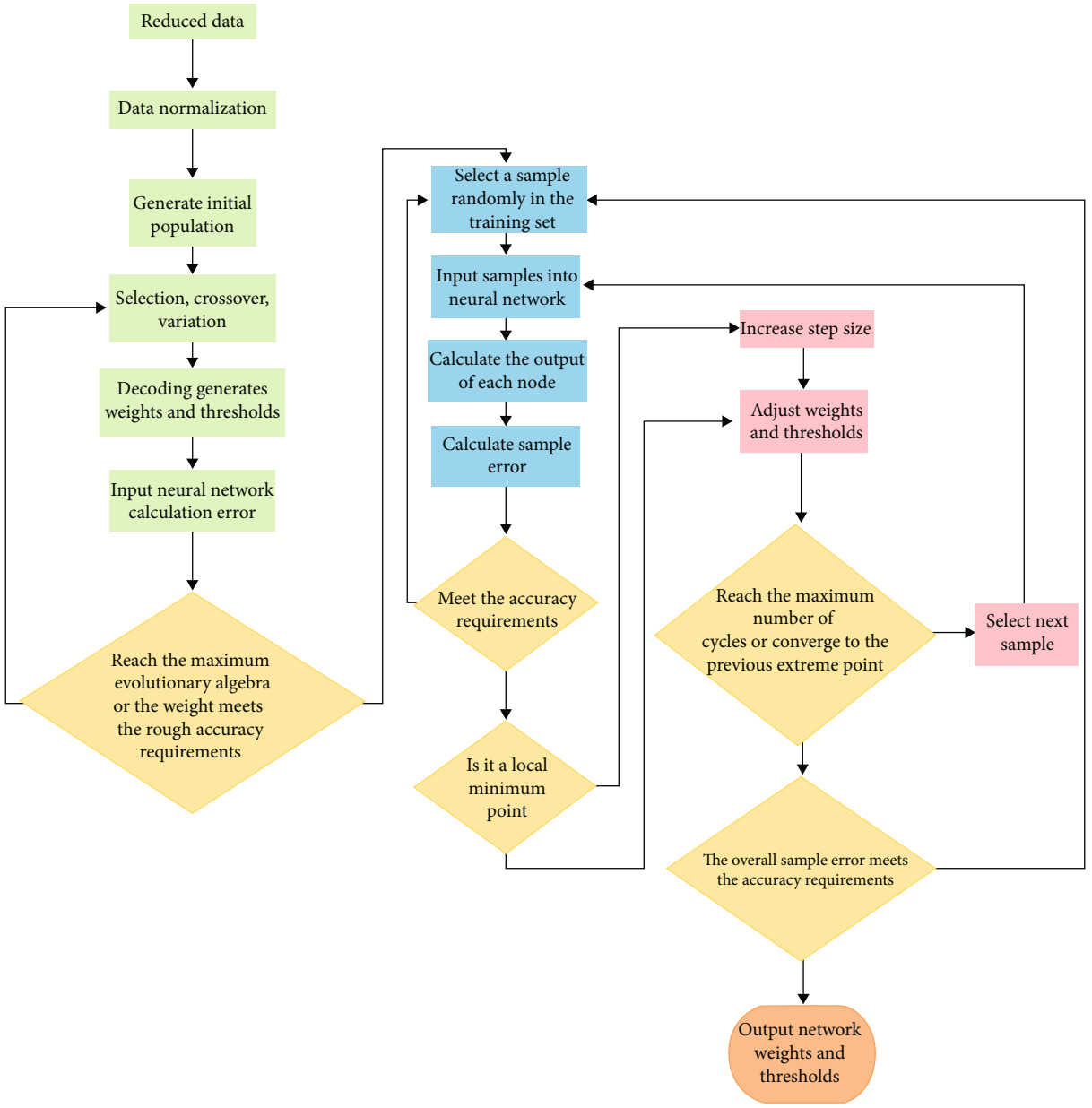



Figure 3: Flow chart of genetic attribute reduction algorithm based on rough set and neural network.

The false alarm rate is calculated as shown in

$$p_F = \frac{N_f + N_m}{N_t}. \tag{14}$$

The false alarm rate is $p_F$, the number of false alarms is $N_f$, and the number of missed alarms is $N_m$.

Completeness is the ability of intrusion detection system to detect all attacks, which includes the completeness of attack means and methods. The calculation is shown in

$$p_C = \frac{N_d}{N_a}. \tag{15}$$

The completeness is expressed as $p_C$, the total number of detected attacks is expressed as $N_d$, and the total number of possible attack methods is expressed as $N_a$.

Because intrusion detection system has its own security vulnerabilities, it needs to have fault tolerance. In addition, intrusion detection itself should be able to resist attacks from the outside, especially denial of service attacks. It can deliberately make the computer or network in an abnormal operation state and cannot continue to provide corresponding services for legitimate users, or the quality of service provided is reduced. Processing performance is the efficiency of audit data processing by intrusion detection system. If the processing performance of intrusion detection system is low, it cannot carry out real-time intrusion detection.

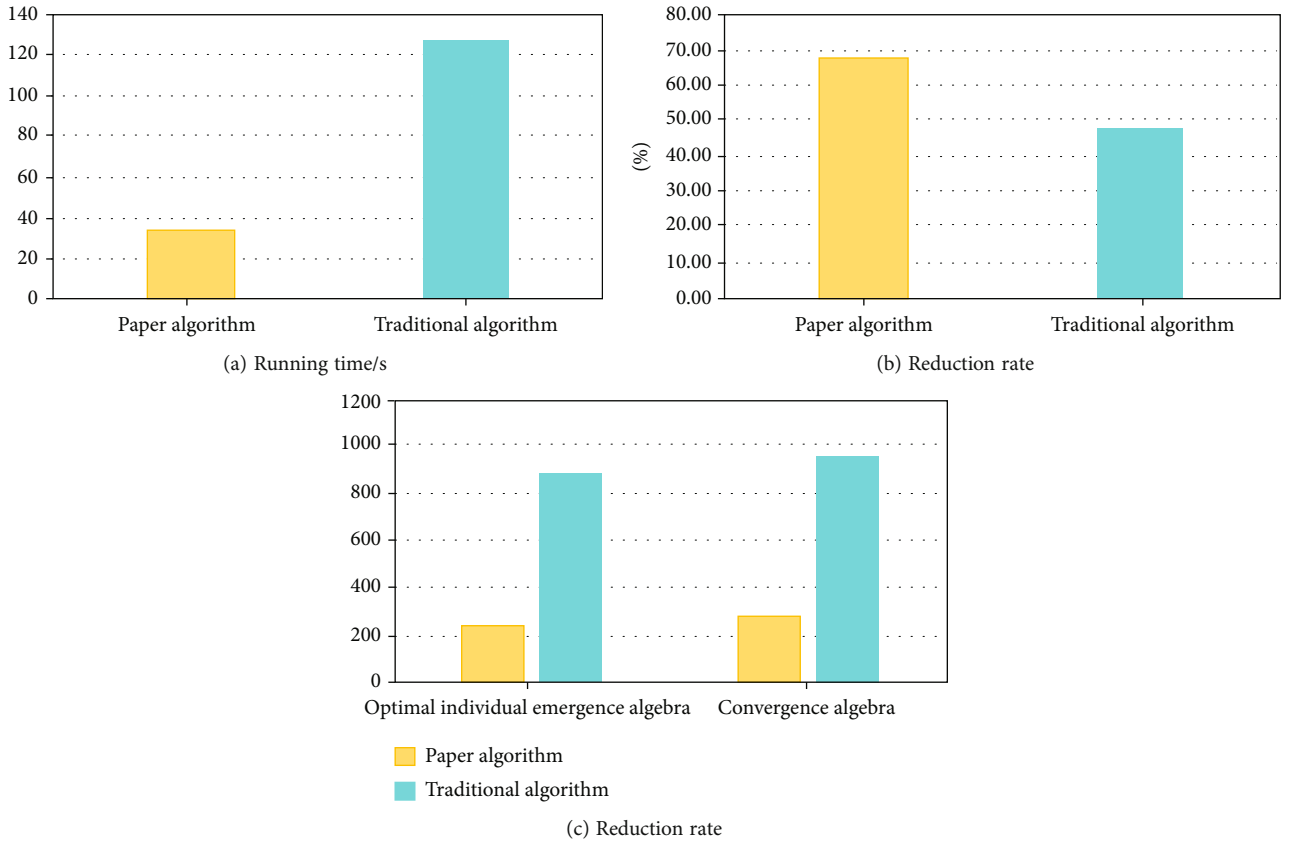



Figure 4: Comparison between genetic attribute reduction algorithm based on rough set and short answer genetic algorithm.

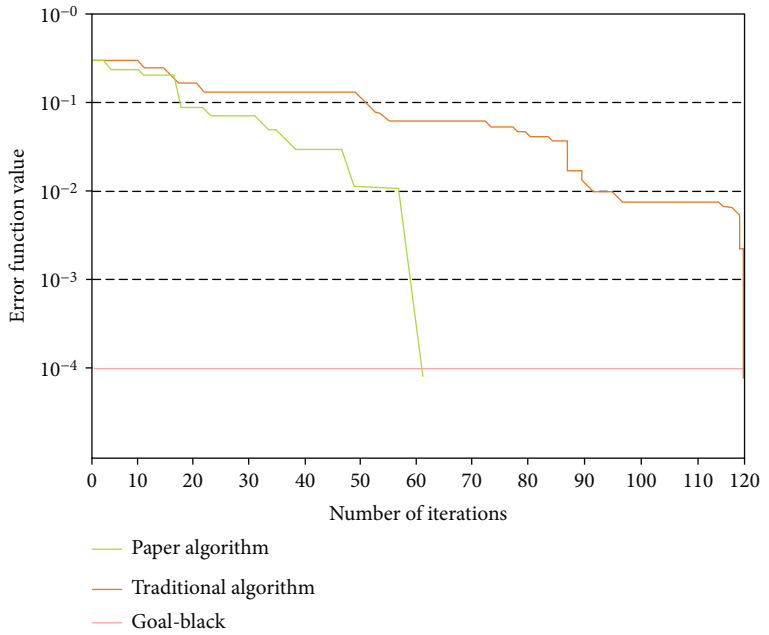



Figure 5: Convergence comparison of traditional algorithm and genetic attribute reduction algorithm based on rough set and neural network.

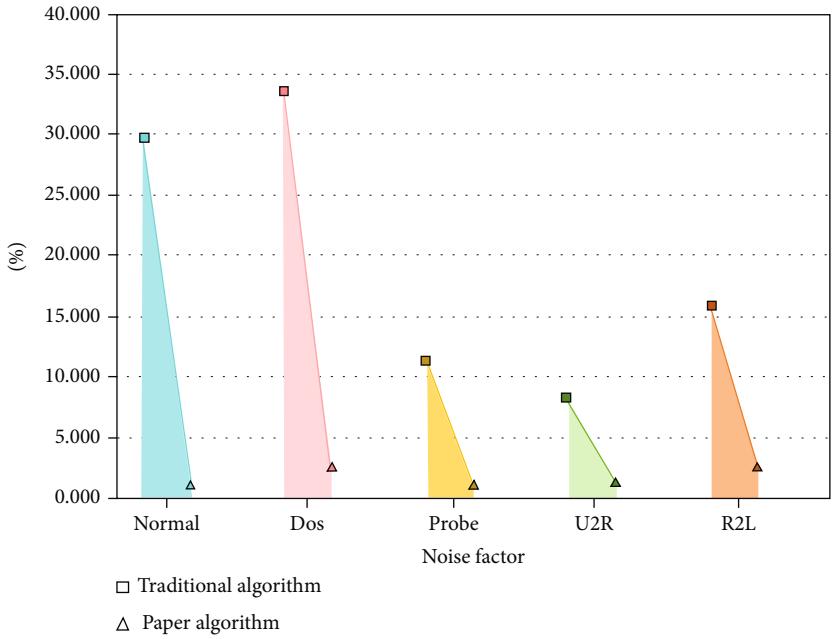



Figure 6: The comparison results of false detection rates of five intrusion attacks between the combination of genetic attribute reduction algorithm based on rough set and neural network and traditional algorithm.

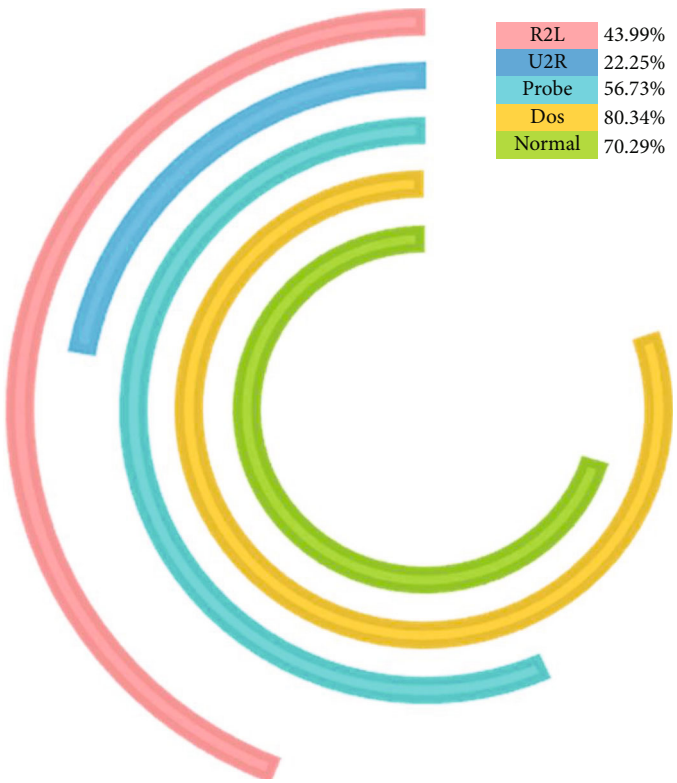



Figure 7: Detection rate of five intrusion attacks by traditional algorithms.

## 4. Simulation Experiment of Intrusion Detection System Based on Rough Set Genetic Attribute Reduction Algorithm and Neural Network

Genetic algorithm is a general algorithm to solve search problems, which can be used for all kinds of general problems. Advantages of genetic algorithm are as follows: independence of the problem domain and fast and random search ability. Search starts from the group, has potential parallelism, and can compare multiple individuals at the same time. In order to illustrate the effectiveness and feasibility of the genetic attribute reduction algorithm based on rough set, this paper selects the simple genetic algorithm as a reference. As shown in Figure 4, the operation results of the genetic attribute reduction algorithm based on rough set and the simple genetic algorithm are compared.

From the running results of the algorithm in the figure, it can be seen that the running time of the genetic attribute reduction algorithm based on rough set is significantly reduced than that of the simple genetic algorithm, and the reduction efficiency is also significantly improved. The genetic attribute reduction algorithm based on rough set starts to converge after 200 generations, while the simple genetic algorithm starts to converge after 900 generations. In the genetic attribute reduction algorithm based on rough set, the optimal individual appears in 242 generations, and in the simple genetic algorithm, the optimal individual appears in 894 generations. It can be seen that the genetic attribute reduction algorithm based on rough set not only has a great improvement in the operation effect, but also its reduction result is better than the simple genetic algorithm.

In this paper, five intrusion attacks are selected to simulate the combination of genetic attribute reduction algorithm based on rough set and neural network, and the simulation results are compared with those of traditional algorithms. In order to accelerate the convergence speed of the neural network, the relevant data are normalized and then input into the neural network for training. As shown in Figure 5, the convergence comparison of the traditional algorithm and the genetic attribute reduction algorithm based on rough set and the neural network algorithm is shown. It can be seen from the figure that the combination of genetic attribute reduction algorithm based on rough set and neural network has faster convergence speed and shorter running time.

As shown in Figure 6, the comparison results of false detection rates of five intrusion attacks by the combination of genetic attribute reduction algorithm based on rough set and neural network and traditional algorithm are shown. It can be seen from the figure that the false detection rate of the genetic attribute reduction algorithm based on rough set combined with neural network is significantly lower than that of the traditional algorithm, which shows that the improvement of the intrusion detection performance of the algorithm is effective.

As shown in Figures 7 and 8, the detection rates of five intrusion attacks by the traditional algorithm and the genetic attribute reduction algorithm based on rough set and the neural network are shown, respectively. It can be seen from the demerit in the figure that the combination of genetic attribute reduction algorithm based on rough set and neural network algorithm can significantly improve the detection rate of DOS type, probe type, and u2r and r2l type attack behavior.

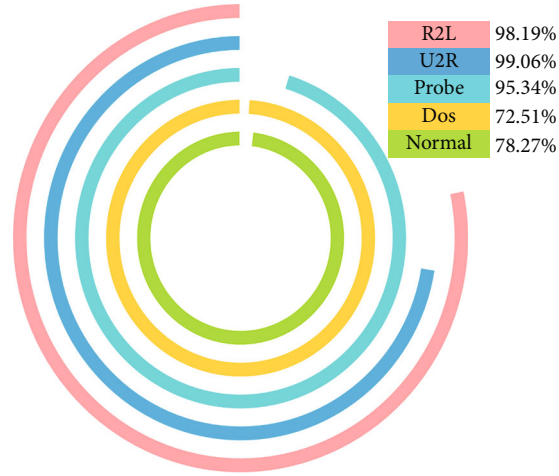



Figure 8: The detection rate of five intrusion attacks by the combination of genetic attribute reduction algorithm based on rough set and neural network.

To sum up, the genetic attribute reduction algorithm based on rough set in the intrusion detection system based on the combination of genetic attribute reduction algorithm based on rough set and neural network can effectively improve the operation efficiency of the system, reduce the operation time, reduce the false detection rate of attack behavior, and significantly improve the detection efficiency. Thus, the intrusion detection system has an effective and obvious optimization effect in terms of real time and effectiveness.

## 5. Conclusion

The development of computer network technology and information network technology provides convenience for people in all aspects and fields of life and greatly improves people's dependence and tightness on intelligent mobile devices and networks. At the same time, network security has become an important issue in the research of computer network technology. Although the traditional intrusion detection technology has laid the foundation for network security, in the face of constantly updated attack behaviors and methods, the resistance of the traditional intrusion detection technology is becoming weaker and weaker. Therefore, this paper proposes an intrusion detection system based on the combination of genetic attribute reduction algorithm based on rough set and neural network. Based on the traditional BP neural network, the genetic attribute reduction algorithm based on rough set is introduced to optimize the structure and performance of the system. The experimental results show that the genetic attribute reduction algorithm based on rough set can improve the operation

efficiency of intrusion detection system and shorten the operation time. At the same time, the intrusion detection system based on the combination of genetic attribute reduction algorithm based on rough set and neural network significantly reduces the false detection rate of five attack behaviors and effectively realizes the optimization purpose of real time and effectiveness of the system intrusion detection.

## Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The authors declared that they have no conflicts of interest regarding this work.

## References

[1] M. Li, M. Chen, and W. Xu, "Double-quantitative multigranulation decision-theoretic rough fuzzy set model," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 11, pp. 3225–3244, 2019.

[2] T. Delkesh and M. A. Jabraeil Jamali, "EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 5, pp. 1897–1914, 2019.

[3] Z. Bang-Bang, W. Shu-Ning, and T. Yong, "ELM network intrusion detection algorithm based on rough set attribute reduction," *Transducer and Microsystem Technologies*, vol. 30, 2019.

[4] J. Pacheco, V. H. Benitez, L. C. Felix-Herran, and P. Satam, "Artificial neural networks-based intrusion detection system for Internet of Things fog nodes," *Access*, vol. 8, pp. 73907–73918, 2020.

[5] G. A. A. Prana, A. Sharma, L. K. Shar et al., "Out of sight, out of mind? How vulnerable dependencies affect open-source projects," *Empirical Software Engineering*, vol. 26, no. 4, pp. 1–34, 2021.

[6] M. Abdolrazzagh-Nezhad, H. Radgohar, and S. N. Salimian, "Enhanced cultural algorithm to solve multi-objective attribute reduction based on rough set theory," *Mathematics and Computers in Simulation*, vol. 170, pp. 332–350, 2020.

[7] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset," *Computer Networks*, vol. 177, no. 18, article 107315, 2020.

[8] S. Jeong, B. Jeon, B. Chung, and H. K. Kim, "Convolutional neural network-based intrusion detection system for AVTP streams in automotive Ethernet-based networks," *Communications*, vol. 29, p. 100338, 2021.

[9] M. H. Haghighat and J. Li, "Intrusion detection system using voting-based neural network," *Tsinghua Science & Technology*, vol. 26, no. 4, pp. 484–495, 2021.

[10] W. Ghanem and A. Jantan, "A new approach for intrusion detection system based on training multilayer perceptron by using enhanced bat algorithm," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11665–11698, 2020.

[11] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, "A Deep Learning Model for Network Intrusion Detection with Imbalanced Data," *Electronics*, vol. 11, no. 6, p. 898, 2022.

[12] A. Azawii, S. Al-Janabi, and B. Al-Khateeb, "Survey on intrusion detection systems based on deep learning," *Periodicals of Engineering and Natural Sciences (PEN)*, vol. 7, no. 3, pp. 1074–1095, 2019.

[13] Y. Humid, F. A. Shah, and M. Sugumaran, "Wavelet neural network model for network intrusion detection system," *International Journal of Information Technology*, vol. 11, no. 2, pp. 251–263, 2019.

[14] C. Iwendi, J. H. Anajemba, C. Biamba, and D. Ngabo, "Security of things intrusion detection system for smart healthcare," *Electronics*, vol. 10, no. 12, p. 1375, 2021.