Hindawi
Journal of Sensors
Volume 2021, Article ID 9089370, 10 pages
https://doi.org/10.1155/2021/9089370

*Research Article*

# Intrusion Detection Algorithm and Simulation of Wireless Sensor Network under Internet Environment

**Jing Jin**

*Tongfang Knowledge Network Technology Co., Ltd. (Beijing), Beijing 100192, China*

Correspondence should be addressed to Jing Jin; cnkijinjing@vikings.grayson.edu

Received 2 October 2021; Accepted 20 October 2021; Published 8 November 2021

Academic Editor: Guolong Shi



As an effective security protection technology, intrusion detection technology has been widely used in traditional wireless sensor network environments. With the rapid development of wireless sensor network technology and wireless sensor network applications, the wireless sensor network data traffic also grows rapidly, and various kinds of viruses and attacks appear. Based on the temporal correlation characteristics of the intrusion detection dataset, we propose a multicorrelation-based intrusion detection model for long- and short-term memory wireless sensor networks. The model selects the optimal feature subset through the information gain feature selection module, converts the feature subset into a TAM matrix using the multicorrelation analysis algorithm, and inputs the TAM matrix into the long- and short-term memory wireless sensor network module for training and testing. Aiming at the problems of low detection accuracy and high false alarm rate of traditional machine learning-based wireless sensor network intrusion detection models in the intrusion detection process, a wireless sensor network intrusion detection model combining two-way long- and short-term memory wireless sensor network and C5.0 classifier is proposed. The model first uses the hidden layer of the bidirectional long- and short-term memory wireless sensor network to extract the features of the intrusion detection data set and finally inputs extracted features into the C5.0 classifier for training and classification. In order to illustrate the applicability of the model, the experiment selects three different data sets as the experimental data sets and conducts simulation performance analysis through simulation experiments. Experimental results show that the model had better classification performance.

## 1. Introduction

The Internet continues to develop rapidly, and wireless sensor network technology continues to advance rapidly. In today's big data era, the scale of data traffic is getting larger and larger, and the way of intrusion has become more complicated. Traditional intrusion detection technologies such as artificial immune detection methods and intrusion detection methods based on information theory have many shortcomings. As intrusion data continue to become more complex and feature diversified, the model has problems such as false alarm rate, high false alarm rate, poor attentiveness, and low detection rate [1]. Therefore, it is necessary to choose a new type of intrusion detection technology to improve the current wireless sensor network security defense capabilities. A good dimensionality reduction method will directly affect machine-based performance of the learned intrusion detection model. Therefore, the problem of high-dimensional data processing is the biggest challenge faced by traditional machine learning-based intrusion detection algorithms [2].

Due to the overall weakness of the Internet in terms of defense and autonomous management capabilities, this makes it vulnerable to attacks. This is also an important factor that makes it difficult to solve wireless sensor network security problems. In order to further improve its proactive defense capabilities, it is necessary to significantly improve its intrusion detection accuracy level, thereby greatly reducing the false alarm rate. At the same time, it can also weaken data overload and other problems and apply data mining technology to wireless sensor network intrusion detection to achieve the establishment of an intrusion detection system with self-adaptability and good scalability [3]. With the increasingly profound impact of the Internet on our lives,

research on intrusion and anti-intrusion will receive continuous attention, and from the perspective of the current development form, the level of development of anti-intrusion technology lags behind that of intrusion technology, which makes the former face a bigger dilemma; it is extremely necessary to optimize and innovate the intrusion detection system if only to improve the initiative of the former technology [4, 5].

This article focuses on the important research direction of wireless sensor network security, studies the intrusion detection technology based on radial basis function neural wireless sensor network, and designs and implements the intrusion detection system based on radial basis function neural wireless sensor network. Section 1 is the introduction. Here, we introduce the current situation of wireless sensor network security and the current research status of intrusion detection technology at home and abroad and explore and summarize the intrusion detection technology, intrusion detection system, and an artificial neural wireless sensor network. Section 2 is the research of the network intrusion detection algorithm and simulation under the Internet environment. The data dimension is reduced through an information gain feature selection algorithm; from the perspective of image recognition, the feature subset is transformed from a text type to a gray image through a multivariate correlation analysis algorithm. Dong et al. [6] pointed out that the model obviously improves the detection and classification accuracy and reduces the false alarm rate and no longer relies on feature selection algorithms. Section 3 discusses the result analysis. The seamless integration of digital simulation and a physical test bed is realized by constructing a virtual and real wireless sensor network fusion simulation system. Based on this system, the physical wireless sensor network can be flexibly configured and arbitrarily connected to the digital simulation wireless sensor network. Through this method, a complex virtual and real wireless sensor network is constructed. Section 4 is the conclusion. Based on summarizing the work of the thesis, the problems of the model proposed in the thesis are analyzed in depth, and the future research and development of wireless sensor network intrusion detection models based on deep learning are prospected.

## 2. Research on Wireless Sensor Network Intrusion Detection Algorithm and Simulation in Internet Environment

*2.1. Related Work.* Wireless sensor network security is an eternal topic in the era of mobile Internet and information. Wireless sensor network security not only requires wireless sensor network users to pay attention to it but also requires wireless sensor network security practitioners to adopt certain technical means to protect wireless sensor network users' data, information, equipment, and other software and hardware. In the article, the intrusion rules are set in advance to determine whether the current behavior is abnormal. Although the system has a high detection rate for unknown behaviors, it is difficult to analyze and detect encrypted wireless sensor network environments, and the system can only detect external attacks [7]. Verma and Ranga proposed to combine the Snort-based intrusion detection system and Bayesian classifier to the Internet environment. The system uses the Snort detection system to collect wireless sensor network data in the Internet environment and pass the Yes classifier which classifies and processes the collected data. This model can effectively detect unknown attacks and has a low false detection rate [8]. Siddique et al. proposed an intrusion detection algorithm that combines genetic algorithms and support vector machines in the Internet environment. The article points out that genetic algorithms are used to extract features from data, and then, support vector machines are used for intrusion detection [9]. Experimental analysis shows that the algorithm improves the accuracy of intrusion detection and shortens the detection time. But so far, intrusion detection research for cloud environments has not really achieved real-time detection and autonomous analysis, and there are no more mature applications related to the Internet on the market [10]. As a new research field, Internet security issues, especially intrusion detection technology, pose a large number of challenging topics for scientific and technological workers in the two levels of basic theory and detection technology.

In a wireless sensor network security system, the firewall plays a role similar to a door guard and is the outermost line of defense of the system, blocking the inner wireless sensor network from the outer Internet, and can selectively accept or deny Internet access. However, with the improvement of hacker technology, the diversification of attack methods, and the complexity of attack software, firewalls as the main countermeasures are far from enough. Deng et al. used the clustering method to filter some types of intrusion detection data, used the random forest algorithm in machine learning to reduce the dimensionality of the features, and finally inputted the convolutional neural wireless sensor network to complete the intrusion detection. The average recognition accuracy was as high as more than 99%. The effect is very significant [11]. Liang et al. used the authoritative KDD Cup 99 data in the field of intrusion detection and used an autoencoder to reconstruct the data dimension and input it into a deep neural wireless sensor network, which doubled the recognition rate of rare types of intrusion detection data [12]. Wu et al. used the differential evolution algorithm in the evolutionary algorithm to improve the deep belief wireless sensor network and applied it to the field of intrusion detection, which greatly improved the performance of recognition [13]. Ling et al. used an improved genetic algorithm and an improved tabu search algorithm to better set the initial values of the parameters of the BP neural wireless sensor network, which made up for the shortcomings of the BP neural wireless sensor network and improved the performance of the intrusion detection system [14]. Li et al. used the particle swarm optimization algorithm and the iteration of the population to improve the radial basis function neural wireless sensor network used in the field of intrusion detection, reducing other intrusion detection evaluation indicators except accuracy [15].

The existing wireless sensor network intrusion detection technology has improved the detection efficiency. However,

in the face of the massive, high-dimensional intrusion data generated in the current wireless sensor network environment, it also exhibits some problems. One is the traditional machine learning intrusion detection model [16, 17]. Feature engineering is usually required when detecting massive, high-dimensional data sets. Feature selection methods or feature extraction methods will directly affect the detection effect of the model. Second, traditional intrusion detection models based on machine learning algorithms often use a single classifier for classification in the output layer. Network intrusions have high dimensionality, diversity, and complexity, it is difficult for traditional detection methods to correctly identify various characteristics of network intrusions, resulting in low accuracy of network intrusion detection and false alarms.

*2.2. Research on Wireless Sensor Network Intrusion Detection Algorithm.* The construction of wireless sensor network does not need to install other software on the computer, so it does not occupy computer resources and does not affect the performance of the host business system. In the wireless sensor network intrusion detection system, if we use switched Ethernet, it can only detect the information of the wireless sensor network segment connected to the computer and cannot detect the data of different wireless sensor network segments. Therefore, it is difficult for this method to achieve the results we want when using switched Ethernet. Moreover, the cost of the wireless sensor network adapter is greatly increased due to the installation of multiple wireless sensor network intrusion detection systems. The wireless sensor network-based intrusion detection model is shown in Figure 1.

In response to the high dimensionality of intrusion detection data sets [18], the feature selection algorithm used in this paper is an information gain algorithm. Information gain is shown in the following formula:

$$\mathrm{Info}(M,N) = F(M) - F\left(\frac{M}{N}\right) + \alpha * \sum_{i=0}^{m} F\left(\frac{M_i}{N_i}\right). \quad (1)$$

$F(M)$ is expressed as the information entropy of random variable $M$, as in the following formula:

$$F(M) = \sum_{i=0}^{m} f(M_i) \ln_2\left(f\left(\frac{M_i}{N_i}\right)\right). \quad (2)$$

$F(M/N)$ represents the information entropy of random variable $M$ obtained by random variable $N$, as shown in the following formula:

$$F\left(\frac{M}{N}\right) = \sum_{i=0}^{m} f\left(\frac{M_i}{N_i}\right) \ln_2\left(f\left(\frac{M_i}{N_i}\right)\right) * \sum_{j}^{n} f(N_j). \quad (3)$$

$G_{fi,j}^{i}$ represents the area of the unknown triangle in the row $i$ and the column $j$. When $i = j$, $G_{fi,j}^{i} = 0$. Because the geometric relationship between two different attributes is studied, from this, we can get a symmetric matrix whose main diagonal is all 1/2. That is the SYM matrix. Formula (4) is a 4-dimensional SYM matrix [19]. The characteristic description of network traffic data is to better distinguish between normal traffic data and abnormal traffic data. We use the information theory method to analyze the correlation between the network traffic attributes and the correlation between the records and find the correlation between the normal data and abnormal data characteristics to construct the correlation rule set.

$$\mathrm{SYM}_i^m = \begin{Bmatrix} \frac{1}{2} & G_{f1,2}^{i} & G_{f1,3}^{i+1} & G_{f1,4}^{i+2} \\ G_{f2,1}^{i} & \frac{1}{2} & G_{f2,3}^{i+2} & G_{f2,4}^{i+2} \\ G_{f3,1}^{i} & G_{f3,2}^{i+1} & \frac{1}{2} & G_{f3,4}^{i+2} \\ G_{f4,1}^{i} & G_{f4,2}^{i+1} & G_{f4,3}^{i+2} & \frac{1}{2} \end{Bmatrix}. \quad (4)$$

In the Internet environment, the use of the BP neural network for intrusion detection can improve detection efficiency. However, the BP neural network needs to be trained on historical data to achieve the detection purpose. The learning rate of the neural network is fixed, and network convergence speed is slow. Due to the large number of attack behaviors that need to be processed in the Internet environment, the training time required for the BP neural network must be very long. And because the neural network uses the gradient descent method for sample training, it is easy to fall into a local minimum that cannot reach the global optimum, which will result in low detection efficiency, and it is difficult to completely guarantee the security of the Internet system [20]. There are mainly two general improvement methods: one is to improve according to the standard gradient descent method, such as the BP neural network algorithm with additional momentum, and the adaptive learning rate adjustment method. There is also an adjustment method through numerical optimization, including the quasi-Newton method, the conjugate gradient method, and the LM method. With the development of artificial intelligence, many scholars have applied intelligent algorithms to neural networks.

*2.3. Research on Optimization of Network Intrusion Detection Algorithm.* The algorithm trains the samples to adjust the weight value and linearly combines these classifiers by learning multiple classifiers to achieve the purpose of improving the classification accuracy. In the C5.0 classifier algorithm, Boosting technology usually stacks multiple C4.5 weak classifiers into a strong classifier. Figure 2 shows the Boosting-integrated optimization diagram. The algorithm inputs the training data set into the classifier and trains the weak classifiers one by one in the order of a ladder-like training process. Each time, the training set of the weak classifier is transformed according to a certain strategy, and finally, the weak classifier is combined into a strong classifier in a certain way.

The detection module requires virtual memory load, processor load, and detection capabilities. We perform statistical analysis and processing on the network bandwidth

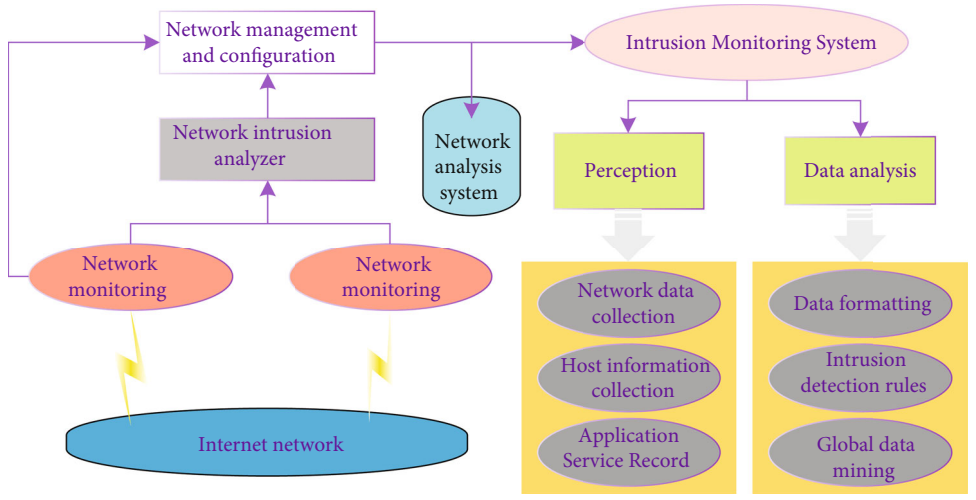


Figure 1: Wireless sensor network-based intrusion detection.

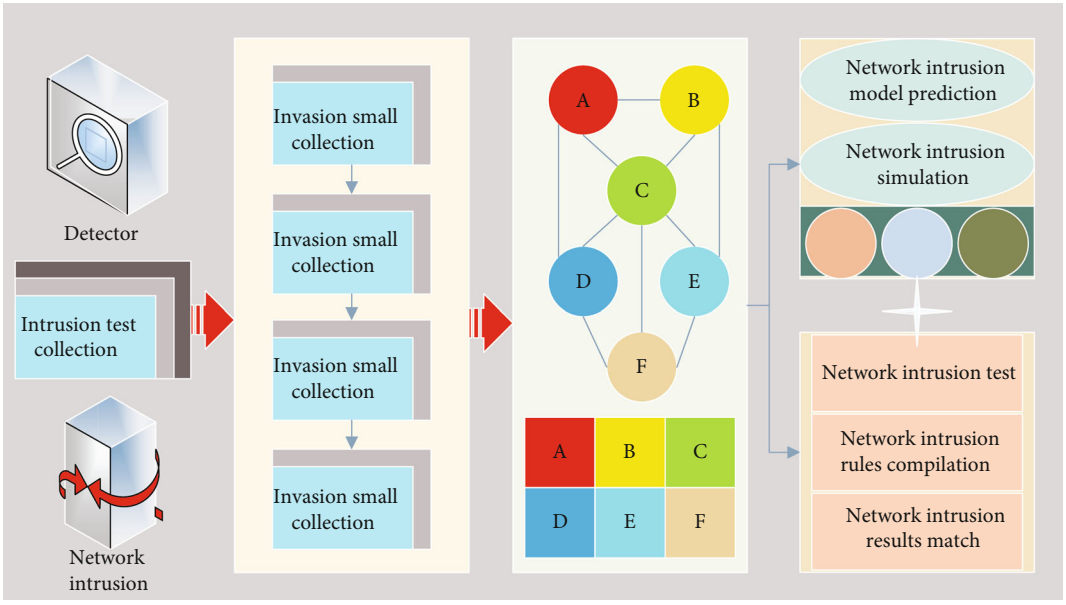


Figure 2: Algorithm integration optimization.

and other characteristics and create a virtual machine performance characteristic score table [21]. The higher the score, the better the detection performance of the virtual machine. The scheduling module queries the performance and resource load of each virtual machine through a specific access protocol. At the same time, the scheduling module calculates the TSD of each detection module according to the performance characteristic score table and records it in the score book of the resource scheduling module. TSD is usually calculated by the following formula:

$$\mathrm{TSD}_i = \frac{\sum_{i=0}^{M} SD_{ij} * T_j * \ln_2 F(i/j)}{\beta * \left(\sum_{j=0}^{N} T_j + 1/2\right)} * 100\%. \quad (5)$$

Using the min–max method, the generated feature data are scaled to the range of [0.1, 0.9], and formula (6) is used in each feature.

$$H(K) = \frac{K - \min}{\max - \min} * \sum_{i=\min}^{\max} F(i), \quad \min \le K \le \max. \quad (6)$$

True Positive (TOP) means to correctly identify the attack sample as an attack sample, True Negative (TON) means to correctly identify a normal sample as a normal sample, False Positive (FOP) means to correct a normal sample misrecognition as an attack sample, and False Negative (FON) means that an attack sample is incorrectly identified as a normal sample. Each evaluation index and the calculation formula of the detection performance of the intrusion detection system are given below.

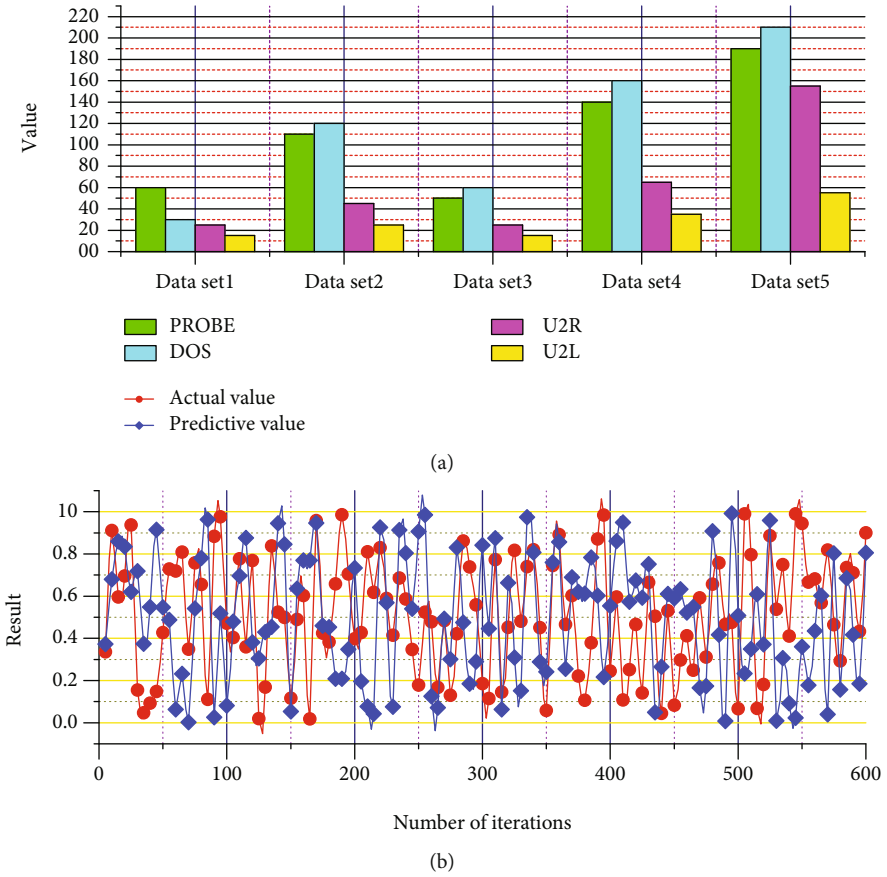


Figure 3: Wireless sensor network intrusion simulation analysis.

Accuracy represents the proportion of the number of samples correctly predicted to all samples, and the formula is as follows:

$$\begin{cases} A = \beta * \dfrac{\text{TOP} + \text{TON}}{\text{TOTAL}} * 100\%, \\ \text{TOTAL} = \text{TOP} + \text{TON} + \text{FOP} + \text{FON}. \end{cases} \tag{7}$$

The detection rate is the ratio of the number of correctly detected intrusion samples to the total number of intrusion samples, as shown in the following formula:

$$B = \beta * \frac{\text{TOP}}{\text{TOP} + \text{FON}} * 100\%. \tag{8}$$

The False Positive Rate (FPR) represents the proportion of normal samples that are falsely reported as intrusive samples to all normal samples, as shown in the following formula:

$$C = \beta * \frac{\text{FOP}}{\text{FOP} + \text{TON}} * 100\%. \tag{9}$$

The False Negative Rate (FNR) represents the proportion of undetected intrusion samples to all intrusion samples, as shown in the following formula:

$$D = \beta * \frac{\text{FON}}{\text{TOP} + \text{FON}} * 100\%. \tag{10}$$

Wireless sensor network simulation technology is often used in the field of wireless sensor network research. This chapter will analyze the performance of wireless sensor network simulation and what is the purpose of analyzing wireless sensor network simulation performance. Next, a brief introduction will be given. The analysis and research of performance lay the foundation for improving the performance of wireless sensor network simulation. Only by first understanding the simulation performance can the simulation performance be improved. For example, when we have a clear understanding of what factors can affect the simulation performance, we can know where to start the research when performing wireless sensor network simulation experiments or when performing wireless sensor network simulation optimization. The subsequent research has a purpose and will greatly reduce blind thinking and behavior in the research process [22]. When the network simulation task is divided, the network simulation topology is divided into multiple small network topologies according to certain algorithms or rules, and the simulation tasks of each small

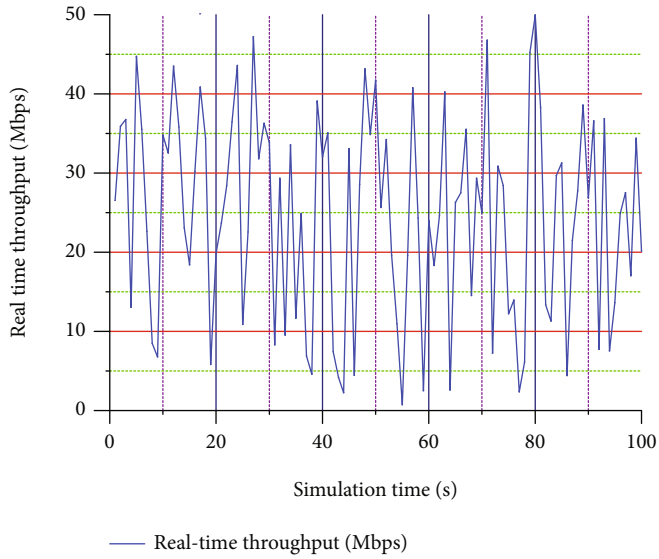


Figure 4: Real-time throughput.

network topology can be assigned to different computing nodes for execution, which can reduce the pressure on the computing nodes. Each computing node is responsible for a corresponding proportion of simulation tasks based on its own performance, so that it will not cause a computing node with a high configuration to be responsible for few simulation tasks and a computing node with a low configuration to be responsible for many simulation tasks, resulting in imbalance of the simulation platform. The more balanced the load, the more stable the distributed network simulation platform, the more reasonable the resource allocation, and the higher its simulation performance.

## 3. Result Analysis

*3.1. Algorithm Simulation Analyses.* In this study, the selected data set is the KDD Cup 100. Usually, in the corresponding simulation experiment research field, the data source selection is quite important, which will inevitably help the experiment. Firstly, the collected data are classified accordingly. Currently, the four main attack methods are scanning, denial of service, unauthorized access by remote users, and unauthorized local super authority. The following uses the corresponding English abbreviations to represent them, respectively. They are PROBE, DOS, U2L, and U2R. The data used in this paper are shown in Figure 3(a), and the classification result is shown in Figure 3(b).

Since the congestion control process of the TCP protocol is difficult and is the focus of the computer network course, for this purpose, the congestion control experiment of the TCP protocol is used as the object to carry out related experiments. Since congestion control is related to link bandwidth, delay, and other parameters, first set the bandwidth and delay of all links as follows: the link between R3 and R4 is set as the bottleneck link, the bandwidth is set to 20 Mbps, the delay is 160 ms, and the bandwidth of all links between routers is set to 100 Mbps with a delay of 160 ms;

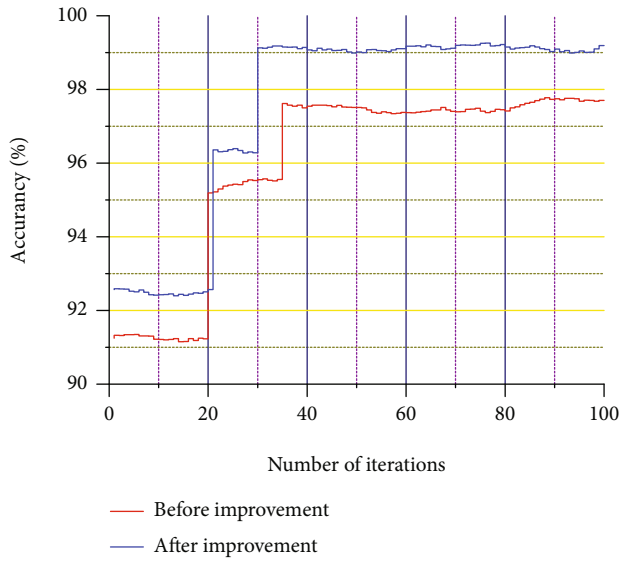


Figure 5: The number of iterations and accuracy curve.

the link bandwidth from all hosts to the connected routers is set to 100 Mbps with a delay of 10 ms. The wireless sensor network performance test tool is installed on hosts H1 and H3, the TCP traffic sending from the hosts H1 to H3 is started, and the throughput is recorded in real time. The real-time throughput of the first 50 seconds is shown in Figure 4.

*3.2. Algorithm Performance Analyses.* Figure 5 shows the comparison curve of iteration times and accuracy between the improved intrusion algorithm and the unimproved intrusion algorithm. As shown in Figure 5, the improved intrusion algorithm converges at the 18th generation iteration, and the model training accuracy rate at convergence is 98.87%. Although this method is slightly slower than the

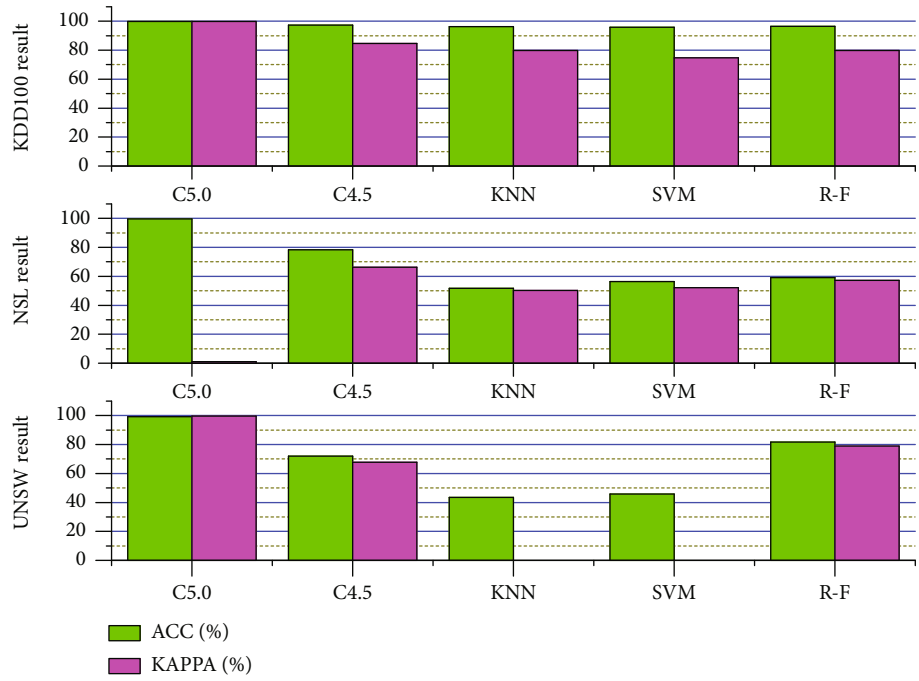


Figure 6: Feature binary classification results.

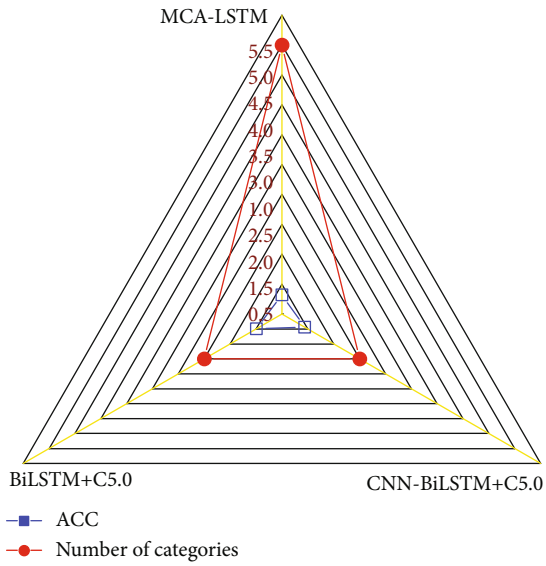


Figure 7: Model ACC value comparison.

unimproved intrusion algorithm training speed, this method improves the accuracy of the model.

It can be seen from Figure 6 that compared with the other four classifiers, the C5.0 classifier has the best feature classification performance, followed by C4.5. The ACC values of the C5.0 classifier are 99.91% (KDD100), 99.61% (NSL), and 99.29% (UNSW). Compared with the method in the literature, with the ACC value of 93.12% (KDD100), 80.12% (NSL), and 78.41% (UNSW), the proposed method is superior. The Kappa values of the C5.0 classifier proposed in this paper are 99.9% (KDD100), 1.00% (NSL), and 99.62% (UNSW). It can also be reflected from Figure 6 that when testing the classification performance of the same data set, not only does the SVM classifier consume the most time, but also, the overall ACC of the classification is lower than that of other classifiers.

Through comparison, the two-class ACC values of the three models of MCA-LSTM, CNN-BiLSTM+C5.0, and BiLSTM+C5.0 on the NSL data set are 80.39%, 93.87%, and 99.57%, respectively. The results are shown in Figure 7. Among them, the two-classification performance on LSTM is the best, the two-classification performance of CNN-BiLSTM+C5.0 is second, and the performance of MCA-LSTM is relatively weak. In addition, the five-class ACC values of the MCA-LSTM and BiLSTM+C5.0 models are 82.16% and 99.68%, respectively. Based on the above data, it can be seen that the classification performance of the CNN-BiLSTM+C5.0 and BiLSTM+C5.0 models has a greater improvement than that of the MCA-LSTM model. The classification ACC of the BiLSTM+C5.0 model is significantly higher than the classification ACC of the CNN-BiLSTM+C5.0 model. In today's large-scale wireless sensor network environment with complex traffic data, a method with stronger classification performance and better adaptability is needed to deal with the current network environment. The excellent classification performance of the BiLSTM+C5.0 model is more suitable for the current network environment.

*3.3. Algorithm Result Analyses.* In order to test the performance of the model after outlier detection, it is compared with the traditional radial basis neural network model based on the gradient descent on the premise of using the same training samples. The program is run 100 times. While comparing the average accuracy, it also uses the variance index to compare the stability between the two. The comparison

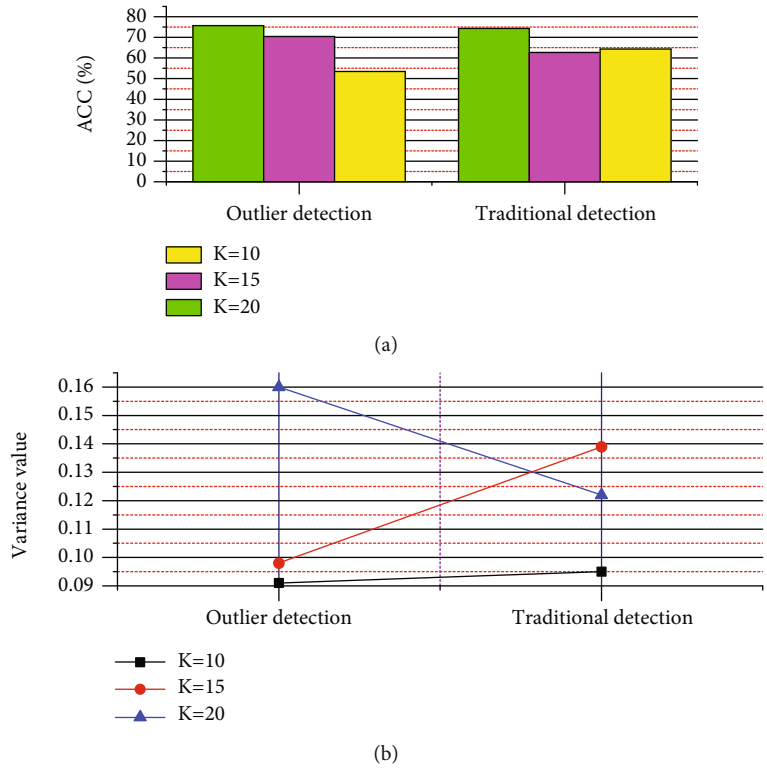


Figure 8: Wireless sensor network classification error graph.

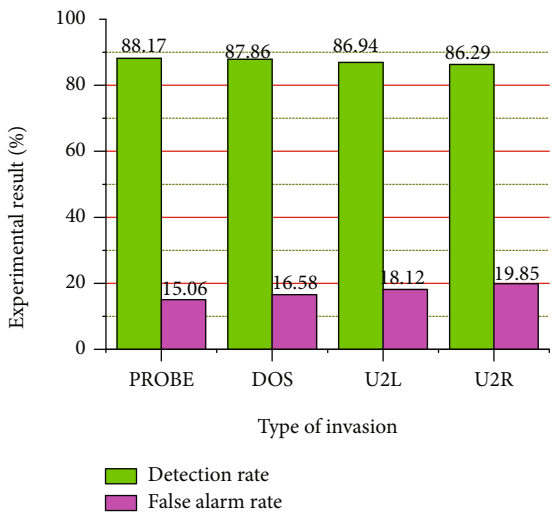


Figure 9: Algorithm detection result.

of experimental results is shown in Figure 8 below. When the number of hidden nodes selected is 5, the experimental results are shown in Figure 8. When the number of hidden nodes selected is 10, the experimental results are shown in Figure 8. When the number of hidden nodes selected is 15, the experimental results are shown in Figure 8. Figure 8(a) is the accurate results of the algorithm for different $k$ values, and Figure 8(b) is the algorithm variance for different $k$ values. Analyzing the above experimental results, it can be seen that although the effect may be biased when $K = 15$, as a whole, selecting the initial values of the parameters of the gradient descent method for outlier detection can obtain relatively high accuracy, and the relatively low variance improves the performance and stability of the model.

We train 4 kinds of data sets and test them. Figure 9 shows the data analysis results. The specific detection effect of the wireless sensor network intrusion algorithm is generally better in the detection of the four types of attack behaviors, and it has a strong wireless sensor network security defense function. The detection rate has reached an ideal effect, but there are also individual intrusions that cannot be accurately detected. The false alarm rate is high, and the experimental results are unstable. Sometimes, the highest false alarm rate is 19.85%. In terms of wireless sensor network intrusion algorithms based on unsupervised learning, from the perspective of the overall detection rate index, although the expected goal is achieved, the shortcomings still cannot be ignored, and individual intrusions cannot be detected.

The detection rates and false alarm rates of the four types of attacks are shown in Figure 10. We can see that the detection rates of DOS attacks and Probing attacks are very high, 94.31% and 94.61%, respectively, but the detection rates of U2R and R2L are different. They are not very high. This is because the amount of data in R2L and U2R attacks is small, and it is easy to form misjudgements. The experimental results show that the algorithm proposed in this paper can effectively distinguish normal data from abnormal data. In terms of detecting these intrusion attack samples, the algorithm adopted in this paper is superior to the BP neural network algorithm optimized by the bee colony algorithm in

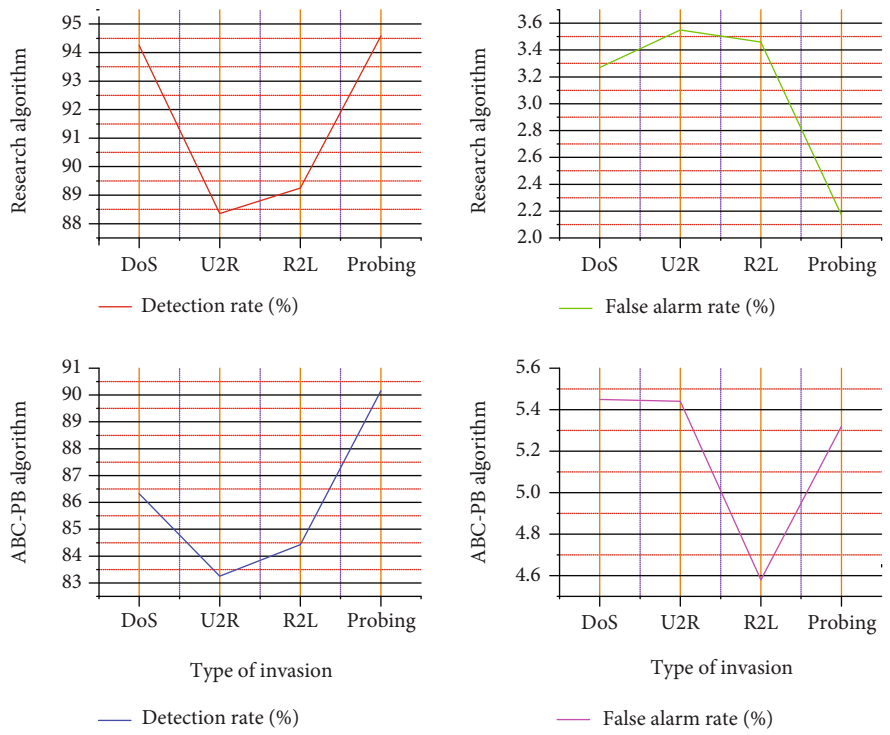


Figure 10: Analysis of algorithm intrusion detection results.

terms of accuracy and detection performance and has a higher detection rate and a lower false alarm rate.

## 4. Conclusion

Carrying out research on intrusion detection technology facing the Internet environment is the primary issue to ensure the security of Internet services, in order to improve the problem of low detection accuracy and high false alarm rate caused by high-dimensional data. The information gain feature selection algorithm is used to select the optimal feature subset to reduce the problem of high data dimensions. Through the multivariate correlation analysis algorithm, the feature subset is transformed from a text type to a gray-scale image, which enhances the time correlation of the data, and creates a data advantage for the long- and short-term memory wireless sensor network, in order to avoid designing feature extraction algorithms to extract the features of high-dimensional intrusion data. The thesis studies the wireless sensor network intrusion detection model based on the Internet environment and has achieved certain results. However, there are still many shortcomings in the research, and there is still a certain gap with the actual application. In the follow-up research work, we consider the real time and adaptability in the actual wireless sensor network environment to make relevant demonstrations. By simplifying and perfecting the parameter tuning process in deep learning model training, the model time cost and results will be further improved. In follow-up research, we try to introduce other deep learning models.

## Data Availability

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

## Conflicts of Interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgments

This work was supported by the Tongfang Knowledge Network Technology Co., Ltd. (Beijing) and OpenStack Private Cloud System.

## References

[1] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida, "New anomaly network intrusion detection system in cloud environment based on optimized back propagation neural network using improved genetic algorithm," *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 61–84, 2019.

[2] S. Venkatraman and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," *Multimedia Tools and Applications*, vol. 79, no. 5-6, pp. 3993–4010, 2020.

[3] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based

on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[4] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 493–501, 2019.

[5] E. Besharati, M. Naderan, and E. Namjoo, "LR-HIDS: logistic regression host-based intrusion detection system for cloud environments," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 9, pp. 3669–3692, 2019.

[6] R. H. Dong, X. Y. Li, Q. Y. Zhang, and H. Yuan, "Network intrusion detection model based on multivariate correlation analysis – long short-time memory network," *IET Information Security*, vol. 14, no. 2, pp. 166–174, 2020.

[7] G. Vaseer, G. Ghai, and D. Ghai, "Novel intrusion detection and prevention for mobile ad hoc networks: a single-and multiattack case study," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 35–39, 2019.

[8] A. Verma and V. Ranga, "Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1571–1594, 2019.

[9] K. Siddique, Z. Akhtar, F. Aslam Khan, and Y. Kim, "KDD Cup 99 data sets: a perspective on the role of data sets in network intrusion detection research," *Computer*, vol. 52, no. 2, pp. 41–51, 2019.

[10] Y. Qi, "Computer real-time location forensics method for network intrusion crimes," *IJ Network Security*, vol. 21, no. 3, pp. 530–535, 2019.

[11] L. Deng, D. Li, X. Yao, and H. Wang, "Retracted article: mobile network intrusion detection for IoT system based on transfer learning algorithm," *Cluster Computing*, vol. 22, no. S4, pp. 9889–9904, 2019.

[12] W. Liang, K. C. Li, J. Long, X. Kui, and A. Y. Zomaya, "An industrial network intrusion detection algorithm based on multifeature data clustering optimization model," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2063–2071, 2020.

[13] W. Wu, R. Li, G. Xie et al., "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 919–933, 2020.

[14] T. Ling, L. Chong, X. Jingming, and C. Jun, "Application of self-organizing feature map neural network based on K-means clustering in network intrusion detection," *Computers Materials & Continua*, vol. 61, no. 1, pp. 275–288, 2019.

[15] D. Li, Z. Cai, L. Deng, X. Yao, and H. H. Wang, "Information security model of block chain based on intrusion sensing in the IoT environment," *Cluster Computing*, vol. 22, no. S1, pp. 451–468, 2019.

[16] Y. Hamid, L. Journaux, J. A. Lee, and M. Sugumaran, "A novel method for network intrusion detection based on nonlinear SNE and SVM," *International Journal of Artificial Intelligence and Soft Computing*, vol. 6, no. 4, pp. 265–286, 2018.

[17] M. C. Chen, S. Q. Lu, and Q. L. Liu, "Uniqueness of weak solutions to a Keller-Segel-Navier-Stokes model with a logistic source," *Applications of Mathematics*, pp. 1–9, 2021.

[18] A. Davahli, M. Shamsi, and G. Abaei, "Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 5581–5609, 2020.

[19] F. E. Ayo, S. O. Folorunso, A. A. Abayomi-Alli, A. O. Adekunle, and J. B. Awotunde, "Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection," *Information Security Journal: A Global Perspective*, vol. 29, no. 6, pp. 267–283, 2020.

[20] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9042–9053, 2019.

[21] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Rule generation for signature based detection systems of cyber attacks in IoT environments," *Bulletin of Networking, Computing, Systems, and Software*, vol. 8, no. 2, pp. 93–97, 2019.

[22] V. Kanimozhi and T. P. Jacob, "Calibration of various optimized machine learning classifiers in network intrusion detection system on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," *International Journal of Engineering Applied Sciences and Technology*, vol. 4, no. 6, pp. 209–213, 2019.