Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2017) 25: 2737 – 2748
© TÜBİTAK
doi:10.3906/elk-1603-248

Study on the recognition method of airport perimeter intrusion incidents based on laser detection technology

Huazhu WU[1,*], **Zengcai WANG**[2], **Changyou WANG**[1]
[1]Department of Automation, Faculty of Electronics & Information Engineering, Dalian Jiaotong University, Dalian, P.R. China
[2]Department of Automation & Electronics, City Institute, Dalian University of Technology, Dalian, P.R. China

Received: 24.03.2016 • **Accepted/Published Online:** 20.10.2016 • **Final Version:** 30.07.2017

Abstract: Currently, detection technology is very important for airport perimeter security. When the perimeter is invaded or destroyed, the perimeter security alarm system can promptly alert personnel. In this paper, based on analysis and comparison of several detection technologies commonly used in airport perimeter security and according to the characteristics of airport perimeters and laser detection, an airport perimeter security alarm system based on laser detection is proposed. It analyzes factors that affect the performance of a laser alarm system, divides intrusions into six categories, estimates the different alarm thresholds by testing, and judges the intrusion category according to the number of blocked laser beams and the duration of the block. In order to improve the rapid response and the robustness of the system, it uses a pattern recognition method based on radial basis function neural network technology to train and learn different samples of intrusion categories, uses the classifier to determine the cluster center of each sample node, and uses the weights of the center variance and the weights of hidden nodes to establish the alarm curve of each intrusion category. Meanwhile, when the feature value of an intrusion sample is distributed along the classification boundary of two categories, it uses Bayes' theorem to calculate the probability of an invasive category to reduce the false alarm risk. According to sample testing, the above recognition method of airport intrusions based on laser detection technology effectively improves the intrusion detection probability.

Key words: Pattern recognition, neural network, Bayesian theory, laser detection

1. Introduction

Currently, detection technologies for airport perimeter security usually include vibration cables, infrared detection, microwave detection, underground cables, tension fencing, video surveillance, and other technologies, but it is rare that laser detection technology is used [1,2]. Compared with those detection technologies, laser technology has many advantages: high density of transmitted power, small divergence angle, concentrated light beam, and adaptability to poor weather and environmental conditions. Under the same conditions, the power density is hundreds to thousands of times that of infrared light-emitting diodes, the detection range is up to several hundred meters or several kilometers, the transmission attenuation is much smaller than other similar detectors, and it has a strong ability to penetrate rain and fog so it can greatly reduce false alarms due to the impact of climate and environment [3,4].

The circumference of an airport perimeter can range from a few kilometers to tens of kilometers. The

[*] Correspondence: dlwhzh@163.com

scope of its protection is relatively long and vast. The illustrative graphics of an airport perimeter are shown in Figure 1.

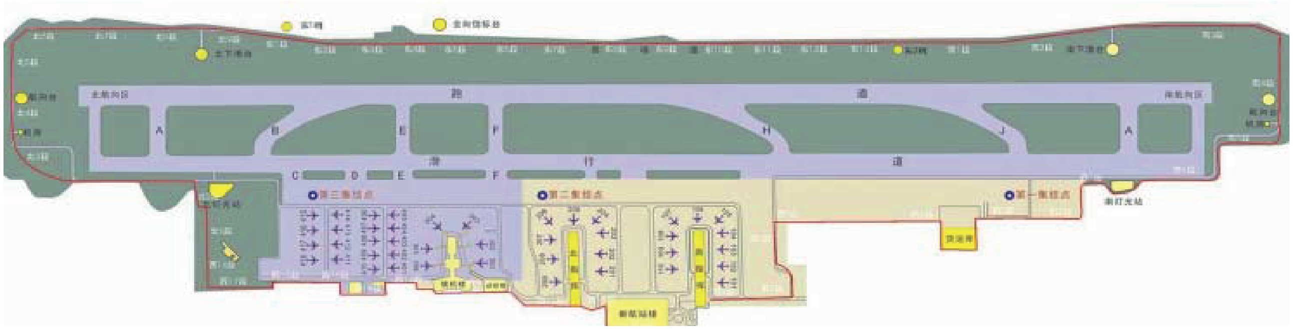

Figure 1. Illustrative graphics of an airport perimeter.

In view of the characteristics of airport surroundings, the laser antiintrusion security system is divided into three parts: the decision-making system, the monitoring system, and the front-end laser detection system. The configuration diagram of the antiintrusion laser alarm system is shown in Figure 2.

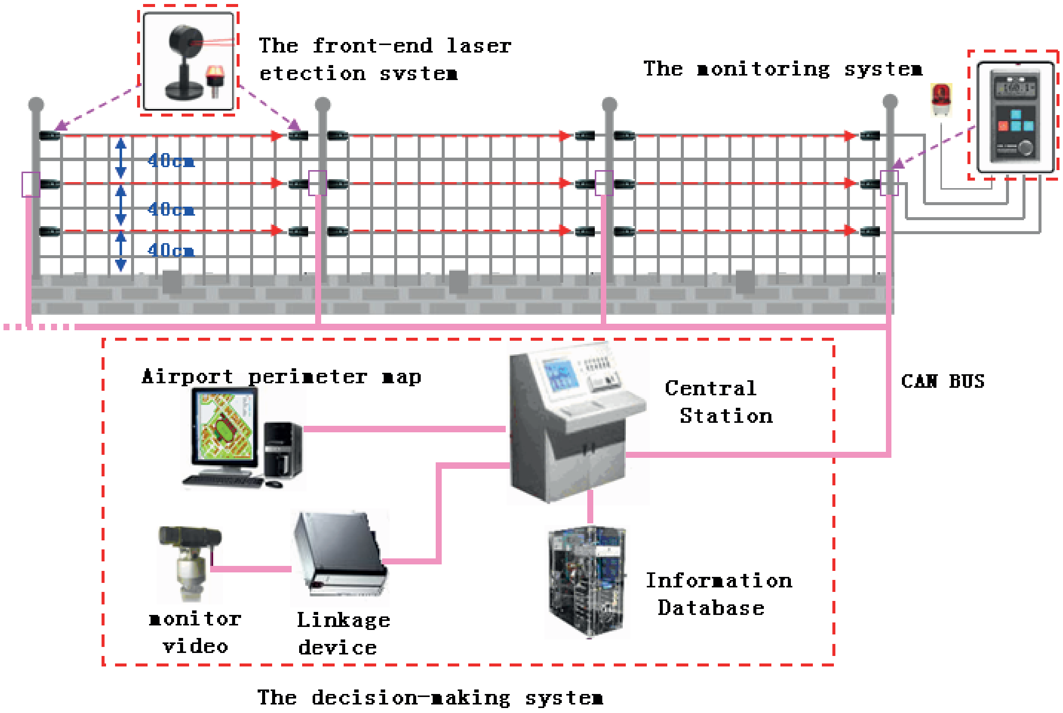

Figure 2. An antiintrusion laser alarm system.

The front-end laser detection system is made up of a laser correlation device group. In order to enhance the recognition capabilities of the security system, three sets of transceiver devices are respectively placed at heights of 40, 80, and 120 cm, which correspond to the heights of a human's lower leg, waist, and breast. Because the high performance of intrusion prevention is very important, the stability of the laser transmitter is crucial. The system uses a military-grade laser transmitter, device model EL65D80IG4. Its parameters are as follows: 0.1 mrad laser divergence angle, 980 nm probe laser wavelength, >1 kHz laser modulation frequency,

>1000 m detection range, >60 mw light emitting power, and –40 °C to 70 °C working temperature. The laser transmitter and the optical receiver are shown in Figure 3. The receiver circuit of the optical signal is shown in Figure 4.

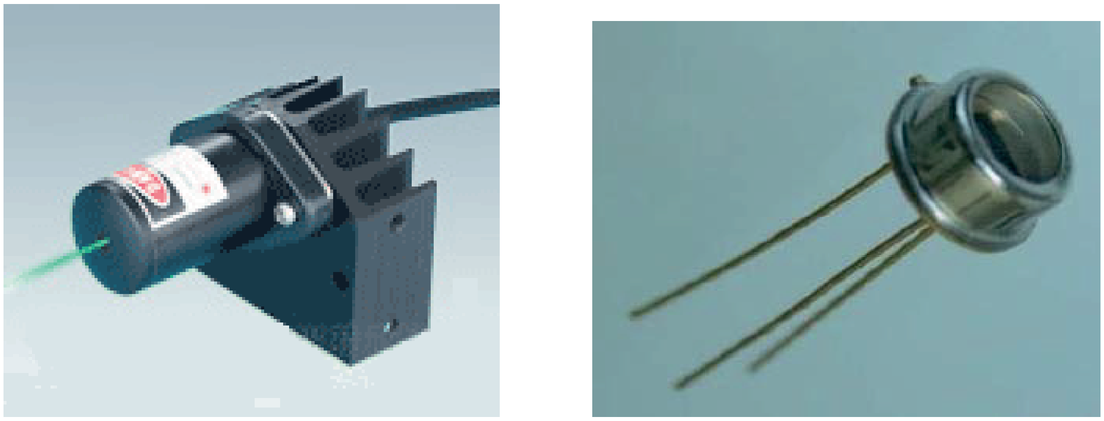

Figure 3. Laser transmitter and its supporting optical receiver diode.

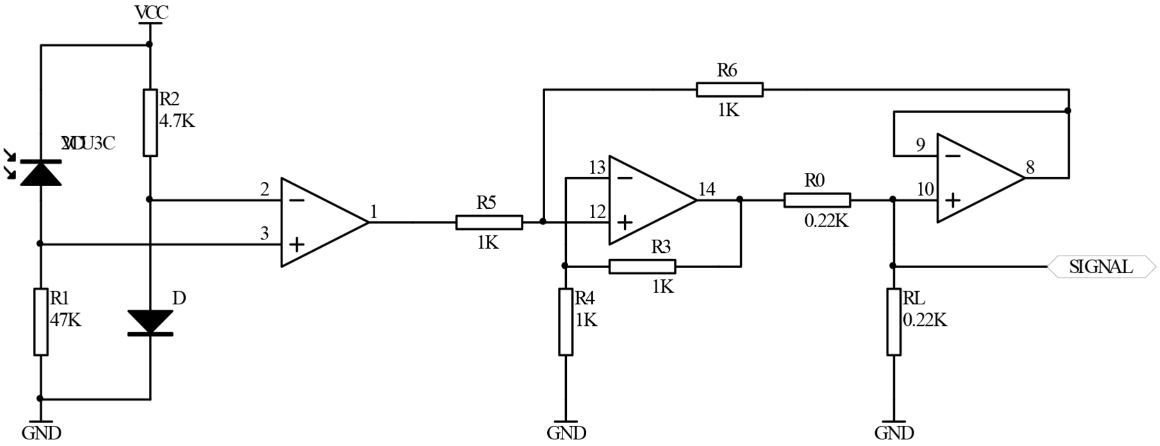

Figure 4. Receiver circuit of the optical signal.

The monitoring system uses an LM3S8962 microcontroller of ARM, which offers 64 KB of SRAM, 256 KB of flash memory, and a rich peripheral interface for extensions, including a CAN bus interface, an Ethernet controller interface, and a JTAG interface. It is shown in Figure 5. It detects the laser signal in real time to judge whether an intrusion occurred, records the duration of the block, and transmits the data to the decision-making system via CAN bus.

The decision-making system is a control system based on a computer, which determines whether an invasion occurred and the type of invasion according to the data from the monitoring system. If an intrusion occurs and threatens security, it will drive the linkage device and video monitor to the alarm zone.

2. Sample statistics and analysis

Intrusion incidents for airport perimeters are usually divided into six categories: human, large animal, small animal, small bird, large bird, and other debris. The laser detector is mainly used to identify human intrusion.

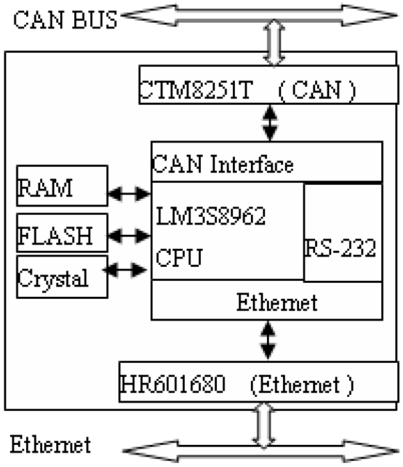

Figure 5. Extended interface based on the LM3S8962 microcontroller.

For animal and bird intrusions, the number of blocked lasers is different from individual to individual. Large animals (such as cattle), which are similar in size to humans, block a maximum of three lasers while small animals (such as antelope) block a maximum of only two. Similarly, the number of blocked lasers is not same for large birds and small birds, so the number of the blocked lasers can be used to judge the kind of intrusion.

In addition to the number of blocked laser beams, another indicator is the duration of the block. Humans and large animals can both block off three emission devices, but they are distinguishable from each other by looking at the duration of the laser block. Because the walking speeds of humans and animals are different from each other, and the body structures of different species are different, the corresponding duration of the blocked laser is different at different heights. These are important criteria for categorizing an intrusion. For example, the flying speed of birds is quite fast, but the wingspan of large birds is wide compared with small birds, so the duration of the blocked laser is longer for large birds than for small birds.

In the experiment, we measured the time it took for people to pass through three sets of laser detection devices. At the same time, we did some interference experiments, such as with plastic bags and advertising flyers, and recorded how long they blocked the devices.

The distribution of the original data points is shown in Figure 6. The horizontal axis of Figure 6 is the serial number of data points, and the vertical axis is the time value. Since the unit of time in the experimental data is 10 ms, the value of the ordinate in Figure 6 multiplied by 10 is the blocked time of a laser detector. Numbers 1–34 on the horizontal axis correspond to the blocked duration of the lower laser detector, 35–68 correspond to the blocked duration of the middle laser detector, 69–102 correspond to the blocked duration of the upper laser detector, 103–122 correspond to the blocked duration of the paper, and 123–134 correspond to the blocked duration of the hard plastic.

The height of the lower laser detector was 40 cm, corresponding to a human's lower leg. When the legs pass through the laser detector, sometimes a block occurs twice, or when one leg is stepping on the grating, the barrier may have a longer duration. A situation where the lower laser detector was blocked twice is shown in Figure 7.

In a separate test, 30 samples each of six different categories were collected, for a total of 180 samples. Each sample data point corresponds to the duration of the block in the upper, the middle, and the lower laser devices. The number of blocked laser detectors and the duration for different intrusions, according to testing and statistical analysis, are listed in Table 1, and the differences among the above-mentioned categories of intrusions can be observed from the data in Table 1.

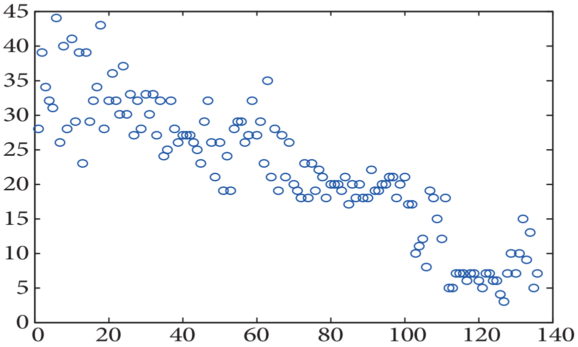

Figure 6. Distribution of the original points.

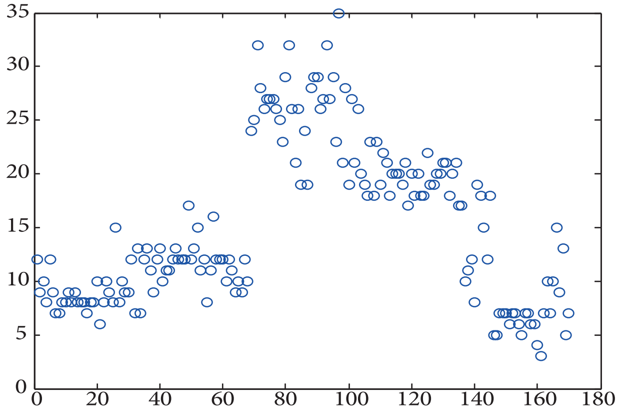

Figure 7. Describing the block points of instances when the lower laser was blocked twice.

Table 1. The number of blocked lasers and duration of the block for different intrusions.

Intrusion category	Number of blocked lasers	Up-way time (ms)	Midway time (ms)	Low-way time (ms)
Human	3	24	26	28
Human	3	18	28	32
Human	3	19	27	40
Large animals	2	0	20	50
Large animas	2	0	70	780
Large animas	3	5	40	540
Small animals	1	0	0	50
Small animals	1	0	0	340
Small animals	1	0	0	760
Large birds	1	2.34	0	0
Large birds	1	0	2.76	0
Large birds	1	0	0	1.98
Small birds	1	0.54	0	0
Small birds	1	0	0.48	0
Small birds	1	0	0	0.39
Other subjects	1	5	0	0

Table 2. RBF network classification results.

Intrusion category	Classification accuracy	Total accuracy
Human	99.75%	99.50%
Large animals	99.30%	
Small animals	99.76%	
Large birds	98.97%	
Small birds	99.80%	
Other subjects	99.43%	

3. The classification and recognition of the radial basis function (RBF) neural network

Intrusion incidents at airport perimeters can be divided into six categories. The classification of incidents is a process of pattern recognition: correct classification and description by the cognition of things. Current pattern recognition methods have tended to use artificial intelligence, including expert systems, fuzzy theory, genetic algorithms, neural networks, and other methods. Among these methods, artificial neural networks have the unique capability of processing nonlinear information and distributed storage ways for information [5].

The RBF neural network is a two-forward type neural network. The intermediate layer node's output is the value of the RBF. The network model is shown in Figure 8. $X = \{x_1, x_2, \ldots, x_n\}$ are n-dimensional input vectors and the output of the hidden layer nodes are the RBF values. The hidden layer unit performs a nonlinear transformation, which is the input mapping to a new space. Commonly, RBF is a Gaussian function and its expression is as follows:

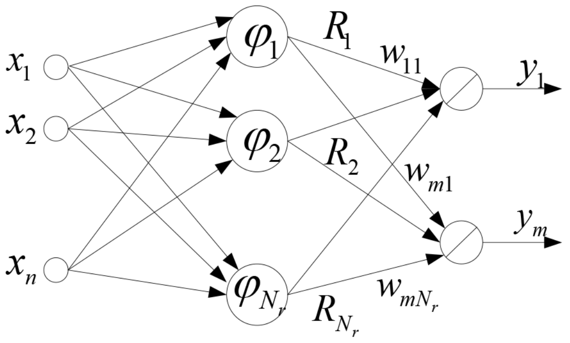

Figure 8. The structure of the RBF neural network.

$$R_j = \varphi_j(X) = e^{-\|X - C_j\|^2/(2\sigma_j^2)}, j = 1, 2, \ldots, N_r \tag{1}$$

C_j is the center of the jth Gaussian function of the hidden layer, and σ_j^2 is the normalization parameter of the j hidden layer nodes, namely its variance. $\|X_i - C_j\|^2 = \sum_{i=1}^{n} (x_i - c_{ij})^2$, and the value of R_j is located in (0, 1); if the input vector X is closer to the center point, the output value is closer to 1. Conversely, if the input vector X and the center point are farther away, the output value is closer to 0. The output of the RBF neural network is a linear combination of the output of the hidden units.

$$y_i = \sum_j w_{ij} R_j, i = 1, 2, \ldots, p \tag{2}$$

$y_1, y_2, \ldots, y_p$ are the output vectors and w_{ij} is the weight of the hidden nodes to the output nodes. The RBF network converts the M-dimensional original space to P-dimensional output space by this nonlinear mapping.

In the RBF network, there are three parameters determined by dynamic learning: the center vector C_j, the center vector variance σ_j^2 of the Gaussian function, and the weight vector w_n of the hidden layer nodes to the output layer nodes. The center of the Gaussian function can be obtained by clustering. Common clustering methods are the k-means method, nearest neighbor method, etc. For the determination of the Gaussian center vector, its variance calculation is given by Eq. (3).

$$\sigma_j^2 = \frac{1}{M_\text{i}} \sum_{X(k)\in class(i)} \left\| X(k) - C_i \right\|^2, i = 1, 2, \cdots, N_r \tag{3}$$

When the above parameters have been determined, the weight vector of the hidden nodes to the output layer nodes can be obtained by dynamic learning. The RBF neural network will be constructed and then it can be used to classify new samples.

The characteristics of RBF neural networks are as follows: learning ability, nonlinear mapping ability, distributed storage, high dimensionality, and high flexibility. They can applied in the fields of classification and identification and improve classification accuracy and performance in the RBF [6].

4. Classifier design of intrusion samples based on RBF

The design of the classifier is important in pattern recognition, which studies sample data to effectively and correctly classify items into different categories. It determines the final judgment effect [7]. In actual application at airport perimeters, the probability of misjudgment should be very small. Otherwise, it is very difficult to have actual application value. The following describes the classifier of the RBF neural network and how to achieve the process and the parameters.

The design process of the classifier determines the hidden node cluster center, the center of variance, weights of hidden nodes, and the output nodes. It can achieve classification and recognition after the above parameters are determined. The hidden node cluster variance is determined by the K-means clustering method and its implementation steps are as follows:

Suppose that there are N input sample vectors $\{X(k), k = 1, 2, \cdots, N\}$.

(1) Initialization: $t \leftarrow 0$, $C_j(0)$ randomly selected N_r training sample value as $C_j(0)$.

(2) (a) $k \leftarrow 1$, (b) input $X(k)$, (c) calculate the distance between $X(k)$ and each $C_j(t)$, calculate the minimum distance $d_j = \left\| X(k) - C_j \right\|^2, d_q = \min\{d_j\}$, (d) assign $X(k)$ to the class q, denoted as $X(k) \in class(q)$, (e) $t \leftarrow t + 1$ and go to (b) until $k \geq N$.

(3) Calculate each C_j, $C_j = \frac{1}{M_\text{j}} \sum_{X(k)\in class(j)} X(k), j = 1, 2, \cdots, N$, where M_j is the number of samples $X(k) \in class(j)$.

(4) $t \leftarrow t + 1$, go to (2) until each C_j reaches convergence.

The $class(q)$ in the aforementioned algorithm represents the subsets of training samples that belong to the q class model (around C_q); it is { the subject of all $X(t)$ with C_q center distance recent } = $class(q)$.

The clustering procedures are as follows:

```
While ( flag_stop_circule > 0.001 )
{ for ( i = 0; i < m_train_count*model_count; i++ )
        {for ( j = 0; j < m_hid_count; j++) // calculate the distance between the cluster center and each sample
{sum_distance[j] = dist(train_sample[i].m_sour,clustering[j].m_sour,m_in);}
        flag_location[i] = min_subscribe(sum_distance,m_hid_count);
//Calculate minimum distance subscript} // calculate the new cluster centers
        for (i = 0; i < m_hid_count; i++)
{for ( j = 0; j < m_in; j++ ){ clustering_temp[i].m_sour[j] = clustering[i].m_sour[j];
// Temporary storage of the current cluster centers}
                initialtozero(clustering[i].m_sour,m_in);}
        initialtozero(sum_distance,m_hid_count);
        for ( i = 0; i < m_train_count*model_count; i++)
        {for (j = 0; j < m_in; j++ )
        {clustering[flag_location[i]].m_sour[j] = train_sample[i].m_sour[j]// Adding the same class sample}
        sum_distance[flag_location[i]] = sum_distance[flag_location[i]]+1.0;
// Statistical number of certain category samples}
            for ( i = 0; i < m_hid_count; i++ )
            {for ( j = 0; j < m_in; j++ )
        {If (sum_distance[i]! = 0)
        clustering[i].m_sour[j] = sum_distance[i];
// calculate the new cluster centers} }
        for ( i = 0; i < model_count; i++ )
        {sum_distance[i] = dist(clustering[i].m_sour,clustering_temp[i].m_sour,m_in);// calculate the distance between each category }
        flag_stop_circule = max(sum_distance,model_count);//Stop condition
        cout << ”flag_stop_circule=” << flag_stop_circule << endl;}
```

After completing the clustering, the formula of the normalization-seeking parameter σ_j^2 is

$$\sigma_j^2 = \frac{1}{M_{\mathrm{j}}} \sum_{X(k)\in class(j)} \left\| X(k) - C_j \right\|^2 \quad , \tag{4}$$

where M_j is the number of $X(k) \in class(j)$ in $\{X(k)\}$.

The cluster variance procedures are as follows:

```
for (i = 0; i < m_train_count*model_count; i++)
{drta[flag_location[i]]+= dist(train_sample[i].m_sour,clustering[flag_location[i]].m_sour,m_in);
sum_temp[flag_location[i]] = sum_temp[flag_location[i]]+1.0;} ;
```

The weights between the hidden layer and the output layer are determined by the energy minimization criterion; it is the smallest difference between the actual output results with theoretical output. The error energy function is as follows:

$$E(W) = \frac{1}{2} \sum_k \sum_j \left(d_j(k) - y_j(k)\right)^2 \xrightarrow{W} \min \tag{5}$$

The network output result is calculated as follows:

$$y_j(k) = \sum_{i=0}^{N_r} W_{ji} \varphi_i(X(k)) = \sum_k W_{ji} R_i, \quad \varphi_i(X(k)) = R_i \tag{6}$$

The updating formula of the output layer weights is as follows:

$$\Delta W_{ji}(k) = \alpha(d_j(k) - y_j(k))R_i, \quad W_{ji} \longleftarrow W_{ji} + \Delta W_{ji} \tag{7}$$

The procedure of output layer weights is as follows:

```
while(flag_stop_circule > 0.001)
{       for (i = 0; i < m_train_count*model_count; i++)
        {initialtozero(y,m_out);
        assignment(w,w_temp,m_hid_count,m_out); // Assignment operator
        for (j = 0; j < m_hid_count; j++)
        {R[j] = rbf_function(train_sample[i].m_sour,clustering[j].m_sour,drta[j],m_in);// The output value of the
middle layer }
                for (m = 0; m < m_out; m++)// Output layer
                {for (n = 0; n < m_hid_count; n++)// Hidden layer
                {y[m]+ = w[m][n]*R[n];}
                for (n = 0; n < m_hid_count; n++)
                {drta_w[m][n] = alfa*(train_sample[i].m_des[m]-y[m])*R[n];
// Weights change} }
                For (m = 0; m < m_out; m++)
                {for (n = 0; n < m_hid_count; n++)
                {w[m][n]+ = drta_w[m][n]; } }
                initialtozero(sum_temp,m_out);
                For (m = 0; m < m_out; m++)
                {sum_temp[m] = dist(w_temp[m],w[m],m_hid_count);   }
                flag_stop_circule = max (sum_temp,m_out);       } }
```

In the actual construction process, the network hidden layer RBF is taken as a Gaussian function, which has a sensitive response only to the vectors of nearby area and not to other regions. The output layer of the network uses the competitive output approach, the so-called competition output, where the maximum network output node is set to 1 when it is output but the output values of the other nodes are set to 0, so that only one element of each output vector is 1 every time, thereby avoiding the rejection problem.

The input of the RBF network is the dimension of the sample characteristic vector, so the number of input nodes in the network is the same as the dimensions of the sample mode. Each mode in the present experiment is 4-dimensional data, so the input node of the RBF network is 4. Owing to output layer nodes corresponding to the respective modes of coding, the coding and pattern are the same as the number of categories of the respective modes, so the output layer node is 6. Through experimentation, the number of hidden nodes can be selected based on the highest classification accuracy. The number of hidden nodes is 48, and therefore the classification model of the RBF neural network is 4-48-6.

5. Analysis of the alarm threshold

The decision process of the decision-making system is actually a classification and identification process. In order to accurately establish the alarm threshold of each intrusion category, it is very critical to effectively improve intrusion detection accuracy for the decision-making system. Based on experimental data that we collected for 180 samples, as well as sample data in Table 1, we use the MATLAB HIST () function to parse the probability distribution of sample data to verify the reasonableness of all kinds of alarm thresholds in Table 1 [8].

Figures 9–12 show the distribution of sample data that each laser transceiver collected. The probability distribution of the sample data from the upper laser detector is shown in Figure 9, the probability distribution of the sample data from the middle laser detector is shown in Figure 10, the probability distribution of the sample data from the lower laser detector is shown in Figure 11, and the probability distribution of paper is shown in Figure 12.

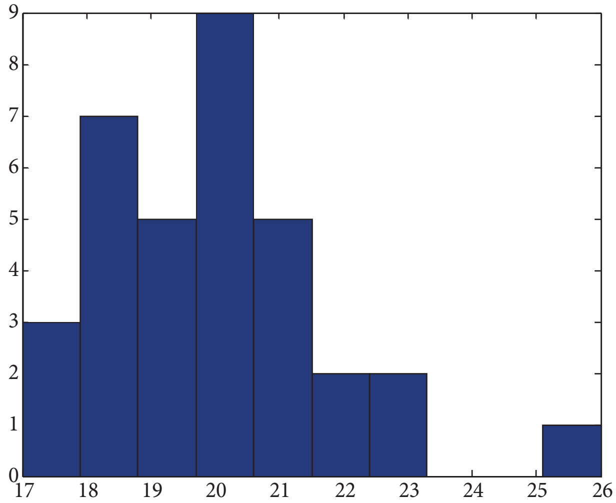

Figure 9. Probability distribution of the upper laser sample data.

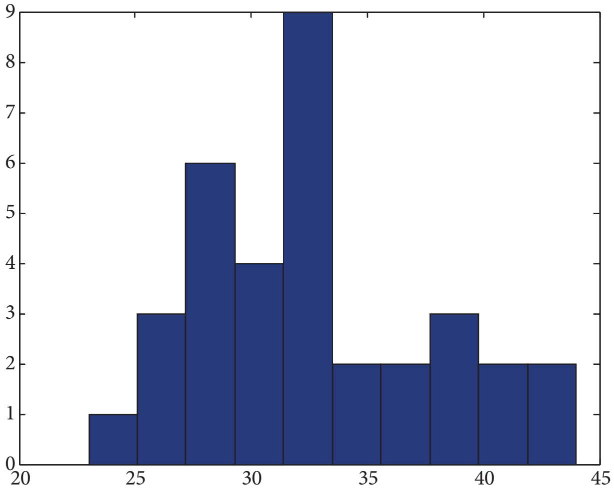

Figure 10. Probability distribution of the middle laser sample data.

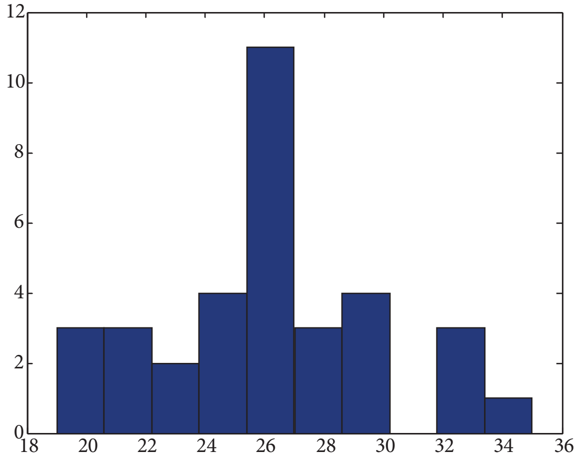

Figure 11. Probability distribution of the lower laser sample data.

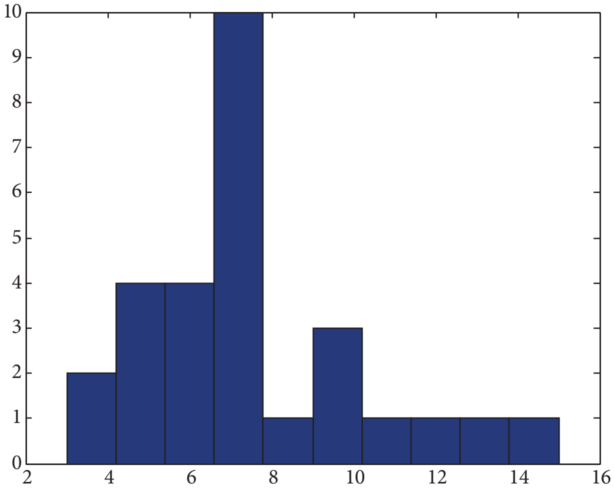

Figure 12. Probability distribution of the paper sample data.

Based on analysis of the sample data, in order to distinguish between humans and animals as well as birds, 150 ms can be set as the threshold of the block duration and 2 is set as the threshold of number of blocked laser detectors. In some special circumstances, the feature values of a sample are distributed along the classification boundary of two categories, such as the blocked duration of a falling plastic bag being very close to the amount of time that people blocked the laser beam with the same number of blocked lasers. This will result in a false alarm. Wrong classifications can hardly be avoided, and the Bayesian decision theory addresses how to make a reasonable decision to minimize risks and losses [9–11].

Because the sample data are distributed regularly, $P(\omega_i\,|x\,)$, a function of class conditional probability density based on Bayesian theory, can be obtained after testing a large amount of sample data [12–14]. When the feature vector x appears, the Bayesian formula can calculate the probability that the sample belongs to the categories. The formula can be expressed as in Eq. (7).

$$P(\omega_i\,|x\,) = \frac{P(x\,|\omega_i\,)P(\omega_i)}{\sum\limits_{j=1}^{m} P(x\,|\omega_i\,)P(\omega_i)} \tag{8}$$

How to calculate the minimum Bayes risk decision-making according to this formula was described in detail in Wu and Wang's study [15].

6. Conclusion

Based on the above structural parameters of the RBF network system, 180 samples were classified and identified. Half of the samples were used as training samples and the other 90 samples were used as test samples to test the classification result. Selection of the training and test samples was random. Test results are the averages of 50 tests and are shown in Table 2.

As seen in Table 2, recognition of airport perimeter intrusion incidents based on the RBF neural network yields better classification results. The classification accuracy of human intrusion is relatively high, meaning that when human intrusion incidents happen and threaten security, the decision-making system can alarm and drive the linkage device and video monitor to the alarm zone, so that it can prevent an illegal intrusion. Compared with traditional classification methods, classification based on the RBF neural network has improved classification accuracy, and its classification speed is so fast that it can take real-time effective action in the case of an intrusion.

Through experimental verification, if the laser beam angle of the transceiver is adjusted to ensure normal signal reception, an identification system of airport perimeter intrusion incidents based on laser detection technology has a number of benefits, including fast response time, constant uptime, and low cost. It can meet the security requirements for an airport perimeter.

Acknowledgment

This project was funded by the Education Department of Liaoning Province and the funding number is L2015100.

References

[1] Liu ZY. Safety monitoring alarm system research and design. Chin J Sec Saf Technol Mag 2008; 1: 39-41.

[2] Li CY. Intrusion alarm detection system. Chin J Polic Technol 2003; 1: 23-24.

[3] Juarez JC, Maier EW. Distributed fiber optic intrusion sensor system. J Lightwave Technol 2005; 6: 13-16.

[4] Cheng Y, Li XZ. Research on anti-jamming laser intrusion detecting equipment. Chin J Laser Infrar 2008; 12: 1204-1206.

[5] Bezerra JMB, Aquino RRB, Oliveira JB, Silveira TMA, Costa EG, Néri MGG, Ferreira TV, Dantas JLP, Mendonça PL. Application of pattern recognition techniques to non invasive insulation monitoring. In: 2008 IEEE International Symposium on Electrical Insulation; 9–12 June 2008; Vancouver, BC, Canada. New York, NY, USA: IEEE. pp. 96-99.

[6] Kim SH, Park BJ, Jang EH, Chung MA. A study on neural network recognizer based on fuzzy rules and fuzzy inference fuzzy driven neural network recognizer in pattern recognition. In: 2014 International Conference on Information Science, Electronics and Electrical Engineering; 26–28 April 2014; Sapporo City, Japan. New York, NY, USA: IEEE. pp. 1913-1917.

[7] Libby V. A wireless perimeter protection and intrusion detection system. In: 44th Annual 2010 IEEE International Carnahan Conference on Security Technology; 5–8 October 2010; San Jose, CA, USA. New York, NY, USA: IEEE. pp. 364-368.

[8] Zhang LF, Lu HM. The research on the application of laser scanning measurement technology in forestry. In: 2009 IEEE International Conference on Mechatronics and Automation; 9–12 August 2009; Changchun, China. New York, NY, USA: IEEE. pp. 4490-4494.

[9] Bencomo N, Belaggoun A. A world full of surprises: Bayesian theory of surprise to quantify degrees of uncertainty. In: 36th International Conference on Software Engineering; 31 May–7 June 2014; Hyderabad, India. pp. 460-463.

[10] Cai LQ, Zheng XS. Risk accident simulation using virtual reality and multi-agent technology. International Journal of Digital Content Technology and Its Applications 2011; 2: 181-190.

[11] Kalantarnia M, Hawboldt K. Dynamic risk assessment using failure assessment and Bayesian theory. J Loss Prevent Proc 2009; 22: 600-609.

[12] Elias HA, Abdelaziz L. Combined anomalies prediction using the Bayesian theory. Qual Reliab Eng Int 2012; 28: 363-367.

[13] Bolstad MW. Understanding Computational Bayesian Statistics. Hoboken, NJ, USA: John Wiley & Sons, 2010.

[14] Weise K, Woger W. Measurement Science and Technology. Philadelphia, PA, USA: IOP Publishing Press, 2009.

[15] Wu HZ, Wang ZC. Research on laser system of airport perimeter based on ARM. Journal of Convergence Information Technology 2012; 7: 140-148.