Research on the Recognition Method of Leaky Cable Intrusion Alarm Signal

Lu Teng[1,a],Xu Lei[*1,b]

[1]North China Electric Power University, Beijing, China

[a]luteng@ncepu.edu.cn, [b]*xl@ncepu.edu.cn

Keywords:leaky cable, perimeter intrusion detection, feature extraction, similarity matching

Abstract. With the growing demand for security products, intrusion alarm system, based on leaky cables, is favored by majority of enterprises, with advantages of system stability, high concealment and installation location unlimited. Traditional intrusion detection method relies on signal amplitude threshold. However, this method is prone to produce false positives with complex environment interference and false negatives when the leaked electromagnetic field is weak. To solve this problem, this paper, by analyzing time and frequency domain features of the intrusion and interference signals, attempts to use a time-domain analysis method to recognize the intrusion signal. Then we research on how to establish the feature model of intrusion signal, and finally we propose an intrusion signal recognition algorithm based on similarity matching. Through identifying and verifying a large number of actual sample signals, results show that the similarity matching method can effectively reduce the false positives and false negatives, and improve the accuracy of alarm system.

Introduction

Increasing with the security awareness of businesses and households, the demand for security product is growing. Leaky cable intrusion alarm system is a kind of outdoor perimeter intrusion detection system. Due to its stability, high concealment and installation location unlimited, it widely used in placeswhere needs outdoor perimeter protection.

Traditional intrusion detection method relies on signal amplitude threshold, which can effectively detect intrusion. However, some non-controllable factors can cause false alarms. In addition, the amplitude threshold is an empirical value, which may cause false negative. Therefore, how to advance the accuracy rate of leaky cable intrusion alarm system needs further research and exploration.

Currently, related researches on the intrusion signal mostly concentrate in time and frequency domain analysis, such as Fast Fourier Transform (FFT), wavelet analysis, Hilbert-Huang Transform (HHT). FFT [1] is applied to the detection on multitude electromagnetic perturbation. In this literature, a signal detection and location method of multipoint simultaneous invasions is proposed. But the simulation based on sine wave, is not enough to reflect the complex features and regularity of the signal in actual invasion scenario. Then literature [2] points out that the invasion signal has the characteristics of non-stationary random, and we can use time-frequency analysis method to detect the intrusion signal. By comparing the simulation of various time-frequency analysis methods, it proves that HHT has a great advantage for perimeter intrusion signal detection. The literature also points out the excessive decomposition and pseudo component of HHT which needs further improvement. Literature [3] proposes using wavelet transform method to identify the signal of optical fiber sensor perimeter alarm system. The simulation and actual verification show that the detail information of layer 2 of db8 wavelet decomposition can reflect frequency variation and discontinuous point location of the intrusion signal, and this method is used to reduce the false alarms on weather interference. However this paper researches on the signal of leakage coaxial cable radiating electromagnetic fields. The intrusion signal features of cable sensor and fiber optic sensor will be different.

*Corresponding author: xl@ncepu.edu.cn

This paper, based on of a large number of sample data, starting from the features and regularity of actual complex intrusion signals, researches on the statistical method to establish the feature model, and then generates the feature sequence(the base sequence). Finally, a method of similarity analysis is proposed to recognize and classify the signals. The result of testing on the sample set verifies the effectiveness of the algorithm.

Leaky Cable Intrusion Alarm System

Principleand Structure of the System. The basic working principle of leaky cable intrusion alarm system is that two buried leakage coaxial cables at intervals of 1 to 1.5 meters, one of them as transmitting unit, and the other as receiving unit. The two cables outward electromagnetic field of stable frequency to form a warning area. When an intruder enters the warning area, the electromagnetic field is disturbed. Then the disturbance signal is send to the monitoring host to process and recognize. Finally monitoring host sends out alarm signal and uploads the information to PC via the communication interface. System structure is shown in Fig. 1.

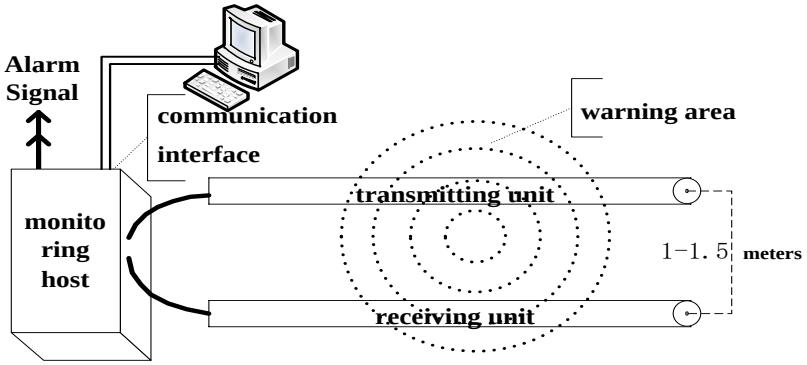


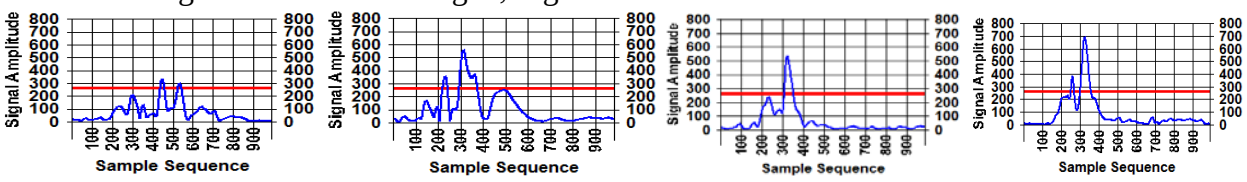
Fig. 1 Structure of leaky cable intrusion alarm system

Feature Analysis of Intrusion Signal in Time Domain and Frequency Domain. Analyzing the features is a prerequisite for further signal recognition. We collected 8 kinds of signals of typical scenarios, divided into two categories: intrusion signals and interference signals. Intrusion signals include slow, walk, brisk walk and jump. Each scenario collected more than 60 samples of different position and repeated sampling. Interference signals include electric switches, animal, vehicle and live conductor interference. Furthermore, we also repeat sampling 5 kinds of atypical intrusion scenarios. So we collected a total of more than 500 samples, which constitute the entire sample set in this paper.

Features of typical sample signals in time domain and frequency domain are as follows:

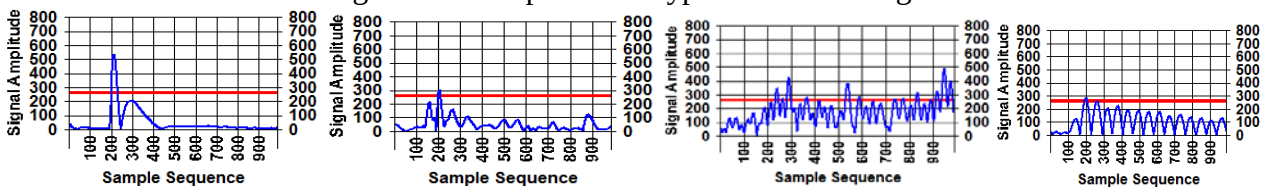
(1)Time domain features

Time-Amplitude relationship of4 kinds of typical intrusion signals and 4 kinds of typical interference signals are shown in Fig. 2, Fig. 3.



(a) slow (b) walk (c)briskwalk (d)jump

Fig. 2 Time-amplitude of typical intrusion signals



(a) electric switches (b) animal (c) vehicle(d) live conductor

Fig. 3 Time–amplitude of typical interference signals

Time domain features of the signals are that, movement range and speed impact signal amplitude, the faster the speed, the higher the amplitude and the narrower the peak. The signal wave of interference is relatively narrow. From the time domain, intrusion and interference signal waveforms has obvious differences.

(2)Frequency domain features

Time and frequency domain analysis methods, STFT, wavelet transform, Gabor transform and Wigner-Vile are all based on FFT with time windows, which follow the Heisenberg uncertainty principle[2,4]. The spectrogram from Hilbert transform of IMF component contains physically meaningful frequency-energy characteristics [5]. Through the spectrums we can see that large energy components of typical signals mainly focus on several points in the range of 0.5 ~ 70 Hz. However, the difference is not obvious, and the two kinds of signals have cross section.

Intrusion Signal Recognition Method Based On Similarity Matching

Through the preliminary analysis of sample signals, and considering the limited resources of monitoring host, this paper tries to study a time-domain analysis method.

Feature Extraction of Intrusion Pattern. Feature extraction is the key of signal recognition. We try to extract features from intrusion patterns, as a base sequence for intrusion signal recognition.

The intrusion signal can be treated as random signal. The same pattern of different test samples will be distributed in the feature space with a certain statistical regularity. So specific patterns can be regarded as time series of the random signal in the feature space:

$$X(n) = \{X_1, X_2, X_3, \dots, X_i, \dots, X_n\} \quad (1)$$

The length of time series,n,depends on the sample sequence and feature extraction. $X_i$is a component at the point$i$. It is also a random variable and its value ranges in the possible value spaces. Study on the statistical features of the random sequence$X(n)$, and its mathematical expectation forms a new sequence as follows:

$$E(X) = \{E(X_1), E(X_2), E(X_3), \dots, E(X_i), \dots, E(X_n)\} \quad (2)$$

Generally, for continuous values,$x \in [a, b]$, in signal value space, there is:

$$E(X_i) = \int_a^b x P_i(x) dx \quad (3)$$

$P_i(x)$is the marginal density function ofX_i.

Then we quantify the sample sequence of k quantization level according to the value domain:

$$E(X_i) = \sum_{j=1}^{k} x_j P_{ij}(x_j) \quad (4)$$

The above statistical feature model is used for feature extraction.Ω represents the intrusion pattern, so its sub-patterns can be expressed as $\{\omega_1, \omega_2, \omega_3, \dots, \omega_p, \dots, \omega_m | \omega_p \in \Omega\}$. Considering statistical features of a particular sub-pattern, we get the mathematical expectations of the random sequence $X(n)$ about each intrusion sub-pattern:

$$C_p(n) = \{E(X|\omega_p)\} \quad (5)$$

As for the sub-pattern ω_m, the feature sequence $C_m(n)$ is:

$$C_m(n) = \{C_{m1}, C_{m2}, C_{m3}, \dots, C_{mi}, \dots, C_{mn}\} \quad (6)$$

For each component:

$$C_{mi} = E(X_i|\omega_m) = \sum_{j=1}^{k} x_j P_{ij}(x_j|\omega_m) \quad (7)$$

Based on the above feature model, we can further identify the intrusion signals with fine-grained pattern recognition.However, fine-grained matching algorithm means more requirements for the platform.For the limited resources platform, we can also consider another compromise algorithm:

$$C(n) = \{c_1, c_2, c_3, \dots, c_i, \dots, c_n\} \quad (8)$$

For each component:

$$c_i = \sum_{p=1}^{m} \sum_{j=1}^{k} x_j P_{ij}(x_j|\omega_p) P(\omega_p) \quad (9)$$

$P(\omega_p)$ is the prior probability of intrusion sub-patternω_p. Its value depends on the historical statistics or experience estimation.

The feature sequence calculated byEq. 8 and Eq. 9 is the basic sequence.

Similarity Analysis Based On the Feature Sequence. The quantitative analysis of signal similarity needs to use a similarity measure function. In addition to a variety of well-known distance metric methods [6], based on the correlation coefficient to measure the similarity degree is commonly used [7]. In this paper, we use the correlation coefficient metric.

Two energy limited signals are$x(t)$and$y(t)$. We select an appropriate coefficient$a$, making $ay(t)$ to approach$x(t)$, then the error energy ΔE, to measure the similarity of two signals [8]:

$$\Delta E = \int_{-\infty}^{+\infty}[x(t) - ay(t)]^2 dt \tag{10}$$

Coefficient a to ensure ΔE minimum and when the derivation of a by (10) equals 0, $\Delta E$is the minimum, that $ay(t)$ is closest to $x(t)$:

$$a = \int_{-\infty}^{+\infty} x(t)y(t)dt / \int_{-\infty}^{+\infty} y^2(t)dt \tag{11}$$

ρ_{xy}represents the correlation coefficient of $x(t)$ and $y(t)$, so the relative error energy is:

$$\Delta E / \int_{-\infty}^{+\infty} x^2(t)dt = 1 - \rho^2{}_{xy} \tag{12}$$

According to (10)~(12), we can deduceρ_{xy}:

$$\rho_{xy} = \int_{-\infty}^{+\infty} x(t)y(t)dt / \sqrt{\int_{-\infty}^{+\infty} x^2(t)dt \int_{-\infty}^{+\infty} y^2(t)dt} \tag{13}$$

Also, as the method above, the correlation coefficient of two discrete signals$x(i)$ and $y(i)$ is as:

$$\rho_{xy} = \sum_{i=1}^{n} x(i)y(i) / \sqrt{\sum_{i=1}^{n} x^2(i) \sum_{i=1}^{n} y^2(i)} \tag{14}$$

$n$represents the sequence length. From Cauchy inequality, we know$|\rho_{xy}| \leq 1$.

Greater the correlation coefficient means higher the similarity of two signals[9]. For real time recognition of the field signal, taking the time interval $\Delta t$of sample points as the calculating step, judge the correlation coefficient of base sequence x and real time signal y one by one:

$$\rho_{xy}(\lambda) = \sum_{i=1}^{n} x(i)y(i + t_s) / \sqrt{\sum_{i=1}^{n} x^2(i) \sum_{i=1}^{n} y^2(i + t_s)} \tag{15}$$

Where$t_s = \lambda \Delta t, (\lambda = 0,1,2,3, \dots \dots)$.

Intrusion Signal Recognition Based On Similarity Matching. Steps of signal recognition:

(1) Build the feature sequence of intrusion pattern as the base sequence of similarity matching.

First of all, eliminate saturated, incomplete invalid sample signals. Secondly, according to the wave range, gain the characteristic part and the length is 500.Then based on the Eq. 8 andEq. 9, we extract 50% of the typical intrusion signals as a training set, to construct the feature sequence.The prior probabilities of intrusion patterns (walk, brisk walk and jump) are determined as: 0.6, 0.3 and 0.1, and the number of quantization levelsare80. Generate the feature sequence (the basis sequence).

(2) Calculate and analyze the correlation coefficients, then determine similarity threshold.

The length of sample sequence is 1000, thus$t_s = \lambda \Delta t, (\lambda = 0,1,2,3, \dots ,500)$. According to Eq. 15, taking Δt as the calculating step, calculate their correlation coefficient. The maximum value of $\rho_{xy}(\lambda)$ is the final similarity between the sample sequence and the base sequence.

Select the typical intrusion signals and the interference signals of the sample set as the validation set. Table 1 shows their similarities with the base sequence.

Table 1 Similarity calculation results

Signal types	Typical intrusion signals	Interference signals
Similarity values range	0.88~0.98(95%)	0.79~0.88(70%)

Through Table 1, we can see that similarity values of the base sequence with more than 95% of the typical intrusion signals are in the range of 0.88 ~ 0.98, and with about 70% of the interference signals are in the range of 0.79~0.88. Combined with the actual engineering requirements for intrusion pattern recognition rate, we define the similarity threshold as 0.88.

Experiment and Discussions. We use the sample sets (a total of 500 sample sequences as the test set) to test the similarity matching recognition algorithm. The results are shown in Table 2.

Table 2 shows that, except animal disturbance,similarity matching algorithm rates are all higher than the traditional threshold recognition rates. It is worth noting that recognition rate of slow intrusion scenario was low with two methods. Possible reason is relatively weak electromagnetic disturbance and irregular movements. Not considering the particularity of slow intrusion scenario, the average recognition rate of intrusion signal can reach 98.8% with similarity matching algorithm,

while traditional threshold method is only 91.2%. For the average recognition rate of the interference signal, similarity algorithm is 63.38%, while traditional threshold method is 34.8%. In addition, similarity matching algorithm for atypical intrusion signals also works well.

Table 2 Results of the recognition rates and comparison

Signal types		Similarity matching	Traditional threshold
Typical intrusion signal	Walk	98.2%	92.8%
	Brisk walk	100%	80.70%
	Jump	100%	100%
	Slow	62%	62%
Interference signal	electric switches	87.5%	0
	vehicle	28.5%	14.3%
	live conductor	100%	50%
	animal	37.5%	75%
Atypical intrusion signal		99.28%	89.58%

To sum up the experiments, signal recognition method based on similarity matching is better than traditional threshold detection method and can improve the accuracy of alarm system effectively.

Conclusions

This paper researches on a method of extracting features. We propose a similarity matching method based on the feature modelto recognize the signals. The test results of the proposed methodon the sample sets showthat it can improve the signal recognition rate to 98% and can effectively eliminate the interferences of electric switches, animal, vehicle and live conductor. In addition, the similarity matching algorithm is simple and efficient, so it is more suitable for the monitoring system of limited computing and storage resources. Next work is to improve the discrimination of intrusion patterns and interference patterns, so that the algorithm has a better recognition of atypical signals.

References

[1] Zhigang Li.The Using Of FFT In The Leakey Cable Perimeter Intruder System[D]. Daqing Petroleum Institute, 2009. In Chinese.

[2] Lei Zhu. Research on the method of Leakage cable perimeter intrusion signal detection[D]. Northeast Petroleum University, 2013. In Chinese.

[3] Zhengli Yang, in: Opto-Electronic Engineering, 2013(1): 84-89. In Chinese.

[4] Huang N E, Shen S S. Hilbert-Huang transform and its applications[M]. World Scientific, 2005.

[5] Zhongyun Luo. Transmission Line Faults Classification Method Based On HHT AndFuzzy Support Vector Machine[D]. Southwest Jiaotong University, 2014. In Chinese.

[6] Tongtong Liu. Research on Similarity Analysis for Biomedical Signal[D]. Tianjin University of Technology, 2013. In Chinese.

[7] Kennedy H L. A new statistical measure of signal similarity[M]. IEEE, 2007.

[8] GQ Zhang, YQ Lin, MZ Guo. Functional analysis handouts[M]. Peking University Press, 1990.

[9] Dexiang Zhao. Study of the Detection and Analysis about Electromagnetic Signal Leakage[D]. Xidian University, 2009. In Chinese.