International Journal of Autonomous and Adaptive Communications Systems

ISSN online: 1754-8640 - ISSN print: 1754-8632
https://www.inderscience.com/ijaacs

Real time detection of intrusion trace information in sensor network based on Bayesian belief network

Hongli Deng, Tao Yang

DOI: 10.1504/IJAACS.2023.10052877

Article History:
Received: 17 April 2020
Accepted: 01 September 2020
Published online: 17 March 2023

Real time detection of intrusion trace information in sensor network based on Bayesian belief network

Hongli Deng and Tao Yang*

Education and Information Technology Center,
China West Normal University,
Nanchong 637002, China
Email: 407290982@qq.com
Email: taoyang@mls.sinanet.com
*Corresponding author

Abstract: In order to overcome the singularity of intrusion detection in sensor networks, a real-time detection method of intrusion trace information in sensor networks based on Bayesian belief network is proposed. This method constructs the intrusion detection model of Bayesian belief network based on the directed bipartite graph, uses the improved wavelet threshold to denoise the sensor network signal, and extracts the trace information features with abnormal conditions in the denoised signal. The most representative abnormal trace information feature is extracted by principal component analysis (PCA). Based on this feature, Bayesian belief network intrusion detection model is used to realise the real-time detection of trace information of sensor network intrusion. The experimental results show that the overall detection rate is higher than 90%, the detection accuracy is higher; the recall rate and precision rate are both higher than the traditional method, and the maximum error of the detection results is only 0.05.

Keywords: Bayesian belief; network; sensor network; intrusion trace; real-time detection; directed bipartite graph; denoised signal.

Reference to this paper should be made as follows: Deng, H. and Yang, T. (2023) 'Real time detection of intrusion trace information in sensor network based on Bayesian belief network', *Int. J. Autonomous and Adaptive Communications Systems*, Vol. 16, No. 1, pp.48–65.

Biographical notes: Hongli Deng received her PhD in Computer College of SiChuan University in 2018. She is currently an Associate Professor in Education and Information Technology Center of China West Normal University. Her research interests include machine intelligence and deep learning.

Tao Yang received his PhD in Computer College of SiChuan University in 2018. He is currently an Associate Professor in Education and Information Technology Center of China West Normal University. His research interests include network security, artificial immune systems, and expert systems.

1 Introduction

With the popularisation of micro sensors, short-range wireless communication and other technologies, small sensor nodes with sensing, computing and communication as a whole, low cost and low consumption also have a high development trend (Kazim et al., 2017). Wireless sensor network also extends from the application in the military field to other fields such as environmental science, medical and healthcare. It has very significant military value and application prospects. Wireless sensor network has become a hot analysis problem (Subhashis and Bappa 2017). With the extensive use of wireless sensor networks in many fields, in the 20th century, the cover article of business week in the USA set it as the concept of significant interference to human development in the new century (Na, 2019). Wireless sensor network enters every corner of human society with the identity of sensing technology. However, due to poor computing performance, small memory space, constraints in resource application, poor anti-interference and guard ability of wireless communication, information privacy and integrity are damaged when the network transmits information (Norman et al., 2019). Encryption and authentication, public key system and other means can protect the sensor network to a certain extent, but are constrained by the performance of nodes. Such technologies cannot be set in all sensor nodes. Therefore, the design of an intrusion detection method has certain practical significance (Yan and Pang, 2019). Intrusion detection belongs to a kind of non passive defence method, which can detect and identify hidden attacks in the network, implement targeted solutions in turn, and complete the security defence of sensor network (Bao et al., 2018). How to design an intrusion detection method which can be carried by technology nodes, meet the network characteristics and implement high efficiency under the premise of the performance constraints of wireless sensor network nodes is the core of wireless sensor network which can be widely used (Li et al., 2019).

In Sangjune et al. (2017), the detection algorithm is set in an independent detection node, in which monitoring data is set, detection scheme and intrusion detection are used. The scheme used in this paper consists of forwarding scheme, repeating scheme and radio transmission area scheme. Forwarding method can detect acquisition black hole and selective forwarding attack, repeating scheme can deny service attack, radio transmission area scheme can detect acquisition wormhole and Hellflood attack, etc. However, when analysing intrusion detection, if the number of failures caused by non-compliance with the rules is not less than the number of failures caused by network accidental reasons, the intrusion is considered to exist. According to the linear detection principle, a mathematical prediction model of Markow is constructed based on a single sensor node. If the absolute value of the difference between the actual and predicted network traffic is not lower than the set threshold, it is considered to have an attack behaviour. This strategy has the advantages of low detection difficulty and real-time, but it has some limitations. Jiang et al. (2017) uses the advantages of high stability of sensor nodes, and sets a simple detection algorithm in each node based on the model. This method can obtain abnormal nodes around, but the intrusion behaviour detected by this method is one-sided.

Therefore, this paper proposes a real-time detection method based on Bayesian belief network for intrusion trace information of sensor network. In this method, a Bayesian belief network intrusion detection model is constructed based on the directed bipartite graph. By combining the soft and hard threshold functions, the wavelet threshold

is improved to remove the dryness of the sensor network signal and extract the trace information features of the abnormal situation in the denoised signal. The most representative trace information features are extracted by the principal component analysis (PCA) and the Bayesian belief network is used based on this feature. The network intrusion detection model realises the real-time detection of the intrusion trace information of the sensor network. The experimental results show that the overall detection rate of this method is higher than 90% in the complete training set. When detecting the intrusion trace information of incomplete sensor network in real time, the detection rate is as high as 98.23%. The recall rate and precision rate are higher than those of the Markov based detection method of the intrusion trace information of sensor network. The maximum error of the detection result is only 0.05, which can better remove the noise in the sensor network.

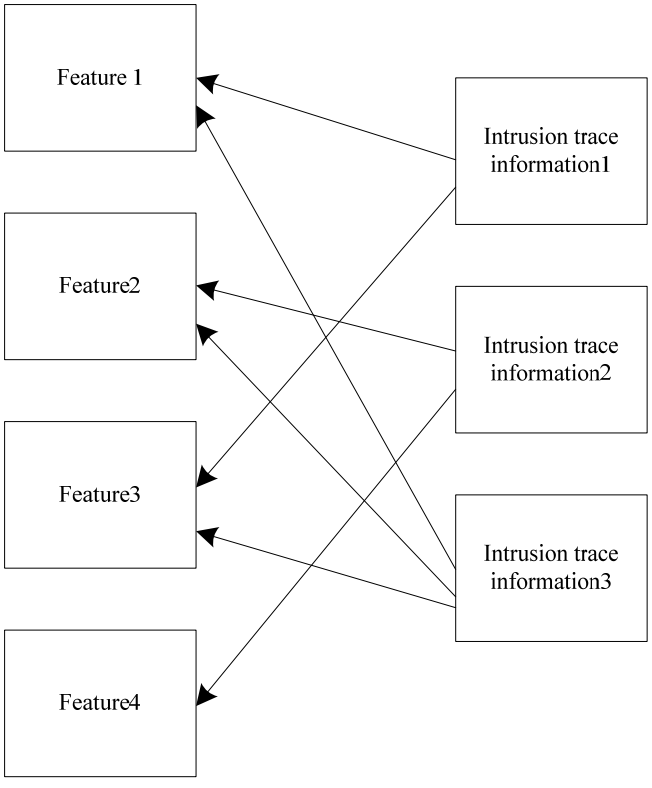
2 Real time detection of intrusion trace information in sensor network based on Bayesian belief network

2.1 Denoising of Bayesian belief network intrusion information based on directed bipartite graph

When the expert knowledge is insufficient, the significant causal relationship between the intrusion types and each type of alarm in the sensor network cannot be determined with high accuracy, so the Bayesian belief network model of intrusion detection cannot be obtained with high accuracy (Liu et al., 2019). Bayesian network performs well on small-scale data, can handle multi classification tasks, and is suitable for incremental training, especially when the amount of data exceeds the memory, it can be a batch of incremental training. In this case, we can directly learn the topological structure and related parameters of Bayesian belief network according to the most representative core characteristics of sensor network. In reality, the structure of learning network is very complex, even though many researchers pay attention to this kind of aspect at present, and the learning effect and efficiency do not meet the needs. Therefore, this paper proposes a Bayesian belief network intrusion detection model based on directed bipartite graph. The Bayesian belief network structure model of the detailed directed bipartite is shown in Figure 1.

The difference between the directed bipartite graph based Bayesian belief network and the conventional Bayesian belief network is that the node set U of the directed bipartite graph based Bayesian belief network consists of two parts: E and W, in which E describes the first level node set, representing all the characteristic attributes of the sensor network; W describes the second level node set, representing all the intrusion types. The directed edge set V is regarded as the edge from node set E to W, and all the edges are from the first layer to the second layer. In this model, there are two kinds of nodes in the attributes of intrusion and intrusion features. The intrusion belongs to the parent node and the intrusion features belong to the child node (Magnus et al., 2018).

Figure 1 Structure of Bayesian network intrusion detection model based on directed bipartite graph



If there is independence between each result, based on this assumption, each parameter value in the model can be easily learned in the sensor network. Compared with some common intrusion detection models, the model established in this paper can not only detect single intrusion trace information, but also detect a variety of intrusion trace information at the same time.

Assuming that the sensor network signal is:

$$\mu(t) = \psi(t) + m(t) \tag{1}$$

Where $\mu(t)$ represents the sensor network signal with noise, $\psi(t)$ and $m(t)$ describe the original signal and Gaussian white noise respectively.

When $\mu(t)$ is transformed into discrete wavelet, then:

$$\varpi_x(i,t) = \varpi_t(i,t) + \varpi_m(i,t) \tag{2}$$

In formula, $i = 0,1,2,\ldots,N, t = 1,2,\ldots,M$. $\varpi_x(i,t)$ represents a sensor network signal with noise; $\varpi_t(i,t)$ and $\varpi_m(i,t)$ represents the original signal and noise in turn based on the wavelet coefficients in layer i; N describes the number of decomposition layers; M describes the signal length.

Because the wavelet transform belongs to linear transformation, after discrete wavelet transform of noisy signal $\varpi_x(i,t)$, the obtained wavelet coefficient $\varpi_x(i,t)$ is set as

$\varpi_{i,t}$, which includes the wavelet coefficient $\varpi_t(i,t)$ of original signal $\psi(t)$, it is set as $v_{i,t}$, and it also includes the corresponding wavelet coefficient $\varpi_x(i,t)$ of noise $m(t)$, which is set as $u_{i,t}$.

The denoising method used in this paper is a combination of soft and hard threshold functions. The schematic diagram of the two threshold functions is shown in Figures 2 and 3.

Figure 2 Soft threshold function

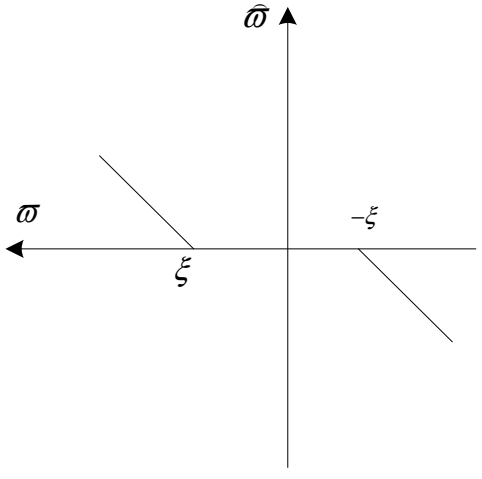
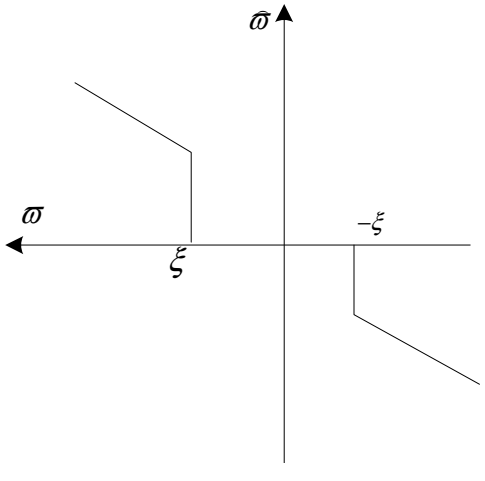


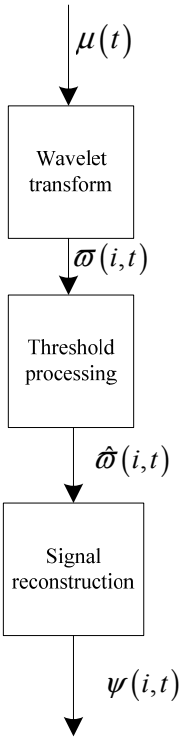
Figure 3 Hard threshold function



The essence of wavelet threshold denoising method is: if $\varpi_{i,t}$ is not higher than the threshold, and $\varpi_{i,t}$ is caused by noise, then $\varpi_{i,t} \approx u_{i,t}$ can be ignored; if $\varpi_{i,t}$ is not less than the threshold, and the wavelet coefficient is caused by signal, then $\varpi_{i,t} \approx v_{i,t}$. Both the soft and hard threshold methods deal with $\varpi_{i,t}$ which is not less than the threshold (Gao, 2019). The former is to shrink this part of wavelet coefficients to 0 according to a certain amount; the latter is directly set as $\varpi_{i,t} = v_{i,t}$. After that, the

wavelet coefficients $\hat{\varpi}_{i,t}$ after processing are reconstructed by wavelet, and the denoised signal $\hat{\psi}(t)$ (Siqi et al., 2018) is obtained. In conclusion, the principle of wavelet threshold denoising is shown in Figure 4.

Figure 4 Principle of denoising with wave threshold



The core of wavelet threshold denoising is threshold processing, which consists of two parts: threshold estimation and threshold function selection. This paper only analyses the selection of threshold function. The soft and hard threshold functions proposed by D.L. Donoho are as follows:

$$\hat{\varpi}_{i,t} = \begin{cases} sgn(\varpi_{i,t})(|\varpi_{i,t}| < \xi), & |\varpi_{i,t}| \gg \xi \\ 0, & |\varpi_{i,t}| < \xi \end{cases} \tag{3}$$

$$\hat{\varpi}_{i,t} = \begin{cases} \varpi_{i,t}, & |\varpi_{i,t}| \gg \xi \\ 0, & |\varpi_{i,t}| < \xi \end{cases} \tag{4}$$

In formula, *sgn*() represents symbolic function; ξ represents the threshold.

To sum up, a Bayesian belief network intrusion detection model is constructed based on directed bipartite graph. By combining the soft and hard threshold functions, the wavelet threshold is improved to de dry the sensor network signals.

2.2 Feature extraction and detection method of trace data

Based on the denoised sensor network signal, the method of trace data feature extraction and detection is used to obtain the abnormal trace information of the sensor network. When detecting the abnormal trace information of the sensor network in real time, it is necessary to extract the trace information features of the sensor network with abnormal conditions, where the features belong to the frequency domain features (Shangqi et al., 2017). The acquired trace data of sensor network is turned into frequency-domain signal, conducted spectrum or power spectrum research, and changed into frequency-varying power according to the amplitude of time variation (Hodo et al., 2017). According to the frequency centre g_{FC}, root mean square frequency g_{RMSF} and root variance frequency g_{RVF}, the research of frequency spectrum describes the signal main frequency direction, main frequency variation and concentration level of power spectrum in sequence. The formulas are as follows:

$$g_{FC} = \int_0^{+\infty} gK(g)dg \Big/ \int_0^{+\infty} gK(g)dg \tag{5}$$

$$g_{RMSF} = \left[\int_0^{+\infty} gK(g)dg \Big/ \int_0^{+\infty} gK(g)dg \right]^{1/2} \tag{6}$$

$$g_{RVF} = \left[\int_0^{+\infty} (g - g_{FC})^2 K(g)dg \Big/ \int_0^{+\infty} gK(g)dg \right]^{1/2} \tag{7}$$

The power spectrum is set to $K(g)$. Then the acquired trace data of the sensor network can be transformed into the frequency domain signal

$$y_j = (g_{FC} + g_{RMSF} + g_{RVF})K(g) \tag{8}$$

The frequency-domain features of all abnormal trace data signals in the sensor network can be expressed as a feature vector, and the space established by the feature vector belongs to the feature space (Bang et al., 2017). In this paper, the feature of abnormal trace data signal in sensor network is acquired by PCA, which belongs to the nonlinear form of PCA. Its core content is to map the abnormal trace data signal of sensor network sample into the non low dimensional feature space in the input control, and then implement the frequency domain of abnormal trace data signal using PCA in the non low dimensional space. The specific implementation form of feature extraction is shown in the following (Xu et al., 2018).

Supposing that the anomaly trace data vector of m dimensions is y, and let a kind of abnormal trace data set of y be y_j, $j = 1, 2, \ldots, M$. Non-linear G is used to map the abnormal trace data signals of sensor network samples in space Q^m to non low dimensional feature space Q^t, and then complete the PCA based on this non low dimensional feature space (Xu et al., 2017).

Assuming that the sample set $G(y_j)$ of the abnormal trace information of the nonlinear sensor network is de mean $\sum_{j=0}^{M} G(y_j) = 0$, then the covariance matrix B of the inner product $G(y_j)$ is:

$$B = \frac{1}{M} \sum_{j=1}^{M} G(y_j) G(y_j)^T \tag{9}$$

The correlation between eigenvalues and eigenvectors is as follows:

$$\varepsilon_k u_k = B u_k \tag{10}$$

Where, the value of eigenvalue ε_k is not less than 0, and u_k represents the eigenvector.

If formula (9) is imported into formula (10), then:

$$B u_k = \frac{1}{M}\sum_{j=1}^{M} \mathrm{G}\left(y_j\right) < \mathrm{G}\left(y_j\right), \quad u_k > \varepsilon_k u_k \tag{11}$$

It is assumed that u_k has all the eigenvectors corresponding to the non-zero eigenvalues in the plane formed by $\mathrm{G}(y_j)$, and also has a non-zero coefficient $[F_j,\ j = 1, 2, \ldots, M]$, then

$$u_k = \sum_{j=1}^{M} F_j \mathrm{G}\left(y_j\right) \tag{12}$$

Using formula (10) to formula (12), we can get:

$$\begin{aligned} &\varepsilon_k < \mathrm{G}\left(y_j\right), u_k > \varepsilon_k \sum_{j=1}^{M} F_j < \mathrm{G}\left(y_j\right), \left(y_j\right) \geq \left\langle G\left(y_j\right), B u_k \right\rangle \\ &= \frac{1}{M}\sum_{j=1}^{M} \left\langle \mathrm{G}\left(y_j\right), \mathrm{G}\left(y_j\right) \right\rangle \sum_{j=1}^{M} F_j \times \left\langle \mathrm{G}\left(y_j\right), \mathrm{G}\left(y_j\right) \right\rangle \end{aligned} \tag{13}$$

If the $\mathrm{M} \times \mathrm{M}$ matrix is $C_{ji} = d\left(y_j, y_j\right) = \left\langle \mathrm{G}\left(y_j\right), \mathrm{G}\left(y_j\right) \right\rangle$, $d\left(y_j, y_j\right)$, D represents the kernel function satisfying Mercer's theorem, the formula (9) is simplified to $\mathrm{M}\varepsilon_k B\mathrm{F} = B^2 F$, then:

$$\mathrm{M}\varepsilon_k \mathrm{F} = BF \tag{14}$$

Then the eigenvalues and eigenvectors of B are expressed as $\mathrm{M}\varepsilon_k$ and F^k. The eigenvalues are arranged according to the order from arrogance to small. If the ratio of the sum of the first n eigenvalues to the sum of the total eigenvalues is greater than the set threshold, then the number of principal elements is n (Rajib and Sipra, 2017).

In order to normalise the feature vector u_k, the feature vector F is normalised:

$$\underset{F^k}{\rightarrow} = F^k / \sqrt{\varepsilon_k} \tag{15}$$

Then we can get the projection of the signal sample y_j of abnormal trace data based on the tth principal vector u_k in Q^t space, then the eigenvalue of y_j is:

$$u_k = \sum_{j=1}^{M} \underset{F^k}{\rightarrow} B\left(y, y_j\right) \tag{16}$$

To sum up, trace information features with abnormal conditions in denoising signals are extracted, and the most representative trace information features are extracted by PCA.

2.3 Parameter learning of Bayesian belief network

According to the Bayesian belief network based on the conditional probability γ of each characteristic attribute in each intrusion type w, then $\gamma=(u_1|w_1),\ldots,$ $\gamma=(u_n|w_2),\gamma=(u_2|w_2),\gamma=(u_n|w_2);\ldots,\gamma=(u_n|w_m),\gamma=(u_n|w_m)$. Where n represents the number of attributes and m represents the number of intrusion types.

If each feature data is independent of each other, then according to Bayes theorem, it exists:

$$\gamma(w_j|\vec{u})=\frac{\gamma(\vec{u}|w_j)\gamma(w_j)}{\gamma(\vec{u})} \tag{17}$$

Because each attribute is assumed to be independent of each other, there are:

$$\gamma(\vec{u}|w_j)\gamma(w_j)=\gamma(u|w_j)\gamma(u_2|w_j),\ldots,\gamma(u_n|w_j)\gamma(w_j)=\gamma(w_j)\prod_{j=1}^{n}\gamma(u_j|w_j) \tag{18}$$

PCA is a statistical technique which transforms many factors into a few core factors. From the perspective of probability, redundant attributes and attributes with small amount of information are removed, and then the core factors obtained represent the original data set, so as to achieve dimension reduction (Wen et al., 2017). If the attribute set of sensor network is u_1, u and u_m, and the requirement attribute is set to X_1, X_2 and X_n, then $n < m$, at the same time, X_1, X_2 2 and X_2 have no relevance. Then these n new variables can describe a large amount of information of the existing dataset represented by the existing m variables (Hui et al., 2018). The detailed process of the algorithm is as follows:

- Let $u_k=(u_1,u_2,\ldots,u_m)$, $u_j=(u_{1j},u_{2j},\ldots,u_{qj})^T$, q represents times, standardise the existing characteristic matrix u, and describe it with u.
- According to u, the matrix $u=(u_{ij})_{m\times m}=u'u$ is calculated.
- Calculate the characteristic equation $\Delta(u-uB)=0$ to obtain the characteristic roots $\partial_1,\partial_2,\ldots,\partial_m$.
- According to the value of real demand $|u|$, judge the value of the required core factor n:

$$\frac{\sum_{j=1}^{n}\partial_j}{\sum_{j=1}^{n}\partial_j}\gg|u| \tag{19}$$

- According to the required n core factors, the corresponding eigenvector a_j of ∂_j used in the operation
- Calculate X_1, X_2, X_n, in which it has:

$$X_j=a_{1j}u_1+a_{2j}u_2+\ldots+a_{mj}u_m \tag{20}$$

Where, j = 1, 2, …, n.

According to the above process, we can get the value that can represent the maximum value n of the core factor of the existing feature set according to the actual needs, and then through the N core factors to represent the data set again, we can also achieve dimension reduction (Miguel and Member, 2017; Prodromos et al., 2018).

To sum up, if the attribute is discrete, $\gamma\left(\vec{u}\left|w_j\right.\right)$ can be obtained by dividing the frequency in each category based on the statistical training samples.

In this paper, the real-time detection of intrusion trace information is transformed into the reasoning problem of Bayesian belief network. On the premise that the causal relationship of the sensor network mode is regarded as a certain point known value, one or more joint probability distributions (in short, the marginal probability distribution $\gamma\left(u_p\left|u_c\right.\right)$) of unknown value are calculated.

$$\gamma\left(u_p\left|u_c\right.\right)=\gamma\left(u_{p1},u_{p2},\ldots,u_{pk}\left|u_{\varphi 1},u_{\varphi 2},\ldots,u_{\varphi k}\right.\right) \tag{21}$$

Where, φ describes the node set that can be observed (belonging to the evidence variable); p describes the node set to be queried (belonging to the query variable) that must calculate the joint probability distribution.

The Bayesian belief network model has a complete description of the total joint probability distribution of all variables. Based on the theory, this kind of probability distribution is set, the principle of conditional probability is used, the low-order joint probability is calculated through the high-order joint probability, and all possible reasoning retrieval can be processed. Therefore, the joint probability distribution of all variables in the sensor network can be obtained directly, and then the edge probability distribution of query variables for a certain value can be obtained by using Bayesian formula. Then:

$$\gamma\left(u_p\left|u_c\right.\right)=\frac{\gamma\left(u_p\left|u_c\right.\right)}{\gamma\left(u_c\right)}=\frac{\sum\gamma\left(u_1,\ldots,u_m\right)}{\left(u_1,\ldots,u_m\right)} \tag{22}$$

In the formula, all joint probability distributions can be obtained by multiplying all conditional probability distributions in the Bayesian belief network according to the chain rule:

$$\gamma\left(u_1,\ldots,u_m\right)=\prod_{j=1}^{m}\gamma\left(u_{j-1},\ldots,u_1\right) \tag{23}$$

Before multiplication, the probability distribution of such conditions and non conditions must be set according to the detailed value of the evidence variable group in the sensor network, but after multiplication, the values obtained by such operations can be added together to obtain $\gamma\left(u_p\left|u_c\right.\right)$ and $\gamma\left(u_c\right)$.

Based on the Bayesian belief network model, because the child nodes share all the parent nodes, and it is assumed that each child node does not have correlation with each other when setting the value combination of the parent node, but in reasoning, all the child nodes are set as evidence variable group and the parent node is set as query variable group, so, based on obtaining the probability distribution of the full joint, it is simplified as:

$$\gamma\left(u_{p1},u_{p2},\ldots,u_{pk}\left|u_{\varphi 1},u_{\varphi 2},\ldots,u_{\varphi k}\right.\right)=\frac{\prod_{j=1}^{m}\gamma\left(u_{pi}\right)\prod_{j=1}^{m}\gamma\left(u_{ci}\left|u_{p1},\ldots,u_{pi}\right.\right)}{\beta} \tag{24}$$

Where β represents the normalisation factor. The combination with the highest possibility can detect the intrusion trace information with high precision.

A Bayesian belief network intrusion detection model is constructed based on the directed bipartite graph. By combining the soft and hard threshold functions, the wavelet threshold is improved to remove the dryness of the sensor network signal and extract the trace information characteristics of the abnormal situation in the denoised signal. The most representative trace information characteristics are extracted by the PCA method and the Bayesian belief network intrusion is used based on the characteristics The detection model realises the real-time detection of the intrusion trace information of the sensor network.

3 Results

3.1 Experimental scheme

The experiment uses the intrusion data of sensor network in KDD99 database to simulate the occurrence of intrusion events. Network environment is a LAN with a maximum load of five computers. Hardware environment of detection end is: personal computer with Inter (R) core (TM) i5-321M2.5GHz CPU and 2GRAM memory. After learning the experimental data, judging the Bayesian parameters, the experimental program is programmed with PNL library, and 14 attribute nodes and 5 attack types of nodes are obtained. And the attack test data are shown in Table 1.

Table 1 Attack test data

Frequency	*Type of attack*	*Number of attacks*
50 frames per second	Tcp Sync	2270
	Ping	2263
	IP Ver	2259
	IP Addr	2254
	Arp	2232
500 frames per second	Tcp Sync	2641
	Ping	2603
	IP Ver	2541
	IP Addr	2530

3.2 Performance index research

True positive (TP) real attack triggers IDs to generate an alarm, which is the correct alarm; false positive (FP) event triggers IDs to generate an alarm when no actual attack occurs, which is a false alarm; false negative (FN) IDS fails to detect the actual attack; true negative (TN) has an attack and no alarm.

- *Detection rate and false detection rate*:

$$\text{Precision rate} = \frac{(TP + TN)}{(TP + FP + FN + TN)} \tag{25}$$

$$\text{False positive rate} = \frac{(FP)}{(FP + TN)} \tag{26}$$

- *Recall rate and precision rate*: Both are important indexes reflecting the retrieval effect. PR curve of the system can be drawn according to the precision and recall, and the system can be judged according to the curve.

  Recall rate = (retrieved relevant information/total relevant information in the system) × 100%.

  Precision rate = (relevant information retrieved/total information retrieved) × 100%.

3.3 Test results of application of complete training set

In the complete training set of sensor network, this method detects the intrusion trace information of three kinds of sensor network test sets, and the results are shown in Table 2.

Table 2 Detection rate and false detection rate of three kinds of sensor network test sets

Invasive species	*Test set 1 (training set)*		*Test set 2 (unknown attack)*		*Test set 3 (known attacks)*	
	Detection rate/%	*Noise factor/%*	*Detection rate/%*	*Noise factor/%*	*Detection rate/%*	*Noise factor/%*
Normal	96.27	2.47	97.89	6.66	97.89	8.44
DoS	98.22	0.12	95.45	0.36	98.13	0.18
Probe	95.17	1.16	99.18	9.02	99.04	2.12
R2L	95.84	2.73	97.17	8.23	99.28	2.51
U2R	95.01	6.37	97.12	6.39	91.55	2.74
Whole	97.81	–	91.06	–	96.47	–

For test set 3, which has almost the same distribution of intrusion types in the training set of sensor network, the detection rate of the method in this paper is higher than 90%, and the detection rate of test set 1 is as high as 96.47%. It can be seen that the real-time detection accuracy of the proposed method is high.

3.4 Test results of incomplete sensor network

In the training set of sensor network, some unknown data of incomplete sensor network are randomly selected. Among them, the probability of missing data is 11%, and the missing nodes are randomly selected. Table 3 is the real-time detection results of the method for the intrusion trace information of incomplete sensor network.

Table 3 Real time detection results of intrusion trace information of incomplete sensor network by the method in this paper

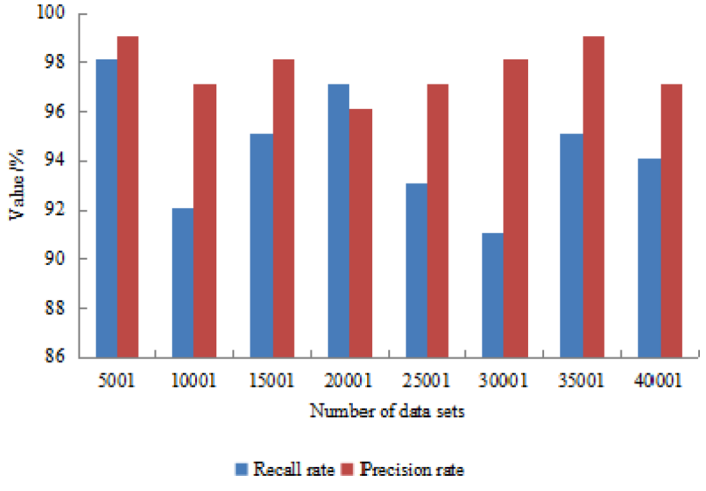
Invasive species	*Normal*	*DoS*	*Probe*	*R2L*	*U2R*	*Detection rate/%*
Normal	59,308	402	287	549	52	97.89%
DoS	6648	219,379	3829	0	0	95.45%
Probe	357	361	3298	152	0	96.67%
R2L	14,508	0	498	1158	27	97.98%
U2R	39	0	134	19	40	98.23%
Noise factor/%	6.66%	0.36%	8.99%	8.23%	5.39%	–

It can be seen from Table 3 that the real-time detection rate of the proposed method for the intrusion trace information of incomplete sensor network is up to 98.23%, and the detection accuracy is high.

3.5 Test performance analysis

In order to highlight the detection performance of the method in this paper, the comparison test is carried out by using the method in this paper and the intrusion trace information detection method based on Markov, and the recall rate and precision rate of the two methods are analysed. The obtained results are shown in Figures 5 and 6.

Figure 5 Test results of this method (see online version for colours)



It can be seen from the analysis of the above figure that after using the method in this paper to detect the intrusion trace information of the sensor network, the recall rate and precision rate are greater than those of the Markov-based detection method for the intrusion trace information of the sensor network, so the detection performance of the proposed method is good.

The method in this paper and the intrusion trace information detection method based on Markov are used to carry out the comparative test, analyse the consistency between

the detection results of the two methods and the real results, and judge the monitoring error. The results are shown in Figure 7.

Figure 6 Test results of intrusion trace information detection method based on Markov (see online version for colours)

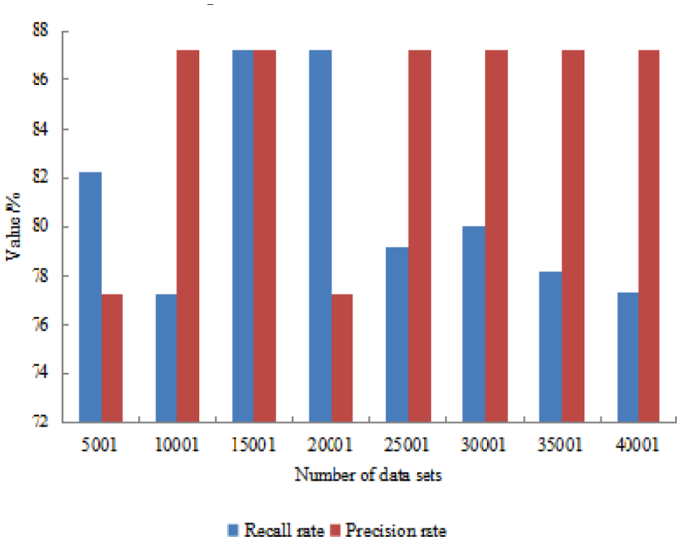
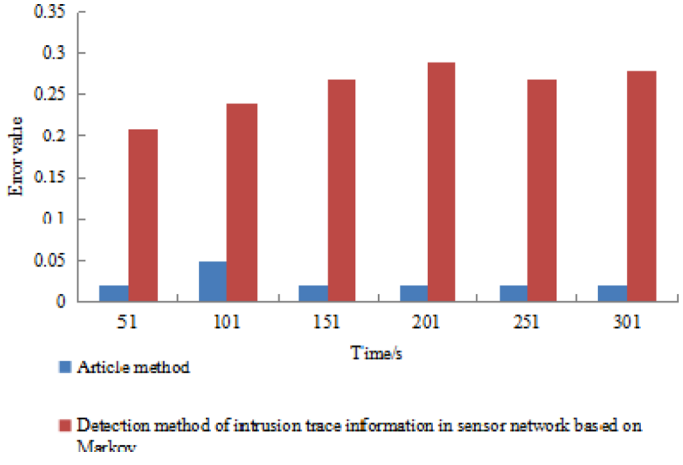


Figure 7 Comparison results of detection errors between two methods (see online version for colours)



As can be seen from Figure 7, the maximum error of the detection results of the method in this paper is only 0.05, but the error of the detection results of the intrusion trace information detection method of sensor network based on Markov is always higher than that of the method in this paper, which verifies the high detection accuracy of the method in this paper again.

Noise is introduced into the sensor network used in this experiment, and the denoising effect of the proposed method and the intrusion trace information detection method based on Markov is analysed. Figure 8 is the schematic diagram after introducing noise

into the sensor network used in this experiment. Figures 9 and 10 are the denoising effect of the proposed method and the intrusion trace information detection method based on Markov.

Figure 8 The schematic diagram after noise is introduced into the sensor network used in this experiment

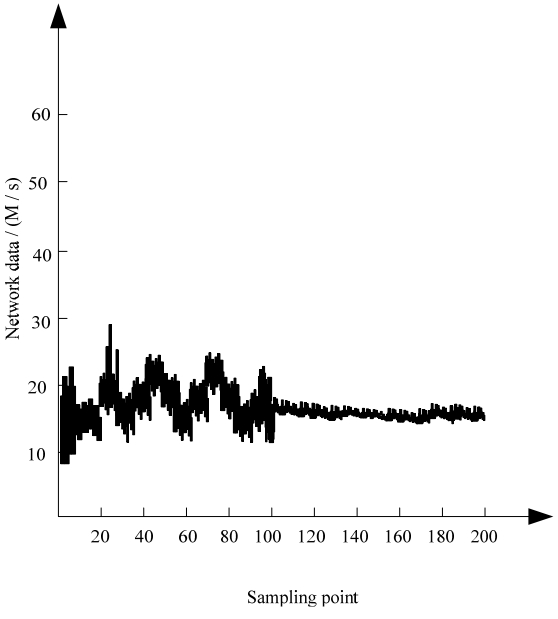


Figure 9 Denoising results of the method in this paper

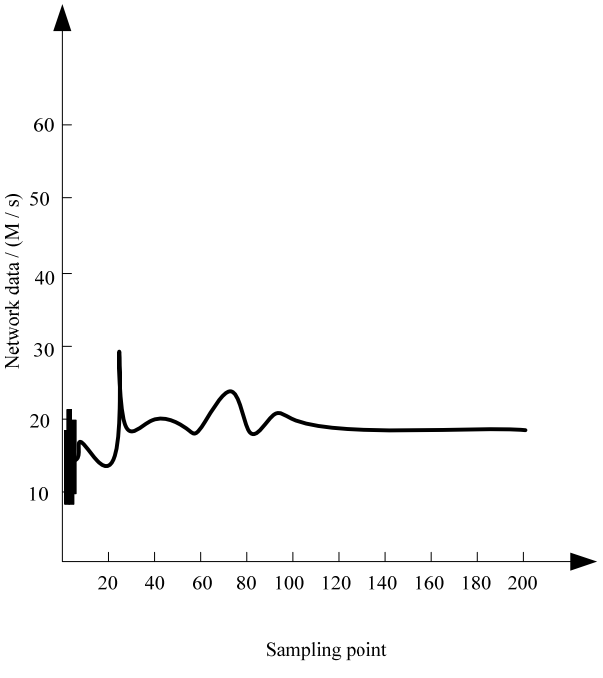
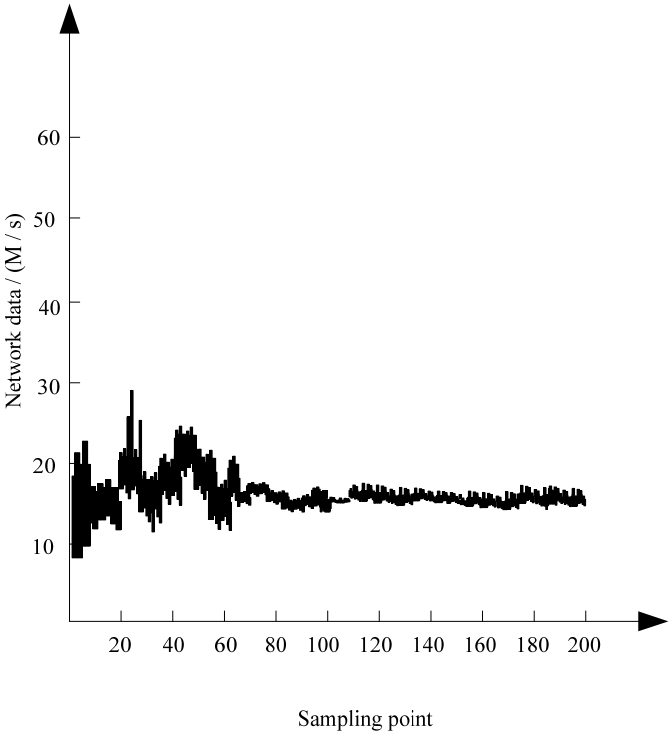


Figure 10 Denoising effect of intrusion trace information detection method based on Markov



Compared with Figures 8–10, the method in this paper can better remove the noise in the sensor network, the signal fluctuation of the sensor network after denoising has not changed, and the denoising effect of the intrusion trace information detection method based on Markov is not as good as that of the method in this paper, and the sensor network after denoising still has noise. Then the proposed method has the best denoising performance.

4 Conclusions

In this paper, a real-time detection method of sensor intrusion trace information based on Bayesian belief network is proposed. This method constructs a Bayesian belief network intrusion detection model based on directed bipartite graph, uses improved wavelet threshold denoising to process sensor network signals, extracts trace information features of abnormal conditions in denoising signals, and extracts the most representative abnormal traces through PCA. Based on Information features, Bayesian belief network intrusion detection model is used to realise real-time detection of sensor network intrusion trace information. The experimental results show that in the complete training set, the detection rate of the proposed method is higher, the overall detection rate is higher than 90%, and the overall detection rate for test set 1 is as high as 96.47%; in the real-time detection of intrusion trace information of incomplete sensor network, the detection rate is as high as 98.23%, and the detection accuracy is high; the recall rate and

precision rate are both higher than that of the intrusion trace information detection method for sensor network based on Markov; the maximum error of the detection result is only 0.05, which can remove the noise in the sensor network, and the fluctuation of the sensor network signal after denoising has not changed. This paper only studies the core algorithm, the next step is to continue to explore the architecture of the sensor network anomaly detection system based on improving and improving the anomaly detection algorithm.

Acknowledgements

This work was supported by Sichuan Science and Technology Program No. 2019JDRC0084, Provincial Department of Education Key Project No. 18ZA0472, China West Normal University Deep Learning Innovation Team Project No. CXTD2017-6, and Research and Science & Technology Program of Nanchong City No. 17YFZJ0016.

References

Bang, C.Z., Guan, Y.H. and Zhi, J.Z. (2017) 'Network intrusion detection based on directed acyclic graph and belief rule base', *Etri Journal*, Vol. 19, No. 39, pp.592–604.

Bao, Y., Leslie, Y. and Jing, T. (2018) 'Artificial neural network enhanced Bayesian PET image reconstruction', *IEEE Transactions on Medical Imaging*, No. 99, pp.1–1.

Gao, J. (2019) 'Simulation of dynamic user network connection anti-interference and security authentication method', *Computer Simulation*, Vol. 47, No. 36, pp.230–233+254.

Hodo, E., Bellekens, X. and Hamilton, A. (2017) 'Threat analysis of IoT networks using artificial neural network intrusion detection system', *Tetrahedron Letters*, Vol. 33, No. 42, pp.6865–6867.

Hui, Z., Xiao, X.Z. and Jing, C.S. (2018) 'Study on PWM rectifier without network voltage sensor based on virtual flux delay compensation algorithm', *IEEE Transactions on Power Electronics*, No. 99, pp.1–1.

Jiang, X., Yan, L. and Xu, Z. (2017) 'A Bayesian network model for predicting type 2 diabetes risk based on electronic health records', *Modern Physics Letters B*, Vol. 41, No. 31, p.1740055.

Kazim, T., Hasmet, U. and Asil, O. (2017) 'Predicting pediatric clinic no-shows: a decision analytic framework using elastic net and Bayesian belief network', *Annals of Operations Research*, Vol. 29, No. 263, pp.1–21.

Li, L.B., Zhu, Y.Z. and Tian, Y.J. (2019) 'RUL indirect prediction of lithium-ion battery based on Elman neural network', *Chinese Journal of Power Sources*, Vol. 24, No. 43, pp.1027–1031.

Liu, Y., Wang, T. and Xu, X. (2019) 'New adaptive activation function for deep learning neural networks', *Journal of Jilin University (Science Edition)*, Vol. 36, No. 57, pp.857–859.

Magnus, M., Kim, S. and Alexander, M.T. (2018) 'A Bayesian network model to explore practice change by smallholder rice farmers in Lao PDR', *Agricultural Systems*, Vol. 58, No. 164, pp.84–94.

Miguel, F. and Member, I. (2017) 'Distributed affine projection algorithm over acoustically coupled sensor networks', *IEEE Transactions on Signal Processing*, No. 99, pp.1–1.

Na, Y. (2019) 'Study on cluster routing protocol for cognitive radio sensor networks', *Journal of China Academy of Electronics and Information Technology*, Vol. 37, No. 14, pp.1022–1026.

Norman, F., Takao, N. and Martin, N. (2019) 'An extension to the noisy-OR function to resolve the 'explaining away' deficiency for practical Bayesian network problems', *IEEE Transactions on Knowledge and Data Engineering*, pp.1–1.

Prodromos, V.M., Elli, K. and Angelos, A. (2018) 'Connectivity analysis in clustered wireless sensor networks powered by solar energy', *IEEE Transactions on Wireless Communications*, pp.1–1.

Rajib, B. and Sipra, D.B. (2017) 'An energy efficient image compression scheme for wireless multimedia sensor network using curve fitting technique', *Wireless Networks*, Vol. 35, No. 25, pp.1–17.

Sangjune, B., Nam, H.K. and Chanyoung, P. (2017) 'Confidence interval of Bayesian network and global sensitivity analysis', *Aiaa Journal*, Vol. 43, No. 55, pp.1–9.

Shangqi, G., Zhaofei, Y. and Fei, D. (2017) 'Hierarchical Bayesian inference and learning in spiking neural networks', *IEEE Transactions on Cybernetics*, No. 99, pp.1–13.

Siqi, N., Meng, Z. and Qiang, J. (2018) 'The deep regression Bayesian network and its applications: probabilistic deep learning for computer vision', *IEEE Signal Processing Magazine*, No. 35, pp.101–111.

Subhashis, C. and Bappa, M. (2017) 'A Bayesian belief network based model for predicting software faults in early phase of software development process', *Applied Intelligence*, Vol. 26, No. 48, pp.1–15.

Wen, Y., Yu, Z. and Chao, Y. (2017) 'Online power scheduling for distributed filtering over an energy-limited sensor network', *IEEE Transactions on Industrial Electronics*, pp.1–1.

Xu, S.Y., Wen, A.Z. and Michael, Z.Q. (2017) 'Hybrid sequential fusion estimation for asynchronous sensor network-based target tracking', *IEEE Transactions on Control Systems Technology*, No. 25, pp.669–676.

Xu, Y., Peng, P.C. and Shou, W.G. (2018) 'CSI-based low-duty-cycle wireless multimedia sensor network for security monitoring', *Electronics Letters*, Vol. 137, No. 254, pp.323–324.

Yan, J. and Pang, Z. (2019) 'Novel Bi-directional Tandem-type Z-source NPC three-level inverter', *Journal of Power Supply*, Vol. 49, No. 17, pp.48–55.