EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

An intrusion detection method for internet of things based on suppressed fuzzy clustering

Liqun Liu[1], Bing Xu[2*], Xiaoping Zhang[3] and Xianjun Wu[4]

Abstract

In order to improve the effectiveness of intrusion detection, an intrusion detection method of the Internet of Things (IoT) is proposed by suppressed fuzzy clustering (SFC) algorithm and principal component analysis (PCA) algorithm. In this method, the data are classified into high-risk data and low-risk data at first, which are detected by high frequency and low frequency, respectively. At the same time, the self-adjustment of the detection frequency is carried out according to the suppressed fuzzy clustering algorithm and the principal component analysis algorithm. Finally, the key factors influencing the algorithm are analyzed deeply by simulation experiment. The results shows that, compared to traditional method, this method has better adaptability.

Keywords: Internet of things, Intrusion detection, Suppressed fuzzy clustering algorithm, Principal component analysis algorithm

1 Introduction

Owing to the rapid development and wide applications of the Internet of Things (IoT) techniques, security of IoT has attracted increasing attentions. IoT is a sensor network consisting of various sensor nodes, which are readily exposed to attacks as they are usually located in sites with no monitoring [1, 2]. To make it worse, attacks on IoT may lead to huge damages in a wide range, compared with computer networks. Hence, security risks in all aspects of IoT and strategies should be analyzed as a whole and the simplification of end security set-up is of IoT great significance [3]. The detection systems should be further optimized based on analysis of risk categories and security structures of IoT [4].

The intrusion detection method judges attacks based on data collected by multiple collection points in a computer network [5, 6]. The intrusion detection is an active protection technique that can intercept and respond to intrusions before they reach the network. However, the huge network data traffic is a huge challenge to intrusion detection systems as it induces high requirements on the detection efficiency so that attacks can be detected in real time. The restricted Boltzmann machine (RBM) network was trained using the greedy algorithm, and low dimension expressions of the RBM network output were classified downwards using the back propagation algorithm [7]. The results indicated that the proposed model shows improved accuracy of intrusion detections, thus suitable for information extractions in high-dimension space. For data compression and low clustering efficiency issues, a modified self-adjustment clustering method is established based on direct correlation to samples close to cluster center [8]. This method effectively reduced clustering sample size and clustering time-space consumption and improves the effectiveness of intrusion detection. Aimed at feature optimization and selection in intrusion detections, a support vector machine (SVM) based two-stage feature selection method was proposed based on feature evaluations of the ratio of detection rate and false alarm rate [9]. In this method, filter noises and irrelevant features were filtered using Fisher classification and information gain in the filtering mode, respectively, to obtain overlapping feature subsets and effectively reduce modeling and detection time. For intrusion detections of internal nodes in wireless sensor networks (WSN), a layer-clustered intrusion

* Correspondence: Xubing@Gdupt.Edu.Cn
[2]School Of Computer And Electronic Information, Guangdong University Of Petrochemical Technology, Maoming, China
Full list of author information is available at the end of the article

detection method for trust value of node a based on the Beta distribution theory and outlier factor was proposed [10]. This method identifies abnormal nodes based on the Mahalanobis distance and exhibits low false alarm rates. Based on classification methods in data mining, optimized solutions were identified by direction calculations of relevant matrices and multi-category network attacks are analyzed by multi-objective mathematical programming model [11]. This method exhibits advantages such as low complexity, effective detections of multi-category attacks, and low false alarm rates. A fuzzy clustering intrusion model based on genetic algorithm and hierarchical algorithm was proposed [12]. Herein, the feature volume was determined by deletion of data set features using the Youden index, the susceptibility to initial cluster centers was relieved, and the local optimization issues in iteration were overcome. Experimental results demonstrated excellent detection performance of the proposed model for network attacks. For Kernel restriction issues in minimum enclosing ball algorithm, an intrusion detection method based on minimum enclosing ball with extensive Kernel was proposed [13]. This method can obtain the minimum enclosing ball of the sample set according to updates of the center and the radius of sphere and categorize network intrusions according to distributions of support vectors. To enhance the accuracy of intrusion detections, an intrusion detection method combining artificial immunity and rough set was proposed for vaccine injections [14]. This method can achieve real time detections of unknown attacks with improved effectiveness and efficiency. Also, a network intrusion detection model was proposed and an alarm system combining multiple proof techniques was established to filter false alarms [15]. An improved multi-objective genetic algorithm-based intrusion detection integrated method has been proposed [16]. This algorithm can effectively solve feature selection issues in intrusion detections, and the method based on this algorithm exhibited excellent detection accuracy and wide applicability to different categories of attacks.

Although intrusion detection technology has been widely used, there are still many problems, such as large number of alerts, high false alarm rate, poor generality, and false report. In this article, an intrusion detection method for IoT was proposed based on suppressed fuzzy clustering (SFC) algorithm [17, 18] and principal component analysis (PCA) algorithm [19, 20]. Simulations demonstrated high detection efficiency and significantly reduced detection time of the proposed method. Section 2 describes the objective prejudgment model of intrusion detections, Section 3 proposes solution of intrusion detections, Section 4 involves simulations, and Section 5 includes a conclusion.

2 Objective prejudgment model

IoT consists of multiple sensor nodes with low communication traffic and short communication range. All nodes are identical and abnormal data packets can be detected by monitoring of wireless ports at all nodes. An intrusion detection system (IDS) for IoT is a solid system consisting of six closely related parts, including data packet monitoring, boundary identification, key management, local detection, voting, and local responses [21].

As the sensor nodes in IoT are readily exposed to attacks, IDS proxy was designed for each node in IoT to realize network monitoring, group decision, and other operations. However, current algorithms are limited by drawbacks such as late alarms, high false alarm rate, and low detection efficiency [22]. This study focuses on optimization of efficiency and effectiveness of intrusion detections. Owing to the rapidly increasing data transmission size in IoT, feature extraction can be extremely time consuming and its efficiency has a severe effect on detections. To guarantee good efficiency and effectiveness of intrusion detections, extractions of feature vectors of the data obtained were achieved by the PCA algorithm. In this way, the efficiency and effectiveness intrusion detection algorithm were significantly improved.

With one sample size, p variables of n groups of data were monitored (e.g., abnormal request data packets, missing data packets). The sample monitoring data matrix X can be described by:

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & \cdots & x_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{np} \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{bmatrix} \tag{1}$$

where X is a matrix consisting of p column vectors, n is the size of data to be monitored, and each data is a coordinate in the nth dimension. The monitoring data of original samples were standardized:

$$x_{ij}{}^{*} = \frac{x_{ij} - \overline{x_j}}{\sqrt{V(x_j)}}, (i = 1, 3, \cdots, n; j = 1, 2, \cdots, p) \tag{2}$$

$$\overline{x_j} = \frac{1}{n}\sum_{i=1}^{n} x_{ij} \tag{3}$$

Then, X was projected to the low dimension space vector (T), as follows:

$$T = W^{T}X \tag{4}$$

where W refers to the projection matrix, which is an orthogonal matrix consisting of covariance matrices ($V(x_j)$), it can be calculated by:

$$V\left(x_j\right) = \frac{1}{n}\sum_{i=1}^{n}\left(x_{ij}-\overline{x_j}\right)^2, (j = 1, 2, \cdots, p) \tag{5}$$

$$\mathrm{VW_i} = \lambda_i\overrightarrow{\mathrm{W_i}}, (i = 1, 2, \cdots, p) \tag{6}$$

where the covariance matrix (W_i) is located in the ith column of W, and $\overrightarrow{\mathrm{W_i}}$ is the feature vector corresponding to one specific feature (λ_i) of V. To achieve rapid detections, features with ambiguous values were eliminated to enhance the detection efficiency. The feature vectors with relatively large values were selected. Herein, an objective prejudgment-based intrusion detection, frequency self-adjustment algorithm for IoT was proposed. In this algorithm, the huge data flow is integrated and analyzed. More specifically, the data is classified using the clustering algorithm: the data sent to potential objectives to be attacked is classified as high-risk data, while other data is classified as low-risk data. The high-risk data and the low-risk data are detected under high frequency and low frequency, respectively.

Define the data set to be clustered as $X = \{x_1, x_2, \ldots, x_n\}$, where each sample x_k (1, 2, …, n) has several features, including data transmission rate, average length of data packets, and intervals of data emission. $x_\mathrm{k} = (x_\mathrm{k1}, x_\mathrm{k2}, \ldots, x_\mathrm{kj})^\mathrm{T} \in \mathrm{R}^\mathrm{j}$ is the corresponding feature vector, which represents a point in the data feature space, and x_{kj} is the feature vector in the jth dimension. In this way, data in X is categorized as high-risk data or low-risk data. The result is denoted as a matrix in order of c*n ($\mathrm{U} = [\mathrm{u_{ij}}]_{\mathrm{c^*n}}$), which satisfies

$$\forall i, j, u_{ij} = [0, 1] \tag{7}$$

$$\forall j, \sum_{i=1}^{c} u_{ij} \tag{8}$$

$$\forall i, 0 < \sum_{j=1}^{n} u_{ij} < n \tag{9}$$

The weight distances from samples to the cluster center are defined as objective functions, which can be calculated by

$$J_m(U, V) = \sum_{j=1}^{n}\sum_{i=1}^{c}\left(u_{ij}\right)^m\left(d_{ij}\right)^2 \tag{10}$$

$$d_{ij} = \sqrt{\sum_{t=1}^{s}\left(x_{jt}-v_{it}\right)^2} \tag{11}$$

where $U = [\mathrm{u_{ij}}]_{2^*n}$ is fuzzy classification matrix ($\mathrm{u_{ij}} \in [0, 1]$), m is the weighed index, $m \in [1, \infty]$, d_{ij} is the Euclidean distance (d_{ij}) between x_j, and the ith cluster center v_i ($i = 1, 2, \ldots$, c). d_ij can be calculated by Eq. (11).

3 Intrusion detection method

To ensure rapid and effective detections of attacks, an objective prejudgment-based intrusion detection, frequency self-adjustment method for IoT is proposed. With no distortions of original data guaranteed, the PCA algorithm can reduce the number of variables and eliminate features with low discriminations. The dimension reduced data was divided by SFC algorithm as high-risk and low-risk data, which are detected using different frequencies to achieve enhanced detection efficiency and accuracy. The procedures are as follows:

(a) Data initialization: define fuzzy clustering set as $c = 2$ and optimized classification threshold as $\varepsilon = 0.3$, initialized detection machine number as n, minimum detection frequency of low-risk data as l_{min}, maximum detection frequency of high-risk data as l_{max}, time intervals as Δt.

(b) Data pre-processing: randomly initialize the affiliation matrix $\mathrm{U} = [\mathrm{u_{ij}}]_{\mathrm{c^*n}}$ ($\mathrm{u_{ij}} \in [0,1]$) and Eq. (9) was satisfied. The cluster centers v_i ($i = 1, 2, \ldots$, c) were determined and the Euclidean distance (d_{ij}) between the jth sample data and the ith cluster center. d_{ij} can be calculated by

$$v_i = \frac{\sum_{j=1}^{n}\left(u_{ij}\right)^m x_j}{\sum_{j=1}^{n}\left(u_{ij}\right)^m}, (i = 1, 2, \cdots, c) \tag{12}$$

$$d_{ij} = \sqrt{\sum_{t=1}^{s}\left(x_{jt}-v_{it}\right)^2} \tag{13}$$

The objective function was calculated using Eq. (10). If the value of objective function was no lower than the given optimized classification threshold, the process was repeated; if the value of objective function was lower than the given optimized classification threshold and no changes of any cluster was observed, the process ends.

Due to the slow converging rates of conventional fuzzy clustering algorithms, a suppressor λ_{ij} ($0 < \lambda_\mathrm{ij} < 1$) was introduced to d_{ij} for the purpose of correction. Define the corrected distance as $d_{ij}^{'}$

$$d_{ij}^{'} = 1-\lambda_{ij}\sum_{i\neq j} d_{ij} \tag{14}$$

It satisfies

$$\left| d_{ij} - \frac{1}{n}\sum_{j=1}^{n} d_{ij} \right| > \lambda_{ij} \tag{15}$$

(c) First, classified data was analyzed using the PCA algorithm and features with low discriminations were eliminated to accelerate the detection process.

(d) Then, data was detected with self-adjustment of detection frequency according to the detection results. Assume that the quantity of objective machines that can be effectively detected by objective prejudgment based methods is

$$n = n' + \Delta n \tag{16}$$

where n is the quantity of monitored objective machines, n' is the quantity of monitored objective machines before application of objective prejudgment, and Δn is the quantity of monitored objective machines after application of objective prejudgment.

The total number (N) of data packets that can be detected per second can be obtained by:

$$N = n \cdot l_{\min} + \left(\frac{l_{\max} - l_{\min}}{l_{\min}} \right) \cdot t - n' \tag{17}$$

where $l_{\min}$ refers to the minimum detection frequency of low-risk data, $l_{\max}$ refers to the maximum detection frequency of high-risk data, and t $(0 \le t \le n)$ refers to the total number of objective data under attack. In cases of no attacks to the IoT system, the detection frequency of low-risk data (P') to each objective with detection effectiveness guaranteed is defined as

$$P' = \frac{N}{n} \tag{18}$$

The detection frequency can be neither over-adjusted (high-risk data is identified as low-risk data) nor under-adjusted (high-risk data cannot be detected) and an appropriate frequency difference is of great significance. With detection effectiveness and accuracy guaranteed, the adjustable data detection frequency difference is defined as

$$\Delta f = \sum_{i=1}^{n-k} P' - l_{\min} \tag{19}$$

In this way, detection frequencies of high-risk data ($P^{i}{}_{\max}$) and low-risk data ($P^{i}{}_{\text{low}}$) of the ith objective machine by the NIDS system can be obtained

$$P^{i}{}_{\max} = P' + \frac{\eta_{\mathrm{i}} \cdot \Delta f}{\mathrm{k}} \tag{20}$$

$$P^{i}{}_{low} = \frac{1}{n-k}\left(N - \sum_{i=1}^{n} P_{\max} \right) \tag{21}$$

$$\eta_i = \frac{A_i}{C_i} \tag{22}$$

where η_i is the ratio of abnormal data sent to the ith objective machine in Δt, A_i refers to the detected abnormal data sent to ith potential target in Δt, and C_i refers to all detected abnormal data sent to ith potential target in Δt. In detections, the detection frequency of the objective was adjusted in real time according to η_i to optimize the detection accuracy.

4 Simulations

In this study, the objective prejudgment-based intrusion detection system for IoT was employed. The data was pre-processed using SFC algorithm and PCA algorithm and then detected by frequency self-adjustment. The results indicated that the proposed algorithm can not only enhance the detection efficiency but also reduce the false alarm rate. The accuracy index is the most important performance index of the intrusion detection system, and its value depends on the sample set and the test environment used in the test. The three parameters of detection duration, accuracy rate, and false alarm rate are usually used as evaluation indexes. Therefore, in this study, detection duration (T), accuracy (P), and false alarm rate (F) were employed as evaluation parameters:

$$P = \frac{N_t}{N'} \times 100\% \tag{23}$$

$$F = \frac{N_f}{N} \times 100\% \tag{24}$$

where N_t is the size of attack samples that are accurately detected, N_f is the size of false alarms, and N' is the size of overall attacks identified by the system, and N is the size of overall real attacks.

Table 1 summarizes detection results of the proposed algorithm, the neural network algorithm, and the Bayesian algorithm. As observed, the accuracy of the proposed algorithm is higher than those of the other two algorithms. This can be attributed to data dimension reduction by PCA algorithm, which eliminates interferences

Table 1 Properties of raw materials

Algorithm	Accuracy (%)	False alarm rate (%)
The proposed algorithm	97.1	1.5
Neural network algorithm	93.4	4.5
Bayesian algorithm	95.2	3.2

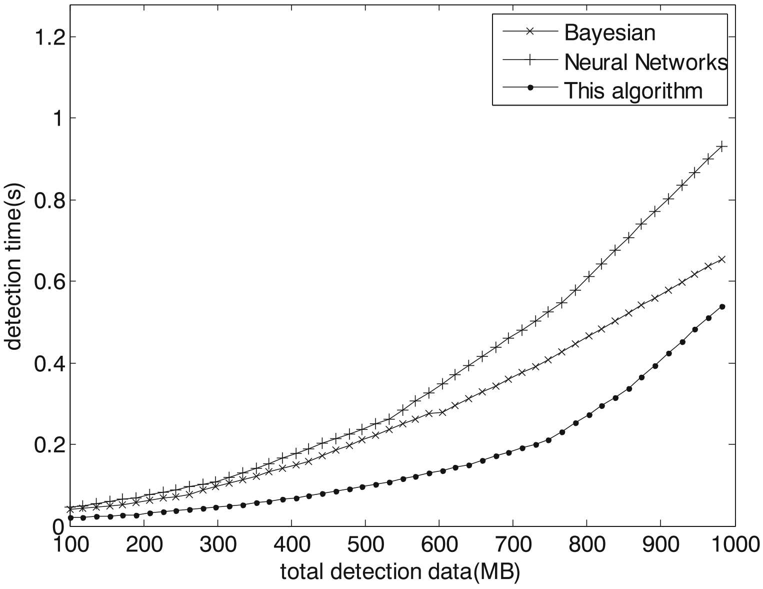

Fig. 1 Overall data size vs. detection efficiency

by irrelevant factors. Additionally, the false alarm rate of the proposed algorithm is lower than those of the other two algorithms. Hence, it can be concluded that the proposed algorithm is viable.

Figure 1 summarizes the effects of the overall data size on the detection efficiency using different algorithms. As observed, detection efficiencies of the three algorithms decreased as the data size increased, while the detection efficiency of the proposed algorithm is lower than those of the other two algorithms. The detection efficiency of the proposed algorithm is higher than those of the other two algorithms, regardless of the overall data size. Therefore, it can be concluded that the proposed algorithm can enhance detection efficiency.

Table 2 summarizes detection results of the proposed algorithm. As observed, the detection rate of abnormal data increased as the time increased. This can be attributed to the continuous self-adjustment of detection frequency according to the responses received.

The accuracy is a key indicator for intrusion detections. The effects of overall data size on the detection accuracy were investigated using different algorithm models, and the results are shown in Fig. 2. As observed, the detection accuracy degraded as the data size increased in all three cases, as the increasing data size leads to decreasing detection efficiency. However, the decreasing rate of the proposed algorithm model was lower than those of the other two algorithms and the accuracy of the proposed algorithm model was higher than those of the other two algorithms in all cases. Therefore, the proposed algorithm model is viable.

Table 2 Detection results of the proposed algorithm

Time (s)	Actual abnormal data packet	Detected abnormal data packet	Detection rate (%)
0–10	3290	3175	96.5
10–20	4367	4227	96.8
20–30	3632	3534	97.3
30–40	3487	3396	97.4

5 Results

With the rapid development of the IoT technology, the security problem is becoming more and more serious. All sensor nodes in IoT are vulnerable to external attacks. The huge network data traffic is a huge challenge to intrusion detection systems as it induces high requirements on the detection efficiency so that attacks can be detected in real time. However, current algorithms are limited by drawbacks such as late alarms, high false alarm rate, and low detection efficiency. Aimed at low effectiveness of intrusion detections for IoT, an intrusion detection method for IoT based on SFC algorithm and PCA algorithm is proposed. In this method, the data obtained are classified by objective prejudgment into high-risk data and low-risk data, which are detected at high frequency and low frequency, respectively. Meanwhile, the self-adjustment of detection frequency is achieved by employing the SFC algorithm and the PCA algorithm. Experimental results revealed improved applicability of the proposed method, compared with conventional methods (e.g., neural network algorithm, Bayesian algorithm). The innovation of this paper is to propose an objective prejudgment-based

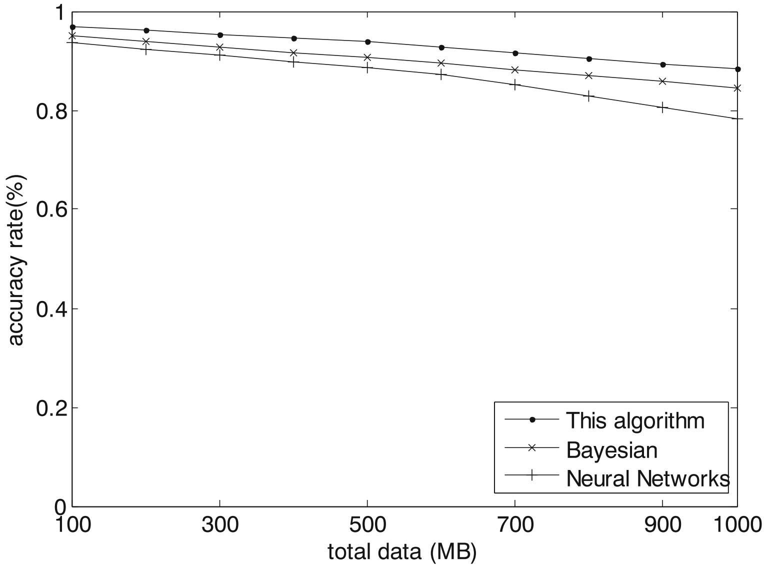

Fig. 2 Overall data size vs. detection accuracy

intrusion detection, frequency self-adjustment method for IoT. With no distortions of original data guaranteed, the PCA algorithm can reduce the number of variables and eliminate features with low discriminations. The dimension reduced data was divided as high-risk and low-risk data, and then tested at different frequencies, which are detected using different frequencies to achieve enhanced detection efficiency and accuracy. This method can quickly improve the effectiveness and accuracy of intrusion detection.

6 Discussion

In this study, the number of samples and the detection time are several important factors that affect the efficiency of the algorithm. The key factors affecting this algorithm are analyzed by simulations. Experimental results show that with the increase of data volume, the efficiency and accuracy of intrusion detection algorithm will gradually decrease. Compared with Bayesian algorithm and neural network algorithm, the new algorithm in this paper still has better detection efficiency.

With the continuous development of related research, new intrusion detection models of IOT will be more and more, and the evaluation index will also continue to expand. In subsequent research, we can consider the combination of other indicators and new features of IOT to improve the intrusion detection model.

Abbreviation

IDS: Intrusion detection system; IoT: Internet of things; PCA: Principal component analysis; RBM: Restricted Boltzmann machine; SFC: Suppressed fuzzy clustering; SVM: Support vector machine; WSN: Wireless sensor networks

Acknowledgements

The research presented in this paper was supported by the Funds of Science & Technology Research of Guangdong Province and the Natural Science Foundation of Guangdong Province, China.

Funding

The authors acknowledge the Funds of Science & Technology Research of Guangdong Province, China (Grants: 2015B010128015 and 2017A040403070) and the Natural Science Foundation of Guangdong Province (Grant: 2017A030307027),China.

Authors' contributions

LL is the main writer of this paper. She proposed the main idea, deduced the performance of the algorithm detection, completed the simulation, and analyzed the result. BX introduced the suppressed fuzzy clustering algorithm and principal component analysis algorithm and analyzed the data of the simulation experiment. XZ analyzed the key factors influencing the algorithm. XW gave some important suggestions for intrusion detection. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

[1]School Of Mathematics And Computer, Guangdong Ocean University, Zhanjiang, China. [2]School Of Computer And Electronic Information, Guangdong University Of Petrochemical Technology, Maoming, China. [3]School Of Mathematics And Statistics, The University Of Sheffield, Sheffield S3 7rh, UK. [4]School Of Computing Center, Guangdong University Of Petrochemical Technology, Maoming, China.

Received: 3 February 2018 Accepted: 25 April 2018
Published online: 09 May 2018

References

1. XD Hu, ZM Jia, A method of lightweight intrusion detection for the Internet of things. J. Chongqing Univ. Posts Telecommun. **2**(27), 255–259 (2015)
2. GY Tang, Network intrusion detection method based on constraint fuzzy clustering thought. Natl. Sci. J. Xiangtan Univ. **3**(39), 61–64 (2017)

3. F Jia, LZ Kong, Intrusion detection algorithm based on convolutional neural network. Trans. Beijing Inst. Technol. **12**(37), 1271–1275 (2017)
4. XC Liu, SF Lu, W Zhao, et al., A cloud computing intrusion detection with objective function optimization based on fuzzy C-means clustering algorithm. J. Cent. South Univ. **7**(47), 2320–2325 (2016)
5. GD Li, JP Hu, KW Xia, Intrusion detection using relevance vector machine based on cloud particle swarm optimization. Control Decision. **30**(4), 698–702 (2015)
6. YH Yang, HZ Huang, QN Shen, et al., Research on intrusion detection based on incremental GHSOM. Chin. J. Comput.. **37**(5), 1216–1224 (2014)
7. N Gao, L Gao, YY He, Deep belief nets model oriented to intrusion detection system. Syst. Eng. Electron. **38**(9), 2201–2207 (2016)
8. J Jiang, ZF Wang, TM Chen, et al., Adaptive AP clustering algorithm and its application on intrusion detection. J. Commun. **36**(11), 118–126 (2015)
9. XN Wu, XJ Peng, YY Yang, et al., Two-level feature selection method based on SVM for intrusion detection. J. Commun. **36**(4), 2015127-1–2015127-8 (2015)
10. WM Tong, JQ Liang, L Lu, et al., Intrusion detection scheme based node trust value in WSNs. Syst. Eng. Electron **37**(7), 1644–1649 (2015)
11. B Wang, XW Nie, Multi-criteria mathematical programming based method on network intrusion detection. J. Comput. Res. Dev. **52**(10), 2239–2246 (2015)
12. CH Tang, PC Liu, SS Tang, et al., Anomaly intrusion behavior detection based on fuzzy clustering and features selection. J. Comput. Res. Dev. **52**(3), 718–728 (2015)
13. QA Wang, B Chen, Intrusion detection system using CVM algorithm with extensive kernel methods. J. Comput. Res. Dev. **49**(5), 974–982 (2012)
14. L Zhang, ZY Bai, SS Luo, et al., Integrated intrusion detection model based on rough set and artificial immune. J. Commun. **34**(9), 166–176 (2013)
15. ZH Tian, BL Wang, WZ Zhang, et al., Network intrusion detection model based on context verification. J. Comput. Res. Dev. **50**(3), 498–508 (2013)
16. Y Yu, H Huang, An ensemble approach to intrusion detection based on improved multi-objective genetic algorithm. J. Softw. **18**(6), 1369–1378 (2007)
17. B Liu, SX Xia, Y Zhou, et al., A sample-weighted possibilistic fuzzy clustering algorithm. Acta Electron. Sin. **40**(2), 371–375 (2012)
18. AG Chen, ST Wang, Fuzzy clustering algorithm based on multiple medoids for large-scale data. Control Decision. **31**(12), 2122–2130 (2016)
19. ZZ Liang, Y Li, SX Xia, et al., Principal component analysis based on L1-norm maximization with Lp-norm constraints. PR AI **26**(2), 211–217 (2013)
20. Y Ruan, HW Chen, ZH Liu, et al., Quantum principal component analysis algorithm. Chin. J. Comput **37**(3), 666–676 (2014)
21. M Ahmed, AN Mahmood, J Hu, A survey of network anomaly detection techniques. J. Netw. Comput. Appl. **60**, 19–31 (2016)
22. Y Chen, An efficient feature selection algorithm toward building lightweight intrusion detection system. Chin. J. Comput. **30**(8), 1398–1408 (2015)