Contents lists available at YXpublications

International Journal of Applied Mathematics in Control Engineering

Journal homepage: http://www.ijamce.com

An Intrusion Detection Method of Internet of Things Based on Agent

Shuo Lin*, Zhenbo Wu, Yuanwei Qi, Zhonghua Han

Faculty of Information and Control Engineering, Shenyang Jianzhu University, Shenyang 110168, China

ARTICLE INFO

Article history:
Received 2 July 2018
Accepted 24 September 2018
Available online 25 December 2018

Keywords:
Internet of Things
cluster
multi-Agent
intrusion detection
principal component analysis

ABSTRACT

With the development of the Internet of Things (IOT), the application of IOT technology faces information security risks such as user privacy leakage, as well as interception and falsification of measurement and control instructions, due to the open deployment and limited resources of Internet of Things. In the light of the characteristics and potential security problems of Internet of Things, this paper proposes an intrusion detection system combined CFSFDP clustering algorithm based on multi-Agent and principal component analysis (PCA). Simulation experiment is carried out with KDD Cup99 dataset. In addition, the validity of the method is determined from three indexes: detection rate, false positive rate and false negative rate. The simulation results show that the method has faster response speed and higher detection accuracy, which can improve the security of the Internet of Things.

1. Introduction

As Internet of Things becomes widely used, it has provided great convenience to people as well as many insecurities. The IOT sensor layer is composed of sensor network and sensor device. On the one hand, the attacker maliciously controls the normal node and the gateway node, which brings about the invalidation of physical label, failure to identify a legitimate normal node and congestion caused by a large amount of interference signals on the network. On the other hand, it will be subject to denial of service and illegal access attacks from the Internet, resulting in the collapse of the node and the sensor network. Intrusion detection is an active defense method to ensure network security. By collecting and analyzing key information in a computer network or system, it can find out whether there are violations of security policies and signs of attacks, so as to improve the ability of IOT system to deal with external threats. In recent years, many experts and scholars have conducted research on intrusion detection for the Internet of Things.

Xiong Weicheng (2017) studied the IOT security system based on intrusion detection, proposing an IOT security model combined anomaly detection system and misuse detection system. The misuse detection system only works after being triggered by anomaly detection system, which has good energy saving. Sun Qingbo used the improved BP neural network to design the intrusion detection system of the Internet of Things, but the system's false positive rate and false negative rate were quite higher. Zhang Xin and Yuan Yuyu (2012) compared application effects of intrusion detection technology on the Internet of Things, indicating that the intrusion detection technology based on multi-Agent can be applied to the Internet of Things because of its autonomy and mobility, and the intrusion detection technology based on machine learning has good self-adaptive capabilities. Mansour Sheikhan and Hamid Bostani (2016) proposed a proxy-based distributed intrusion detection system combined anomaly detection and misuse detection, applying the optimal path of forest model to intrusion detection, which has superior performance.

Based on the above researches, this paper proposes an IOT intrusion detection system based on multi-Agent. The CFSFDP clustering algorithm and principal component analysis (PCA) are combined to establish a feature rule-base and detect the intrusion data. It can ensure the detection accuracy while reducing the false positive rate, and effectively improve the security of the IOT system.

2. Intrusion detection model

2.1 Generic intrusion detection model

Intrusion detection refers to the active security protection strategy adopted to detect computer network intrusion behavior. It collects and analyzes network data at some key nodes of the computer network or computer system to detect whether there are abnormal behaviors that violate security rules.

* Corresponding author.
E-mail addresses: farewell_lin@163.com (S. Lin)

CIDF is a generic intrusion detection framework model consisting of four basic components: event generator, event analyzer, response unit, and event database. The purpose of the event generator is to obtain the data to be analyzed from the entire computing environment and transmit the data to other units of the system. Based on the feature information or the historical-behavior model, event analyzer analyzes the events generated by the event generator and transmits the results to the response unit. According to the analysis results of the time analyzer, the response unit makes response such as disconnection, alarm, and so on. The event database is used to store detection rules and attack-type data, which can be designed as a simple text file or a complex database. The generic framework model of the intrusion detection system is shown in the Fig. 1.

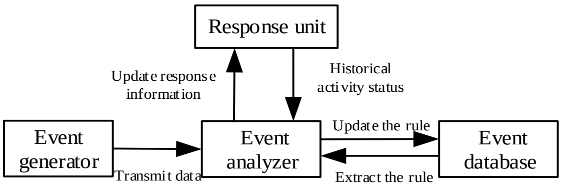


Fig. 1. CIDF intrusion-detection generic framework model.

2.2 Agent-based network intrusion detection model design

Most of the existing intrusion detection systems use a single architecture. All work including data collection and analysis is done by a single program on a single host. The dependencies between the modules are strong and the scalability is poor. What's more, the number of monitored hosts and the size of network are greatly limited. As such, when the amount of data is too large, it will result in data overload, untimely processing or network packet loss. With the rapid growth of network data and increasingly obvious network security problems, intelligent and flexible intrusion detection systems, which can respond quickly to environmental changes and require no human intervention, are needed. In this situation, the intelligent Agent is a better solution. Agent is a software entity that can run autonomously in a specific detecting environment, implementing certain functions independently. It can communicate and cooperate with other Agent components to detect network security threats and abnormal intrusions.

The intrusion detection model proposed in this paper is realized by AGENT technology. Each Agent detection unit is relatively independent, which can minimize the dependencies between detection components, and realize the distribution of data collection, intrusion detection and real-time response. The basic components of the intrusion detection model are composed of host Agent, network Agent, communication Agent, analysis Agent and center Agent. This distributed hierarchical structure complies with the top-down and layer-by-layer control mechanism. The upper layer can control lower-layer components, and all of them are controlled by the center to prevent the spread of damage. The system model is shown in the Fig. 2.

The design goals of this model are as follows:

(1) Intrusion analysis and detection of network data utilize data mining technology to combine CFSFDP clustering algorithm and principal component analysis (PCA) to meet the function of detecting abnormal intrusion in the IOT environment.

(2) The system model consists of multiple Agent components, which can reduce the dependencies between the modules and improve the robustness and portability of the system.

(3) Each Agent component performs its own duties, and the work does not interfere with each other, which can improve the response speed of the system.

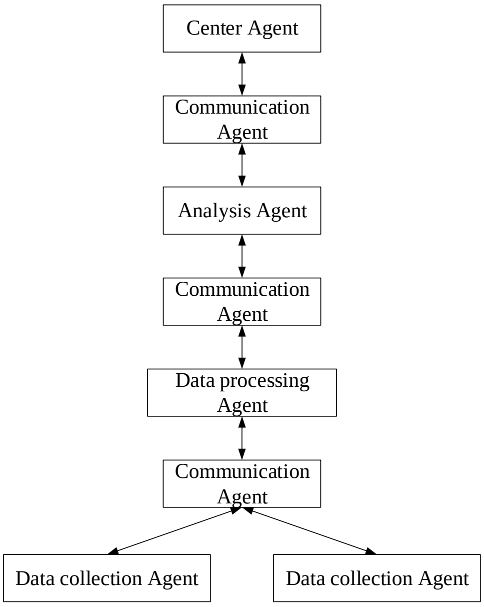


Fig. 2. Agent-based network intrusion detection model.

Center Agent: It focuses on the entire network and provides the user interaction interface. Moreover, it can monitor, uniformly configure and manage all Agents in the entire system, displaying alarm information and responding to them.

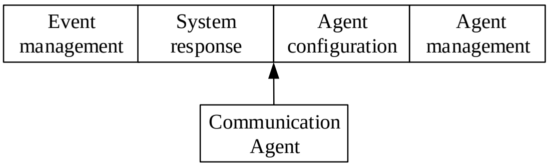


Fig. 3. Structure of center Agent.

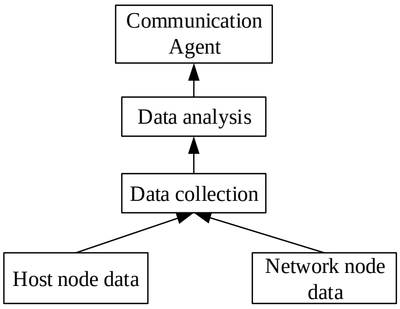


Fig. 4. Host Agent and network Agent.

Host Agent and Network Agent: The host Agent is configured on each server of the Internet of Things, which is responsible for collecting system logs, system calls, and monitoring user behavior. In addition, network Agent is set up on the IOT gateway or route, in charge of collecting the original data packets in the network, classifying and filtering them, so as to search for sensitive information such as potential intrusion.

Analysis Agent: Located in the middle layer of the entire intrusion detection system, it is responsible for collecting the information uploaded by host Agent and network Agent to determine whether an intrusion has occurred. As the brain of the whole intrusion detection system, the analysis Agent employs data mining technology to extract features, and dynamically expands the intrusion pattern library through continuous learning to give full play to the detection ability of analysis Agent.

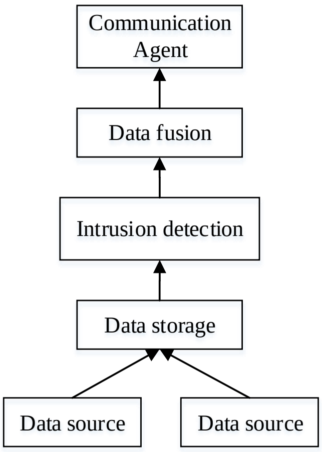


Fig. 5. Analysis Agent.

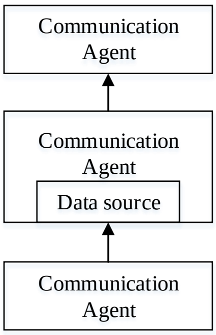


Fig. 6. Communication Agent.

Communication Agent: It is a data transmitter between modules, transmitting data information between modules. Its existence allows other modules to focus more on their own work. After obtaining the data from each module, the communication agent becomes an extended data-source-cum agent that will be back to the previous state (without data source) as the data source has been transferred to the destination module.

3. Intrusion detection method combined CFSFDP and PCA

3.1 Principal Component Analysis (PCA)

There is a lot of redundant information among numerous data actually transmitted by the IOT system. Therefore, before the intrusion detection system starts to use the clustering algorithm, it is necessary to simplify the data in advance, remove unnecessary information, and retain the main data that can optimize the clustering effect and minimize the amount of information. This can improve the efficiency, speed and accuracy of the algorithm. Removing the unimportant data to the greatest extent can greatly reduce the running time of the algorithm and improve the system efficiency without affecting the accuracy of the algorithm.

Principal Component Analysis (PCA) is a feature extraction method that linearly transforms a high-dimensional input vector into a low-dimensional vector by calculating the eigenvectors of the covariance matrix of the input vector.

The sample X is composed of m N-dimensional data, each of which is treated as a coordinate in the N-dimensional space. The sample matrix is $X=\left(X_1,X_2,\cdots X_N\right)^T$, which is projected to vector Y in the low-dimensional space:

$$Y=W^TX \tag{1}$$

First construct a covariance matrix which is defined as:

$$C=\frac{1}{N}\sum_{i=1}^{N}\left[\left(X_i-E(X_i)\right)\left(X_i-E(X_i)\right)^T\right] \tag{2}$$

where $E\left(X\right)$ is the average of the i-th dimensional data, and the expression is:

$$E(X)=\frac{1}{N}\sum_{i=1}^{N}X_i \tag{3}$$

Then, solve the problem shown in equation (2):

$$\gamma_i W_i=CW_i \tag{4}$$

W_i is the i-th column of the orthogonal matrix W; γ_i is the eigenvalue of the covariance matrix C, and W_i is the eigenvector corresponding to the eigenvalue. Eigenvalue γ_i is arranged in descending order from the greatest to the least, and the first-K corresponding maximum eigenvectors are selected to form a projection matrix W^T. Through equation (1), we can obtain K-dimensional data of the sample data X after the dimensional reduction from N dimension.

The basic process of the PCA algorithm is as follows:

Input: $N\times m$ original dataset's matrix is $X=(X_1,X_2,\cdots X_N)^T$.

Output: K-dimensional data after dimensional reduction.

Step (1): Zero-mean for each row of matrix X.

Step (2): Find the covariance matrix.

Step (3): Find eigenvalues and eigenvectors of the covariance matrix.

Step (4): Arranging eigenvalues from top to bottom according to the amount of corresponding eigenvectors, and taking the first-K rows to form matrix W^T.

Step (5): $Y=W^TX$ is K-dimensional data after dimensional reduction.

3.2 CFSFDP clustering algorithm

The CFSFDP algorithm is a clustering analysis algorithm based on density peak. Because of its simple idea and few parameters, it has become a popular research topic in the field of clustering analysis in recent years. The basic idea of the algorithm is: first calculate the local density and the adjacent density point distance, and then select the cluster center to judge the distance between cluster center and other non-cluster center points. When the distance is small enough, the non-cluster center point is classified into the class-cluster in which the cluster center is located. The idea of selecting a cluster center needs to satisfy two conditions. First, the local density of the point is relatively large, surrounded by points whose densities are smaller. Second, the distance between this point and other points with higher local density is relatively far.

The parameters and variables in the algorithm are defined as follows. The cluster data sample set is $S=\{X_i\}_{i=1}^{N}$, and the corresponding index set is $I_S=\{1,2,\cdots,N\}$; any data point X_i in the cluster dataset S can be described by local density ρ_i and adjacent density point distance δ_i.

(1) Local density

As shown in the equation, d_c means the distance between data points X_i and X_j, which is specified by the user in advance. Local density ρ_i indicates that the number of points whose distance is between data point X_i and other data points in the dataset S is less than that of d_c. The algorithm indicates that the clustering effect is the best when the number of adjacent data points of each data point is between 1% and 2% of the total number of points in the range of d_c.

$$\rho_i = \sum_{i,j\in I_s} \varphi\left(d_{ij}-d_c\right) \tag{5}$$

$$\varphi(x)=\begin{cases}1, x<0\\ 0, x\ge 0\end{cases} \tag{6}$$

(2) Adjacent density point distance

The adjacent density point distance is described as: the shortest distance between X_i and other points whose local densities are larger than that of X_i. For a point with the largest local density, its adjacent density point distance is the maximum of the distance between the point and all data points.

$$\delta_i = \min\left(d_{ij}\right) \tag{7}$$

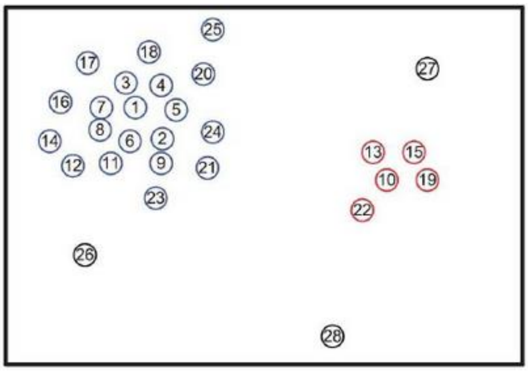


Fig. 7. Two-dimensional distribution map.

The distribution of original data points of dataset S is as shown in the figure. For each data point $X_i(\rho_i,\delta_i)$ of data set S, the plane rectangular coordinate system is established with ρ as abscissa and δ as ordinate. And the cluster decision diagram of the dataset is drawn.

According to the description of selecting cluster center by the CFSFDP algorithm, when a data point is with a large ρ and δ at the same time, the point has a large possibility to become a cluster center. When δ of a data point is large and its ρ is small, the point is regarded as an outlier.

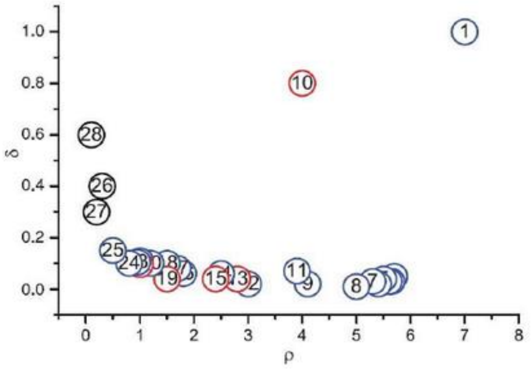


Fig. 8. Cluster decision diagram.

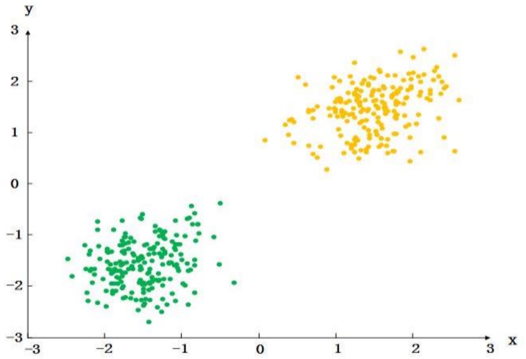


Fig. 9. Clustering result of two clusters dataset.

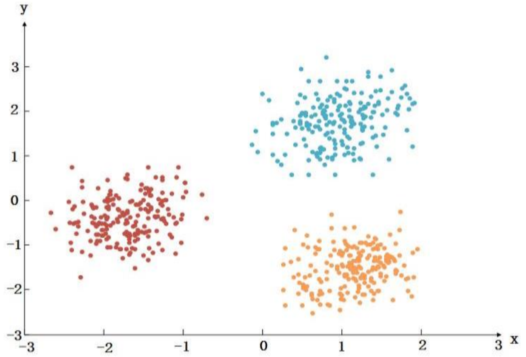


Fig. 10. Clustering result of three clusters dataset.

The basic process of the CFSFDP algorithm is as follows:

Input: Dataset S

Output: The corresponding class-cluster number of dataset S.

Step (1): Calculate the distance d_{ij} between each data point and arrange them in ascending order.

Step (2): Determine d_c according to the number of data points in the dataset, calculate local density ρ_i of each data point and sort them from high to low.

Step (3): Let $\delta_1=\max\left(d_{ij}\right)$, calculate the rest δ_i according to the equation and sort them from big to small.

Step (4): Calculate $\gamma_i = \rho_i \delta_i$, and select some points with larger γ_i value as the center point of the class-cluster according to the principle of decision diagram.

Step (5): According to the class-cluster center point and the density boundary threshold, the remaining data points are divided into different class-clusters.

To verify the availability and feasibility of CFSFDP algorithm with varieties of the data sets, two artificial linear data sets and three artificial non-linear data sets are selected to carry out the simulation, whose results are shown in Fig. 9~Fig. 13.

From the two resulting figures above, it could be clearly seen and realized that the selected data sets are categorized suitably (with the scenario of the dataset which has two subgroups, two resulting clustering domains are shown; and for the dataset with three subgroups, three domains are pictured). Hence, it is reasonably guaranteed that the CFSFDP clustering algorithm has a strong power to cluster and adapt to the linear data, as well as to the non-linear data, seen in figures below (Fig. 11~Fig. 13).

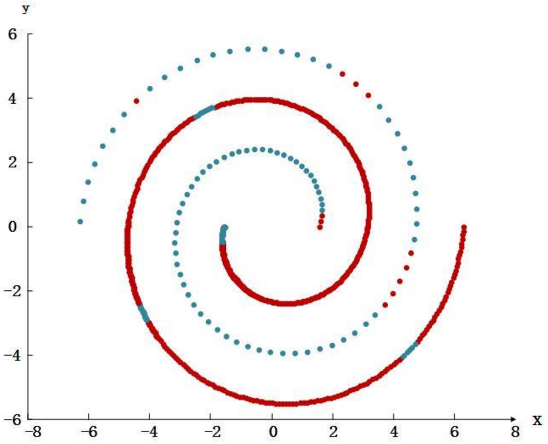


Fig. 11. Clustering result of spiral unbalance dataset.

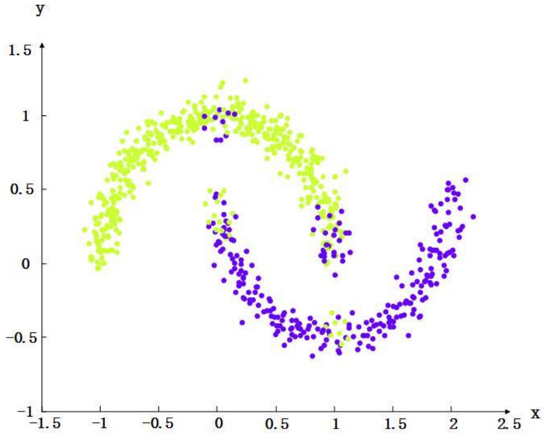


Fig. 12. Clustering result of two moons dataset.

In the numerical simulation, the Purity evaluation measure is as an evaluation index to test the clustering effectiveness and accuracy of the clustering algorithm. In Purity, only the proportion of the number of the data points with clustering currently to the total number of the data points should be considered and computed, the expression of the Purity is shown as:

$$purity(\Omega, C) = \frac{1}{N} \sum_k \max(\omega_k \cap c_j) \tag{8}$$

where $\Omega = \{\omega_1, \omega_2, \omega_3, \cdots, \omega_k\}$ represents the set of the clusters, and ω_k means the set of the k-th cluster; $C = \{c_1, c_2, c_3, \cdots, c_j\}$ is the real category of the data set, and c_j represents the j-th type of data; N represents the total number of data in the dataset.

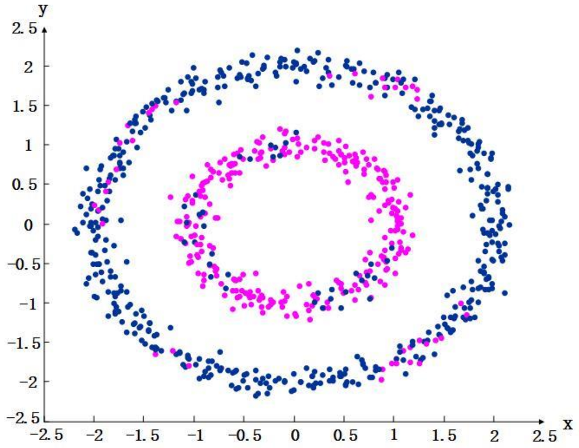


Fig. 13. Clustering result of two circles dataset.

The purity method is suitable for describing the accuracy of the clustering algorithm, which can effectively reflect the influence of the number of clusters to the precision of clustering results within the clustering process. The larger purity value generally means the more approximate between the clustering group and the real category.

Tab. 1. The number of actual categories in each data set

Dataset	Ionosphere	Seeds	Wine	Glass
Number of classes	2	3	3	6

Tab. 2. Clustering accuracy of K-means algorithm

Dataset	Number of clusters	Purity
Ionosphere	4	0.69
Seeds	3	0.71
Wine	4	0.63
Glass	7	0.42

Tab. 3. Clustering accuracy of AP algorithm

Dataset	Number of clusters	Purity
Ionosphere	38	0.45
Seeds	42	0.39
Wine	51	0.34
Glass	40	0.49

Tab. 4. Clustering accuracy of CFSFDP algorithm

Dataset	Number of clusters	Purity
Ionosphere	2	0.84
Seeds	3	0.90
Wine	3	0.79
Glass	6	0.75

In the experimental simulations, 5 data sets selected from UCI database are applied. And to validate the accuracy and the degree of precision, K-means and AP algorithm are both taken into consideration for comparing with CFSFDP.

According to the four resulting tables above, it is apparently known that as for the same dataset, comparing with the real number of the subgroups of the dataset, more subgroups will be generated by AP algorithm, and the accuracy and the degree of precision of CFSFDP are significantly higher compared with K-means and AP algorithm.

3.3 Establishment and detection process of feature rule-base

Firstly, the CFSFDP clustering algorithm is used to cluster the sample data, so that the data with large similarity is in the same class, and the data similarity between the classes is the smallest. In this case, PCA is applied to perform data dimensional reduction and feature extraction on various types of data after clustering, which can reduce the impact of unnecessary features on the running speed and accuracy of the system. After forming the principal-component feature set of each cluster, it is stored in the feature rule-base to test the dataset for feature matching of intrusion detection. The detection process is as follows:

(1) Use the PCA for feature extraction on the test data;

(2) Perform the Euclidean Distance comparison with the cluster center point to cluster the test data;

(3) Conduct feature matching with feature rule-base;

(4) If the matching degree exceeds the threshold, alarm response is made and corresponding measures are taken.

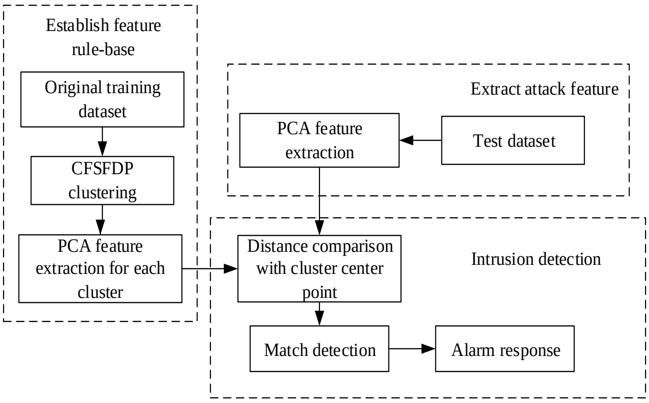

Establish feature rule-base
Original training dataset
CFSFDP clustering
PCA feature extraction for each cluster
Extract attack feature
PCA feature extraction
Test dataset
Distance comparison with cluster center point
Intrusion detection
Match detection
Alarm response

Fig. 14. Detection model combined CFSFDP with PCA.

4. Simulation experiment and result

The experiment in this paper is carried out in a PC environment with Intel Core i5, 4G memory, and Windows7 system. Performance evaluation of the intrusion detection model is performed using the MATLAB2014a simulation platform.

Tab. 5. Identification classification of KDD Cup99 dataset

Identification type	Specific classification	Description
Normal	normal	Normal record
DOS	back、pod、 smurf、 neptune、teardrop,、land	Denial of service attack
Probing	ipsweep、portsweep、 nmap、satan	Surveillance and other detection activities
R2L	tp_write、warezclient、 imap、multihop、 phf、spy、guess_passwd、 warezmaster	Illegal access from a remote machine
U2R	buffer_overflow、perl 、 loadmodule 、 rootkit	Ordinary user's illegal access to local superuser privileges

In this experiment, the KDD Cup99 dataset is applied to verify the above method. The KDD Cup99 dataset consists of training dataset and test dataset. Each training and test data will record 41 feature attributes and one type tag. The training dataset is divided into normal-type data identified "normal" and 22 attack-type data. In addition, in order to test the generalization ability of the classifier model, 17 unknown types of attack data are also included in the test dataset (no identification).

Tab. 6. Feature attributes of KDD Cup99 dataset

Feature attributes	Feature number
Basic features of network connection	No.1-9
Content features of network connection	No.10-22
Time-based network traffic statistics	No.23-31
Host-based network traffic statistics	No.32-41

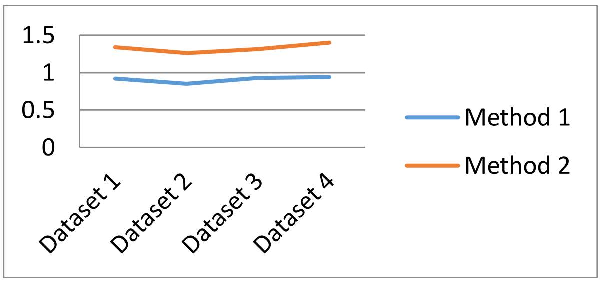


Fig. 15. Comparison of detection time between two methods.

The 20,000 pieces of data randomly extracted in the 10% training dataset (kddcup.data_10_percent.gz) are selected as training dataset of the feature rule-base. Four groups are randomly selected from the test dataset (kddcup.newtestdata_10_percent_unlabeled), and 1000 pieces of data of each group are subjected to the attack test. In this paper, the performance of the algorithm will be evaluated by two performance indexes: detection rate P_{Fdr} and false positive rate P_{err}. These two indexes are respectively defined as:

$$P_{Fdr} = \frac{N_c}{N_s} \times 100\% \tag{9}$$

$$P_{err} = \frac{N_{err}}{N_n} \times 100\% \tag{10}$$

where N_c, N_s, N_{err} and N_n respectively indicate the number of intrusion samples correctly detected, the sum of intrusion samples, the number of normal samples that are wrongly judged, and the sum of normal samples. In order to verify the effectiveness of this method and the superiority of its performance, the method is compared with the method combined K-means and PCA. The method in this paper is recorded as method 1, and the latter is recorded as method 2. In the method described in the paper, parameter d_c is obtained by equation $d_{f(Mt)}$, N is the total number of data points, $M = \frac{1}{2}N(N-1)$ and $f(Mt)$ represents the rounding value of Mt product. As to t, it is selected between 1% and 2% N. After repeated trials, the training dataset has the best clustering effect when the value of t is 0.15. The comparison of detection time between two methods is shown in Fig. 15.

Tab. 7. DOS detection rate and false positive rate

Method	Detection rate	False positive rate
1	79.5%	6.9%
2	87.1%	5.4%

Tab. 8. Probing detection rate and false positive rate

Method	Detection rate	False positive rate
1	80.7%	4.7%
2	88.3%	4.1%

Tab. 9. R2L detection rate and false positive rate

Method	Detection rate	False positive rate
1	76.2%	5.5%
2	85.6%	4.9%

Tab. 10. U2R detection rate and false positive rate

Method	Detection rate	False positive rate
1	77.2%	5.9%
2	84.2%	3.8%

As shown in Tab. 7 to 10, the intrusion detection method 1 combined CFSFDP and PCA has a significant improvement in detection rate and false positive rate compared with method 2.

5. Summary

This paper first proposes an intrusion detection model based on multi-Agent for Internet of Things. The basic components are composed of host Agent, network Agent, communication Agent, analysis Agent and center Agent. Then, an intrusion detection scheme combined CFSFDP algorithm and PCA algorithm is proposed. The final simulation results show that the proposed method has better improvement in detection time, with higher detection rate and lower false positive rate.

Acknowledgements

This work was supported by Liaoning Provincial Science Foundation (No. 201602615, 201602608), Natural Science Foundation of China (No. 61873174, 61503259), Project of Liaoning Province Education Department（LJZ2017015）, Shenyang Municipal Science and Technology Project (No. Z18-5-015) and Liaoning Provincial Archives Science and Technology Fund (L-2018-X-10)

References

Yating Wu, 2016. Internet of Things Network Security Protection. J. Network Security Technology & Application. (12),15-16.

Weicheng Xiong, 2017.Research on Internet of Things Security System Based on Intrusion Detection. J. Internet of Things technologies.7(09),78-80.

Qingbo Sun, 2012. Research of Intrusion Detection System of the Internet of Things Based on Neural Network. D. Jinan University.

Wei Wei, Bo Liang, Min Zuo,2018. Linear Active Disturbance Rejection Control for Nanopositioning System, International Journal of Applied Mathematics in Control Engineering, 92-95.

xin Zhang, Yuyu Yuan, 2012. Research of Intrusion Detection Technology Applying to Internet of Things. J. Software. 33(11):160-164.

Hamid Bostani,Mansour Sheikhan., 2017. Modification of supervised OPF-based intrusion detection systems using unsupervised learning and social network concept. J. Pattern Recognition ,62.

Qiang Chen, Yinqiang Wang, Zhongjun Hu ,2018. Finite Time Synergetic Control for Quadrotor UAV with Disturbance Compensation, International Journal of Applied Mathematics in Control Engineering ,31-38.

Wangwei Zhong, Xiaoou Huang, 2006. Analysis and Research on Common Model of Intrusion Detection System. J. Modern computer. (03):86-89.

Ming-sheng Guo, 2007. Struture Rules Base of IDs base on Multi Agent. D. Southwest University,.

Yachao Niu, 2018. Research and Design of the Intrusion Detection System Based on the Wireless LAN. D. Sichuan Normal University.

Qian Wang ,2017. Research and Implemention of Intrusion Detection Technology Based on Data Mining. D. Beijing University of Posts and Telecommunications.

Tongjuan Zhao, Jiuhe Wang ,2018. Multimodal Transport Path Planning based on Multilateration (MLAT) System Using a Pulse Neural Network Model, International Journal of Applied Mathematics in Control Engineering, 55-61.

Mehmood R, Bie R, Dawood H, et al. , 2015. Fuzzy Clustering by Fast Search and Find of Density Peaks. J. Personal & Ubiquitous Computing. 20(5):785-793.

Chunlai Ma, Hong Shan, Tao Ma, 2016. Improved Density Peaks Based Clustering Algorithm with Strategy Choosing Cluster Center Automatically. J.Computer Science. 43(7):255-258.

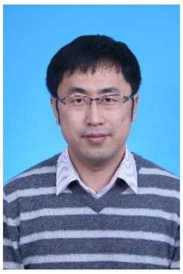
Yun-feng Yang,2017. Applied Research of Principal Component Analysis in Intrusion Detection. J. Journal of Hechi University. 37(05):76-81.

Guangzhen Zhao, Cui-xiao Zhang, 2018. Intrusion Detection Method Based on Principal Component Analysis and Probabilistic Neural Network. Journal of Shijiazhuang Tiedao University (Natural Science Edition). 31(01):91-95.

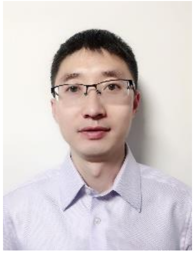
Cheng-hua Guo, 2017. Design and Implementation of Intrusion Detection System Based on KDDCUP99 Data Set. J. Network Security Technology & Application. (12):57-60.

Songjie Wang, Xiaofei Zhang, 2008. Analysis and preprocessing of KDDCup99 network intrusion detection data. J. Science & Technology Information. (15):407-408.

Wu Zhenbo is currently pursuing his M.S study at the Institute of Information and Control Engineering, Shenyang Jianzhu University, Shenyang, China. He obtained his B.S degree from Shenyang Jianzhu University, China in 2012. His main research interests are in the areas of network security, internet of things and intelligent building.



Lin Shuo is an associate professor at the Institute of Information and Control Engineering, Shenyang Jianzhu University, Shenyang, China. He obtained his M.S degree from Northeastern University, China in 2003 and his Doctor degree from Shenyang Institute of Automation, Chinese Academy of Sciences in 2012. His main research interests are in the areas of production process modelling, enterprise informatization reconstruction and manufacturing execution system.



Qi Yuanwei, born in 1982. He is now a lectorate in Shenyang Jianzhu University, Shenyang, China. He received his Master degree in computer application technology from Shenyang Jianzhu University in 2008.His research interests include image processing techniques, data mining and pattern recognition.

Han Zhonghua received his PhD at the Shenyang Institute of Automation, China in 2014. He is currently a Professor with the Faculty of Information and Control Engineering, Shenyang Jianzhu University, Shenyang, China. His main research includes production and operation management, integrated technology of automation system in enterprise, and the engineering application research of production scheduling method.