Measurement 157 (2020) 107536

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

Data transmission method for sensor devices in internet of things based on multivariate analysis

Jiangtao Xu [a,*], Fengbo Tao [a], Yang Liu [a], Chengbo Hu [a,b], Yang Xu [a], Farhad Keivanimehr [c], Narjes Nabipour [d,*]

[a] State Grid Jiangsu Electric Power Co., Ltd. Research Institute, Nanjing 210001, China
[b] School of Electrical Engineering, Southeast University, Nanjing 211189, China
[c] Department of Chemical Engineering, Amirkabir University of Technology, Mahshahr Campus, Mahshahr, Iran
[d] Institute of Research and Development, Duy Tan University, Da Nang 550000, Viet Nam

ARTICLE INFO

Article history:
Received 3 December 2019
Received in revised form 8 January 2020
Accepted 20 January 2020
Available online 23 January 2020

Keywords:
Multivariate analysis
Internet of things
Sensor network
Equipment
Data
Transmission

ABSTRACT

In this paper, tree diagrams and symbols in visualization technology are selected to display the security status of sensor networks, and fully mine the micro-details of the network through multi-dimensional display of monitoring target status. Time series maps are used to predict the operation trend of sensor networks in eight dimensions, and analyze network attack modes combined with image characteristics to evaluate the security situation of the Internet of Things. On this basis, a centralized wireless routing method is adopted to find the optimal path from all the sensing nodes to sink, which ensures that the sum of links' average transmission times of the optimal path and the minimum energy consumption of data transmission are the minimum. The results show that this method can identify the state of sensor network and discriminate attack modes, and has less data transmission times and low energy consumption.

1. Introduction

As the core information infrastructure of the future society, the Internet of Things has rapidly become the focus of competition in recent years. The main goal of the Internet of Things is to realize the wide interconnection and deep integration of information space and physical world. The wireless sensor network composed of various sensing devices is an important way to effectively perceive the physical environment, and is also one of the key means for the Internet of Things to thoroughly perceive the physical world [1]. As an Internet of Things endpoint network, wireless sensor network can provide the Internet of Things with the means of active perception of the physical world on a large scale of time and space [2]. In a typical wireless sensor network, many sensor nodes with physical sensing, data processing and wireless communication capabilities are written in a given monitoring area to monitor some physical states in the area cooperatively. The sensing data is transmitted from the source node to the remote sink node in a wireless multi-hop mode [3].

In the field of Internet of Things applications, sensor networks formed by sensor devices need to transmit a large amount of data. Sensor nodes rely on batteries for power supply, which has limited charges. A large amount of data collected by sensor networks need to be transmitted to sink nodes through sensing nodes for further in-depth analysis [4]. Therefore, how to use limited energy to transmit as much data as possible has become a major challenge for data transmission in wireless sensor networks. With the expanding scale of computer network, the increasing speed of information superhighway and the increasing application of network, network security is facing more and more severe challenges. The scale of Internet of Things attacks is increasing, e.g. distributed denial-of-service attacks can often trigger thousands of devices to attack a sensor host at the same time; more and more types of attacks, new attack modes and variants of viral Trojans are invincible; attacks change more and more rapidly, and a premeditated network attack often contains multiple steps and a variety of contingency plans. Therefore, it is of great practical significance to study the secure data transmission method for sensor devices in the Internet of Things [5].

There are many studies on data transmission methods for sensor networks at home and abroad. Based on heuristic optimization algorithm, Jiang et al. proposed an optimization model for big data transmission of sensor networks, including optimization objective

* Corresponding authors.
E-mail addresses: xujiangtao_sgo@163.com (J. Xu), narjesnabipour@duytan.edu.vn (N. Nabipour).

https://doi.org/10.1016/j.measurement.2020.107536
0263-2241/

function and various restriction mechanisms. Finally, the heuristic algorithm was used to locate the optimal solution of decision space [6]. Mozaffari et al. put forward a data transmission model, which calculated the average transmission times of the links by using the transmission characteristics of the sensing nodes' transmission link conditions. On this basis, by finding the data transmission path with the shortest average transmission times, the data transmission from the sensing nodes to sink was realized [7]. Ngai et al. proposed a clustering transmission model for big data in sensor network environment. Using Bernoulli sampling algorithm, the clustering and mean results with high accuracy were obtained. The approximate results were transmitted to sink nodes by tree model for further in-depth analysis, so that the clustering model realized efficient data transmission in sensor network and saved energy [8].

In order to solve the problems of the above methods, a multi-element analysis based data transmission method for Internet of things sensor equipment is proposed. The overall scheme of the method is as follows:

(1) The typical dimension features of heterogeneous security log data are extracted by using information entropy and other related algorithms.
(2) Through the introduction of symbol and tree chart, we can fully mine the micro details of data, through the introduction of time series chart, we can predict the trend of network operation, through the induction of image features, we can intuitively analyze the security status of the Internet of things.
(3) The optimal data transmission path from sensor node to receiver node is obtained by multivariate analysis method, which ensures that the expected transmission time of all links in the path from sensor node to receiver is minimum [9].

Through the above scheme, the data can be transmitted safely and effectively.

2. Materials and methods

The selection of security data sources determines the comprehensiveness and accuracy of the Internet of Things security analysis. Therefore, the representative, real-time, low redundancy and richness of the Internet of Things sensor data provided by VAST Challenge 2013 as the research object. The data set contains three kinds of data recorded by sensors, Netflow (in switching devices, used to monitor the traffic changes of sensor network communication in the Internet of Things), HostStatus (in the host, used to monitor the performance changes of resource subnet) and IPS (in the outlet device, used to check and disconnect connections with security risks), which can simultaneously grasp the trend of change of network data's coverage, representativeness and real-time performance [10].

2.1. Micro details

In order to realize multi-dimensional display of monitoring target status, tree diagrams and symbols in visualization technology are selected to display the security status of sensor networks in a certain period of time. In addition, the sub-network is planned by using class B reserved address according to the actual situation, and the hierarchical management of the whole Internet of Things-sub-sensor network-host [11] is realized by combining tree diagram. As shown in Fig. 1, it is a tree diagram and a symbol schematic diagram. The rectangular box represents the monitoring target host, whose size is proportional to the number of streams, and the red degree of color is proportional to the flow rate. In addition, there are CPU, memory, hard disk, IPS alarm icons in the rectangular space to indicate the status of the host, and different states are distinguished by color.

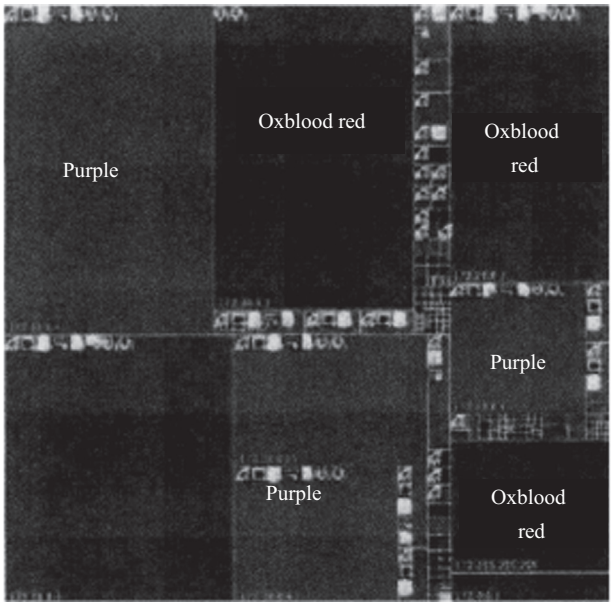


Fig. 1. Tree and Symbol Diagrams.

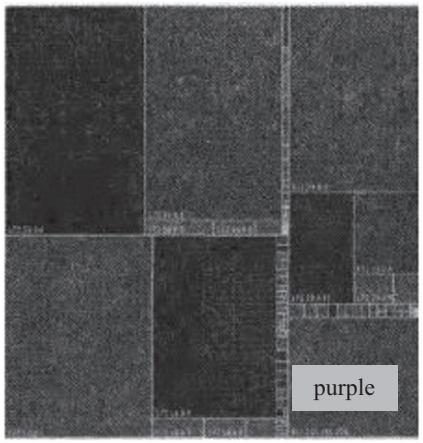
In the algorithm of tree diagram, Squarified algorithm, which can arrange rectangles in descending order (highlighting representative objects), has good real-time performance (generating fast) and aesthetics (aspect ratio can be approximated to 1), is chosen as the main algorithm to deal with the large-scale heterogeneous data of the Internet of Things [12], which has high real-time requirement of the system.

In the feature analysis of the tree diagram, the actual distribution of the tree diagram can be used to effectively analyze the flow state of the sensor network. Generally, when the rectangular distribution in the image is over-dispersed or centralized, the network is prone to abnormalities. As shown in Fig. 2, it is a tree diagram distribution image of normal and abnormal sensor network flow (Table 1).

The exponential distribution function is used to describe the flow of sensor networks. The corresponding exponential distribution mathematical expression is shown in Eq. (1):

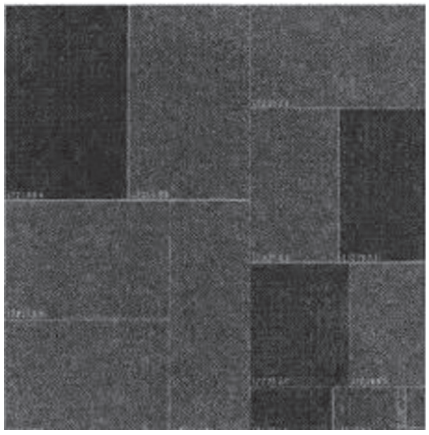
$$f(x) = \begin{cases} \lambda e^{-\lambda x}, & x > 0 \\ 0, & x \leqslant 0 \end{cases} \tag{1}$$

If $\lambda \geqslant 0.3$, the image shown in Fig. 2(b) shows only a few rectangular blocks, because a large number of sensor network flows launched a network attack on a few individual hosts (probably denial of service attack); if $0.1 \leqslant \lambda < 0.3$, in the image shown in Fig. 2(a), one side of a large rectangle is surrounded by some small blocks. This is due to the distribution of users and large traffic servers in the target network, so the server load is heavy, so that the tree diagram shows the phenomenon that the larger space on the left side of each sub-network area is occupied. The small traffic of other users is shown as surrounding blocks; if so, it is the image shown in Fig. 2(c), and the image distribution is relatively uniform. This is because more uniform network traffic attacks the host, showing the relevant characteristics of port scanning [13].



(a) Normal flow

(b) Denial of service



(c) Port Scanning

Fig. 2. Flow Tree of Sensor Networks.

2.2. Macro trends

The time series diagram is used to visually and clearly reflect the change and development trend of each observation point data in each dimension. In terms of dimension selection, according to the characteristics of heterogeneous data sources, the following eight dimensions are used to describe the security trend of the Internet of Things [14], as shown in Table 2. Because these eight dimensions can not be directly used from different sources, the corresponding feature processing algorithm is selected according to the characteristics of each data dimension. For Netflow data, the measurement index chooses information entropy (reducing uncertainty); for Host Status data, the comprehensive parameter weighting method is used to highlight some indicators; for IPS data, the statistics in the rejected connection process can be used.

Table 1
Description of experimental parameters.

Parameter	Meaning
x	Distributed parameter
λ	Distribution index
$P(x_i)$	Observation period frequency
L	Information entropy length
b	Poisson distribution parameters
P_i	Discrete distribution function in P
q_i	Discrete distribution function in Q
a	Cross dynamic entropy
$Normal$	Information entropy of normal period
$Current$	Information entropy of current cycle
$Previous$	Information entropy of the last period
$Service_i$	The first indicator in the host state
$Weight_i$	Weighting coefficient

For Netflow (including 6 data dimensions), x is used to represent discrete random variables, and the expression of information entropy is shown in Eq. (2):

$$H(x) = -\sum_{i=1}^{n} P(x_i) lbp(x_i) \tag{2}$$

where, $P(x_i)$ in the equation represents the frequency of x_i in the observation period. If the network data is centralized to a certain point, the information entropy will behave as 0; if the data distribution is loose, the value of information entropy will become larger. In addition, cross-entropy is introduced to distinguish whether the network state is normal in time window t. Its definition is shown in Eq. (3):

$$L_a(P,Q) = \frac{1}{1-a} lb \sum_{i-1}^{n} \frac{P_i^a}{q_i^{a-1}} \tag{3}$$

where, P_i and q_i in the equation are discrete distribution functions of P and Q respectively, and a generally takes 0.5 to simplify the calculation. Unlike single information entropy, cross-entropy examines dynamic changes. Ultimately, the exception state of Netflow is represented as shown in Eq. (4):

$$\beta L_{0.5}(Current, Normal) + (1-\beta) L_{0.5}(Current, Previous) > Threshold \tag{4}$$

where $Normal$, $Current$ and $Previous$ in the equation represent the information entropy calculated in the normal period, the current

Table 2
Internet of Things Security Data Eigenvalues.

Serial number	Feature name	Source	Processing method
Dimension 1	SrcIP	Netflow	Information entropy
Dimension 2	DestIP	Netflow	Information entropy
Dimension 3	SrcPort	Netflow	Information entropy
Dimension 4	DestPort	Netflow	Information entropy
Dimension 5	SrcBpp	Netflow	Information entropy
Dimension 6	DestBpp	Netflow	Information entropy
Dimension 7	HostStatus	Host Status	Comprehensive Weighting Method
Dimension 8	IPSDeny	IPS	Statistical value

Table 3
Time Series Characteristics.

Type of attack	SreIP red	DestIP Brownish red	SrcPort green	DestPort Fresh green	SrcBpp blue	DestBpp Light blue	HostStatus purple	IPSDeny Bright purple
Multi-port Scanning for Single Target Host	Decline	Decline	Decline	Increase	Decline	Decline	Unchanged	Increase
Multi-target Host Single Port Scanning	Decline	Increase	Decline	Decline	Decline	Decline	Unchanged	Increase
Multi-target host multi-port scanning	Decline	Increase	Decline	Increase	Decline	Decline	Unchanged	Increase
Single-source Denial-of-Service Attacks	Decline	Decline	Increase	Decline	Decline	Decline	Increase	Increase
False Source Address Denial of Service Attack	Increase	Decline	Increase	Decline	Decline	Decline	Increase	Increase
Distributed Denial of Service Attacks	Increase	Decline	Increase	Decline	Decline	Decline	Increase	Increase
Normal condition	Unchanged	Unchanged	Unchanged	Unchanged	Unchanged	Unchanged	Unchanged	Unchanged

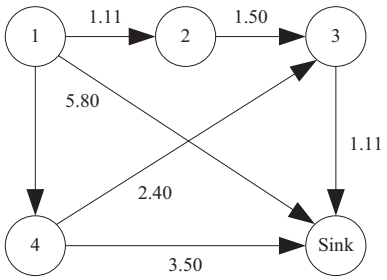


Fig. 3. Calculates the optimal path from each perception point to sink.

period and the last period respectively, while *Threshold* represents the basic threshold.

According to the relevant characteristics of *HostStatus*, the weighted method of comprehensive parameters is used, as shown in the following Eq. (5):

$$HostStatus = \sum_{i} Weight_i \times Service_i \tag{5}$$

In the equation, $Service_i$ and $Weight_i$ represent the first index and the corresponding weighting coefficients in the host state respectively. Finally, the state of the host of the sensor network can be defined by Eq. (6):

$$AllHostStatus = \sum_{j} WeightHost_j \times HostStatus_j \tag{6}$$

In the equation, $HostStatus_j$ and $WeightHost_j$ represent the state values and corresponding weighting coefficients of the j-th J host, respectively.

In the analysis of time series characteristics, it can discover the anomalies of Internet of Things by observing the obvious changes of some dimensions [15]. For example, in Table 3, if malicious software scans the same port in an Internet of Things, the attack type corresponds to a single port scan on a multi-target computer [16]. The results show that SrcIP information entropy decreases, DestIP information entropy increases, the effect of port scanning is minimum and the *HostStatus* change tends to be stable, while IPSDeny tends to increase (which should be caused by preventing scanning). If the network flow is normal, the information entropy values fluctuate relatively smoothly.

2.3. Routing method for data transmission

Based on the security situation of the Internet of Things network composed of sensor devices, a centralized wireless routing method is proposed to obtain the optimal data transmission path from all the sensing nodes to sink, to ensure that the sensing nodes to sink have the minimum number of data transmission, and to minimize the energy consumption [17]. Assuming that the node sensor network architecture is shown in Fig. 3, the optimal path from node 1 to sink is obtained.

The steps of the centralized routing method are as follows:

(1) $E(i) \leftarrow$ is the expected number of transfers from node 1 to node i, where i is all nodes except node 1.
(2) Find out the $\min(E[j], 1 \leqslant j \leqslant n)$, and node j joins the path.

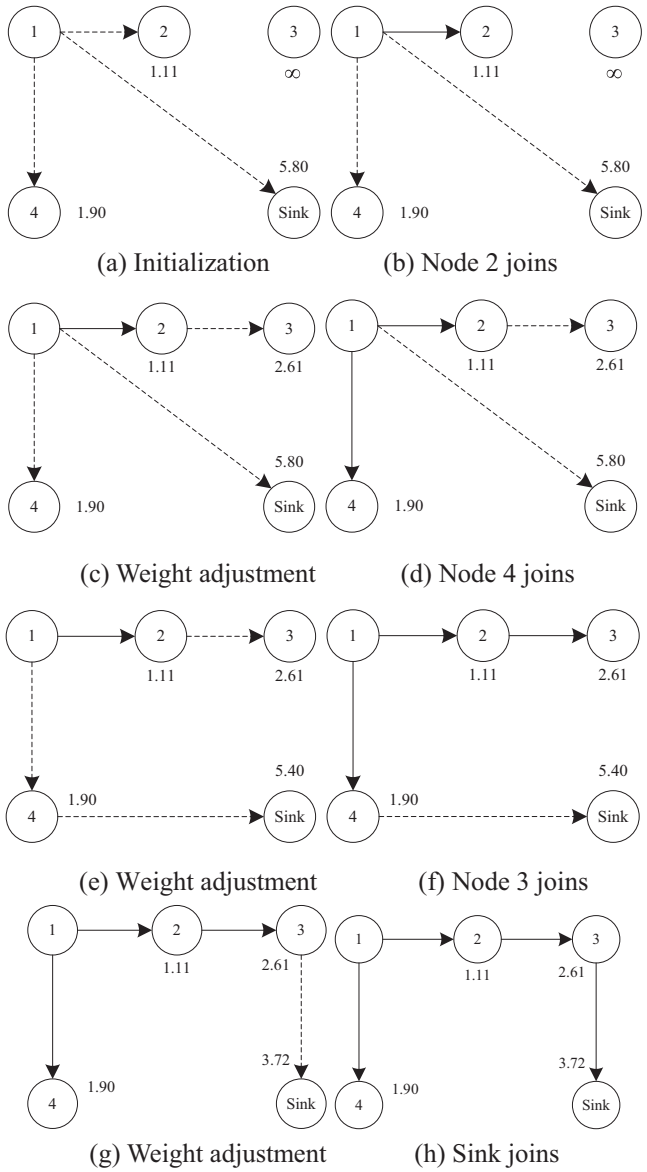


Fig. 4. Method Applied to Sensor Network Architecture Execution Process.

(3) Adjust the number of new nodes j, $for(i = 1; i \leqslant n; i++)$, $if(E[j]+$is the number of transfers from node j to node $i < E[i]$, while i does not join the path, and $E[i] = E[j]+$ is the number of transfers from node j to node i.

The centralized wireless routing method defines an array $E[n]$, which preserves the sum of the expected transmission times of the path from the starting node 1 to each node, i.e. the sum of weights.

The centralized wireless routing method consists of two parts. The first part is the initialization part. The weights of node 1 to all nodes are infinite if there is no communication link between node 1 and other node. The second part is a loop, in turn, the possible nodes are added to the path. The first step of the loop is to find the minimum number of transmission links in the array $E[n]$, and the corresponding nodes join the path [18]. The second step is to adjust. Comparing the original path of the new node with the new path after the new node joins, the path with less transmission times is taken as the new data transmission path.

The centralized wireless routing method is executed in Fig. 3 as shown in Fig. 4.

Step 1: Initialize the path weights from node 1 to node 4, node 2 and sink node, which are 1.9, 1.11 and 5.8 respectively, then store them in $E[4], E[2], E[5]$ (assuming node 5 is sink) and the rest of the nodes do not have links to node 1, so $E[3] = \infty$.
Step 2: Node 2 has the minimum weight, so node 2 joins the path.
Step 3: For node 2 with new paths, adjust the expected transmission times of other nodes as follows: the weights of node 2 + node 2 to node 3 are the sum of path weights of starting node 1 to node 3, specifically 1.11 + 1.50 = 2.61, then $E[3] = 2.61$. The rest of the nodes do not need to be adjusted according to the *if* statement of the *for* loop in step 3 of the method. The next step is to find out the minimum weight, and then analogy.

This method can be applied to other nodes as starting nodes, and the path of minimum expected transmission times from all nodes to sink can be obtained. The main feature of this method is the centralized method. The time complexity of the method is mainly reflected in the loop. The time complexity of the method itself is $0(n^2)$. If the optimal path from all nodes to sink is required, the method needs to run $n-1$ times, and the overall time complexity is $0(n^3)$ [19].

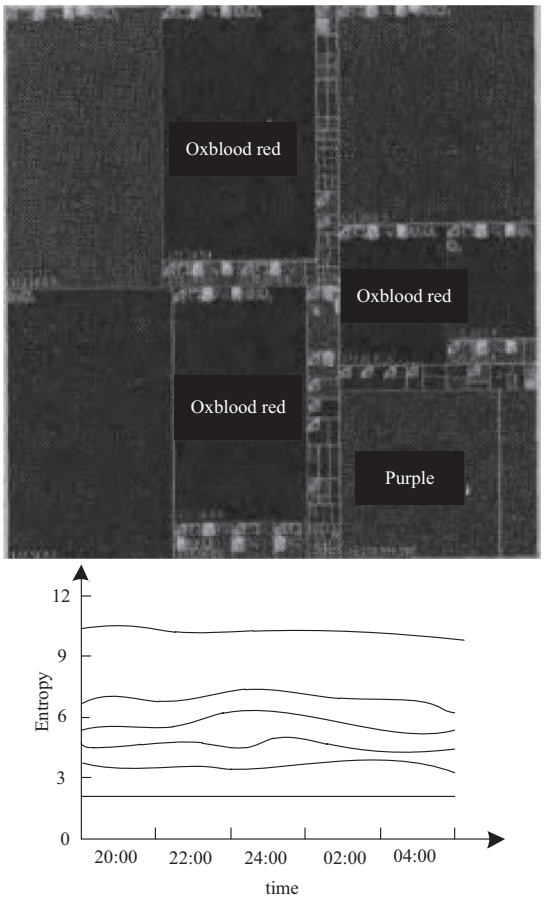
3. Results

3.1. Security state analysis of internet of things

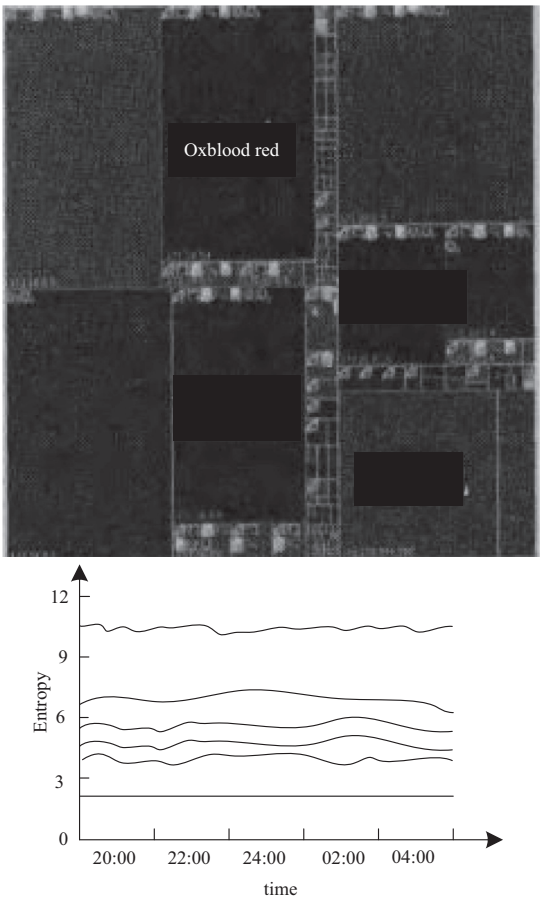
By analyzing the security situation of the Internet of Things on the time series diagram, the image features are matched, the abnormal time window of the Internet of Things sensor network is found out, and the characteristics of the sensor network on the tree diagram are further analyzed, to define the state of the sensor network, identify the attack mode and eliminate false alarms.

3.1.1. Normal state analysis

The time window from 20:00 on May 12, 2015 to 04:00 on May 13, 2015 of a sensor network of the Internet of Things is selected as



(a) Intranet comparison



(b) Comparison of Sensor Networks

Fig. 5. Normal State.

the experimental analysis object. The tree diagram and time sequence diagram of the normal state are shown in Fig. 5.

From Fig. 5, it can see that the change of time series chart is relatively stable in a longer period of time, and it can judge that the network is in normal state during this period. It can also be seen from Fig. 5(a) that the upper left of each subnet area is occupied by hosts with relatively large number of flows in the network. Among them, the large dark red block is the server with the largest number of streams and the heaviest load. The dark red area of Fig. 5(b) shows that the host with IP address 172.10.0.4 in the sensor network has the heaviest load and the largest number of streams. In addition, by carefully observing and analyzing all the symbols shown in Fig. 5, the green color of the symbols indicates that the host is working normally. However, the host hard disk flag with IP address 172.10.0.4 has been warned. It is preliminary speculated that the warning originated from the overload on the host. Through the analysis of the tree diagram, we can further confirm that the current sensor network is in the normal state.

3.1.2. Abnormal state analysis

Fig. 6 is a tree diagram and time sequence diagram of the time window of May 12, 2017. Fig. 6(a) and (b) are the tree and time sequence diagrams of 8:00–l6:00 and 9:00–17:00 respectively.

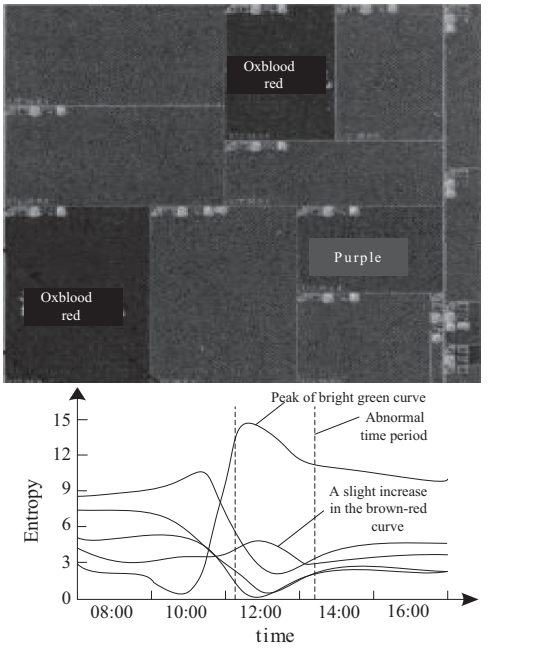
As can be seen from Fig. 6(a), the ordinates marked as red state in time series graph indicate that mutual information has exceeded the threshold at this time, and some abnormal situations occur in the enterprise network. The bright green lines on behalf of DestPort increase significantly, the brown red lines on behalf of DestIP increase slightly, and the other lines have a certain degree of sinking. Looking at Table 3, we can see that it should be the attack type of multi-port scanning for multi-target hosts. Further analysis of the network with tree diagram shows that the rectangular block is larger and more uniform. It shows that the mainframe has a large number of streams, but the flow is low. In addition, most of the symbols in the tree are green, which indicates that the scanning will not seriously affect the host performance to a large extent, and is consistent with the characteristics of port scanning.

As can be seen from Fig. 6(b), the ordinates of time series graphs have been marked as red, and the bright green curve representing DestPort has dropped to the bottom, indicating that the same port between the external host and the internal host is connected; The peak value of bright purple lines indicates that a large number of connections have been banned. By referring to Table 3, we can see that it should be the attack type of single-port scanning for multi-target host. Further analysis of the network state based on tree diagram shows that there are many yellow warning shields in the rectangle, and the target of attack basically involves the whole sensor network.

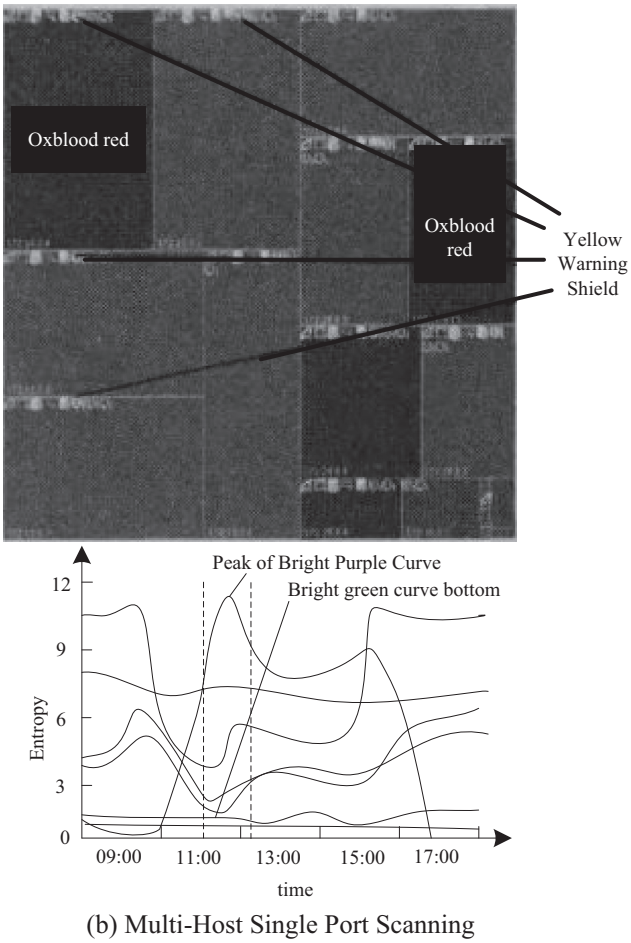
3.2. Data transmission

In order to test the correctness and reliability of the proposed scheme, the data transmission of sensor sensing nodes is tested and evaluated.

Experimental environment: 802.15.4 sensor network, 802.15.4 low-rate physical layer and media access control protocol are used for low-rate wireless sensor networks. TinyOS operating system is used for running experimental sampling nodes, and Intel Mirage experimental bed is run. The experimental nodes are fixed in the sensing area, and sink nodes are installed to collect data transmitted by the sensing nodes. More than 10,000 sampling nodes are used to collect temperature and other humidity data. After sampling the data, the sensing nodes send the data directly to the adjacent nodes to measure the packet reception rate of the link. MPR, Cluster and Pruning are selected to compare with the method in this paper. The comparison of average transmission times is shown in Fig. 7. Link quality refers to packet loss during data transmission. The relationship between link quality and average transmission times is shown in Fig. 8.



(a) Multi-Host Multi-Port Scanning



(b) Multi-Host Single Port Scanning

Fig. 6. Port scan.

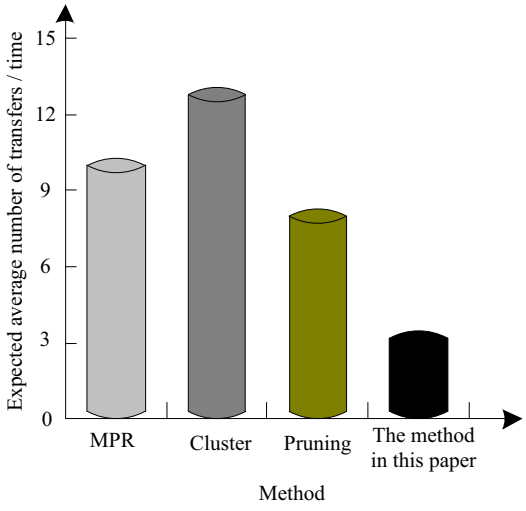


Fig. 7. Comparison of average transmission times of different methods.

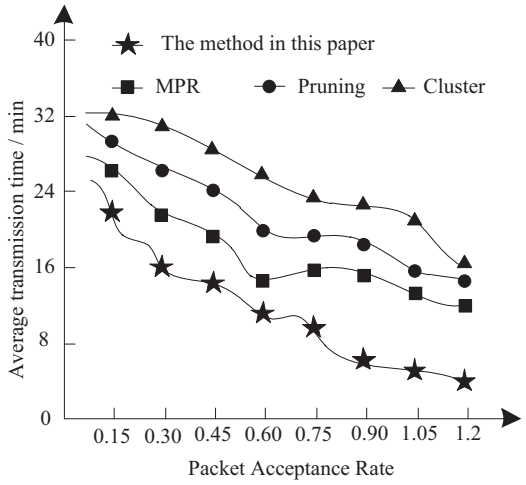


Fig. 8. The relationship between link quality and average transmission times.

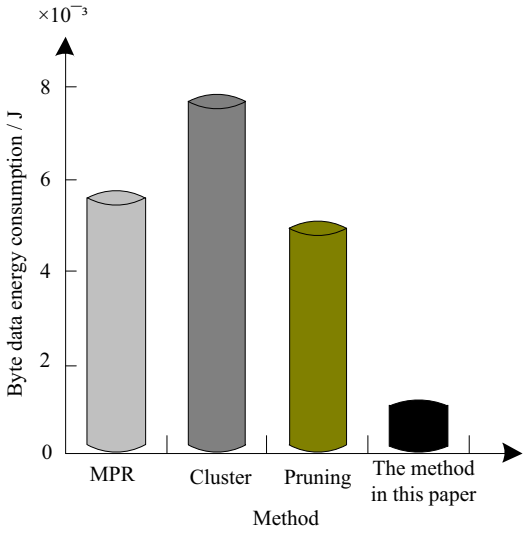


Fig. 9. Energy consumption comparison of different methods.

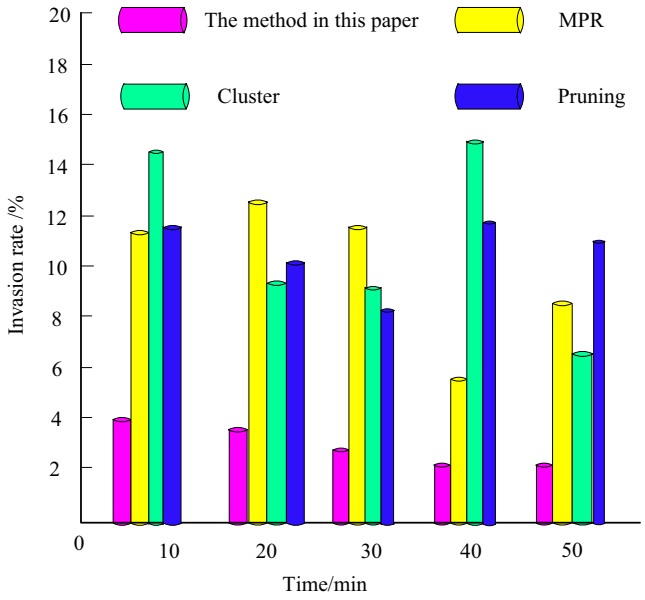


Fig. 10. Comparison results of intrusion rates of different methods.

In this method, an average of about 3.98 transfers are required from Node 1 to ensure that the data is transferred to the sink node, while the other methods require more transfers. Since the link data reception rate will change gradually with the decrease of node power, the relationship between link quality and average transmission times can be seen from Fig. 8. With the improvement of link quality, the average number of transmission decreases gradually.

Fig. 9 shows a comparison of the energy consumption of different methods.

In Fig. 9, the energy consumption of the proposed method is the energy consumption of the node with the largest load. From the analysis of Fig. 9, it can be seen that the energy consumption of the proposed method has obvious advantages over other methods.

In order to further verify the performance of transmission methods, four methods are compared and verified with intrusion rate as the comparison index. In the same experimental environment, the intrusion rate comparison results of the four methods are shown in Fig. 10.

It can be seen from the analysis of Fig. 10 that, with the increasing transmission time, the intrusion rate of the proposed method is lower than that of the three comparison methods, which fully shows that the proposed method has high security.

4. Discussions

In order to study the secure data transmission method of sensor devices in the Internet of Things, this paper firstly uses the visualization method based on multivariate analysis to fuse all kinds of Internet of Things security data to improve the comprehensiveness and accuracy of network status recognition, anomaly recognition and pattern recognition [20]. Eight main data dimensions are extracted from multiple heterogeneous log data to show the network situation. Different feature extraction algorithms are used for different dimensions. Netflow uses information entropy, HostStatus uses comprehensive weighting method, IPSDENY uses information statistics to draw time series maps. Through simple image feature analysis and matching, analysts can grasp network problems more intuitively and find attacks mode. Compared with the lattice representation of internal host, the hierarchical structure of tree diagram is adopted in this system. For the management of

large and super large networks, this method will not cause the problem of image congestion due to insufficient display space, and can not distinguish the image, so as to reduce the image blockade. At the same time, symbols are used to expand the representation dimension of tree diagram and enhance the ability of the whole system's visual expression and fusion. Based on the security situation analysis of the Internet of Things, a centralized routing method for data transmission of sensor devices in the Internet of Things is proposed by using the average transmission times of links. The centralized routing method determines the optimal path of data transmission from perception nodes to sink, ensures that the sum of average data transmission times of links in the path reaches the minimum. The minimum average transmission times means the minimum energy consumption. Compared with MPR, Cluster and Pruning methods, the advantages of the proposed method are verified by experiments. This research is mainly for battery-powered interconnection. The safe data transmission of network sensor device has important practical significance.

5. Conclusions

The main goal of the Internet of Things is to realize the extensive interconnection and deep integration of information space and physical world. As the end network of the Internet of Things, wireless sensor networks composed of sensor devices provide the means of active perception of the physical world for the Internet of Things. The security situation of wireless sensor networks is the basic guarantee of data transmission in the Internet of Things. In this paper, aiming at the trend of multi-heterogeneity of security log data in sensor networks, the trend of data operation in multi-heterogeneity sensor networks is analyzed from micro-details and macro-trends. Combining with image characteristics, network attack modes are analyzed and judged, and network security situation is evaluated. On this basis, a centralized wireless routing method is used to find the optimal path from all the sensing nodes to sink, which ensures that the sum of the average link transmission times in the optimal path is minimized. Despite extensive and in-depth research on the secure data transmission method for sensor devices in the Internet of Things, there are many factors affecting the secure data transmission in the sensor network, and various factors affect each other, so a lot of work still needs to be further studied.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The research is funded by the National Key Research and Development Program (2018YFB0904700), Key Technologies and Applications of Medium and Low Voltage DC Power Distribution System.

References

[1] J. Shu, S. Liu, L. Liu, et al., Research on link quality estimation mechanism for wireless sensor networks based on support vector machine, Chinese J. Electron. 26 (2) (2017) 377–384.
[2] N.S. Wang, X.F. Li, C. Fang, et al., Design of contactless power and data transmission system for buoy's underwater sensors, Chinese J. Power Sources 41 (1) (2017) 131–133.
[3] H. Huang, T. Gong, Y. Ning, et al., Private and secured medical data transmission and analysis for wireless sensing healthcare system, IEEE Trans. Ind. Inf. 13 (3) (2017) 1227–1237.
[4] X. Liu, J. Yu, W. Lv, et al., Network security situation: from awareness to awareness-control, J. Network Comp. Appl. 139 (2019) 15–30.
[5] L. Jian, W. Dan, H. Yan, et al., A method for extracting angle information of direct P wave in shallow burst point localization based on wireless sensor array, Sensor Rev. 37 (1) (2017) 61–70.
[6] B.B. Jiang, H. Yu, Clustering algorithm for wireless sensor networks with integrated load balancing and energy consumption, J. Jilin Univ. (Sci. Ed.) 55 (06) (2017) 1552–1556.
[7] M. Mozaffari, W. Saad, M. Bennis, et al., Mobile unmanned aerial vehicles (UAVs) for energy-efficient internet of things communications, IEEE Trans. Wireless Commun. 16 (11) (2017) 7574–7589.
[8] E. Ngai, F. Dressler, V. Leung, et al., Guest editorial special section on internet-of-things for smart cities and urban informatics, IEEE Trans. Ind. Inf. 13 (2) (2017) 748–750.
[9] W. Cheng, J. Yu, F. Zhao, et al., SSDNet: small-world super-dense device-to-device wireless networks, IEEE Network 32 (1) (2018) 186–192.
[10] L. Chen, Anti jamming design of fractal microstrip antenna receiving signal sensor, Comp. Simulation 34 (11) (2017) 163–167.
[11] Y.W. Kuo, C.L. Li, J.H. Jhang, et al., Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications, IEEE Sens. J. 18 (12) (2018) 5187–5197.
[12] S. Zhang, X. Xu, J. Peng, et al., Physical layer security in massive internet of things: delay and security analysis, IET Commun. 13 (1) (2019) 93–98.
[13] Deng Rui, He Jing, Yu. Jianjun, et al., Increasing data rate of an optical IMDD system using a cost-efficient dual-band transmission scheme based on RTZ DAC and sub-nyquist sampling ADC, Opt. Express 26 (9) (2018) 11599–11607.
[14] W.X. Zhu, Design and implementation of intelligent sports system based on wireless sensor network technology, Automation Instrument. 232 (2) (2019) 82–85.
[15] D. Zhang, Z. Chen, J. Ren, et al., Energy-harvesting-aided spectrum sensing and data transmission in heterogeneous cognitive radio sensor network, IEEE Trans. Veh. Technol. 66 (1) (2017), 1-1.
[16] Daisuke, Kamiyama., Akira, Yoneyama., Motoharu Matsuura, Multichannel data signals and power transmission by power-over-fiber using a double-clad fiber, IEEE Photon. Technol. Lett., PP(99) (2018) 1-1.
[17] Z.J. Lu, X. Liu, Y.G. Qin, et al., An adaptive multi-sensor management method for cooperative perception, J. China Acad. Electron. Inform. Technol. 12 (4) (2017) 353–358.
[18] R. Kumar, D. Kumar, D. Kumar, EACO and FABC to multi-path data transmission in wireless sensor networks, IET Commun. 11 (4) (2017) 522–530.
[19] S. Kang, J. Kim, S. Yang, et al., Electric field energy harvesting under actual three-phase 765 kV power transmission lines for wireless sensor node, Electron. Lett. 53 (16) (2017) 1135–1136.
[20] P. Zhang, Q.F. Zhang, S.C. Song, et al., Permanent magnet motor vector control using hall effect position sensor, J. Power Supp. 15 (1) (2017) 81–86.