Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2021 SCPE. Volume 22, Issues 2, pp. 149–159, DOI 10.12694:/scpe.v22i2.1880

RESEARCH ON DATA SECURITY DETECTION ALGORITHM IN IOT BASED ON K-MEANS

JIANXING ZHU *, LINA HUO †, MOHD DILSHAD ANSARI ‡ AND MOHAMMAD ASIF IKBAL§

Abstract. The development of the Internet of Things has prominently expanded the perception of human beings, but ensuing security issues have attracted people's attention. From the perspective of the relatively weak sensor network in the Internet of Things. Proposed method Aiming at the characteristics of diversification and heterogeneity of collected data in sensor networks, the data set is clustered and analyzed from the aspects of network delay and data flow to extract data characteristics. Then, according to the characteristics of different types of network attacks, a hybrid detection method for network attacks is established. An efficient data intrusion detection algorithm based on K-means clustering is proposed. This paper proposes a network node control method based on traffic constraints to improve the security level of the network. Simulation experiments show that compared with traditional password-based intrusion detection methods; the proposed method has a higher detection level and is suitable for data security protection in the Internet of Things.This paper proposes an efficient intrusion detection method for applications with Internet of Things.

Key words: Internet of things; intrusion detection; clustering algorithm; network security.

AMS subject classifications. 68M25, 68M18

1. Introduction. Internet is a global tool through which people from across the globe share their personal and important information. Availability of this private and personal information at fingertip causes misuse of these data. The main cause for this is the various ways created by internet itself for stealing the security and stability of interrelated system. A data cited in figure 1.1 is representing the surge in cyber-crime from 2018-2019 and depicts the loss faced by the companies in dollars [1]. The reasons can be classified as dynamic and static. Dynamic security is provided by the static mechanism like software update and firewalls; it also provides mechanism such as intrusion detection system. In today's scenario keeping ones data safe is a major challenge for all the technocrats. That is why we need both the dynamic and static mechanism to protect valuable information of the users irrespective of other precautionary measure build in the technology. With the help of intrusion detection system any violation of the security will be monitored and identified with necessary action [2,3].

There is a standard component of a security infrastructure that allows network administrators to detect policy violations. Check all incoming and outgoing network activity and determine suspicious patterns that indicate network or system attacks from people trying to break or compromise the system. With the help of intrusion Detection System network administrators can identify any breach in the policies related to the security. It monitored the traffic over the specified network and identifies any suspicious activity from the end of user. The essentials to attribute any system as a safe system must include data confidentiality, data integrity and data availability [4].

The importance of network security becomes more vital considering the continuous development of computer technology and electronic technology that has promotes the continuous progress of science and technology, and the world information industry has set off an upsurge of the Internet of Things [5]. At present, various countries are conducting related theories and application research. As the development of the Internet of Things industry

*College of Mathematics and Information Technology, XingTai University, XingTai 054001, China (ZhuJianxing873@gmail.com).
†College of Mathematics and Information Technology, XingTai University, XingTai 054001, China (linahua35@gmail.com).
‡Department of Computer Science and Engineering, CMR College of Engineering and Technology, Hyderabad, India (m.dilshadcse@gmail.com).
§Department of Electronics Engineering, Lovely Professional University, Punjab, India (asif.22797@lpu.co.in).

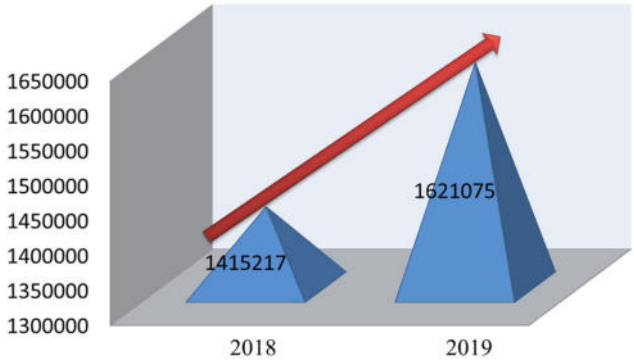

FIG. 1.1. *The average cost of insider attack, source: Accenture and Ponemon's 2019*

is included in our country's 12th Five-Year Development Plan, the development of the Internet of Things will usher in a new opportunity [6]. As a system that aims to realize the ubiquitous perception of things, the Internet of Things is composed of various sensor networks, radio frequency readers and other information acquisition equipment and communication systems [7]. The birth of the sensor network, as an important technology to realize the perception of data of things in the Internet of Things, provides the possibility to realize the ubiquitous perception of things [8]. However, the private-ness of sensing devices and their characteristics of being often deployed in unattended areas have caused the security of sensor networks to become an unavoidable problem [9].

The remaining manuscript is structured as follows: Section 2 scrutinizes fundamental ideas related to K-Means Clustering Algorithms. Section 3 presents IoT Architecture; Section 4 illustrates the Analysis of data Security issues. Section 5 represents Data security detection algorithms: proposed algorithm and Section 6 shows the Experimental results and Analysis Lastly Section 7 summarizes the conclusion of the manuscript.

2. Literature Review. At present, the commonly used security detection methods can be divided into key management, authentication and secure routing protocols, but the existing methods are still unable to defend against many network attacks. Therefore, the Internet of Things system needs to adopt an active defense mechanism to realize the intrusion detection of various attacks in the Internet of Things [10]. In the aspect of intrusion detection, many scholars have carried out many studies. The literature adopts a partition-based intrusion detection algorithm for sybil attacks in the network, but the deployment of nodes requires certain restrictions; The literature uses the method of selecting witness points in the network to achieve witness the goal, but it needs to be carried out under the premise that the position coordinates of each node in the network are known; the literature has modified the problems in the literature, and the selection of witness nodes is no longer carried out in a random mode, but specified deployment [11]; The literature uses an improved routing protocol to achieve rapid detection of attacking nodes; the literature uses location-based cryptographic mechanisms to detect network attacks, but most of the time the location of nodes in the network may not be normally obtained [12]. In [13] the authors have represented the techniques and methods used for the invasion identification. The proposed model was based on designed framework and data mining concepts. This article further articulates the techniques and methods of data mining to accelerate the process of invasion identification. In another referred article authors have presented a novel hybrid model for the identification of any intruder. The efforts made by authors were in a direction to propose an advance version of traditional intruder detection system. The obtained results have showed better performance and intelligent detection [14].

In [15] an IOT and big data based data clustering analysis algorithm was proposed with the help of K-mans. At first, in accordance with the processing technology and complex event relation, the transformation of big data processing of IOT was made into analysis of complex relational scheme and extraction. That will be helpful in simplifying the complex structure of big data. The efforts was made to enhance the traditional k-means algorithm and optimized it so that it can be helpful for big data RFID data network. Further with the help of Hadoop cloud cluster platform, the cluster analysis of k-means was performed. In addition to all these

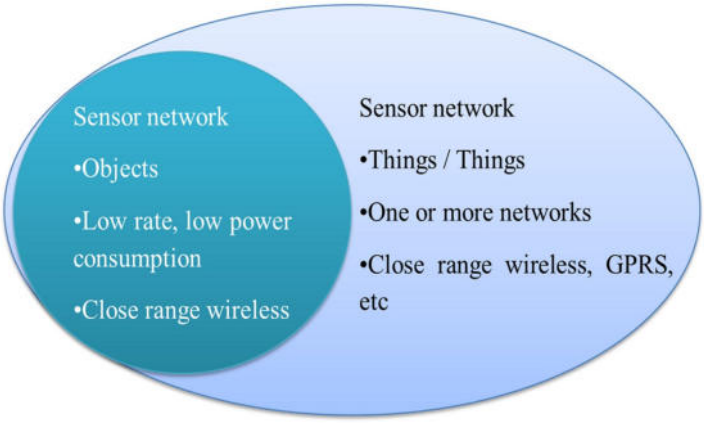

FIG. 3.1. *The relationship between the Internet of Things and sensor networks*

they have use the traditional clustering algorithm a central selection method appropriate for the RFID IOT data clustering was identified. The results have proved that the clustering efficiency has improved significantly. And on the basis on RFID and IOT clustering analysis prototype system was realized.

Although the above research has increased the security of the network to a certain extent, it usually can be completed only with the support of certain hardware. For this reason, this paper analyzes from the network data level, and studies a network intrusion detection method applicable to all IoT sensor nodes.

3. Internet of Things Architecture. According to the different communication process and objects, the Internet of Things can be expressed as a technology used for information interaction between things and people, with the goal of realizing comprehensive perception, information transmission and intelligent transmission. Its realization depends on the sensor nodes that detect the observed things and realize the networking function. A network composed of many sensor nodes is called a sensor network. Sensor network is mainly used to realize the connection between things, and at the same time, it is restricted by network self-organization structure and hardware resources. It generally exists in the form of short-distance, low-power wireless transmission. The relationship between the sensor network and the Internet of Things can be expressed as shown in Figure 3.1. As shown in Figure 3.2, each cluster in the sensor network contains a node with strong communication capability that acts as a gateway node in the network, which is called a cluster head. If data in other nodes needs to communicate with the base station, it needs to be forwarded through the cluster head [16]. Sensor network is the basis of the realization of ubiquitous perception in the Internet of Things. Its nodes are distributed in many places and are mostly in unsupervised locations. At the same time, limited by its hardware resources, its security problem is particularly important in the research of the Internet of Things [17]. How to detect and locate malicious nodes as soon as possible after an attacker appears in the network is an important issue to ensure the security of the communication process of the Internet of Things [18].

4. Analysis of Data Security Issues. In applications such as battlefield surveillance and target tracking, sensor network nodes are usually deployed in harsh environments. Attackers can not only eavesdrop on the radio, but also intercept the transmission information. Its current main forms are mainly as follows [19].

4.1. Black hole attack. A black hole attack means that one or more sensor nodes in the network do not forward the data according to the established method after receiving the data information sent by the neighboring nodes, but discard all the data to form a ”black hole” of data. Generally, a black hole Attacks can be divided into active and passive [20]. In passive black hole attacks, usually black hole nodes simply monitor and discard the data forwarded by themselves; while in active black hole attacks, ”black hole” nodes are attracted by declaring themselves as the next best path to neighboring nodes. More data sources, so passive black hole attacks are more destructive. The principle of black hole attack is shown in Figure 4.1 [21].

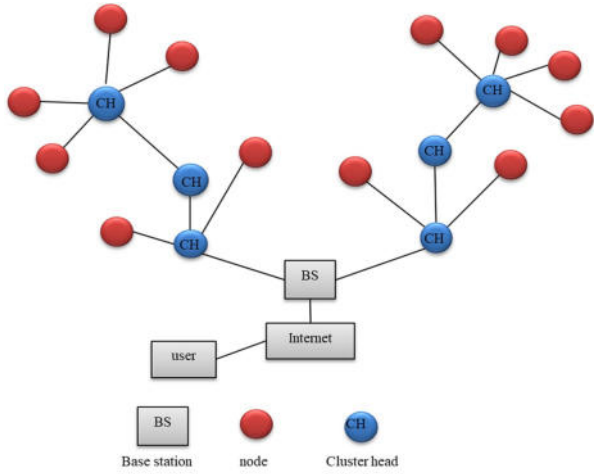

FIG. 3.2. *Network structure diagram*

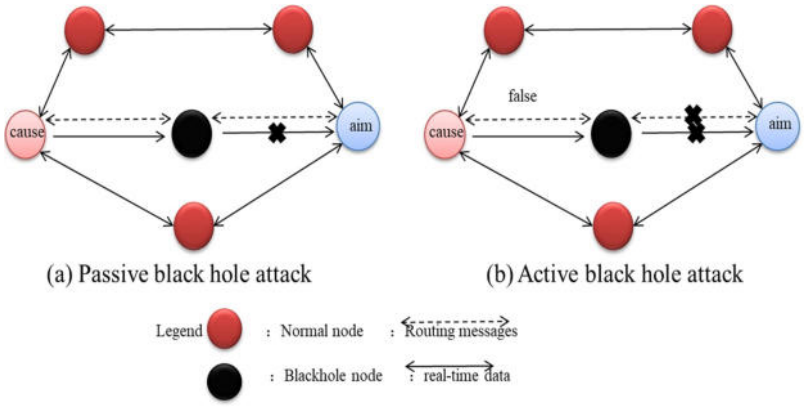

FIG. 4.1. *Black hole attack mode*

4.2. False routing information attack. This type of attack mainly uses tampering with routing information and guiding the network to transmit according to an extended or shortened established path, so as to achieve the purpose of dividing the established network, which will cause the end-to-end transmission delay of data in the network to increase. As shown in Figure 4.2(a), there is a communication path between the source node and the destination node during normal communication, and Figure 4.2(b) is the communication path between the source node and the destination node after being attacked by false routing. It can be seen intuitively from the figure that the network communication path is significantly extended, and the network delay is also greatly increased [22].

4.3. Wormhole attack. The attacker of the wormhole attack contains at least two sensor nodes. It mainly realizes the transmission of the monitored message to another network node for replay by establishing an ideal channel with low latency and high bandwidth between the two attackers. the goal of. Due to the existence of the "ideal channel", this path is preferred in the network, which may eventually lead to the failure of the network discovery process [23].

4.4. Witch attack. The attack mode of the sybil attack is to create false identity information for itself to achieve the purpose of impersonating other nodes"]. Other nodes in the sensor network will also transmit data to the attacking node and the normal node whose identity is copied, and the attacker can achieve the data for the purpose of eavesdropping. At the same time, because there are two nodes with the same identity in the

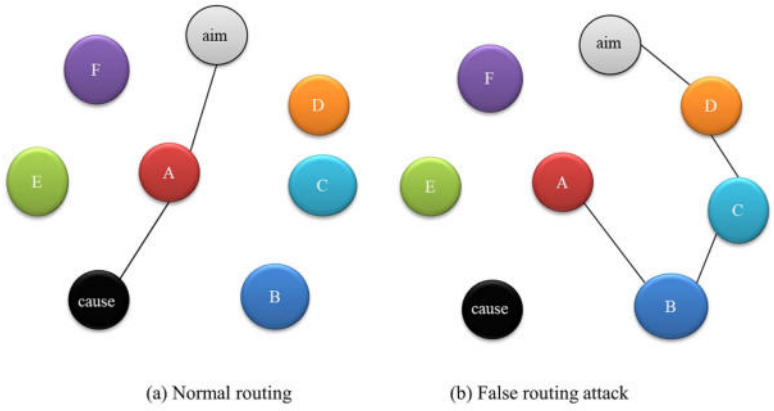

FIG. 4.2. *False routing attack network structure*

network, there may be positioning failures in some positioning services [24].

5. Data security detection algorithm. Aiming at data security issues in sensor networks, this article analyzes the types of special attacks and introduces network intrusion detection algorithms.

5.1. Data attack analysis.

5.1.1. Data feature extraction. According to the above network attack mode, the main feature of black hole attack is the loss of data. Suppose the received and sent traffic of network node i are T_rri and T_rsi respectively. If $T_rri > 0$ exists, And in theory, the sent data should be greater than 0 but the actual $T_rsi = 0$, then there may be black hole attack nodes in the network; in false routing attacks, wormhole attacks, and witch attacks, the significant feature is the change of network routing, so it is directly The result is an increase in data end-to-end delay. Literature proposes a method for obtaining communication data delay in sensor network nodes. Therefore, the data flow and data end-to-end delay at the network node can be used as one of the basis of network intrusion detection. The following is an analysis of the network intrusion detection method in this article [25].

5.1.2. Data cluster analysis. The concept of the Internet of Things is proposed to realize the ubiquitous perception of things, so the data types of the sensor network as the front end of data collection will show the characteristics of diversification and heterogeneity. The size of the transmitted data, the difference of network routing protocols, etc. will cause the difference of the end-to-end delay of the data in the network, so the pre-processing of the data before the data intrusion detection is essential. In order to extract the differences in the data of different sensor network nodes, this paper uses the K-means clustering method to cluster the data. The K-means clustering method has good clustering characteristics. It can divide the data set into k subsets according to the difference in the "distance" between the elements of the data set, and each subset has a cluster center [26,27]. Inter-coupling is zero. The steps of K-means clustering are as follows:

1) Select the value of k according to the clustering requirements, where $k > 1$;

2) In the cluster initialization stage, suppose that the data set contains total data samples, whose samples are represented by v_i, and randomly select k samples $Center_1$, $Center_2$,..., $Center_k$ as Initial cluster center;

$$dis(n) = \sqrt{(v_1)^2 - ((center)_n)^2} \tag{5.1}$$

3) Representation sample x_i The geometric distance from the cluster center $Center_n$. And according to the minimum distance principle, the sample is divided into

$$mindis(n) = 1, 2, ..., k \tag{5.2}$$

In the corresponding cluster C_k;

4) Update the cluster center to

$$Center_n = ((\sum(v_i))/p), \tag{5.3}$$

where p represents the number of samples in this class after clustering. 5) Repeat Step 3) and Step 4), taking the minimum error square as the criterion of clustering performance until the cluster $center_n$ no longer changes.

6) The algorithm ends, and the k clustering center values and clustering results are output.

5.2. Sensor network intrusion detection algorithm.

5.2.1. Symbol description. T_{rsi} : Data traffic sent by node i
T'_{rsi} : The threshold value of node i sending data traffic
T_{rri} : Data traffic received by node i
T'_{rri} : The threshold of node i receiving data traffic
T_i: Transmission delay at node i
T'_i: The transmission delay threshold at node i
d_{ij} : The distance between node i and the previous node j
d_f : The distance to the node with the farthest distance from the center after clustering
$2R$: Maximum communication distance in the network

5.2.2. Implementation of detection algorithm. Assuming that there are n sensor nodes in the Internet of Things, the detection process will be described below.

1) Intrusion detection part

Step 1: Select the network sending and receiving traffic at any node i, T_{rri}, T_{rsi}. And data transmission delay T_i. As the observation object in the network. The feature vector of node i can be expressed as:

$$V_i = (T_{rsi}, T_{rri}, d_i, T_i) \tag{5.4}$$

The feature vectors of all nodes in the network at a certain moment constitute a set V_{set}.

Step 2: Make

$$V_{mean} = (T_{rs} - mean, T_{rr} - mean, d_{mean}, T_{mean}) \tag{5.5}$$

Equal to all V_{set} The average value of the characteristic data in. Assume d_{max} is the maximum actual communication distance between all nodes in the network, and the theoretical value of the node end-to-end communication delay is the maximum T_f. If V_i in d_i, T_f and $V'_i = V_{mean}$ and update the collection V_{set}.

Step 3: Use the K-means clustering method to divide the collected data set into k groups, and use the data set separately C_k. Indicates that the data member is V_i

Step 4: Data detection process Black hole attack detection: for any $V_i \in C_k$, if $T_i > T'_i$ Then the node is identified as an attacking node. Otherwise, if the node is not judged as a black hole attack node, the node is a normal node. For any V_i, $j \in C_k$, if $d_i j < 2R$ and $T_{rri} > T'_{rri}$. The node j is determined to be the cooperative node of the network attack, and i is the attacking node of the network; otherwise, if the node is not identified as the above-mentioned attacking node, the node is a normal node[28,29].

Step 5: Generate data sets of different types of network attacks, and update the thresholds of various attributes in the network attack model.

The above steps can be expressed in pseudo code as:

Input: $V_{set} = V_{i|i} \in G, d_{max}, T_f$
Initial: $V_{mean} = (\sum V_i)/(nodecount(G))$
If $d_i \cdot T_i > d_{max} \cdot T_f$
Then $V'_i = V_{mean}$
Endif
Use K-mean, method to obtain clustering results:C_k, V_i
if $T_i > T'i$

Then i is the attack node
Else if $T_{rri}! = 0$ and $T'_{rsi}! = 0$ and $T_{rsi} = 0$
Then i is the black hole node and added to $V_{blackattack}$
Else if i is a normal node and added to V_{normal}
Endif
If $d_{ij} < 2RANDT_{rri} > T'_{rri}$
Theni is a collaborative node and added to $V_{cooperation}$
Else if i is a normal node and added to V_{normal}
Endif
Output: $V_{blackattack}, V_{cooperation}, V_{normal}$

2) Node authority management part: In order to avoid the influence of misjudgment caused by the abnormal node communication caused by accidental factors on the system, this paper uses the "distance" from the normal node as the judgment basis to control the network node. Assuming that the authority management part of the network is carried out by an independent key, the execution process is as follows:

Step 1: Suspected attack nodes in the computing network V_j;The distance from the cluster center p_j.
Step 2: Limit the node's network traffic to $M = T'_{rrj} - \mu P_j$, where the output is the flow penalty coefficient, which can be set according to needs. When certain p_j, the larger the node, the less traffic is allowed to pass.
Step 3: The master station issues traffic restriction instructions in the form of keys.
Step 4: In the next p times of detection, if the node is judged to be a normal node, the restriction on the node's traffic will be cancelled through instructions [30].

The above steps can be expressed in pseudo code as:

Input: $V_{blackattack}, V_{cooperation}$
Get the cluster center of any node j C_k $P_j = V_j C_k$
Set flow threshold $M_j = T'_{rrj} - \mu P_j$
For 1 to n
Check whether j is a normal node through the intrusion detection program
If j is a normal node
Normal Count ++
End if
End For
If Normal Count==n
Then set the flow threshold $M = T'_{rrj}$
Endif
Output: $M = \{M_j / j \in V_{blackattack}, V_{cooperation}\}$

The flow chart of the algorithm in this paper is shown in Figure 5.1.

6. Experimental results and analysis. This article uses Openet simulation software for simulation, and its simulation environment is shown in Table 6.1. The number of attacking nodes in the network is 10% of the total, or 72. We set 42 nodes as black hole attack nodes, 10 nodes as false routing attack nodes, 4 witch attack nodes, and 16 wormhole attack nodes.

In order to detect the effect of network intrusion, we choose detection rate (DR) and false detection rate (FPR) as the main evaluation indicators. Suppose the number of attacking nodes that are correctly detected in the network is TP, the number of attacking nodes that are not detected is FN; the number of normal nodes judged as attacking nodes is FP, and the number of attacking nodes judged as attacking nodes is TN. Then its expression is:

$$DR = ((TP)/(TP + FN)) \tag{6.1}$$

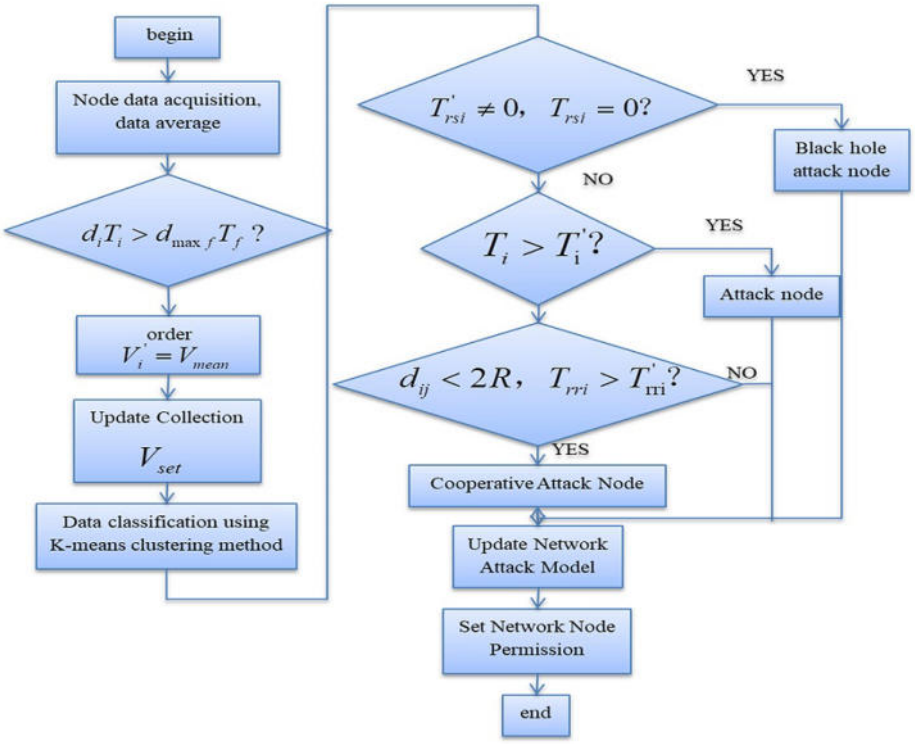

FIG. 5.1. *Algorithm flow chart*

TABLE 6.1
Simulation parameter settings

Parameters	Description
Simulation platform	Opnet 14.5
System platform	Windows XP
Network topology	Tree structure
Routing Agreement	AODV
Number of sensor nodes	720
Number of cluster head nodes	30
Number of nodes per cluster	24
Proportion of attack nodes	10%

(6.2) $$FPR = ((FP)/(TN + FP))$$

Table 6.2 shows the data delay of some nodes in the network. Among them, node 4 is a black hole attack node in the network, which has a certain network delay, but the network delay of wormhole attack node 1 in the network is greater.

As shown in Table 6.3, the data traffic received by node 7 in the network is greater than the normal threshold. By looking up the neighboring nodes of node 7 we can know that it contains node 1, so node 7 is the data forwarding terminal of attacking node 1. In order to verify the effectiveness of the method in this paper, the literature and the method in this paper are used to randomly deploy attack nodes in the above simulation environment to conduct 10 simulation experiments, and the detection rate and false detection rate are counted.

TABLE 6.2
Data end-to-end delay data (unit: second)

Node Number	T_i'	T_i
1	0. 0046	0. 0148
4	0. 0021	0. 0033
7	0. 0054	0. 0054
8	0. 0098	0. 0135
10	0. 0041	0. 0052
17	0. 0037	0. 0037
83	0. 0096	0. 0096
253	0. 003	0. 003
511	0.0107	0. 0107
.....	.....	.....
720	0.0093	0.0093

TABLE 6.3
Table 3: Network node receiving traffic data (unit: bps)

Node Number	T_{rsi}'	T_{rsi}
1	1024	1024
4	1024	1024
7	1024	2048
8	1024	1024
9	1024	2048
36	1024	1024
154	1024	1024
231	1024	1024
655	1024	1024
.....	.....	.....
720	1024	1024

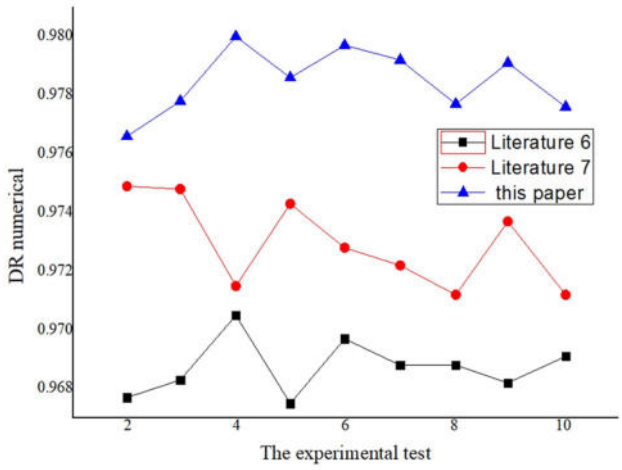

FIG. 6.1. *The detection rate of different experiments*

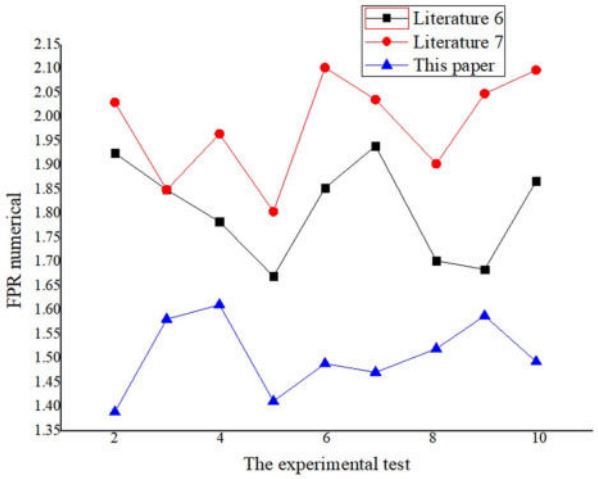

FIG. 6.2. *False detection rate of different experiments*

The detection results are shown in Figure 6.1 and Figure 6.2. It can be seen from the figures that the detection rate of the algorithm in this paper is significantly higher than the other two algorithms, and the probability of false detection is also lower than other algorithms.

7. Conclusion. Aiming at the security issues of the Internet of Things, this paper starts from the weaker wireless sensor network, analyzes the current network attack patterns, and proposes an efficient intrusion detection method for applications with Internet of Things. In order to reduce the drawbacks caused by algorithm detection errors, a node authority control strategy based on traffic restriction is proposed, which improves the security of IoT communication. By comparing with commonly used algorithms, the proposed algorithms significantly improves the detection level of network intrusion, and is applicable to guarantee the security of the Internet of Things in different scenarios. As a future work one can analyze the proposed algorithm with other data mining algorithms and can work on the identification and characterization of intruders attack.it may be further identified that how the proposed methods can be used with other real time environment data set.

REFERENCES

[1] WEI, P. , AND ZHOU, Z., *Research on security of information sharing in internet of things based on key algorithm*, Future Generation Computer Systems, 88(NOV.), 599-605, 2018.

[2] YU, X. , FAN, X. , CHEN, K. , AND DUAN, S., *Multi-attribute missing data reconstruction based on adaptive weighted nuclear norm minimization in IOT*, IEEE Access, 6, 61419-61431, 2018.

[3] LIU, Y. , TONG, K. D. , MAO, F. , AND YANG, J., *Research on digital production technology for traditional manufacturing enterprises based on industrial internet of things in 5g era.*, The International Journal of Advanced Manufacturing Technology,107(3), 1101-1114, 2020.

[4] ZHU, X. , LI, Q. , CHEN, Z. , ZHANG, G. , AND SHAN, P., *Research on security detection technology for internet of things terminal based on firmware code genes*, IEEE Access, PP(99), 1-1, 2020.

[5] LI, Y. Z. , XIA, H. , ZHANG, R. , XU, H. B. , AND CHENG, X. G., *). A novel community detection algorithm based on paring, splitting and aggregating in internet of things*, Sustainability, IEEE Access, PP(99), 1-1, 2020.

[6] BHARTI, M. , KUMAR, R. , AND SAXENA, S., *Clustering-based resource discovery on internet-of-things*, International Journal of Communication Systems, 31(5), e3501.1-e3501.23, 2018.

[7] QIU, T. , WANG, H. , LI, K. , NING, H. , SANGAIAH, A. K. , AND CHEN, B., *Sigmm: a novel machine learning algorithm for spammer identification in industrial mobile cloud computing*, IEEE Transactions on Industrial Informatics, 15(4), 2349-2359, 2019.

[8] ZHOU, Z. , ZHAO, X. , AND ZHU, S., *K-harmonic means clustering algorithm using feature weighting for color image segmentation*, Multimedia Tools and Applications, 77(12), 15139-15160, 2018.

[9] SEDAGHAT, S., *The forensics of ddos attacks in the fifth generation mobile networks based on software-defined networks*, International Journal of Network Security, 22(1), 41-53, 2020.

[10] JINBO, X. , JUN, R. , LEI, C. , ZHIQIANG, Y. , MINGWEI, L. , AND DAPENG, W. , ET AL., *Enhancing privacy and availability for data clustering in intelligent electrical service of iot*,IEEE Internet of Things Journal, PP, 1-1, 2018.

[11] Jia, P. , Wang, X. , and Zheng, K. , *Distributed clock synchronization based on intelligent clustering in local area industrial iot systems*, IEEE Transactions on Industrial Informatics, 16(6), 3697-3707, 2020.
[12] Da Costa, K. A. P. , Papa, J. P. , Lisboa, C. O. , Munoz, R. , and De Albuquerque, V. H. C., *Internet of things: a survey on machine learning-based intrusion detection approaches*,Computer Networks, 1151(MAR.14), 147-157, 2019.
[13] Kapil, S., Chawla, M., and Ansari, M. D., *On K-means data clustering algorithm with genetic algorithm*,In 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 202-206, 2016.
[14] Gautam, P., Ansari, M. D., and Sharma, S. K., *Enhanced security for electronic health care information using obfuscation and RSA algorithm in cloud computing*,International Journal of Information Security and Privacy (IJISP), 13(1), 59-69, 2019.
[15] Ansari, M. D., Gunjan, V. K., and Rashid, E., *On Security and Data Integrity Framework for Cloud Computing Using Tamper-Proofing*,IIn ICCCE 2020, 1419-1427. Springer, Singapore, 2020.
[16] Xiong, J., Chen, X., Yang, Q., Chen, L., and Yao, Z. , *A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing*,IEEE Transactions on Network Science and Engineering, 2019.
[17] Yu, Zhanqiu , *Big data clustering analysis algorithm for internet of things based on K-means*,International Journal of Distributed Systems and Technologies, 10(1), 1-12, 2019.
[18] Guo, Xuancheng, et al. , *A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems*,Future Generation Computer Systems 113 (2020), 407-417, 2020.
[19] Goap, Amarendra, et al. , *An IoT based smart irrigation management system using Machine learning and open source technologies*,IEEE Internet of Things Journal, Computers and electronics in agriculture 155 (2018), 41-49, 2018.
[20] Shakeel, P. Mohamed, et al. , *Cloud based framework for diagnosis of diabetes mellitus using K-means clustering*,Health information science and systems 6.1 (2018), 16, 2018.
[21] Gu, Yonghao, et al. , *Semi-supervised K-means DDoS detection method using hybrid feature selection algorithm*,IEEE Access, 7, 64351-64365, 2019.
[22] Zhang, Guiqing, Yong Li, and Xiaoping Deng., *SK-Means Clustering-Based Electrical Equipment Identification for Smart Building Application*,Information 11(1), 27, 2020.
[23] Soheily-Khah, Saeid, Ahlame Douzal-Chouakria, and Eric Gaussier., *Generalized k-means-based clustering for temporal data under weighted and kernel time warp*,Pattern Recognition Letters 75, 63-69, 2016.
[24] Myridakis, D., Spathoulas, G., Kakarountas, A., Schinianakis, D., and Lueken, J., *Monitoring supply current thresholds for smart device's security enhancement*,In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 224-227, 2019.
[25] Myridakis, D., Spathoulas, G., Kakarountas, A., and Schinianakis, D, *Smart Devices Security Enhancement via Power Supply Monitoring*, Future Internet, 12(3), 48,2020.
[26] Lee, Soo-Yeon, et al., *ProFiOt: Abnormal Behavior Profiling (ABP) of IoT devices based on a machine learning approach*, 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). IEEE, 2017.
[27] Papafotikas, Stefanos, and Athanasios Kakarountas., *A Machine-Learning Clustering Approach for Intrusion Detection to IoT Devices*,2019 4th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). IEEE, 2019.
[28] Ponguwala, Maitreyi, and DR Sreenivasa Rao., *Secure Group based Routing and Flawless Trust Formulation in MANET using Unsupervised Machine Learning Approach for IoT Applications*,EAI Endorsed Transactions on Energy Web 6(24), 2019.
[29] Cauteruccio, F., Cinelli, L., Corradini, E., Terracina, G., Ursino, D., Virgili, L., ... and Fortino, G., *A framework for anomaly detection and classification in Multiple IoT scenarios*,Future Generation Computer Systems, 114, 322-335,2021.
[30] Yousefi, S., Derakhshan, F., Karimipour, H., and Aghdasi, H. S., *An efficient route planning model for mobile agents on the internet of things using Markov decision process*,Ad Hoc Networks, 98, 102053, 2020.

Edited by: Pradeep Kumar Singh
Received: May 16, 2021
Accepted: Sep 20, 2021