Intelligent Campus Security Warning and Decision Making Based on Feature-Aware Recognition Technology

Nan Xu*

Xidian University, Xi'an, China
**Corresponding author*

Abstract: *By proposing a feature-Aware recognition method based on CBRW algorithm and IOT wireless sensing technology,this paper designs a kind of Wireless sensing recognition principle and campus intelligent security system architecture and applicate it in the campus video surveillance system, electronic fence system,traffic management system and information visualization system,which in turn provides intelligent assistance for rapid and accurate decision-making.*

Keywords: *feature-aware recognition; Internet of Things; intelligent security; early warning; decision making*

1. Introduction

At present, many universities have built campus security management platforms based on IOT technology, which generally includes four levels: network layer, sensing layer, transmission layer, platform layer and application layer. However, how to sense and capture all kinds of risk information in time under the condition of information uncertainty, to make quick sensing and identification of various emergency risk events, and to assist decision-making institutions to make timely and accurate decisions are worthy of in-depth study.

The feature recognition technology based on wireless sensing of IOT has theoretical value and practical significance in the study of campus intelligent security. By establishing a perceptron model with stable connection of wireless network, feature recognition and structured extraction of uncertain information such as temperature, concentration, luminosity, location, sound, human body, vehicle, etc., and through all kinds of possible network access, the storage and retrieval of text and picture information after intelligent structured analysis are realized, so as to achieve suggestive early warning and accurate decision-making of the visualization scene.

2. Method

2.1 CBRW algorithm

The traditional sensor network system includes three nodes: sensor node, sink node and management node.The structure of various sensor nodes is shown in Figure 1. As a small embedded system, sensor nodes are randomly arranged in various parts of the sensor network monitoring area. Such a node not only needs to identify and collect data information of the local monitoring environment, but also needs to function as a router that processes data transmitted from other nodes. When the sink node communicates with an external network such as the Internet and the sensor network, it first converts the protocol between the two protocol stacks, and then the node transfers the collected and processed data to the external network hop-by-hop.At present, the wireless sensor network (WSN) has been widely used, because it faces huge possibilities and challenges, and has attracted the attention of experts at home and abroad. Early research on wireless sensor network technology focused on homogeneous wireless sensor networks. In other words, all the knowledge about the structure of wireless sensor network nodes is the same. In recent years, more and more scholars have begun to pay attention to different types of wireless sensor networks.A typical heterogeneous wireless sensor network refers to a network composed of multiple public sensor nodes and several special sensor nodes with various nodes in the sensing range. Among them, only ordinary sensor nodes perform identification and basic data transmission tasks, and there is no need to implement complex functions of sink nodes such as data fusion, node management, and communication. Under the premise of ensuring network service quality and security, heterogeneous sensor networks can effectively combine two kinds of nodes to reduce the overall cost of the system.

At present, the wireless sensor network (WSN) has been widely used, because it faces huge possibilities and challenges, and has attracted the attention of experts at home and abroad. Early research on wireless sensor network technology focused on homogeneous wireless sensor networks. In other words, all the knowledge about the structure of wireless sensor network nodes is the same. In recent years, more and more scholars have begun to pay attention to different types of wireless sensor networks.

A typical heterogeneous wireless sensor network refers to a network composed of multiple public sensor nodes and several special sensor nodes with various nodes in the sensing range. Among them, only ordinary sensor nodes perform identification and basic data transmission tasks, and there is no need to implement complex functions of sink nodes such as data fusion, node management, and communication. Under the premise of ensuring network service quality and security, heterogeneous sensor networks can effectively combine two kinds of nodes to reduce the overall cost of the system.

The feature sense knowledge technique first requires an algorithmic model to identify anomalies. Anomalies are the objects that can not be fitted in advance with the built model[1]. In this paper, we use the CBRW algorithm [2].to perform discrete transformation for uncertain information, that is, category class variables and discrete data.

For the data set X = {α1, 2, 03, ... , Cy}, there are D features and the feature set is F={f1, f2 .... , fp}, there are a total of D features with a different number of categories of values taken under each feature.

The mode of a feature is defined as the one with the most occurrences of the feature :

record as p(m), among ,

Intra-feature anomaly:,

where 0 belongs to the same feature f.

Abnormality of feature values. After iterating to obtain T, we can obtain the anomaly of each feature

Anomalous correlation of features rel(f):

The size of the feature represents the relevance of the feature to the anomaly, and the larger the value, the more relevant the feature is to the anomaly[3]. With this algorithm we can determine the feature selection with a larger value of feature-anomaly correlation supported by a large amount of discrete data[4].

2.2 Wireless sensor network node algorithm

In the monitoring area of the wireless sensor network, in order to ensure the QoS quality of the network, the configuration of nodes is high-density and high-redundancy. As far as sensor node areis concerned, all neighboring nodes are invalid. In this paper, node j is regarded as the effective neighboring node of node i, as long as it satisfies any sensor node j in the monitoring area, such sensor node j belongs to the set of effective neighboring nodes i of the sensor.According to the positional relationship between the sensor node i and its adjacent node group j, the remaining effective adjacent nodes of node amre classified into 3 categories.For the neighboring nodes N first of the first type, k1 is the number of neighboring nodes satisfying the coverage condition in the sensing range of the sensor node i.

$$p = \frac{\pi R_j^2}{\pi R_i^2} \tag{1}$$

In this way, the sensing range of node i can be obtained, and the number of adjacent nodes meeting the coverage condition is

$$k_1 \geq \frac{\ln(1-\Omega)}{\ln\left(1-\left(\frac{R_j}{R_i}\right)^2\right)} \tag{2}$$

The condition is satisfied between sensor node i and neighbor node j

$$(\mathrm{S(j)} \cap \mathrm{S(i)}) \supseteq \mathrm{S}_{\mathrm{j}\to\mathrm{i}} \tag{3}$$

Which is;

$$\mathrm{d(i,j)} \leq \mathrm{R_i}\,,\mathrm{R_i} - \mathrm{R_j} \leq \mathrm{d(i,j)} \tag{4}$$

Such a sensor node j is called the second type of adjacent node of node i, and this adjacent node j is denoted as Condense.

When the second type of adjacent node j crosses node i, the value of d(i, j) is a variable[2]. Regarding the accuracy of the calculation, calculate its mathematical expectation value

$$\mathrm{E(d(i,j))} = \int_{\mathrm{R_i}-\mathrm{R_j}}^{\mathrm{R_i}} \frac{1}{\mathrm{R_j}}\mathrm{x}\mathrm{dx} = \mathrm{R_i} - \frac{1}{2}\mathrm{R_j} \tag{5}$$

The central angles of the common sectors are

$$\alpha_{\mathrm{j}\to\mathrm{i}} = 2 \cdot \arccos\left(\frac{\left(\mathrm{d(i,j)}^2+\mathrm{R_i^2}-\mathrm{R_j^2}\right)}{2\cdot\mathrm{R_i}\cdot\mathrm{d(i,j)}}\right) \tag{6}$$

$$\alpha_{\mathrm{i}\to\mathrm{j}} = 2 \cdot \arccos\left(\frac{\left(\mathrm{d(i,j)}^2+\mathrm{R_i^2}-\mathrm{R_j^2}\right)}{2\cdot\mathrm{R_i}\cdot\mathrm{d(i,j)}}\right) \tag{7}$$

This chapter calculates in detail when the central angle is

$$\alpha_{\mathrm{ji}} = 2 \cdot \arccos \tag{8}$$

The area of the overlapping area between the sensing range S(i) of node I and the sensing range S(j) of node j is as follows:

$$\mathrm{S}_2 = \frac{\mathrm{R_i}\alpha_{\mathrm{j}\to\mathrm{i}}+\mathrm{R_j}\alpha_{\mathrm{i}\to\mathrm{j}}}{2} - \mathrm{R_i}\mathrm{d(i,j)}\sin\alpha_{\mathrm{j}\to} \tag{9}$$

Inferred

$$\mathrm{p} = \frac{\mathrm{S}_2}{\pi\mathrm{R_i^2}} \tag{10}$$

The number of adjacent nodes whose sensing range of node i meets the coverage conditions can be obtained

$$\mathrm{k}_2 \geq \frac{\ln(1-\Omega)}{\ln\left(1-\frac{\mathrm{S}_2}{\pi\mathrm{R_i^2}}\right)} \tag{11}$$

Neighbor node j and sensor node i meet the conditions

$$\mathrm{S}_{\mathrm{j}\to\mathrm{i}} \subset (\mathrm{S(j)} \cap \mathrm{S(i)}) \tag{12}$$

This type of sensor node j is called a third type of neighboring node of node i, and this type of neighboring node j is denoted by N third. When the third type of adjacent node j crosses node i, the value of d(i, j) is still a variable. Calculate the mathematical expectation value of D(i,j).

$$\mathrm{E(d(i,j))} = \int_{\mathrm{R_i}}^{\mathrm{R_i}+\mathrm{R_j}} \frac{1}{\mathrm{R_i}}\mathrm{x}\mathrm{dx} = \mathrm{R_i} + \frac{1}{2}\mathrm{R_j} \tag{13}$$

In this case, the area of the repeated region is the same as the area of the second adjacent node, and the area is as follows:

$$S_3 = \frac{R_i\alpha_{j\to i}+R_j\alpha_{i\to j}}{2} - R_i d(i,j)\sin\alpha_{j\to i} \tag{14}$$

Find the number of adjacent nodes that meet the coverage conditions within the sensing range of node i

$$k_3 \geq \frac{\ln(1-\Omega)}{\ln\left(1-\frac{S_3}{\pi R_i^2}\right)} \tag{15}$$

2.3 Simulation results

This chapter verifies the effectiveness and other performance of the algorithm through the confirmation test and comparative experiment simulation in the MATLAB environment. In the case of heterogeneous sensor networks, in this chapter, two sensor nodes with different detection radii are selected, and they are randomly placed in 100×100 surveillance areas according to the uniform distribution[4]. The sensing radii of the sensor nodes are R1 and R2, respectively.

Figure 1 the red node is a sensor node with a detection radius of 8m, and the blue node is a sensor node with a detection distance of 10m. If the coverage rate is specified, the redundant node is determined and shut down according to the above-mentioned shutdown rule of the redundant node. The result is shown in Figure 2.

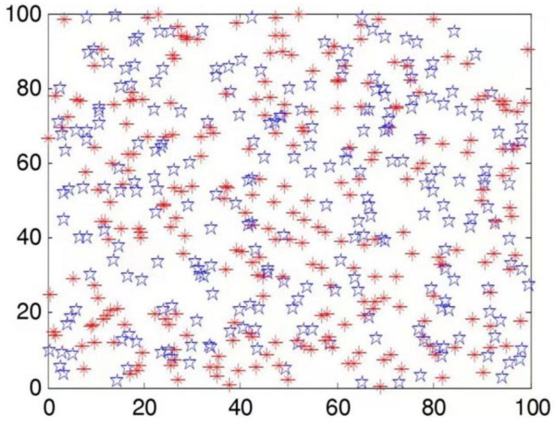

Fig 1. Initial diagram

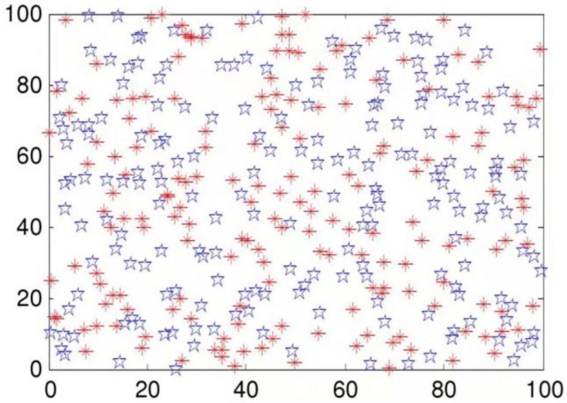

Fig 2. The diagram after the redundant node is shut down

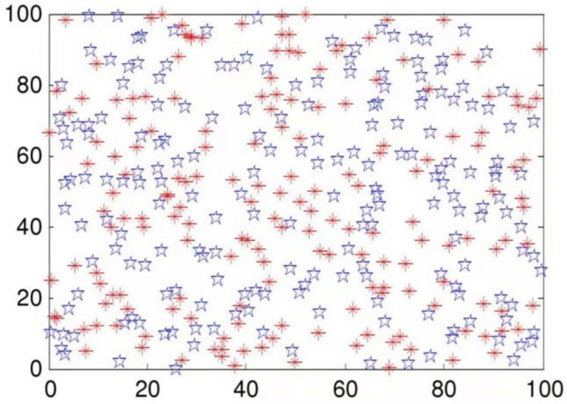

Fig. 3. The diagram after the redundant node is shut down

200 sensor nodes are randomly placed in the monitoring area, and the actual value covered by the NDBS algorithm is compared with the theoretical value. Starting from Table 1, the maximum error between the theoretical coverage rate and the actual coverage rate is ± 0.003, which can confirm the effectiveness of the adjacent node segmentation and redundancy judgment method, and there are two reasons for the error. On the one hand, due to the random expansion of nodes, the position of nodes is

not accurate enough, so the repetition rate of nodes in some areas becomes higher, which affects the actual coverage rate. On the other hand, to achieve actual coverage, the sensor nodes in the edge area must behigher than the theoretical estimate.

Table 1 Comparison of coverage

Theoretical coverage	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.86	0.9	0.96
Actual coverage	0.502	0.549	0.6	0.650	0.703	0.752	0.803	0.85	0.901	0.948

In order to test the performance of the proposed node scheduling algorithm, this paper will compare two grid-based algorithms. The GBS algorithm refers to shutting down the nodes of each small grid until the monitored area is gridded to meet the specified coverage. Random algorithm refers to an algorithm that randomly shuts down sensor nodes under the premise of meeting the specified coverage in the surveillance area. Regarding these three algorithms, this paper analyzes the performance of the algorithms from three aspects: coverage, radius ratio, and number of nodes.

Figure 4 shows the relationship between network coverage and node shutdown rate. As shown in Figure 4, as the coverage requirement increases, the node closure rate will decrease, and as the coverage increases, the degree of decrease will also decrease. Among the three algorithms used to close redundant nodes, the node closing rate of the NDBS proposed in this paper is significantly higher than the other two algorithms, while the node closing rate of the GBS algorithm is the second.

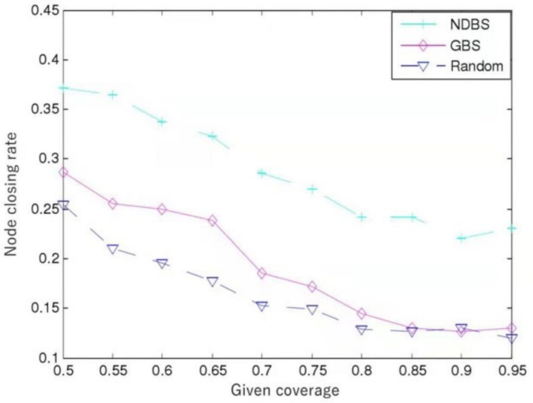

Fig. 4. The influence of network coverage on algorithm performance

Table 2 analyzes the three algorithms from the perspective of performance. In short, the NDBS algorithm proposed in this chapter has obvious advantages in the three redundant node shutdown algorithms, and the grid-based redundant node shutdown algorithm is the second, and the random redundant node shutdown algorithm has the worst performance.

Table 2 Comparison of algorithm complexity

	Time complexity	Space complexity
Random	O (n)	O (n)
GBS	O(n(n/k))	O (n)
NDBS	O (n)	O (n)

2.4 Wireless sensing recognition principle and campus intelligent security system architecture

Wireless sensor networks (WSN) are deployed in specific monitoring areas of the campus to transmit information through the organization of wireless communication sensor nodes, thus building a sensor network system, forming a spontaneous wireless network that establishes a full-coverage campus intelligent security system, where sensor nodes can transmit information collected from the environment to a remote base station, with a working schematic as shown in Figure 5[5].

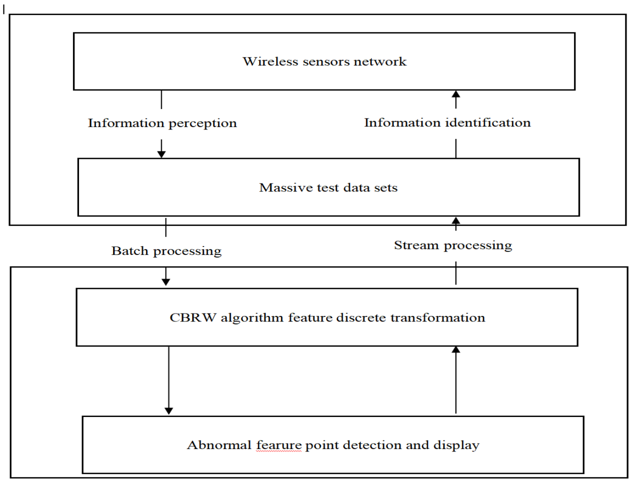
Wireless sensors network
Information perception
Information identification
Massive test data sets
Batch processing
Stream processing
CBRW algorithm feature discrete transformation
Abnormal fearure point detection and display

Fig 5. Wireless sensing recognition principle

Following this working principle, practical applications in the video surveillance subsystem, electronic fence subsystem, and vehicle identification subsystem of the campus intelligent security management platform require equipping wireless sensors with having device-based certificates that can be configured for each IOT device with dedicated network, client and use case profiles and certificates. Figure 4 is signature to communicate with the back-end and enable hassle-free communication with the back-end.

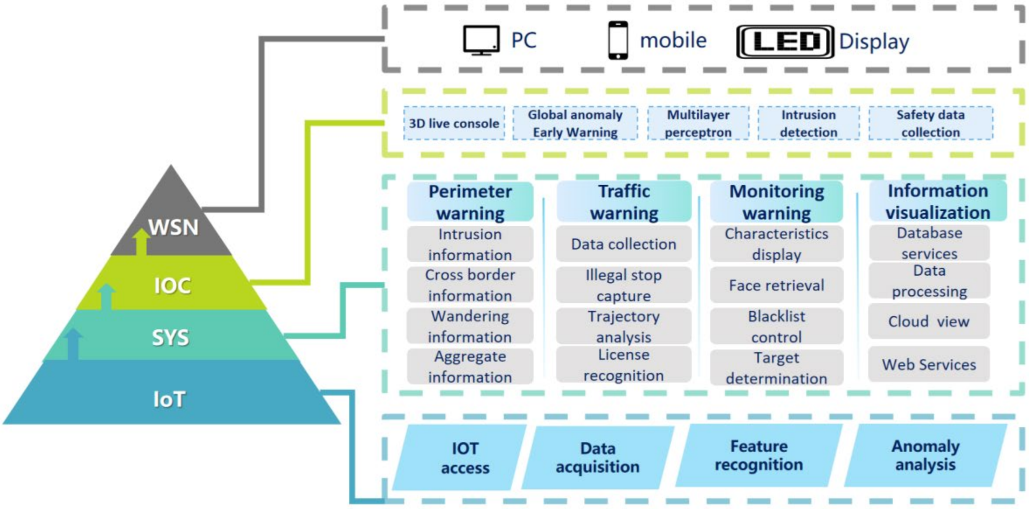

Fig . 6. Campus intelligent security system architecture

3. Application

3.1 Early warning application in the video surveillance system for face recognition features

In the traditional SD monitoring technology framework, in order to ensure that the monitoring coverage, as far as possible to reduce the monitoring of dead spots, the need to install and deploy a considerable number of surveillance cameras, monitoring system scale is constantly expanding, from a few hundred to thousands of roads or even hundreds of thousands of roads scale development. Such a huge scale of monitoring resources, at the same time only a very small part of the real-time monitoring, and the vast majority of monitoring images were recorded and saved indiscriminately, thus forming a massive amount of video recording data[6]. And only a very small part of these massive video data may be associated with certain known events and backup, other video information is constantly covered by new video data.

This is typical of the traditional monitoring system large-scale, high-cost, inefficient construction application status. Under the wireless sensor feature sensing identification based on network networking technology, a single sensor can be equivalent to several ordinary camera monitoring coverage, and higher image resolution, richer information, can be very effective in reducing the size of the system, saving transmission links and equipment, thereby reducing the overall construction cost, anpromotingte the application of video surveillance system construction towards intensiveperformance - oriented surveillanceed change.

3.2 Early warning application of perimeter perception in the electronic fence system

Through the Internet of Things integrated campus electronic fence system networking, instantly in the command center centralized display of the state of the defense zone, wireless sensor perception detection area invasion information, crossing the boundary information, entering the area information, leaving the area information, wandering information, personnel gathering information, scene change information, etc[7]. If the defense zone alarm, it should immediately locate the alarmed defense zone and link the peripheral video monitoring display pop-up.

The defense zones are marked on the GIS electronic map, and each zone is linked with several cameras based on wireless perceptron sensing[8]. The normal state defense zone is displayed in green on the application side, while the alarm state turns into a red flashing line, emits an audible alert, and displays its linked cameras on the screen to patrol the alarmed defense zone.

3.3 Early warning application of vehicle feature recognition in traffic management system

Image sensing and recognition is performed through wireless sensing based on IOT, with wireless sensors detecting the preset position and the corresponding illegal parking detection area, and setting the road section illegal parking capture mode[9].

The identification system mainly consists of data collection module (including parking space detection camera, parking space guiding light, etc.), central control module (including inducement manager, central server, etc.), database server, and information release module (including indoor guiding screen, integrated terminal inquiry machine, etc.). The built-in intelligent analysis algorithm detects the motor vehicles in the illegal parking detection area, extracts the characteristic information after detecting the illegal parking vehicles, the front-end equipment supports the image intelligent analysis technology such as license plate recognition, and supports the license plate capture operation, while the entrance/exit system supports RFID card recognition, which can carry out con tactless active release, and uses the license plate analysis technology and IOT RFID technology for campus Effective management of vehicles. Transmission network layer is responsible for the transmission network is responsible for the front-end video data, vehicle data transmission to the back-end system. The entrance/exit control system and finally the license plate recognition and effective management of all vehicles entering and leaving the campus.

Table 3 Vehicle information feature recognition

Function item	Feature recognition
Vehicle information feature recognition	Identification and extraction of vehicle license plate number, plate color, vehicle color, vehicle type, vehicle brand, vehicle sub brand and other information
	Recognition of 11 body color features: red, yellow, green, orange, blue, purple, pink, brown, white, gray and black
	Identification of 7 types of characteristics of passenger cars, trucks, cars, vans, minivans, SUVs and medium-sized passenger
	Vehicle accident dynamic feature recognition
	Vehicle accident static feature recognition
	Dangerous goods vehicle feature detection and recognition
	Multidimensional detection of vehicle overspeed
	Illegal parking feature recognition
Human feature recognition	Identification of pedestrian gender, age, wearing glasses, cycling, backpacking, , activity track, etc
Activity target information identification	Recognition of color, size, direction, speed, sound and other features of moving targets

3.4 Decision-making application in information visualization system

Information asymmetry is an important influencing factor for campus safety prevention and control and emergency risk event disposal. Essentially, due to the wide coverage of the campus, the distribution and flow of teachers, students, administrators, outsiders, vehicles, locations and places present an unbalanced state and non-organic sequence, the way, direction, scope and distortion of information dissemination are affected by many factors, usually with the information source as the center in a radial linear outward expansion[10]. Therefore, it is necessary to improve the level of information utilization and analysis to reduce and eliminate the information gap.

Wireless sensing recognition has good applicability in this respect. The information collected by the wireless sensing platform is used to access, compare, record, analyze and share data and information. It consists of the following software modules, including: database server, data processing server, and web server. The database server is installed with database software to save all kinds of data information of the system; the data processing server is installed with application processing module responsible for data parsing, storage, forwarding and up-down communication; the Web server is installed with Web Server responsible for providing access service to B/S users[11]. The system supports network performance monitoring, and can form visual daily, weekly and monthly reports. Customized performance thresholds are supported, and two levels of thresholds can be set for the monitored performance indicators, and different levels of alarms are sent according to different thresholds when the performance indicators exceed the thresholds.

4. Conclusion

Based on Feature-Aware Recognition Technology, the fundamental application of wireless sensing technology in four subsystems of campus intelligent security management platform proposed in this paper can better realize more effective and accurate sensing information features under information uncertainty conditions, identify abnormal silver, improve the efficiency of information and data set screening, interconnect the fragmented heterogeneous security systems through network in breadth to achieve the purpose of whole domain monitoring, while in technical depth through intelligent sensing, intelligent big data analysis, etc. to enhance the security monitoring efforts, protection and rescue effects, to achieve the privacy of the Internet of Things decision support. In the future, in order to further develop the function of the equipment and realize the construction of sharing, it is necessary for all the equipment equipped with wireless sensors to realize network interconnection and interoperability, and it is necessary for the security special network equipment to realize network integration and unify the network environment.

Acknowledgement

China Association of Higher Education Professional Committee of Security Studies. Project name : Research on the Theoretical Construction and Application of Intelligent Security Management in Colleges and Universities under the Background of "Double First Class" Construction -- Taking Xidian University as an Example(Project Number :21BWZD020).

References

[1] Milliner, M., Ma, M., Couperin, M., & Godless, P. (2016). Scheduling impact on the performance of relay-enhanced ATE-A networks. IEEE Transactions on Vehicular Technology, 65(4),pp. 2496－2508.

[2] Parsons, J. D. (1992). The Mobile Radio Propagation Channel. Bookend: Wiley.

[3] Dinlin,Liu.(2008). Analysis of the causes of barriers to information resource sharing based on information asymmetry Modern Intelligence,21(2):pp.36-39

[4] T. Pevný(2016). Loda: lightweight on-line detector of anomalies. Machine Learning, 102(2):pp.275-304.

[5] Lee, Ho sub. (2019). Modeling and Prediction of Privacy Decision-Making in IOT, University of California.

[6] N. Pianissimo, A. Cohen, R. Moskovitch, A. Shabbily, M. Edry, O. Bar-Ad, and Y. Elovici(2014). ALPD: active learning framework for enhancing the detection of malicious. pdf fifes. In JISIC,pp.91－98.

[7] K. Hoffman, S(2013). Whiteson, and M. d. Rijke. Balancing exploration and exploitation in listwise and pairwise online learning to rank for information retrieval. Inf. Retr., 16(1):pp.63-90.

[8] Chi, H., Prada, R. V., Kronur, E., & Steersmen, I. G. M. M. (2014). Fairness in wireless networks: Issues, measures and challenges. IEEE Communications Surveys Tutorials, 16(1), pp.5-24.

[9] A. Lazarevic and V. Kumar(2005). Feature bagging for outlier detection. In KDD, pp. 157–166.

[10] JAKHALE A R(2017).Design of anomaly packet detection framework by data mining algorithm for network flow[C]//International Conference on Computational Intelligence in Data Science, Chennai, pp.1-6

[11] WILLIAMS R,MCMAHON E,SAMTANI S,ET AL(2017).Identifying vulnerabilities of consumer Internet of things(IOT)devices: a scalable approach[C]//2017 IEEE International Conference on Intelligence and Security Informatics,pp.179-181.