WiId: A WiFi-BASED INDOOR INTRUSION DETECTION SYSTEM

Yunxiao LUO[1]

This paper proposes an indoor intrusion detection system WiId based on WiFi Channel State Information (CSI) for effective detection and discrimination of personnel intrusion activities. By examining the relevance between human motion and amplitude information in channel state information, the system classifies different activities during intrusion. For better overall performance, this paper proposes dynamic adaptive link selection based on the maximum range. While fusing the subcarrier information in multiple links, it deletes signal data insensitive to human behavior features for higher system recognition accuracy. The experimental results indicate that this method has an average recognition accuracy of 96.2%, demonstrating good robustness and stability.

Keywords: Intrusion Detection, Channel State Information, Link Optimization

1. Introduction

Intrusion detection technology supports real-time monitoring of specific area, which analyzes the data collected by the computer to detect presence of illegal intrusion. In case of abnormality, an alarm notification will be given. Recently, the technology has attracted increasing attention, and new breakthroughs have been made in many aspects, such as smart home [1], police security [2], national defense [3], healthcare for children and the elderly [4] etc.

There are currently many passive intrusion detection systems including ultra-wideband radar system [5], computer vision system [6], radio tomography system [7] and wireless sensor [8] passive detection system. These systems support high detection rates under specific conditions, but still with disadvantages of costly equipment, inconvenient deployment, and easy privacy violation.

To avoid the limitations of traditional approaches, I analyze the effect of personnel intrusion activities on wireless channels so that passive personnel intrusion can be detected. WiFi signal-based human behavior perception technology has become a research hotspot [9]. On the basis of CSI, literature [10] designs and implements a human intrusion detection system AR-Alarm with good applicability. Literature [11] introduces and analyzes the CSI of WiFi signals, which implements action recognition through fine-grained CSI, but a lot of training is required in offline state. Literature [12] proposes a CSI-based WiFall

[1] Eng., Chongqing Technology and Business Institute, China, e-mail: luoyunxiao@cqtbi.edu.cn

system able to detect sudden fall of the target individual in an indoor environment and timely issue alarm message, with a recognition rate of 87%. Nonetheless, only amplitude information of CSI is used without consideration of phase information. Shah et al. Literature [13] proposed combination of CSI with leaky cables for intrusion detection of specific areas. Since leakage cable has quite poor interference to non-metallic bodies and non-human bodies, effective protection is impossible. Han et al. Literature [14] improved support vector classification method, but it is difficult to train on large-scale sample data by using SVM for problem-solving. Methods based on pattern recognition [15-16] are also often used for intrusion detection but have low accuracy due to multipath. Literature [17] introduces the experimental results of SVM, RF and KNN algorithms in daily activity recognition, and achieved good results. Considering the above difficulties, the author proposes an indoor intrusion detection system WiId based on WiFi channel state information, which can effectively detect and discriminate personnel intrusion activities.

This paper has the following main contributions:

(1) I propose WiId, an indoor intrusion detection system based on WiFi channel state information. It uses the channel state information in the WiFi device to perform feature analysis to achieve the detection effect. Compared with some traditional intrusion detection systems, WiId does not demand users to wear special equipment, demonstrating advantages of convenient use and low cost.

(2) I propose dynamic adaptive link selection based on the maximum range. While fusing the subcarrier information in multiple links, it deletes signal data insensitive to human behavior characteristics for higher system recognition accuracy.

(3) I achieve indoor intrusion detection using commercial WiFi equipment and assess it in two real-world scenarios. It turns out that the method can effectively detect human motion and carries practical value in intrusion detection.

2. System model and related theories

2.1 System overview

In this section, I will introduce an indoor intrusion detection system WiId based on dynamic adaptive link selection. The system consists of four parts: data acquisition, data preprocessing, link optimization, feature extraction and behavior classification. The system framework is shown in Fig. 1. First, I access WiFi channel status information through commercial WiFi device. Next, in the data preprocessing design, for the sake of system accuracy and robustness, I use a sliding window to dynamically extract the CSI amplitude and use a Butterworth low-pass filter for filtering. Subsequently, in the link optimization design, after studying the relationship between the MIMO antennas, I adopt dynamic adaptive link selection based on the maximum range (CSI-DALS) to delete the link data insensitive to activity. Finally, in the feature extraction and behavior classification design, I construct a classification model by extracting the time-frequency domain features and employ SVM algorithm to identify the presence of intrusion behavior. In case of intrusion behavior, the specific intrusion behavior will be further identified to derive identification result.

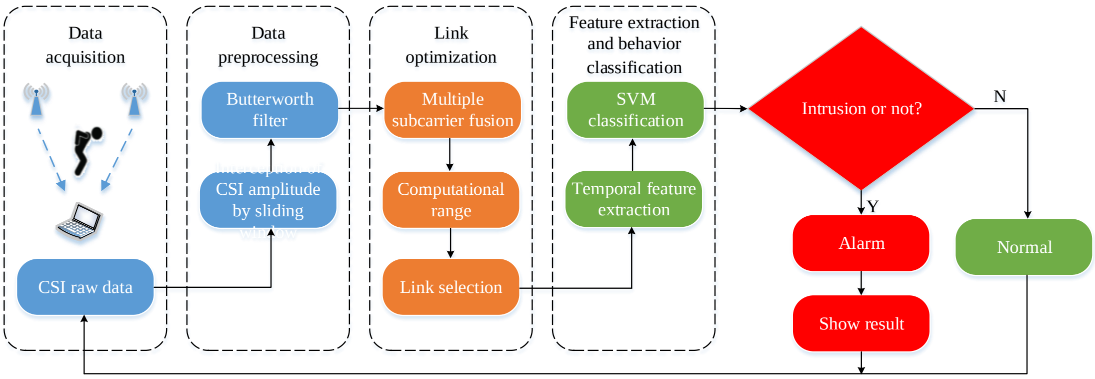


Fig. 1. WiId system framework

2.2 Data preprocessing

(1) Data extraction by sliding window

To let CSI data sequence better describe the changes in wireless signal due to the occlusion of human body, and maintain the continuous fluctuation of wireless signal, WiId sets a sliding window with a fixed width to continuously extract the CSI data at a fixed step size, thereby effectively analyzing and judging the certain amount of CSI data in the window. Fig. 2 shows the schematic flowchart of CSI data extraction by the sliding window.

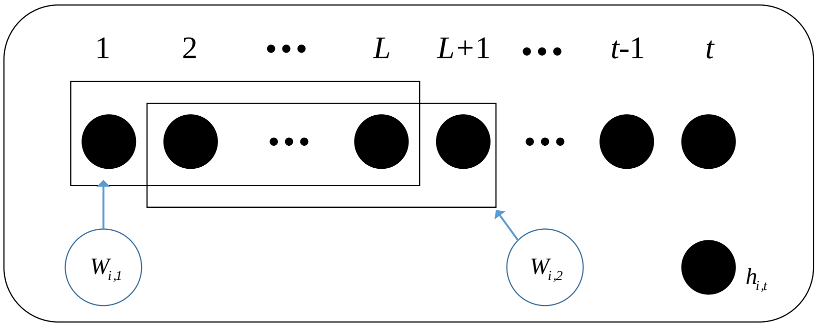


Fig. 2. Schematic diagram of data extraction by sliding window

The extracted CSI data sample in the sliding window $W_{i,t}$ is represented as $CSI_{i,t}$. $W_{i,t}$ represents the sliding window for the detection point to extract the wireless link i at time t (in unit s), the extracted sample in the sliding window

$W_{i,t}$ is expressed as $h_{i,t}$. The window extraction length is $L(L \leq t)$. After extraction of the CSI data sequence by the sliding window. The number of data samples extracted in one wireless link is *N*, and the extracted CSI data set is $CSI_{extract}$. $g(\square)$ is the feature extraction function.

$$N = L \times t \tag{1}$$

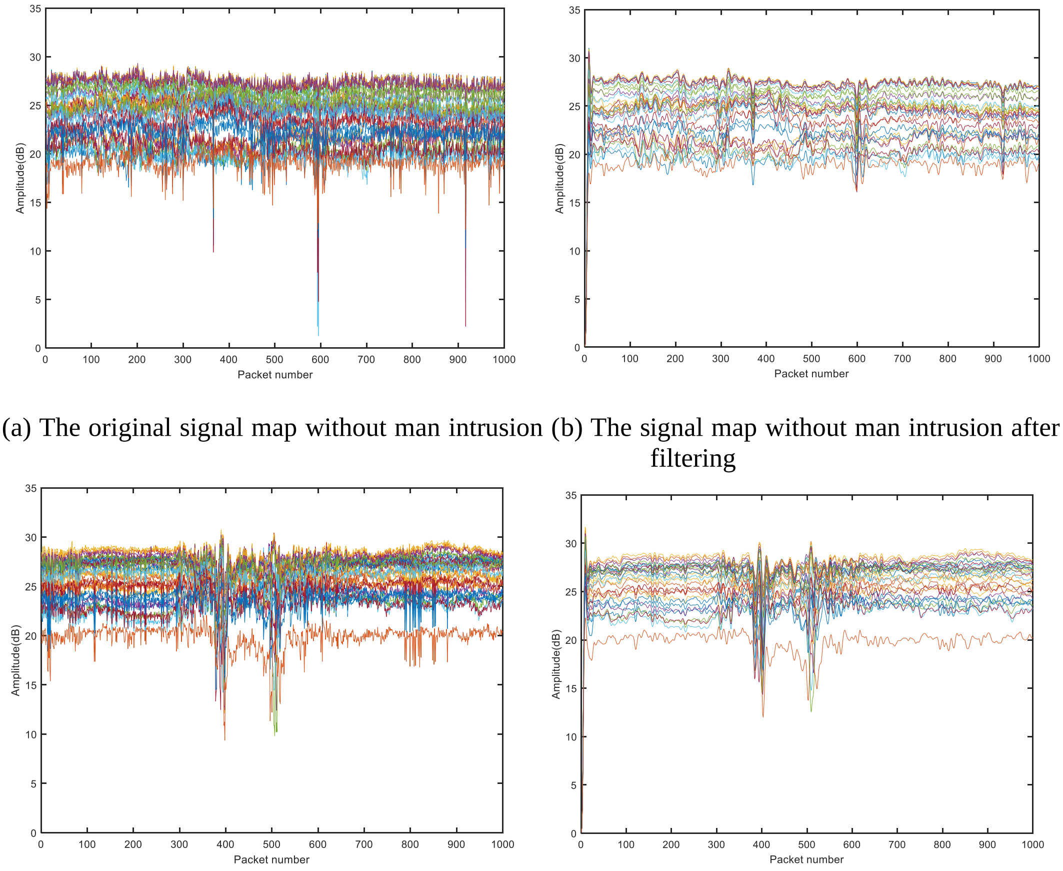
$$CSI_{extract} = \{g(W_{i,1}), g(W_{i,2}) \cdots g(W_{i,t-1}), g(W_{i,t})\} \tag{2}$$

(2) Noise filtering

Since WiFi signal is susceptible to the surrounding environment during transmission, excessive noise exists in the collected CSI raw data. Fig. 3(a) and (c) indicate the raw CSI amplitudes of 30 subcarriers in the same data stream without and with man intrusion. Some mutational fluctuations are observable. Evidently, these noises are not triggered by human behavior, and the existence of noise will lead to misclassification of the classifier and thereby jeopardize recognition accuracy of the system. For higher reliability of the signal, the original data should be preprocessed, and noise of different frequency parts should be filtered. Numerous theories and experiments prove that human activities are usually in a low frequency range, the noise is in the high frequency range. To eliminate such high-frequency noise, WiId adopts a Butterworth low-pass filter for data filtering at different frequencies. The characteristics of Butterworth filter can be expressed by its gain as follows:

$$G(w)^2 = \left|H(jw)\right|^2 = \frac{G_0{}^2}{1 + \left(\frac{w}{w_c}\right)^{2n}} \tag{3}$$

Where, the filter gain is $G(w)$, the angular frequency is w, the cutoff frequency is w_c, and the DC gain is G_0, the order of the filter is n. Fig. 3(b) (d) shows the result after processing by Butterworth low-pass filter, which is sufficient to effectively remove interference noise.



(a) The original signal map without man intrusion (b) The signal map without man intrusion after filtering

(c) The original signal map with man intrusion (d) The signal map with man intrusion after filtering

Fig. 3. Raw CSI and its filtering results

2.3 Link Optimization

Fig. 4 shows CSI information differences between different links in a MIMO system. Owing to the technical characteristics of MIMO, the CSI data features on multiple links are not exactly consistent, and certain differences exist. After indoor intrusion, the CSI information fluctuates greatly on the Rx1-Tx2 and Rx2-Tx2 links, the CSI information fluctuates slightly on the Rx1-Tx1 link, while the CSI information barely changes on the Rx2-Tx1. The CSI amplitudes on the Rx1-Tx3 and Rx2-Tx3 links are significantly different compared to other links. The amplitude range is only 0-2dB, and the amplitudes of the other links are all around 20dB. For reasons of this difference, the third wireless network card interface of Receive Point (RP) has poor performance, unable to successfully receive CSI information. It is noticeable that different links have varying sensitivity to activity. A remarkable feature of non-sensitive link is that it has relatively stable CSI amplitude, while the signal of sensitive link has significant amplitude changes. The signal insensitivity of the link is caused by many factors, such as equipment hardware damage, co-channel signal interference and other influencing factors. If insensitive links are used for classification and identification, the identification accuracy will be seriously jeopardized. To avoid the impact of poor performance links, WiId adopts the dynamic adaptive link selection based on the maximum range for link optimization.

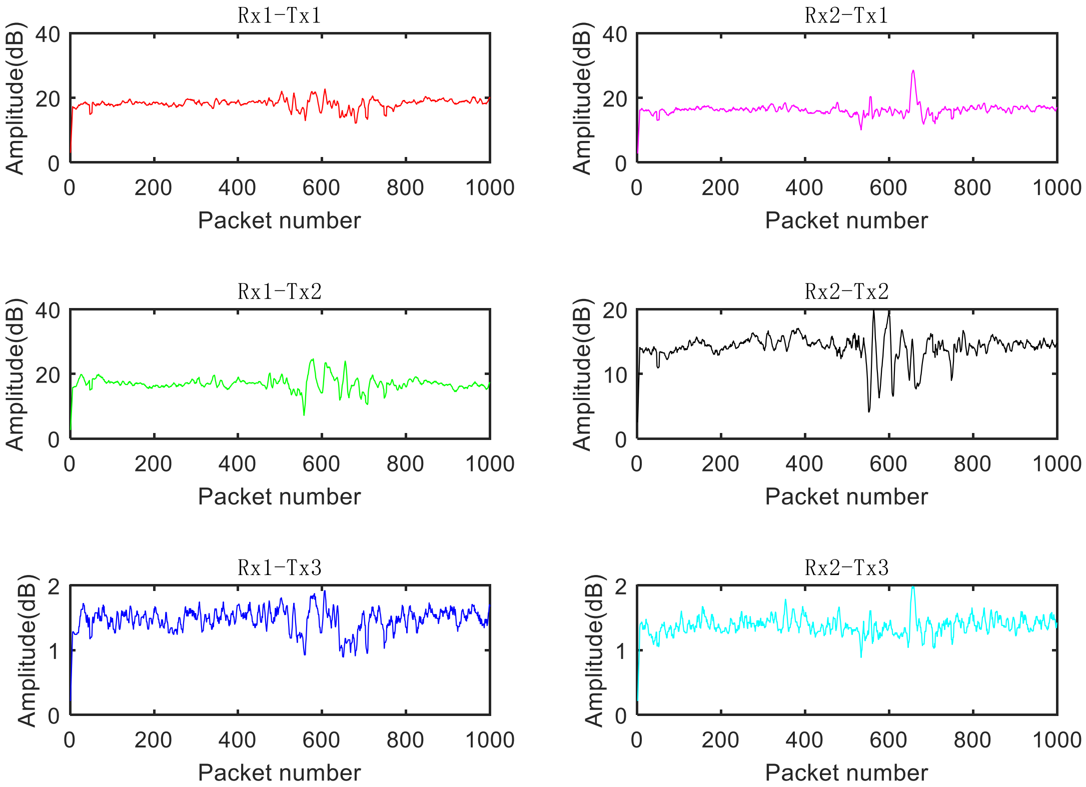


Fig. 4. CSI information difference on MIMO multi-link

(1) Subcarrier fusion

Subcarrier fusion has the following specific processing steps:

Step1: Set the CSI data stream with the CSI data format of $3\times3\times30$ as in formula (4), denote it as $CSI^{N}=\{CSI^{N,n}\}$, CSI^{N} represents the signal received by the N th receiving antenna, and n is the number of subcarriers.

$$\begin{gathered} CSI^{1}=\{CSI^{1,1},\ \ CSI^{1,2},\cdots,\ \ CSI^{1,30}\} \\ CSI^{2}=\{CSI^{2,1},\ \ CSI^{2,2},\cdots,\ \ CSI^{2,30}\} \\ \vdots \\ CSI^{9}=\{CSI^{9,1},\ \ CSI^{9,2},\cdots,\ \ CSI^{9,30}\} \end{gathered} \tag{4}$$

Step2: Calculate CSI_{mean}^{N} of the 30 subcarriers of each link at the corresponding time point, and fusion the 3×30 data streams into 3×1 data streams. The calculation formula is shown in (5). N represents N th receiving antenna, k represents the number of subcarriers, p represents the amplitude of the p th received packet in each subcarrier, and L represents the total number of data packets in the subcarriers.

$$CSI_{mean}^{N}=\frac{1}{30}\sum_{1}^{k}CSI_{p}^{L} \tag{5}$$

Step3: Use the sliding window to calculate the variance of CSI_{mean}^{N} , denote it as $CSI_{mean-\mathrm{var}}^{N}=\mathrm{var}(CSI_{mean}^{N})$, as shown in formula (6). n represents the number of data points in the sliding window, CSI_{i} represents the amplitude of the i th sample, and $\overline{CSI}$ represents the mean value of all sample data in the sliding window.

$$\mathrm{var}=\frac{1}{n-1}\sum_{i=1}^{n}(CSI_{i}-\overline{CSI})^{2} \tag{6}$$

(2) Judgment criteria for maximum range

The link sensitivity to motion is judged by the range. A greater range indicates more significant signal fluctuation, and a smaller range means more stable signal without obvious response to the human motion. However, it is impossible to reliably judge link sensitivity based on the subcarrier fusion data stream with the largest range. Data seriously interfered by noise will easily cause confusion and difficult discrimination. Therefore, for the data stream after subcarrier fusion, WiId adopts sliding window smoothing to calculate the variance in the sliding window for each data stream.

Judgment of the link sensitivity based on the smoothed data has better reliability and lowers the error rate. According to the different requirements on the data volume in the experiment, I can adopt link decision method based on the maximum range to find a link with the optimal quality, or the minimum range method can be used to delete the least sensitive link.

(3) Dynamic adaptive link selection

In view of the above research, WiId proposes a maximum range-based dynamic adaptive link selection method to select or delete links, which can select links with higher signal sensitivity. The experiment compares 30 subcarriers between sensitive and non-sensitive links. It found that sensitive link has quite obvious activity range with obvious amplitude fluctuations. Non-sensitive link is relatively stable, with small fluctuation range and insensitive to human activities. The steps of the dynamic adaptive link selection algorithm are described as follows:

Step1: Calculate the mean value CSI_{mean}^{N} of 30 subcarriers of each link in the original signal at the corresponding time, and fuse 3×30 to form 3×1 to reduce the data complexity.

Step2: Use the sliding window to calculate the variance of CSI_{mean}^{N} , denote it as $CSI_{mean-\mathrm{var}}^{N}=\mathrm{var}(CSI_{mean}^{N})$.

Step3: Calculate the difference D_N between the maximum value and the minimum value of $CSI_{mean-\mathrm{var}}^{N}$.

Step4: Sort D_N in ascending order, filter out the minimum value $\min(D_N)$ of D_N , and use the remaining links as the final selected links.

2.4 Feature extraction and behavior classification

After extracting the eigenvalues, on the basis of analyzing the performance of various classification algorithms, this paper adopts the SVM algorithm which has better performance and is widely used for indoor intrusion detection.

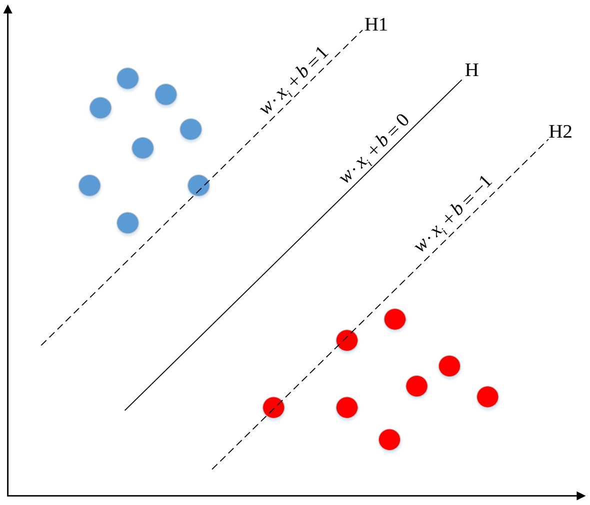


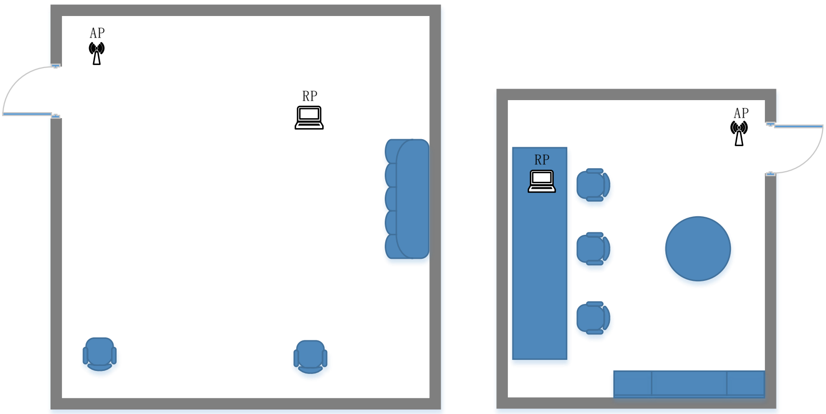
Fig. 5. Separate hyperplane

As shown in Fig. 5, the SVM algorithm finds a "hyperplane", namely, a linear subspace with one dimension lower than the original space, and this space can exactly divide the two types of training samples into two categories accurately and appropriately. Under normal circumstance, SVM algorithm mainly handles binary classification tasks. As sample types grow, SVM algorithm also derives multi-dimensional classification method, which perfectly solves the binary and multi-classification problems in indoor intrusion recognition.

3. Experiment and evaluation

3.1 Experiment setup

To assess the overall performance of the WiId system proposed herein, tests were carried out in two typical scenarios, conference room and laboratory room, respectively, as shown in Fig. 6. The area of the conference room is about 30 ($5m \times 6m$) square meters, including only a sofa and some stools, as shown in Fig. 6(a). There are fewer obstacles in the room, so the multipath interference is weak. In addition, the laboratory area is about 15 ($3m \times 5m$) square meters, with small and compact indoor space, and many pieces of office equipment, desks and chairs, leading to serious multipath interference, as shown in Fig. 6(b).



(a) Conference room (b) Laboratory

Fig. 6. Two test environments

The experimental equipment includes an access point (AP) and a receiving port (RP). In principle, AP should be placed at the entrance of the room, RP can be placed anywhere in the room. But in order to avoid multipath interference, we should choose paths with less interference as much as possible to place RP. The locations of AP and RP are shown in the Fig. 6. AP is a router with model number TL-WR886N, which is equipped with three antennas for data transmission; RP is a laptop equipped with Intel 5300 wireless network card, operating system Ubuntu 12.04 LTS, and three antennas for data receipt. In different scenarios, the transmitter is 3 meters from the receiver and about 1 meter above the ground.

In the experiment, 5 common scenarios in daily life were studied: no activity, falling, sitting, standing, walking. Falling means falling from standing, standing means standing still, walking means moving at a constant speed. The above behaviors are the most likely to occur in indoor scenes, and each behavior is related to another behavior, which can be combined to form more sophisticated daily activities. The system can determine whether there is an intrusion by detecting characteristic behaviors.

The data sets collected in this paper are summarized in Table 2, and the total amount of CSI data in each scenario is $3\times3\times5\times20\times1200$. 80% data was randomly selected from the dataset for model training, with the remaining 20% data for testing. Each activity had 3 different volunteer participants. The data sets collected in this paper are summarized in Table 1, and the total amount of CSI data in each scenario is $3\times3\times5\times20\times1200$. 80% data was randomly selected from the dataset for model training, with the remaining 20% data for testing.

Table 1

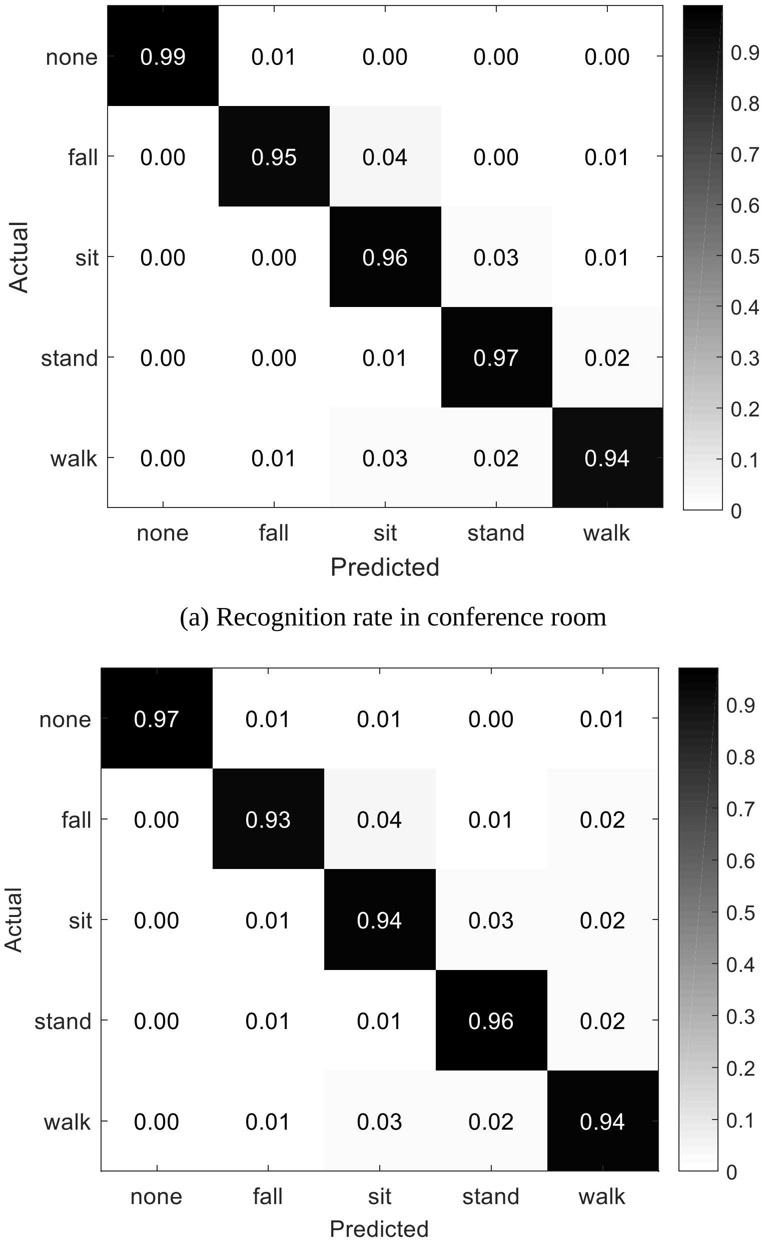
Summary of Datasets

Activity Category	Data Volume
1. no activity	$3\times3\times20\times1200$ (packet)
2. falling	$3\times3\times20\times1200$ (packet)
3. standing	$3\times3\times20\times1200$ (packet)
4. sitting	$3\times3\times20\times1200$ (packet)
5. walking	$3\times3\times20\times1200$ (packet)

3.2 System performance analysis

(1) Impact of different environments

As shown in Fig. 7, it is used the confusion matrix diagram to display the test results, which is more intuitive and accurate. Fig. 7(a) reveals that the average recognition rate of the conference room is 96.2%, and Fig. 7(b) reveals that the average recognition rate of the laboratory is 94.8%. It is found that WiId has high recognition accuracy in both experimental environments with good universality; however, due to more obstacles in the laboratory, more serious multipath effects are caused. Therefore, the recognition rate in the laboratory environment is reduced.



Actual \ Predicted	none	fall	sit	stand	walk
none	0.99	0.01	0.00	0.00	0.00
fall	0.00	0.95	0.04	0.00	0.01
sit	0.00	0.00	0.96	0.03	0.01
stand	0.00	0.00	0.01	0.97	0.02
walk	0.00	0.01	0.03	0.02	0.94

(a) Recognition rate in conference room

Actual \ Predicted	none	fall	sit	stand	walk
none	0.97	0.01	0.01	0.00	0.01
fall	0.00	0.93	0.04	0.01	0.02
sit	0.00	0.01	0.94	0.03	0.02
stand	0.00	0.01	0.01	0.96	0.02
walk	0.00	0.01	0.03	0.02	0.94

(b) Recognition rate in laboratory

Fig. 7. Confusion matrix diagrams in different environments

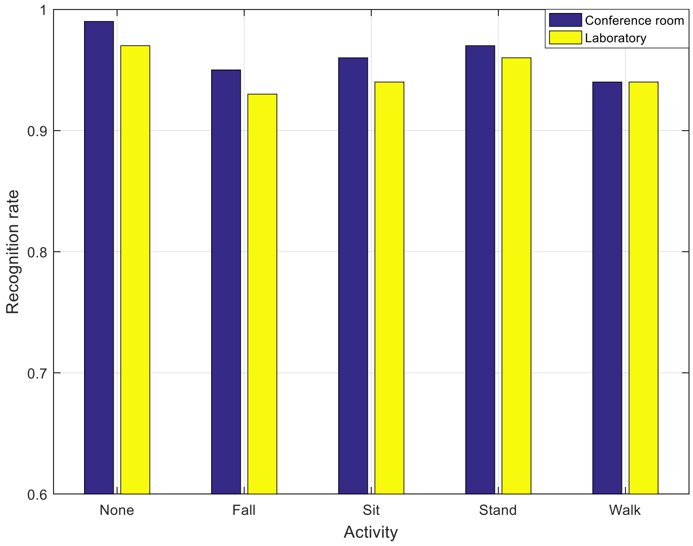


Fig. 8. Recognition rates in different environments

(2) Impact of different experimenters

This experiment was designed to test the effect of different experimenters. In the experiment, 12 experimenters were divided into 3 groups to complete different activities. The experimenter information is shown in Table 2.

Table 2

Experimenter Information

Group	Gender	Age	Height(cm)/ Weight (kg)
Group A	Male	18	180cm/75kg
	Male	25	175cm/85kg
	Male	32	165cm/55kg
	Male	40	157cm/50kg
Group B	Female	20	166cm/52kg
	Female	32	160cm/48kg
	Female	42	155cm/44kg
	Female	35	170cm/58kg
Group C	Male	16	174cm/68kg
	Male	25	169cm/60kg
	Female	36	165cm/53kg
	Female	48	154cm/42kg

Fig. 9 shows that the average recognition rates of group A, B, and C are 94.4%, 95%, and 96%, respectively, indicating that the WiId system has strong robustness, and the system recognition rate is almost unaffected by body type differences.

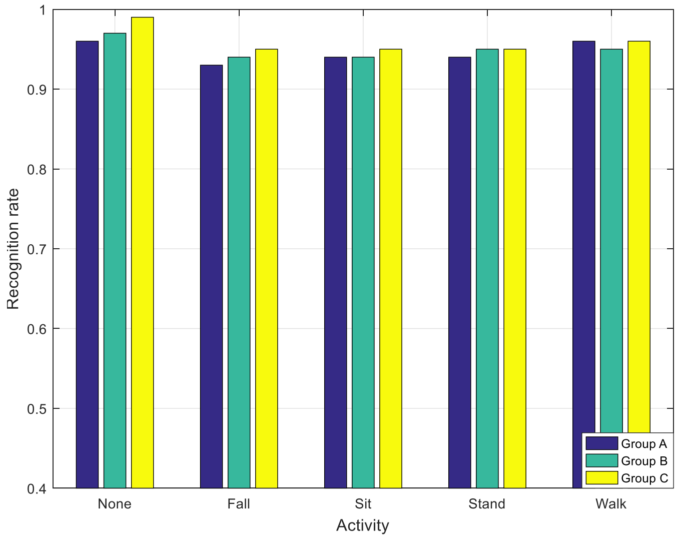


Fig. 9. The impact of different experimenters on the results

(3) Comparison of multi-link and optimal link recognition performance

In the WiId system, I give comprehensive consideration to all the links, and adopt the dynamic adaptive link selection based on the maximum range for link optimization, thus enabling analysis of the link performance and selection of the optimal link. Fig. 10 plots the experimental results when the optimal link and all the links are used respectively.

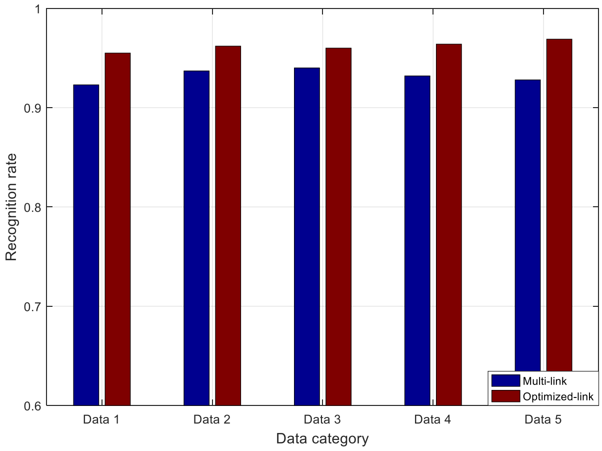


Fig. 10. Comparison of detection accuracy between optimal link and multi-link detection

In the figure, comparison of the detection results of the five datasets shows that when the optimal link is adopted, the indoor intrusion detection method can improve the recognition accuracy by about 3%.

(4) Comparison of different classification methods

To further assess the WiId system performance, this paper selects SVM, RF, and KNN algorithms for comparative analysis.

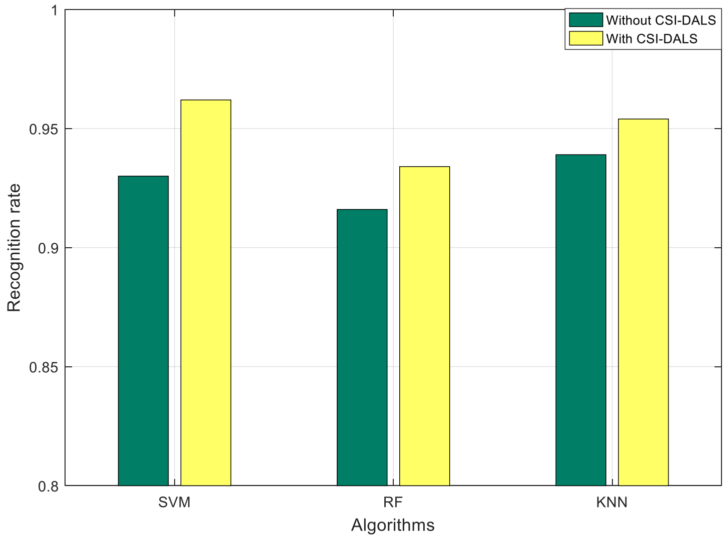


Fig. 11. Performance comparison between different algorithms

As shown in Fig. 11, after using the method proposed herein for data processing, the three machine learning classifiers boast higher recognition accuracy of up to 96.2% compared to direct use of the original signal. The experimental results suggest that link optimization can effectively delete the signal data insensitive to human behavior features, reduce the computational overhead of unnecessary data, so that WiId system has good robustness.

4. Conclusions

In this paper, I proposed a WiFi-based indoor intrusion detection system, WiId. The system utilizes the existing WiFi wireless infrastructure to collect CSI information and achieves passive indoor intrusion detection via the influence of the intruder on the CSI of the wireless environment when the intruder does not carry any wireless equipment. In traditional data processing, there is a lack of fusion processing of multi-link data, so recognition accuracy is relatively low. Therefore, I proposed a dynamic adaptive link selection method based on the maximum range. After fusion of the subcarrier information in multiple links, the signal data insensitive to human behavior feature is eliminated, so that computational overhead of unnecessary data is reduced for higher recognition accuracy. The experimental results show that this method has good robustness and stability, thus enjoying good application prospects. In future work, I consider to use WiFi signal for human identity identification to distinguish between authorized entry and unauthorized entry. It will be dedicated to more novel and effective functions of the WiFi channel state information system for higher adaptability of intrusion detection techniques.

Acknowledgement

This work is supported by the 2021 scientific research project of Chongqing Open University (Chongqing Technology And Business Institute) under Grant NDYB2021-07, Project Name: Research on Indoor Intrusion Detection Method Based on WiFi Channel State Information.

REFERENCES

[1] *D. Zheng，Z. Hong，N. Wang，P. Chen*, “An Improved LDA-Based ELM Classification for Intrusion Detection Algorithm in IoT Application”, Sensors, vol. 20, no. 6, March. 2020, pp. 1706-1724.

[2] *A. D’Alconzo, I. Drago, A. Morichetta, M. Mellia and P. Casas*, “A Survey on Big Data for Network Traffic Monitoring and Analysis”, IEEE Transactions on Network and Service Management, vol. 16, no. 3, Sept. 2019, pp. 800-813.

[3] *O. Stan，A. Cohen，Y. Elovici，and A. Shabtai*, “Intrusion Detection System for the MIL-STD-1553 Communication Bus”, IEEE Transactions on Aerospace and Electronic Systems, vol. 56, no.4, Aug. 2020, pp. 3010-3027.

[4] *Z. Li, X. Zhao, F. Hu, Z. Zhao, J. L. Carrera Villacrés and T. Braun*, “SoiCP: A Seamless Outdoor–Indoor Crowdsensing Positioning System”, in IEEE Internet of Things Journal, vol. 6, no. 5, Oct. 2019, pp. 8626-8644.

[5] *J. W. Choi, S. S. Nam and S. H. Cho*, “Multi-Human Detection Algorithm Based on an Impulse Radio Ultra-Wideband Radar System”, in IEEE Access, vol. 4, Jan. 2017, pp. 10300-10309.

[6] *K. Moria, A. B. Albu and K. Wu*, “Computer Vision-Based Detection of Violent Individual Actions Witnessed by Crowds”, 2016 13th Conference on Computer and Robot Vision (CRV), Jun. 2016, pp. 303-310.

[7] *Y. Zhang, and H. Wang*, “Research of Indoor location Algorithm Based on Radio Tomographic Imaging”, Chinese Journal of Sensors and Actuators, vol. 28, no. 10, Oct. 2015, pp. 1558-1562.

[8] *X. Tang, and H. Hui*, “Optimization of GPS Signal Location Technology in Road Engineering Survey”, Computer Measurement & Control, vol. 24, no. 8, Aug. 2016, pp. 263-266.

[9] *Y. Lu, S. H. Lv, X. D. Wang, and X. M. Zhou*, “A Survey on WiFi Based Human Behavior Analysis Technology”, Chinese Journal of Computers, vol. 42, no. 2, Feb. 2019, pp. 1-21.

[10] *S. J. Li, X. Li, K. Niu, H. Wang, Y. Zhang, and D. Q. Zhang*, “AR-Alarm: An Adaptive and Robust Intrusion Detection System Leveraging CSI from Commodity Wi-Fi”, International Conference on Smart Homes & Health Telematics Springer, vol. 10461, Aug. 2017, pp.

211-223.

[11] *L. Liu, Z. Wei, C. Zhang, W. Wang, and J. Zhao*, “Lifetime estimation for human motion with WiFi channel state information”, Journal of Computer Applications, vol. 39, no. 7, Mar. 2019, pp. 2056-2060.

[12] *Y. Wang, K. Wu and L. M. Ni*, “WiFall: Device-Free Fall Detection by Wireless Networks”, in IEEE Transactions on Mobile Computing, vol. 16, no. 2, Feb. 2017, pp. 581-594.

[13] *S. I. Shah, S. Y. Shah and S. A. Shah*, “Intrusion Detection through Leaky Wave Cable in Conjunction with Channel State Information”, 2019 UK/ China Emerging Technologies (UCET), Aug. 2019, pp. 1-4.

[14] *K. Han，L. Shi，Z. Deng，X. Fu and Y. Liu*, “Indoor NLOS Positioning System Based on Enhanced CSI Feature with Intrusion Adaptability”, Sensors, vol. 20, no. 4, Feb. 2020, pp. 1211-1235.

[15] *J. G. Lv, D. P. Man, W. Yang, L. Y. Gong, X. J. Du and M. Yu*, “Robust Device-Free Intrusion Detection Using Physical Layer Information of WiFi Signals”, Applied Sciences, vol. 9, no. 1, Jan. 2019, pp. 175-191.

[16] *Y. Bao, L. Dong, Y. Zheng and Y, Liu*, “WiSafe: a real-time system for intrusion detection based on wifi signals”, the ACM Turing Celebration Conference – China, no. 26, May. 2019, pp. 1-5.

[17] *Y. He, Y. Chen, Y. Hu, B. Zheng*, “WiFi Vision: Sensing, Recognition, and Detection with Commodity MIMO-OFDM WiFi”, IEEE Internet of Things Journal, vol. 7, no. 9, Jul, 2020, pp. 8296-8317.