



Article

Robust Device-Free Intrusion Detection Using Physical Layer Information of WiFi Signals

Jiguang Lv ¹, Dapeng Man ^{1,*}, Wu Yang ¹, Liangyi Gong ², Xiaojiang Du ^{3,*} and Miao Yu ⁴

¹ Information Security Research Center, Harbin Engineering University, Harbin 150001, China; lvjiguang@hrbeu.edu.cn (J.L.); yangwu@hrbeu.edu.cn (W.Y.)

² The School of Computer Science and Engineering, Tianjin University of Technology, Tianjin 300072, China; gongliangyi@gmail.com

³ Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA

⁴ Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China; yumiao@iie.ac.cn

* Correspondence: mandapeng@hrbeu.edu.cn (D.M.); dxj@ieee.org (X.D.); Tel.: +86-451-8258-9638 (D.M.)

Received: 26 October 2018; Accepted: 27 December 2018; Published: 5 January 2019



Featured Application: Intrusion Detection and Smart Home.

Abstract: WiFi infrastructures are widely deployed in both public and private buildings. They make the connection to the internet more convenient. Recently, researchers find that WiFi signals have the ability to sense the changes in the environment that can detect human motion and even identify human activities and his identity in a device-free manner, and has many potential security applications in a smart home. Previous human detection systems can only detect human motion of regular moving patterns. However, they may have a significant detection performance degradation when used in intrusion detection. In this study, we propose Robust Device-Free Intrusion Detection (RDFID) system leveraging fine-grained Channel State Information (CSI). The noises in the signals are removed by a Principle Component Analysis (PCA) and a low pass filter. We extract a robust feature of frequency domain utilizing Continuous Wavelet Transform (CWT) from all subcarriers. RDFID captures the changes from the whole wireless channel, and a threshold is obtained self-adaptively, which is calibration-free in different environments, and can be deployed in smart home scenarios. We implement RDFID using commodity WiFi devices and evaluate it in three typical office rooms with different moving patterns. The results show that our system can accurately detect intrusion of different moving patterns and different environments without re-calibration.

Keywords: intrusion detection; human detection; channel state information; device-free passive

1. Introduction

Device-free human detection has attracted a lot of interest in recent years. It can detect human presence in the monitoring area without any sensing-related devices attached to the people [1]. It can be used well in intrusion detection systems, which is a vital security component in a smart home. Aiming at handling the security issues in a smart home, many techniques have been utilized to implement device-free human detection, such as video-based, infrared-based, Radio Frequency Identification (RFID)-based and Ultra-Wide Bandwidth (UWB)-based approaches. Although they have a good detection accuracy, these approaches have limited using conditions and need dedicated devices that hinder their adoption. WiFi-enabled devices become the catalyst of device-free sensing as they have been widely deployed in both public and private buildings. Besides being used for communication, WiFi networks can also be used as sensor networks [2–4]. Many applications have emerged based on WiFi infrastructures, human detection [5], indoor localization [6], and even human identification [7] are some representative applications.

A typical WiFi-based device-free human detection system usually contains several pairs of transmitters and receivers. A wireless router can act as a transmitter, while a WiFi-enabled device can act as a receiver. As a result, it doesn't have the problem of key management [8,9] compared with sensor-based approaches. The rationale of WiFi-based device-free human detection is that human presence has an impact on signal propagation, which will cause the signal strength fluctuation at the receiver [10]. Previous WiFi-based human detection systems utilize Received Signal Strength Indicator (RSSI) from Media Access Control (MAC) layer for it is easy to obtain. However, RSSI is a coarse-grained measurement. In the typical indoor scenario, RSSI becomes unreliable due to multipath fading. It may increase, decrease, or even remain the same when a person moves in the monitoring area. Recently, many studies explore CSI from physical layer of wireless networks to detect human motion [11–13]. As indicated in [14], CSI is a subcarrier-level measurement that is more fine-grained compared with RSSI. It is more sensitive to environmental changes while keeps quite stable in static scenarios. As a result, CSI succeeds in improving the performance of human detection.

However, state-of-the-art human detection techniques still have limitations for intrusion detection systems. Common human detection techniques can only detect a human who is walking with a regular pattern. Nevertheless, an intruder in the building is likely to keep away from the security devices or move very slowly to hide himself from being monitored. Furthermore, most human detection techniques require on-site calibration of both static and dynamic environments. On-site calibration is labor intensive and it needs professional deployment and maintenance that makes a human detection system more complex in practical use. Consequently, human detection techniques will fail in detecting intruders in security systems, and we need to explore effective features to model human motion.

To deal with the limitations, in this work, we propose a Robust Device-Free Intrusion Detection (RDFID) system leveraging fine-grained CSI. We investigate the impact of human motion on WiFi signals and demonstrate that different patterns of human motion in different scenarios can be modeled by a unified framework. First, we extract the wavelet variance of CSIs from frequency domain as the feature. It is more sensitive to human motion, and more robust under different moving patterns. In addition, the feature values of static and intrusion can be seen to be generated by different Gaussian Models. As a result, intrusion can be detected using a Gaussian Mixture Model (GMM). As shown in Figure 1, RDFID can detect human motion of different moving patterns. In addition, it can be easily deployed that it can achieve a satisfying performance even using a single pair of transceivers, and needs no re-calibration in different scenarios.

We prototyped RDFID in three typical home and office scenarios with commodity WiFi devices composing only one wireless link. We evaluate the system and compare the performance with Fine-grained Real-time passive human motion Detection (FRID), device-free Passive Detection of moving humans with dynamic Speed (PADS) and Fine-grained Indoor Motion Detection (FIMD). The results show that the detection precision of RDFID can achieve over 97% under different moving patterns. Consequently, it makes intrusion detection systems a step closer to practical use.

In summary, the contributions of our work are as follows:

- We propose RDFID, a novel device-free WiFi-based intrusion detection approach, which can detect intruders with different moving patterns at a high accuracy, and needs no re-calibration in different scenarios. It can be deployed in smart home scenarios to ensure security.
- We extract real-time features from CSIs in frequency domain, which is more sensitive to human motion of various moving patterns.
- We use the Gaussian Mixture Model (GMM) as the classifier based on the observation that the feature values under different moving patterns and different environments can be seen to be generated by different Gaussian Models.

In the rest of this paper, the related works about WiFi-based human detection are reviewed in Section 2. Some preliminaries are introduced in Section 3. Section 4 presents the design details of

our proposed intrusion detection system, while the performance evaluation is provided in Section 5. In Section 6, the potentials and limitations are discussed and we conclude this work in Section 7.

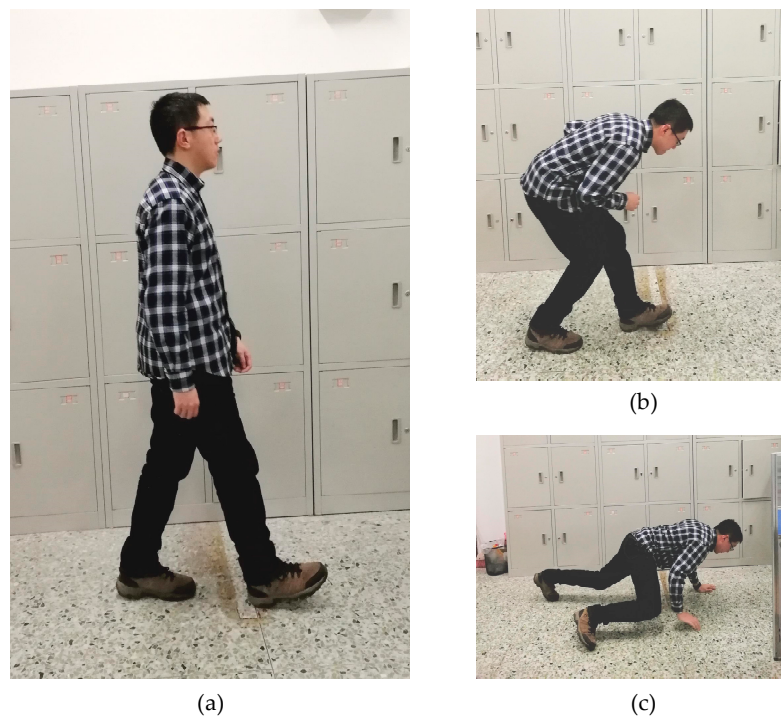


Figure 1. Different moving patterns in intrusion scenarios. (a) Regular walking; (b) walking while bending down; and (c) creeping.

2. Related Work

WiFi-based passive human detection is the fundamental technique of various ubiquitous wireless sensing applications, such as indoor localization, human identification and activity recognition. It can be widely deployed in smart home scenarios to ensure the security. A large quantity of studies about wireless sensing promote the development of wireless sensing.

Earlier passive human detection systems usually utilize RSSI from the MAC layer of the wireless network. After Youssef et al. proposed the concept of device-free passive human motion detection, they optimized their approach and made the system work in real environments [10]. Nuzzer leveraged probabilistic techniques, and had the capability to both localize a single entity and estimate the number of people in the area of interest [15]. Since RSSI is a coarse-grained measurement of wireless networks, many RSSI-based human detection systems deployed multiple pairs of transceivers to achieve a higher accuracy [16]. Another technique of human detection using multiple pairs of transceivers is Radio Tomographic Imaging (RTI) [17]. Researchers also developed various approaches based on RTI, such as the kRTI [18] and dRTI [19]. However, RSSI-based human detection systems suffer from severe multi-path efficiency [20]. As a result, more and more researchers move their attention to the more fine-grained measurement, CSI.

To overcome the shortcomings of RSSI-based human detection systems, Fine-grained device-free Motion Detection (FIMD) utilized the burst pattern of CSIs during human motion to detect human presence [21]. Fine-grained Indoor Localization (FILA) explored the frequency diversity of the subcarriers in Orthogonal Frequency Division Multiplexing (OFDM) systems, and constructed a signal propagation model [22,23]. As human motion can cause the fluctuation of the signal, Bfp harnessed the variance of the amplitude of the CSIs to improve the performance of human detection [11]. PADS took advantages of the whole information of CSI including both amplitude and phase feature to detect human motion with various speeds [24]. It calculates the maximum eigenvalue of covariance matrix of

normalized amplitude and phase information, respectively, as the feature. Support Vector Machine (SVM) is used as the classifier. FRID explored the phase feature of CSIs and achieved calibration-free human detection without the need of a normal profile [25,26]. Short-term averaged variance ratio (SVR) and long-term averaged variance ratio which are two schemes based on the coefficient of variance of phase are introduced to eliminate the re-calibration cost. Conventional human detection systems demonstrated directional monitoring coverage, and Zimu Zhou et al. utilized CSI features to virtually tune the coverage shape into disk-like [27]. Speed Independent Entity Detection (SIED) extracted a novel feature from the whole wireless channel and transformed human detection into a probabilistic problem to achieve a high detection accuracy [5]. AR-Alarm utilized a self-adaptive learning mechanism to achieve intrusion detection without the need of re-calibration [13].

Besides human detection, wireless signals can be used in indoor localization, activity recognition and even human identification. Abdel-Nasser et al. utilized CSI to provide a localization approach with a high accuracy leveraging only a single pair of transceiver [28]. CSI-MIMO utilized frequency diversity of CSI to construct the fingerprint of different locations and achieved a localization accuracy of 0.95 m [29]. SpotFi computed the Angle of Arrival (AoA) of multipath components of different antennas and improved the localization accuracy to 40 cm [30]. HiDFPL proposed a measurement to represent the sensitivity of the receiver and enhanced the localization accuracy [31]. Xuyu Wang et al. proposed PhaseFi, a fingerprinting system, using phase information of CSIs and incorporated a greedy algorithm to train the weights of a deep network [32]. Rui Zhou et al. proposed an indoor localization system based on CSI and SVM [33]. Density-based Spatial Clustering Of Applications With Noise (DBSCAN) was utilized in the system to reduce the noise in CSIs.

CSI based human Activity Recognition and Monitoring (CARM) was proposed based on CSIs of wireless channel that quantified the relationship between the movement speeds of different body parts and activities, and it had the ability to recognize human activities [34]. Activity recognition has a wide range of applications, such as somatosensory games. Wi-Play extracted CSI waveforms from commercial WiFi devices to model some specified activity and achieved an activity recognition system [35]. Wifi-based GEsture Recognition (WiGeR) utilized the fluctuation scheme of CSIs generated by the moving of human hands to recognize gestures [36]. Smokey leveraged WiFi signals and had the ability to recognize smoking activity even in the non-line-of-sight (NLOS) and through-wall environments [37]. Wi-Chase utilized the CSIs from all subcarriers to achieve a higher activity recognition accuracy [38].

It is confirmed that human's gait is unique among different people, thus it can be used to identify the human's identity. WifiU was presented to construct the gait profiles of different people utilizing the unique variations in the CSIs [39]. WiWho was presented as a framework of human identification utilizing human's gait extracted from CSIs [40]. FreeSense combined Principal Component Analysis (PCA), Discrete Wavelet Transform (DWT), and Dynamic Time Warping (DTW) to achieve a nine-user human identification [41]. Wii extracted time and frequency-domain features and used time–frequency analysis to achieve an accurate human identification system [7].

Although there have been quantities of work on human detection, they only perform well when the people move in regular patterns. When an intruder appears, he is more likely to move in an irregular way. As a result, a more robust human detection system is proposed in this paper to meet the challenges of intruder detection.

3. Preliminary

CSI is leveraged in this study, and we will give a brief introduction of the background knowledge in this section.

The wireless signals propagate through multiple paths from the transmitter to the receiver in a typical indoor scenario. As a result, the received signal is the superposition of the signals from LOS path and several reflection paths. OFDM framework is the basis of 802.11 n wireless networks, in which our system works. In this framework, the wireless channel can be described by a Channel

Impulse Response (CIR) in the time domain. Under the assumption of time-invariant, CIR can be expressed as:

$$h(\tau) = \sum_{i=1}^N \alpha_i e^{-j\theta_i} \delta(\tau - \tau_i) + n(\tau), \tag{1}$$

where α_i , θ_i , and τ_i denote the amplitude, phase and time delay of the signal from i^{th} path, respectively; N is the total number of paths; $n(\tau)$ is complex Gaussian white noise; and $\delta(\tau)$ is the Dirac delta function.

Nevertheless, precise CIR can be extracted only from dedicated devices rather than commodity infrastructures. To overcome this limitation, Channel Frequency Response (CFR) can be extracted from frequency domain, which can model the wireless channel. CFR contains amplitude–frequency response and phase–frequency response. Under the assumption of infinite bandwidth, CIR is equivalent to CFR, and CFR can be transformed by Fast Fourier Transform (FFT) from CIR: [20]

$$H = FFT(h(\tau)). \tag{2}$$

We can obtain CFRs in the format of CSI:

$$H = [H(f_1), H(f_2), \dots, H(f_N)], \tag{3}$$

where N is the number of subcarriers in the wireless network.

The CSI is composed of amplitude and phase of a subcarrier:

$$H(f_k) = \|H(f_k)\| e^{j\sin(\angle H)}, \tag{4}$$

where f_k is the central frequency of the subcarrier, and $\angle H$ represents its phase. Thus, a group of CSIs, $H(f_k), (k = 1, \dots, K)$, denote K sampled CFRs in subcarrier level.

4. System Design

4.1. System Overview

The framework of RDFID is presented in Figure 2. The system has four modules: pre-processing; feature extraction; classification; and post-processing. There are various kinds of noise in the raw collected CSI data, and most noise is removed in pre-processing module. We extract wavelet variance as the real-time feature from frequency domain in feature extraction module. In the classification module, a portion of data is utilized to train a system to be universal that can be adaptive to different scenarios. In the post-processing module, the classification result is further processed to be closer to reality.

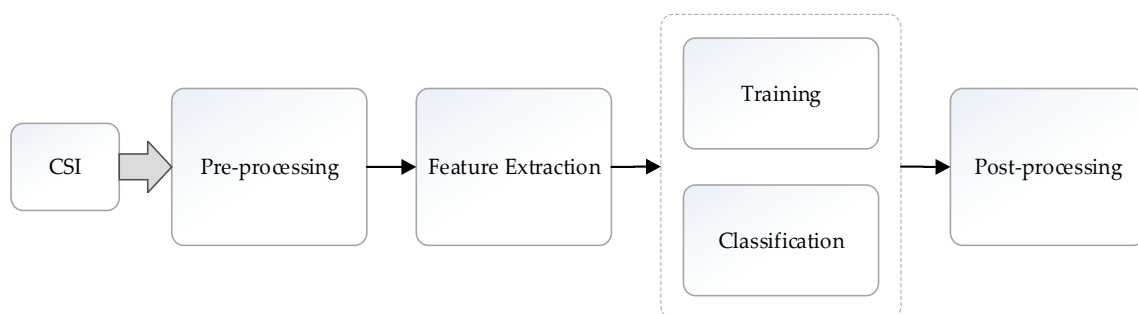


Figure 2. System Framework.

The system can work in typical indoor scenarios with only one pair of commodity WiFi devices, which include a wireless router and a laptop. The wireless router is the Transmit Xmt (TX) that

supports Institute of Electrical and Electronic Engineers (IEEE) 802.11n protocol, while the laptop is the Receive Xmt (RX) that is equipped with Intel 5300 network interface card (NIC). The WiFi devices keep transmitting data to collect CSIs in the monitoring area, and the system estimated intruder existence according to the extracted feature.

4.2. Pre-Processing

The CSI data is extracted from the respond packets of Internet Control Messages Protocol (ICMP) packets. As a result, the number of the group of CSIs is the same as that of ICMP packets theoretically. However, during data collection period, we find that the number of collected CSI records is larger than that of transmitted ICMP packets we had set in advance. In order to calibrate the frequency of the collected data, we conduct the linear interpolation in the raw data and it has a unified frequency. In 802.11 n wireless networks, there are several subcarriers transmitting signals at the same time under the OFDM framework. The subcarriers are independent theoretically. However, the CSIs of adjacent subcarriers have some relationships. In consequence, PCA is used to extract independent data. The related CSI streams can be combined into several independent principle components. For each ICMP packet, a matrix of 3×30 constructed by CSIs can be extracted from the firmware. It can be further reshaped into a 1×90 vector. For a certain time window, n ICMP packets have been received, and we can obtain an $n \times 90$ matrix. During the evaluation of the principle components, we find that in most cases the first principle component can give an 80% contribution rate. As a result, we use the first principle component as the representative data.

Unfortunately, there still exist some kinds of noises in the first principle component, and they have negative impact on detection rate. The one that has the most significant impact is high frequency noise induced by environment changes other than human movement. The movement of torso, arms, and legs cause most of signal reflections. The frequency of the movements is lower than 10 Hz according to our observation. As a result, a low pass filter is utilized to filter out the high frequency noise from the collected data with the frequency higher than 10 Hz.

4.3. Feature Extraction

A proper feature is critical in classification tasks. Generally, the moving speed of a person is constant in a short period, and some periodicity exists when the person is moving. For instance, when the person walks, two steps construct a period. However, it is a challenging task to analyze the periodicity directly from the waveform of the wireless signals. During our early exploration, we find that besides time-domain features, frequency-domain features can better characterize the waveforms in intrusion detection. As a result, in order to explore a scenario independent feature, we utilize time–frequency analysis on the waveform. Continuous Wavelet Transform (CWT) combined with wavelet variance is a proper tool to analyze the periodicity of the waveform. First, the wavelet coefficient of the first principle component of the CSIs after low-pass filter (*cpl*) is calculated utilizing CWT in Equation (5):

$$W_t(a, b) = \int_{-\infty}^{\infty} x(t) \frac{1}{\sqrt{a}} \psi\left(\frac{t-b}{a}\right) dt, \quad (5)$$

where $x(t)$ is the first principle component of the CSIs after low-pass filter (*cpl*), a and b are scale and time, respectively. $\psi()$ is the wavelet function, and db6 (Daubechies) wavelet [42] is selected as it provides the best performance after we have tried different wavelet functions.

As shown in Figure 3, it can be clearly seen that some periodicity exists in the waveform after we conduct continuous wavelet transform. However, it is necessary to quantitatively calculate the significance of the periodicity to confirm that the periodicity is caused by human behaviors.

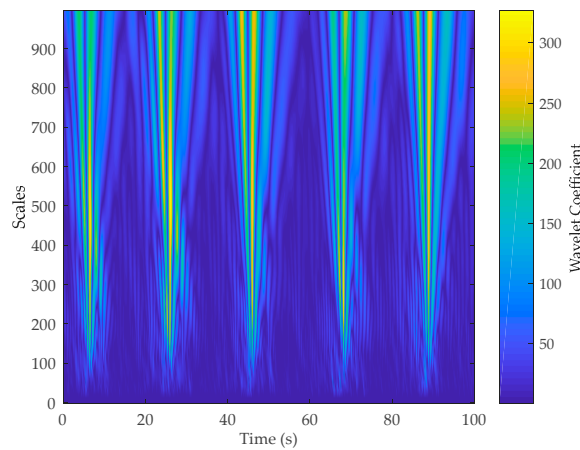


Figure 3. Wavelet coefficient of Channel State Information (CSI) when people move.

Wavelet variance is widely used in meteorology to calculate the periodicity of precipitation. It reflects the distribution of the power of the wavelet coefficients of various scales. As a result, it can also describe the significance of the periodicity of human motion. The wavelet variance is calculated as Equation (6):

$$\text{var}(a) = \int_{-\infty}^{+\infty} |W_f(a, b)|^2 db, \tag{6}$$

where $|W_f(a, b)|^2$ is the power of the wavelet coefficient of scale a at time b .

During our experiment, we find that the distribution of the wavelet variance is different among whether there is human motion as shown in Figure 4. In consequence, the wavelet variance is a proper feature for intrusion detection.

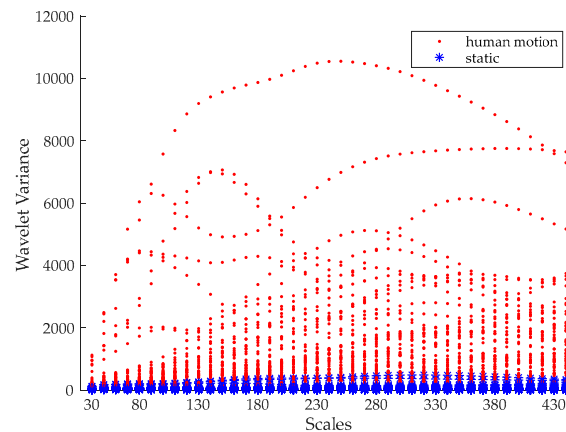


Figure 4. The distribution of wavelet variance when there is human motion and static.

4.4. Training and Classification

As the distribution of the wavelet variance when there is human motion is different from that of static scenario, the Gaussian Mixture Model (GMM) is an appropriate classifier. In this GMM, there are two Gaussian models, one is static model and the other is human motion model. The moving data of different volunteers in different moving patterns and the data collected in the static scenario construct the training data. The GMM only need to be trained once, and it can be used in different scenarios without being re-trained. As a result, after a trained GMM is generated, the intrusion detection system is unsupervised. In the training phase, the vectors of wavelet variance of different scales and the ground truth are utilized to train the GMM. In the classification phase, the inputs are only the vectors of wavelet variance, while the outputs are the detection results whether there exists human motion.

In the end of classification, a post-processing procedure is added to improve the detection accuracy. In this procedure, it is assumed that a person cannot appear and disappear suddenly. As a result, an additional window beyond the detection window is utilized to reduce the detection mistakes. For example, 0 and 1 represent static and intrusion, respectively. If the detection result is 11011 in this additional window, we can consider there always exists intrusion in this window. The cost of this procedure is the time delay in detection, but the detection accuracy can be higher.

5. Evaluation

5.1. Experiment Setup

To evaluate the detection performance of the system, some real experiments are conducted in three typical rooms from several aspects. The three rooms are a meeting room, a typical living room, and a large office, and the sizes of the three room are $5\text{ m} \times 4\text{ m}$, $5\text{ m} \times 4\text{ m}$ and $10\text{ m} \times 6\text{ m}$, respectively. The layout of the three rooms and transceiver deployment are shown in Figure 5. There are desks with glass dam-boards and chairs in the office, while a meeting table and chairs in the meeting room, which causes different multipath effects. Especially, in order to present a reasonable evaluation in a smart home scenario, a typical living room was used as a scenario. In the living room a television, there is a television on the wall, a sofa, a piano, a refrigerator, some other furniture, and some doors to other rooms, which will cause much more complex multipath effects. A TP-Link 802.11n wireless router with a single antenna is used as the transmitter and a Lenovo laptop equipped with a three-antenna Intel WiFi Link 5300 (iwl 5300) NIC running Ubuntu 11.04 OS as the receiver. The firmware of the NIC is modified in order to extract CSIs from data packets utilizing the CSI tools. In addition, we upgrade the antennas of the NIC using three 6dbi gain antennas as shown in Figure 6 in order to increase the signal-noise-ratio.

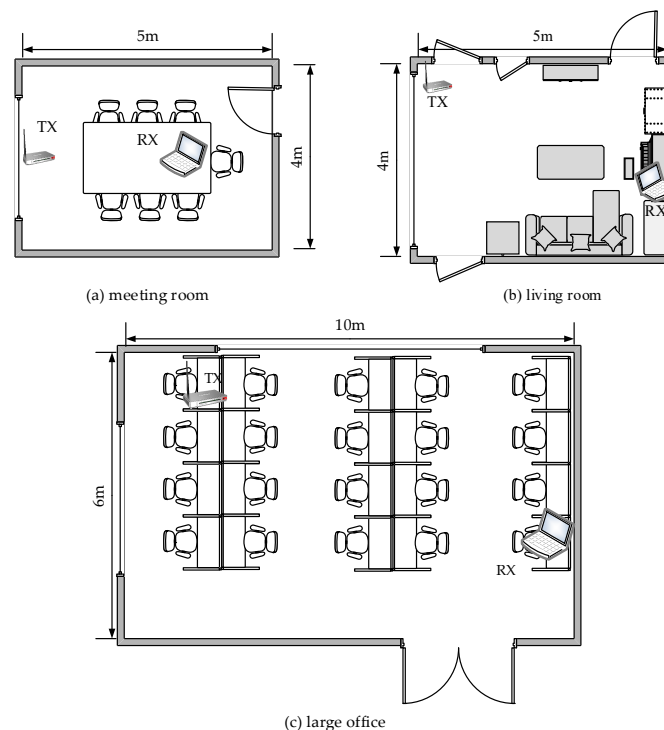


Figure 5. Experimental scenario.

According to CSI tools, the sensing data is the CSIs of the respond packets when the transmitter is continuously sending ICMP packets to the receiver. We recruited four volunteers in our experiments with the basic information shown in Table 1. During data collection period, only a single person

moves back and forth in different moving patterns respectively in the room without a fixed path. The transmission rate in our experiments is configured to 200 Hz. A few cycles of data collection process are conducted for one person, while each cycle contains only one moving pattern and lasts for 100 s. Data collection lasts for one week, and about 20 min moving data is collected for one person moving in one pattern.

False negative (FN), false positive (FP), and the probability of detection (PD) are used as the evaluation metrics in this paper. False negative is the ratio that RDFID fails to detect intrusion, while false positive is the ratio it reports intrusion when nobody is in the room. The probability of detection is the ratio that it successfully detects the existence of the intruder. The three metrics can be illustrated by Figure 7, where P1–P4 are the elements of the confusion matrix in the form of percentage. As shown in Figure 7, P4 represents FN and P1 represents FP. PD is described in Equation (7).

$$PD = P3 / (P3 + P4), \tag{7}$$

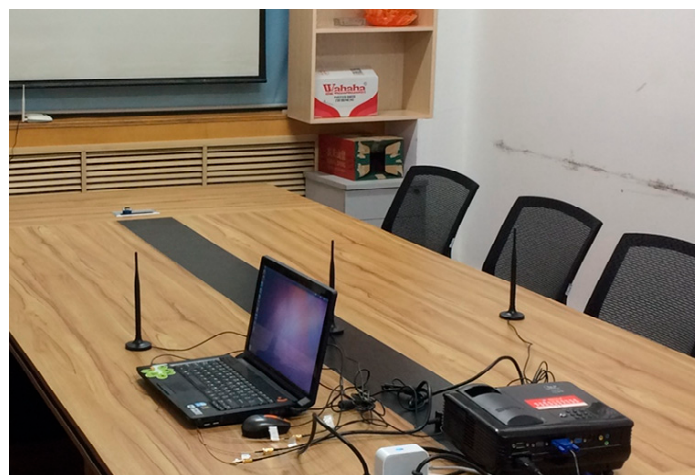


Figure 6. The modified receiver.

		Classified as	
		intrusion	clear
Actual state	clear	P1	P2
	intrusion	P3	P4

Figure 7. Confusion matrix of intrusion detection.

Table 1. Basic information of volunteers.

Volunteers	Gender	Height (cm)	Weight (kg)	Age
1	male	174	63	30
2	male	175	70	27
3	male	170	62	27
4	female	163	51	26

5.2. Performance Evaluation

5.2.1. Intrusion Detection in Different Scenarios

In order to confirm that the performance of RDFID is independent of scenarios, we first evaluate the system in different rooms. In addition, we compare the system with two other device-free human

detection systems, FRID and PADS. When constructing the training set, we use the combination of the data from the three scenarios to form six groups of training set and we name them a, b, c, ab, ac, and bc, respectively, according to Figure 7, and all training sets contain the three moving patterns. Datasets that are opposite to the training sets are used as test sets, which are bc, ac, ab, c, b, and a, respectively. To ensure the reliability of the evaluation, each training set is equally divided into five parts, and five experiments are conducted in which the classifier is trained using each part respectively. The result is the mean of the five experiments. The window size in these experiments is 5 s. The FN and FP rate of the three approaches is shown in Table 2. As indicated in the table, the FN rate of RDFID in different scenarios is around 2%, which is the lowest among the three approaches. The FN rate of PADS is affected more significantly by the selection of the training set because it uses SVM as its classifier, the support vectors in different scenarios are not the same. As a result, the FN rate of PADS is higher. As FRID does not need training data, the estimation of the parameters has particular influence on the performance of human detection.

Table 2. False negative/false positive (FN/FP) of human detection in different scenarios (%).

Training Set	FN						FP					
	a	b	c	ab	ac	bc	a	b	c	ab	ac	bc
RDFID	2.5	2.3	2.4	2.4	2.6	2.5	1.7	2.2	2.1	2.2	2.1	1.9
FRID	4.8	5.8	4.4	4.3	5.7	5.2	8.5	8.2	8.7	8.7	8.2	8.6
PADS	6.0	6.7	6.2	6.1	6.8	5.8	10.8	10.2	10.5	11.8	11.0	10.6

The FP rate of RDFID is lower than the other two approaches. Most of the FP rate is around 2%, which indicates RDFID generates less false alarms when detecting intruders. PADS uses phase information in CSIs that is more sensitive to environmental changes; therefore, it achieves the highest FP rate among the three approaches.

Figure 8 indicates the PD of the approaches in different scenarios. It can be seen from the figure that RDFID achieves the most stable and lowest probability of detection.

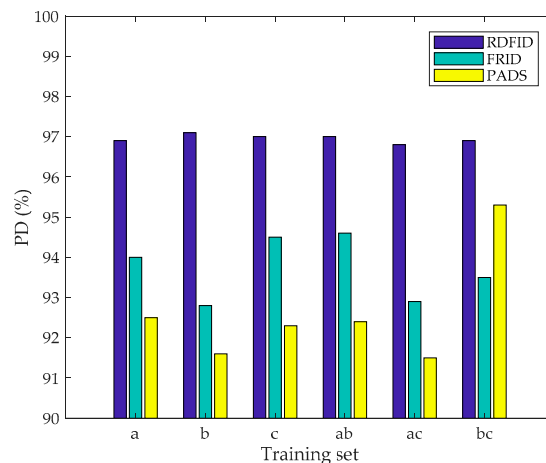


Figure 8. The probability of detection (PD) of human detection in different scenarios.

It can be seen from the results that the detection performance of RDFID is independent of scenarios. The detection model trained in one scenario can be adapted to other scenarios directly in a relative high detection performance.

5.2.2. Intrusion Detection among Different People

In order to evaluate the independence of the intrusion detection performance among different people, we use the moving data of only one volunteer as the training data, while the moving data of

all the four volunteers as the test data. The training data and test data of the first volunteer has no intersection. In addition, the performance of RDFID is compared to that of PADS. When constructing the training set, the moving data of the first volunteer is used as the training set. It contains the moving data in all three scenarios and three different moving patterns. The evaluation is conducted five times, and each time the training data is selected randomly from the moving data of the first volunteer. The result is the mean of the five times. The window size is 5 s; the FN and FP rate of the two approaches are presented in Table 3. It is indicated in the table that the FN rate of RDFID is relatively stable when detecting different people. However, the FN rate of PADS is more sensitive to different people. Its FN rate is even lower than that of RDFID when the test data and training data is from the same person. In contrast, the FN rate of PADS suffers significant fluctuation when the test data and the training data is from different people. The result shows that the FN rate of PADS is sensitive to training data and test data, the moving data from different people can affect the detection performance. As a result, RDFID has a better adaptability to different people.

Table 3. FN/FP of human detection of different people (%).

Volunteer	FN				FP			
	1	2	3	4	1	2	3	4
RDFID	2.1	2.9	3.3	2.8	1.7	1.8	1.8	2
PADS	1.9	7.3	9.1	7.4	2.4	8.8	8.5	9.8

The trend of the FP rate of the two approaches is similar to that of the FN rate. The FP rate of RDFID is still stable in the four tests and maintains about 2%. However, the FP rate of PADS achieves a low level only when the test data and training data is from the same person, and raises significantly using the test data of the other three people.

Figure 9 shows the PD of the two approaches when detection different people. Besides PADS achieves a lower PD when the data of the same volunteer is used in both training set and test set, RDFID has a higher PD when using the moving data of the other volunteers as test set.

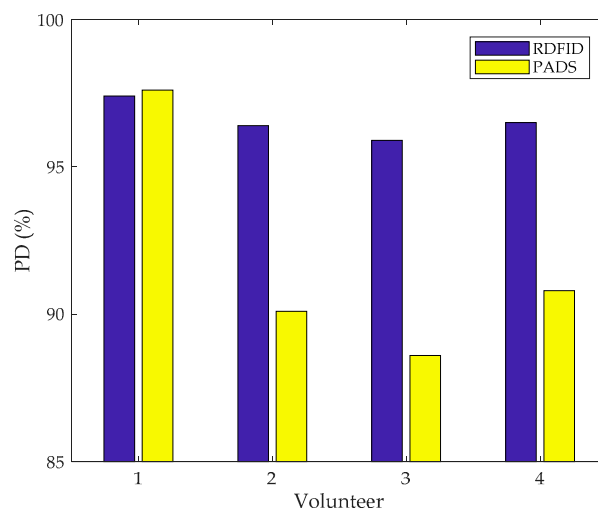


Figure 9. PD of human detection of different people.

In consequence, RDFID is less sensitive to the training and test data, and can achieve a better human detection performance.

5.2.3. Intrusion Detection with Different Window Sizes

As RDFID is a window-based human detection approach, the detection performance is also evaluated under different window sizes. To examine the advancement of RDFID, it is compared to two other human detection approaches, FRID and PADS. In the construction phase of the training set, a 30 s data segment is randomly divided from the regular walking data of the first volunteer in scenario (a). The test data contains the regular walking data of the other three volunteers, while the window size ranges from 1 s to 5 s.

The results are the mean values of the three people. The FN and FP rate of the three approaches under different window sizes are shown in Table 4. It is indicated from the table that the FN rate of RDFID is as high as 11.7% when the window size is 1 s, but it decreases to 5.2% when the window size changes to 2 s. Moreover, the FN rate of RDFID keeps decreasing as the window size increases. It is because the 1-s window is too narrow for human motion, and people can only walk less than two steps within the window. As a result, the periodicity in the extracted frequency-domain features is not significant enough, which leads to a higher FN rate. Although the FN rate of FRID is lower than that of RDFID when the window size is 1 s, it decreases slower when the window size increases. On the other hand, as the training and test data is from the same scenario in this experiment, the variation of the support vector of the features is insignificant; the FN rate of PADS can achieve a low level.

Table 4. FN/FP of human detection under different window sizes (%).

Window Size (s)	FN					FP				
	1	2	3	4	5	1	2	3	4	5
RDFID	11.7	5.2	4.6	3	2.1	2.1	2.3	1.7	1.8	1.7
FRID	9.8	7.4	5.6	4.9	4.4	7	7.6	6.8	7.2	7.3
PADS	6.3	4.6	4.6	3.8	3.2	3.5	3.8	3.5	4	3.3

The FP rate of the three approaches all undergoes a low fluctuation, which indicates that the FP rate of the three approaches can be less affected by the window size. However, as the extracted feature in RDFID has a better discernibility between static and dynamic, this approach achieves the lowest FP rate.

Figure 10 shows the PD of the three approaches when the window size is different. It can be seen that PADS achieves a higher PD when the window size is no larger than 3 s, but the PD of RDFID increases fast as the window size gets larger, and gets the highest of the three approaches when the window size is larger than 3 s.

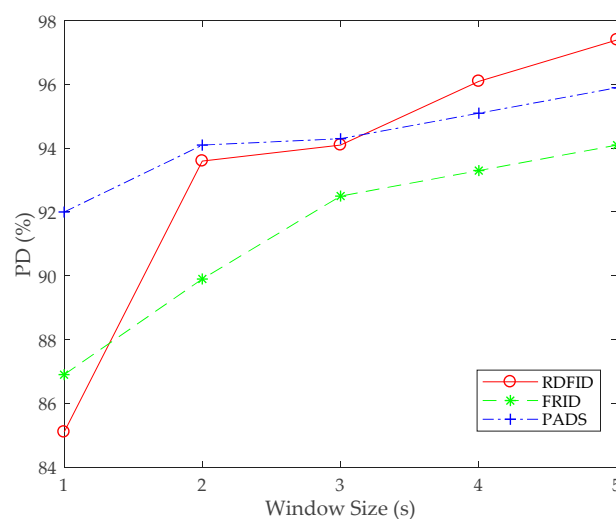


Figure 10. PD of human detection under different window sizes.

5.2.4. Intrusion Detection with Different Moving Patterns

The most important problem that RDFID solves is human detection under different moving patterns. In consequence, to evaluate the ability of RDFID in this problem, the data of different moving patterns is used in this evaluation. To address the importance of this problem, RDFID is compared to FRID, PADS, and FIMD [21]. A 30 s moving data segment of the first volunteer in scenario (b) under regular moving pattern is randomly divided as training data, while the data of the other three volunteers in scenario (b) under three different moving patterns is used as the test data. The results of the three approaches are the mean values of the three volunteers, and the window size is 5 s.

The FN and FP rate of the four approaches under different moving patterns is shown in Table 5. It can be seen from the table that the FN rate of RDFID remains stable under different moving patterns. However, the FN rate of the other three approaches raises significantly when the volunteers creep on the floor. FRID, PADS, and FIMD are affected more significantly because the influence of the human body to the transmission of the wireless signal becomes weak when the volunteers creep on the floor. The FN rate of RDFID has a small fluctuation because the extracted feature is related to the periodicity of human motion. It can detect human at a high accuracy as long as there exists a periodicity of human motion.

Table 5. FN/FP of human detection under different moving patterns (%).

Moving Pattern	FN			FP		
	Regular Walking	Bending Down	Creeping	Regular Walking	Bending Down	Creeping
RDFID	2.3	2.5	2.6	1.7	1.7	1.5
FRID	4.8	5.2	9.8	7.8	6.2	3.6
PADS	4.3	4.8	6.4	4.3	4.1	2.8
FIMD	5.4	5.7	12.5	6.8	6.4	4.8

The FP rate of RDFID is still stable under the three moving patterns, while the change trend of the FP rate of the other three approaches is the opposite to that of the FN rate. The reason is the same that the influence of human body to the transmission of the wireless signal becomes less when the person creeps on the floor. The low FP rate of the other three approaches is on the cost of the high FN rate. In consequence, RDFID has the ability to detect human of different moving patterns. It has the advancement of human detection especially when the person moves in an irregular pattern. The robustness of RDFID is higher that the detection performance is less affected by different moving patterns.

As illustrated in Figure 11, the PD of RDFID is the highest and stable under the three different moving patterns benefiting from the frequency-domain feature.

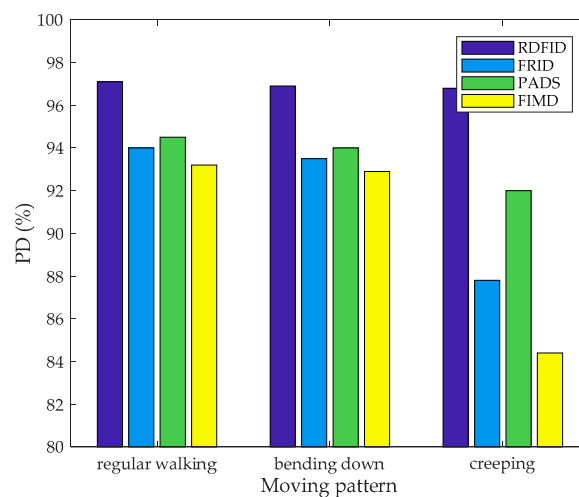


Figure 11. PD of human detection under different moving patterns.

5.2.5. Intrusion Detection under Different Moving Speeds

As a special case, human detection under different moving speeds plays an important role in intrusion detection systems. The four volunteers are asked to walk in a regular pattern at 1.5 m/s, 0.7 m/s, and 0.2 m/s, respectively, in the meeting room. A 30 s data segment is randomly divided from the data of the first volunteer walking at the speed of 0.7 m/s as the training data, while the walking data of the other three volunteers under different speeds is used as the test data. The window size is 5 s, and the results are the mean value of the three volunteers. The human detection performance of RDFID is compared to PADS and FRID. The FN and FP rate of the three approaches under different moving speeds is shown in Table 6. As indicated in the table, the trends of the FN rate of the approaches are the same that they all increase as the moving speed becomes slower. The influence of human motion to the transmission of the wireless signal decreases when the moving speed becomes slower. Especially when the person moves far away from the first Fresnel zone, the reflected signal is submerged in the signal from the LOS path. As a result, it is of great difficulties to extract effect environmental change information from the received signal. On the other hand, it can be seen that the FN rate of RDFID is lower than the other approaches.

Table 6. FN/FP of human detection under different moving speeds (%).

Moving Speed (m/s)	FN			FP		
	1.5	0.7	0.2	1.5	0.7	0.2
RDFID	1.2	1.8	3.4	1.2	1.2	0.9
FRID	2.1	3	4.2	2.1	2.3	1.8
PADS	2.2	3.3	5.7	3.3	2.3	1.2

It can be seen that the FP rate of the three approaches under different moving speeds is relatively stable and keeps at a low level. It indicates that the probability of false alarm of the three approaches is low when detecting human motion.

As can be seen from Figure 12, the PD of the three approaches all suffer a decrease when the moving speed becomes slower. The performance of human detection can be affected by different moving speeds, but the overall detection performance can meet the requirement of security in a regular smart home environment.

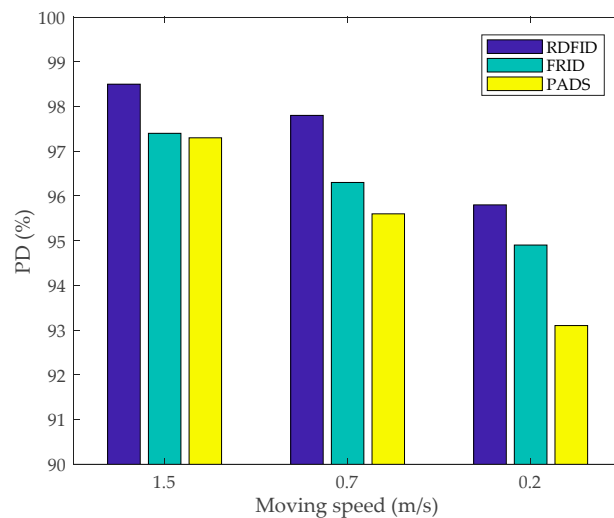


Figure 12. PD of human detection under different moving speeds.

6. Discussion

We did a set of evaluations in this work and demonstrated the effectiveness of RDFID to detect human motion of different moving patterns using WiFi signals. However, there are still some limitations in RDFID. In this section, we will give a discussion about the limitations and potentials of RDFID.

Although the approach can achieve a high intrusion detection accuracy, it may be influenced by several factors.

First, the relative location of the intruder and transceivers can affect the detection accuracy. There exists a relationship between the impact of the intruder to the signal transmission and the distance of the intruder to the transceivers. When the intruder moves far away from the transceivers or the first Fresnel zone, it becomes more difficult to extract effective features from the collected CSI of the ambient wireless signal. As a result, the detection accuracy suffers a degradation when the distance of the intruder to the transceivers.

In addition, in real scenarios there may exist more than one intruder. Nevertheless, the movement of multiple intruders will break the periodicity of the received CSI. In consequence, the detection performance will be affected directly.

Despite these limitations, WiFi signal-based intrusion detection systems have much potential in a smart home. In our future work, we will explore more effective features that less affected as much by the distance of the intruder to the transceivers and the number of the intruders in the environment to make the approach more robust in smart home applications.

7. Conclusions

In this paper, we propose RDFID, a robust device-free passive intrusion detection approach. The moving pattern of the intruder has less influence to the detection performance of RDFID. Furthermore, the detection accuracy can achieve a high level without re-calibration when the scenario has changed. It only need commodity off-the-shelf (COTS) WiFi devices, and extract fine-grained channel state information from the physical layer of the wireless network. The time-frequency analysis technique is utilized to extract the features that are affected less by the environment from the frequency domain. As a result, the performance of RDFID is less affected by the moving pattern of the intruder and the different indoor scenarios. In order to evaluate the effectiveness of RDFID, a set of experiments were conducted from several perspectives. The results demonstrate that RDFID can achieve a high performance of intrusion detection, and can meet the security requirement in a smart home.

Author Contributions: Conceptualization, J.L. and D.M.; Funding acquisition, W.Y.; Methodology, J.L.; Project administration, W.Y.; Supervision, D.M.; Validation, L.G. and M.Y.; Writing—original draft, J.L.; Writing—review & editing, W.Y. and X.D.

Funding: This research was funded by the National Natural Science Foundation of China, grant number 6177010612 and 61831007, and Natural Science Foundation of Tianjin, grant number No. 18JQNJC69900.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Youssef, M.; Mah, M.; Agrawala, A. Challenges: Device-free passive localization for wireless environments. In Proceedings of the 13th annual ACM international conference on Mobile computing and networking, Montreal, QC, Canada, 9–14 September 2007; pp. 222–229.
2. Du, X.; Chen, H. Security in wireless sensor networks. *IEEE Wirel. Commun.* **2008**, *15*, 60–66.
3. Du, X.; Guizani, M.; Xiao, Y.; Chen, H. A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 1223–1229. [[CrossRef](#)]
4. Du, X.; Xiao, Y.; Guizani, M.; Chen, H.-H. An effective key management scheme for heterogeneous sensor networks. *Ad Hoc Netw.* **2007**, *5*, 24–34. [[CrossRef](#)]

5. Lv, J.; Yang, W.; Gong, L.; Man, D.; Du, X. Robust wlan-based indoor fine-grained intrusion detection. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–6.
6. Gong, L.; Yang, W.; Man, D.; Lv, J. Ipil: Improving passive indoor localisation via link-based csi features. *Int. J. Ad Hoc Ubiquitous Comput.* **2016**, *23*, 36–45. [[CrossRef](#)]
7. Lv, J.; Yang, W.; Man, D. Device-free passive identity identification via wifi signals. *Sensors* **2017**, *17*, 2520. [[CrossRef](#)] [[PubMed](#)]
8. Xiao, Y.; Rayi, V.K.; Sun, B.; Du, X.; Hu, F.; Galloway, M. A survey of key management schemes in wireless sensor networks. *Comput. Commun.* **2007**, *30*, 2314–2341. [[CrossRef](#)]
9. Guan, Z.; Li, J.; Wu, L.; Zhang, Y.; Wu, J.; Du, X. Achieving efficient and secure data acquisition for cloud-supported internet of things in smart grid. *IEEE Internet Things J.* **2017**, *4*, 1934–1944. [[CrossRef](#)]
10. Moussa, M.; Youssef, M. Smart devices for smart environments: Device-free passive detection in real environments. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications, PerCom 2009, Galveston, TX, USA, 9–13 March 2009; pp. 1–6.
11. Liu, W.; Gao, X.; Wang, L.; Wang, D. Bfp: Behavior-free passive motion detection using phy information. *Wirel. Pers. Commun.* **2015**, *83*, 1035–1055. [[CrossRef](#)]
12. Al-qaness, M.A.A.; Li, F.; Ma, X.; Liu, G. Device-free home intruder detection and alarm system using wi-fi channel state information. *Int. J. Future Comput. Commun.* **2016**, *5*, 180. [[CrossRef](#)]
13. Li, S.; Li, X.; Niu, K.; Wang, H.; Zhang, Y.; Zhang, D. Ar-alarm: An adaptive and robust intrusion detection system leveraging csi from commodity wi-fi. In *Enhanced quality of life and smart living: Proceedings of the 15th international conference, icost 2017, Paris, France, 29–31 August 2017*; Mokhtari, M., Abdulrazak, B., Aloulou, H., Eds.; Springer International Publishing: Cham, Germany, 2017; pp. 211–223.
14. Halperin, D.; Hu, W.; Sheth, A.; Wetherall, D. Tool release: Gathering 802.11n traces with channel state information. *ACM SIGCOMM Comput. Commun. Rev.* **2011**, *41*, 53. [[CrossRef](#)]
15. Seifeldin, M.; Saeed, A.; Kosba, A.E.; El-Keyi, A.; Youssef, M. Nuzzer: A large-scale device-free passive localization system for wireless environments. *IEEE. Trans. Mob. Comput.* **2013**, *12*, 1321–1334. [[CrossRef](#)]
16. Zheng, X.; Yang, J.; Chen, Y.; Xiong, H. An adaptive framework coping with dynamic target speed for device-free passive localization. *IEEE. Trans. Mob. Comput.* **2015**, *14*, 1138–1150. [[CrossRef](#)]
17. Wilson, J.; Patwari, N. Radio tomographic imaging with wireless networks. *IEEE. Trans. Mob. Comput.* **2010**, *9*, 621–632. [[CrossRef](#)]
18. Zhao, Y.; Patwari, N.; Phillips, J.M.; Venkatasubramanian, S. Radio tomographic imaging and tracking of stationary and moving people via kernel distance. In Proceedings of the 12th International Conference on Information Processing in Sensor Networks, Philadelphia, PA, USA, 8–11 April 2013; pp. 229–240.
19. Wei, B.; Varshney, A.; Patwari, N.; Hu, W.; Voigt, T.; Chou, C.T. Drti: Directional radio tomographic imaging. In Proceedings of the 14th International Conference on Information Processing in Sensor Networks, Seattle, WA, USA, 14–16 April 2015; pp. 166–177.
20. Yang, Z.; Zhou, Z.; Liu, Y. From rssi to csi: Indoor localization via channel response. *ACM Comput. Surv.* **2013**, *46*, 1–32. [[CrossRef](#)]
21. Jiang, X.; Kaishun, W.; Youwen, Y.; Lu, W.; Ni, L.M. Fimd: Fine-grained device-free motion detection. In Proceedings of the 2012 IEEE 18th International Conference on Parallel and Distributed Systems, Singapore, 17–19 December 2012; pp. 229–235.
22. Kaishun, W.; Jiang, X.; Youwen, Y.; Dihu, C.; Xiaonan, L.; Ni, L.M. Csi-based indoor localization. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 1300–1309.
23. Kaishun, W.; Xiao, J.; Youwen, Y.; Min, G.; Ni, L.M. Fila: Fine-grained indoor localization. In Proceedings of the 2012 Proceedings IEEE INFOCOM, Orlando, FL, USA, 25–30 March 2012; pp. 2210–2218.
24. Qian, K.; Wu, C.; Yang, Z.; Liu, Y.; Zhou, Z. Pads: Passive detection of moving targets with dynamic speed using phy layer information. In Proceedings of the 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, 16–19 December 2014; pp. 1–8.
25. Gong, L.; Man, D.; Lv, J.; Shen, G.; Yang, W. Frid: Indoor fine-grained real-time passive human motion detection. In Proceedings of the 2015 IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 10–14 August 2015; pp. 308–311.

26. Gong, L.; Yang, W.; Man, D.; Dong, G.; Yu, M.; Lv, J. Wifi-based real-time calibration-free passive human motion detection. *Sensors* **2015**, *15*, 32213–32229. [[CrossRef](#)] [[PubMed](#)]
27. Zimu, Z.; Zheng, Y.; Chenshu, W.; Longfei, S.; Yunhao, L. Omnidirectional coverage for device-free passive human detection. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 1819–1829.
28. Abdel-Nasser, H.; Samir, R.; Sabek, I.; Youssef, M. Monophy: Mono-stream-based device-free wlan localization via physical layer information. In Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 4546–4551.
29. Chapre, Y.; Ignjatovic, A.; Seneviratne, A.; Jha, S. Csi-mimo: An efficient wi-fi fingerprinting using channel state information with mimo. *Pervasive Mob. Comput.* **2015**, *23*, 89–103. [[CrossRef](#)]
30. Kotaru, M.; Joshi, K.; Bharadia, D.; Katti, S. Spotfi: Decimeter level localization using wifi. In Proceedings of the SIGCOMM 2015, London, UK, 17–21 August 2015; pp. 269–282.
31. Yang, W.; Gong, L.; Man, D.; Lv, J.; Cai, H.; Zhou, X.; Yang, Z. Enhancing the performance of indoor device-free passive localization. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 256162. [[CrossRef](#)]
32. Wang, X.; Gao, L.; Mao, S. Csi phase fingerprinting for indoor localization with a deep learning approach. *IEEE Internet Things J.* **2016**, *3*, 1113–1123. [[CrossRef](#)]
33. Zhou, R.; Lu, X.; Zhao, P.; Chen, J. Device-free presence detection and localization with svm and csi fingerprinting. *IEEE Sens. J.* **2017**, *17*, 7990–7999. [[CrossRef](#)]
34. Wang, W.; Liu, A.X.; Shahzad, M.; Ling, K.; Lu, S. Understanding and modeling of wifi signal based human activity recognition. In Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, Paris, France, 7–11 September 2015; pp. 65–76.
35. Cao, X.; Chen, B.; Zhao, Y. Wi-play: Robust human activity recognition for somatosensory game using wi-fi signals. In *Cloud Computing and Security: Second International Conference, ICCCS 2016, Nanjing, China, 29–31 July 2016*; Sun, X., Liu, A., Chao, H.-C., Bertino, E., Eds.; Springer International Publishing: Cham, Germany, 2016; pp. 205–216.
36. Al-qaness, M.A.A.; Li, F. Wiger: Wifi-based gesture recognition system. *ISPRS Int. Geo-Inf.* **2016**, *5*, 92. [[CrossRef](#)]
37. Zheng, X.; Wang, J.; Shangguan, L.; Zhou, Z.; Liu, Y. Smokey: Ubiquitous smoking detection with commercial wifi infrastructures. In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016; pp. 1–9.
38. Arshad, S.; Feng, C.; Liu, Y.; Hu, Y.; Yu, R.; Zhou, S.; Li, H. Wi-chase: A wifi based human activity recognition system for sensorless environments. In Proceedings of the 2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Macau, China, 12–15 June 2017; pp. 1–6.
39. Wang, W.; Liu, A.X.; Shahzad, M. Gait recognition using wifi signals. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Heidelberg, Germany, 12–16 September 2016; pp. 363–373.
40. Zeng, Y.; Pathak, P.H.; Mohapatra, P. Wiwho: Wifi-based person identification in smart spaces. In Proceedings of the 15th International Conference on Information Processing in Sensor Networks, Vienna, Austria, 11–14 April 2016; pp. 1–12.
41. Xin, T.; Guo, B.; Wang, Z.; Li, M.; Yu, Z.; Zhou, X. Freesense: Indoor human identification with wi-fi signals. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–7.
42. Daubechies, I. *Ten Lectures on Wavelets*; SIAM: Philadelphia, PA, USA, 1992.

