AR-Alarm: An Adaptive and Robust Intrusion Detection System Leveraging CSI from Commodity Wi-Fi

Shengjie Li[1,2], Xiang Li[1,2], Kai Niu[1,2], Hao Wang[1,2], Yue Zhang[1,2], and Daqing Zhang[1,2(✉)]

[1] Key Laboratory of High Confidence Software Technologies, Ministry of Education, Beijing 100871, China
[2] School of Electronics Engineering and Computer Science, Peking University, Beijing, China
{lishengjie,lixiang13,xjtunk,china7,zy.zhangyue,dqzsei}@pku.edu.cn

Abstract. Device-free human intrusion detection holds great potential and multiple challenges for applications ranging from asset protection to elder care. In this paper, leveraging the fine-grained Channel State Information (CSI) in commodity WiFi devices, we design and implement an adaptive and robust human intrusion detection system, called AR-Alarm. By utilizing a robust feature and self-adaptive learning mechanism, AR-Alarm achieves real-time intrusion detection in different environments without calibration efforts. To further increase the system robustness, we propose a few novel methods to distinguish real human intrusion from object motion in daily life such as object dropping, curtain swinging and pets moving. As demonstrated in the experiments, AR-Alarm achieves a high detection rate and low false alarm rate.

Keywords: WiFi · Device-free · Intrusion detection

1 Introduction

Device-free intrusion detection intends to inform whether there is a person breaking in the area of interests without attaching any devices. It is essential for various smart home scenarios such as asset protection, home security, child and elder care. In order to achieve device-free intrusion detection, various techniques have been proposed and studied, among which video-based [3] approach is one of the most popular methods. It utilizes cameras installed in the environment capturing image or video sequences for scene recognition. Its main problems include the privacy concern, inherent requirement for lighting condition and high false alarm rate. Other sensor-based approaches try to make use of information caused by human walking to detect intrusion but disturbance coming from the environment often causes a large portion of false alarms. Moreover, all these methods share the requirement of installing special hardware in the environment.

M. Mokhtari et al. (Eds.): ICOST 2017, LNCS 10461, pp. 211–223, 2017.
DOI: 10.1007/978-3-319-66188-9_18

Due to the limitations of the above-mentioned device-free intrusion detection methods, the low cost, easily available Wi-Fi devices are utilized to sense human intrusion. A typical WiFi based intrusion detection system consists of two phases: off-line calibration and online monitoring. During the off-line calibration stage, both data without human motion and with human motion are gathered to construct a normal profile and determine a detection threshold. Then in the online monitoring stage, once the deviation from the normal profile exceeds a pre-determined threshold, an intrusion event is detected.

Based on this principle, prior works [10,13,15] leverage the correlation of CSI (Channel State Information) measurements over time to infer intrusion occurrence. However, these methods are environment dependent and a labor-intensive learning process is often needed when the environment changes, i.e. furniture moves, WiFi device location changes, or deployment in another environment. Apart from the cumbersome environment dependent learning process, it is also intrinsically challenging for these systems to avoid false alarms caused by common scenes in daily life such as dropping object, swinging curtain and small pets' movement, which could also result in significant changes of CSI profile.

Aiming to overcome the limitations of state of art approaches, in this paper, we propose an adaptive and robust human intrusion detection system, called AR-Alarm. For the first time, AR-Alarm achieves real-time human intrusion detection in different environments without calibration efforts. To reach the goal, we firstly extract a robust feature using the ratio between the dynamic and static CSI profiles of the environment. And based on this feature, our system only needs to learn the static CSI profile through a self-adaptive mechanism when the applied environment changes. In order to further improve the robustness of the system, we consider the common scenes in daily life such as dropping object, swinging curtain and small pets' movement, and have proposed a series of schemes to distinguish human intrusion from these events.

The rest of the paper is organized as follows. We first review the related work in Sect. 2. Then we introduce some preliminaries about channel state information and our study about feature selection in Sect. 3. In Sect. 4, we present the detailed design of our proposed system, AR-Alarm, followed by the experiment evaluation in Sect. 5. Finally, we conclude the work in Sect. 6.

2 Related Work

In this section, we review the related work from two perspectives: research on passive intrusion detection and research on WiFi based intrusion detection.

Related work on passive intrusion detection. The earliest and most researched approach is based on vision techniques. For example, [3] utilized video-based algorithms to analyze sequences of images captured by cameras and to track moving people. However, these video-based systems still have a set of open issues to be resolved, such as privacy concern, intensive computation for real-time processing. Infra-based approaches [8] utilize human blocking of light beams to report an intrusion. They could preserve human privacy but are

restricted to line-of-sight scenarios, and not be able to cover the entire area of an environment. Audio [6] and pressure [9] sensor information could also be used for intrusion detection, whose rationale is that intrusion activities will cause changes in acoustic noise or floor vibration. However, they are easily influenced by other sources of sound or pressure in the environment, leading to false alarms.

Related work on Wi-Fi based intrusion detection. Since RSS (Received Signal Strength) measurements are handily accessible in most existing wireless devices, it is widely studied to detect human presence and intrusion relying on RSS variance [7,16]. Despite its ease of access, RSS can fluctuate dramatically even at a stationary link [14], leading to unreliable detection results. Compared with RSS, CSI (Channel State Information) is a more fine-grained signal feature, that characterizes the multipath effect at the granularity of OFDM subcarrier in the frequency domain [2]. Similar to RSS-based systems, most CSI-based intrusion detection systems also leverage variations in CSI measurement to inform target presence or intrusion. Specifically, FIMD [15] leverages correlation of CSI amplitude over time to extract features and achieves device-free human motion detection. Further, PADS [10] extracts phase information from CSI and combines both phase and amplitude information to improve human detection accuracy. DeMan [13] not only utilizes temporal stability of CSI to detect dynamic human but also observes the periodic fluctuation of CSI due to human respiration to detect stationary human. An omnidirectional passive human detection system is proposed by Zhou [18], which virtually shapes the targeted coverage area by using PHY layer features. The paper [17] proposes a metric for commodity WiFi as a proxy for detection sensitivity to characterize the impact of human presence on wireless signals. However, all these works need on-site and environment-specific threshold calibration or model building when the target environment changes. Although in [4], a link sensitivity indicator is proposed to depict abundance of multipath propagation for accommodating to the environment change but multiple location attempts are still required to calibrate the system in advance.

Unlike existing intrusion detection schemes that require labor-intensive calibration or multiple location data collection when the target environment changes, our work aims to minimize such labor intensive overhead through adopting a robust feature and a self-adaptive learning mechanism. Moreover, we also take the easily confused daily events into account and propose effective schemes to distinguish real human intrusion from object motion, which are often ignored by existing work on human intrusion detection.

3 Preliminaries and Observations

In this section, we firstly introduce the Channel State Information (CSI) accessible on commodity Wi-Fi devices. Then based on intensive empirical study, we present a robust feature to characterize the change of CSI signal for intrusion detection.

3.1 Channel State Information

Channel State Information (CSI) is information that estimates the channel by representing the channel properties of a communication link. In the wireless communication system, the received baseband signal in frequency domain is:

$$y = Hx + n \tag{1}$$

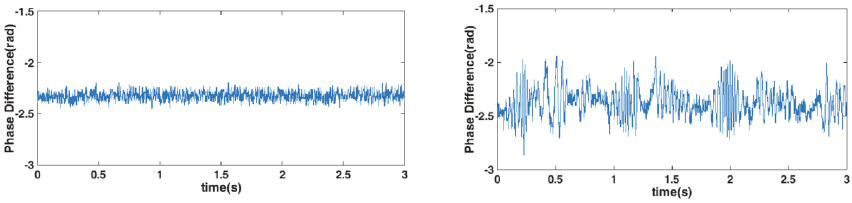
where y and x are the received and the transmitted signal vectors respectively, n denotes the channel noise vector, H is the channel state information matrix. To estimate the channel state information matrix H, a predetermined pilot sequence is transmitted. According to the received sequence, receiver estimates the channel state information matrix by $H = y/x$, which contains the amplitude information and phase information. And CSI can be mathematically depicted as:

$$H = |H|e^{j\theta} \tag{2}$$

where $|H|$ and θ are the amplitude and phase, respectively. To increase communication capacity, current Wi-Fi standards (e.g., IEEE 802.11 n/ac) use orthogonal frequency division modulation (OFDM) technology in physical layer to split the whole spectrum band (20 MHz) into multiple (56) frequency sub-bands, transmitting data across multiple subcarriers in parallel. Each subcarrier can be viewed as an independent communication link and has its own CSI. In other words, every subcarrier CSI of all subcarriers gets together to form the CSI matrix of the system.

3.2 Robust Feature Selection

In typical indoor scenarios, Wi-Fi signals propagate from the transmitter to receiver through multiple paths such as floor, wall and furniture. When a person moves in the environment, additional signal paths are introduced by the reflection of human body. Correspondingly, the value of CSI will reflect the change of these paths. So the amplitude variation and phase in the CSI stream can be leveraged to detect human intrusion. In AR-Alarm, we utilize the phase difference over two antennas as the salient signal to sense the change of the environment,



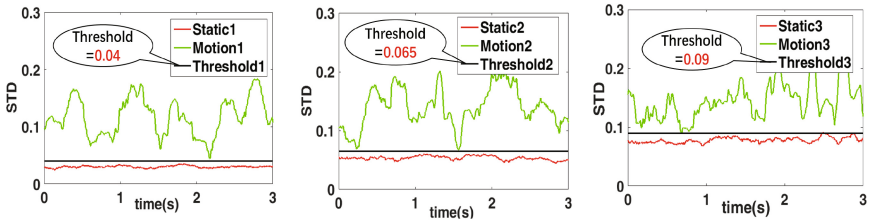
(a) Static Environment (b) Human Intrusion

Fig. 1. Phase difference of static and dynamic environment

for better sensitivity to signal variation [11]. Figure 1 shows the CSI phase difference in static and human intrusion environments. Whenever there is object movement in the environment, we can observe a change in the signal.

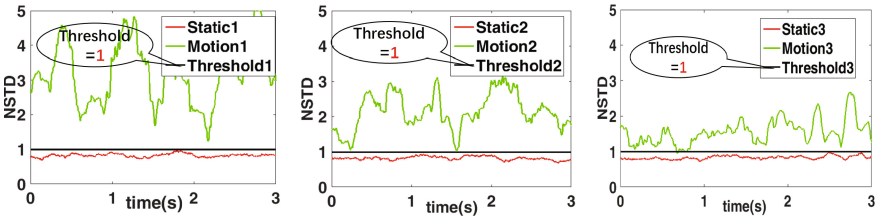
How do we mathematically characterize the signal variance of CSI phase difference? Intuitively, we can use the standard deviation to characterize the variance of the signal as shown in Fig. 2a. Unfortunately, like the fingerprint based solution, the threshold needs to be determined according to the environment change. Specifically, when we adjust the location of the receiver, the standard deviation of the signal variance is shown in Fig. 2b. If we change the room for experiment, the standard deviation changes as shown in Fig. 2c. As we can see, the threshold in scenario 1 (Fig. 2a) can't be applied directly to other scenarios. Through intensive experiment study, we find that if we use the maximum standard deviation of phase difference in static environment to normalize that in human intrusion scenarios, we don't need to learn a new threshold for a new scenario, as shown in Fig. 3. If σ is the standard deviation of CSI phase difference, then the robust feature can be selected as follows:

$$\mu_{motion} = \frac{\sigma_{motion}}{max(\sigma_{static})} \tag{3}$$



(a) Scenario1 (b) Scenario2 (c) Scenario3

Fig. 2. Standard deviation of phase difference in different scenarios



(a) Scenario1 (b) Scenario2 (c) Scenario3

Fig. 3. Normalized standard deviation of phase difference in different scenarios

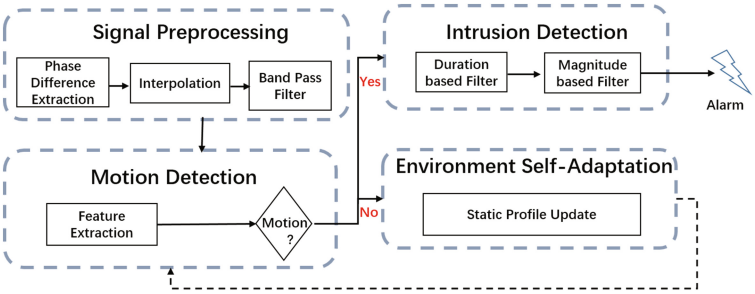


Fig. 4. Overview of the AR-Alarm

4 The AR-Alarm Human Intrusion Detection System

Our proposed real-time intrusion detection system, AR-Alarm, consists of four modules: signal preprocessing, motion detection, environment self-adaptation and intrusion detection. As shown in Fig. 4, the collected CSI signal streams are first fed into the signal preprocessing module to ensure the extracted phase difference continuous in a shared Wi-Fi channel and eliminate out-band interference. Then in motion detection module, we extract features as proposed in previous section to coarsely decide whether there is a moving object or person in the environment. If the answer is YES, the CSI signals are then fed into the intrusion detection module for finer-grained human motion detection. Otherwise, the environment self-adaptation module is triggered to update the static profile frequently to accommodate environment changes in real-time.

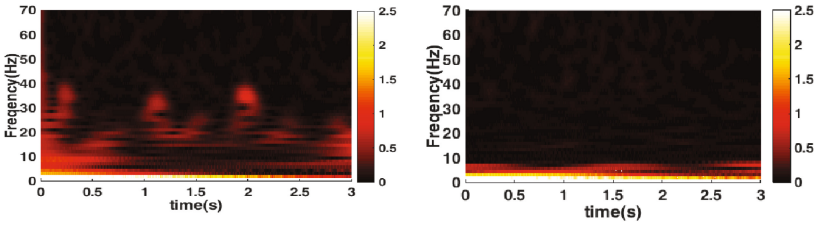
4.1 Signal Preprocessing

The goal of signal preprocessing is threefold: (1) Make the phase difference over two antennas as basic signal; (2) Deal with the uneven arrival of packets caused by the burst Wi-Fi transmissions. (3) Go through a band-pass filter to filter out non-human activities.

Phase Difference Extraction. Because of the phase offset caused by various factors [11], the phase information in commodity Wi-Fi can not be used directly to sense human intrusion. We utilize the phase difference over two antennas to be a robust signal [11].

Interpolation. Wi-Fi is a shared channel, where multiple devices use random access to share the medium. This results in the received packets that are not evenly spaced in time domain. To get evenly received samples, we adopt the 1-D linear interpolation algorithm to process the raw CSI readings. Since the duration of typical human intrusion is greater than one second, the above interpolation operation preserves the human intrusion information.

Band-pass Filter. According to work [12], the frequency of CSI amplitude variation could reveal the human motion speed. Similarly, from the time-frequency



(a) Human Intrusion (b) Swinging Curtain

Fig. 5. Time-frequency analysis of different activities

analysis of phase difference in Fig. 5, we can see human intrusion induces obvious power profile in higher frequency than that caused by swinging curtain. And according to work [1], normal walking speeds ranges from 1.25 m/s to 1.5 m/s for human being. So we extract the signal whose frequency is in the range between 10 Hz (0.3 m/s) and 70 Hz (2 m/s) with a band-pass filter. By applying this filter, our system could filter out not only the high-frequency noise but also the low frequency disturbance caused by swinging curtain.

4.2 Motion Detection

In this module, we first extract feature from the filtered CSI phase difference signal, and then decide whether there is a moving object or human subject in the environment. This module contains two steps: (1) Feature Extraction (2) Motion Discriminant.

Feature Extraction. After the preprocessing in Sect. 4.1, we acquire the filtered phase difference signal as input for this step. Then based on the study in Sect. 3.2, we calculate the normalized standard deviation μ_{now} in a sliding window as the robust feature for further processing. It is depicted as follows:

$$\mu_{now} = \frac{\sigma_{now}}{max(\sigma_{static})} \tag{4}$$

σ_{now} means the standard deviation of current filtered CSI phase difference. $max(\sigma_{static})$ is the maximum value of standard deviation in the static environment which is updated with time. And its initial value was attained when the system was started for the first time. After calculation, both σ_{now} and μ_{now} will be used in next step for processing.

Motion Discriminant. Based on the extracted feature, we further propose a threshold-based method to decide whether there exists any motion in the environment, no matter what causes the motion. To check if the whole sliding window lies in the static state, we compare μ_{now} with a pre-defined threshold δ_{motion}. If it is larger than δ_{motion}, the feature μ_{now} will be passed to intrusion detection module to see if it is caused by human intrusion or object motion.

Otherwise, it implies a static environment and the environment self-adaption module will be triggered.

4.3 Environment Self-adaption

In this module, a real-time static profile update scheme is implemented to accommodate the environment change. Whenever there is no motion in the environment, the static profile will be updated. Specifically, the maximum standard deviation value of σ_{now} is computed, afterwards we update the previous result with $max(\sigma_{now})$ for later feature extraction in the motion detection module. Through this self-learning mechanism, our system could accommodate the environment change in real time and achieve the environment self-adaption.

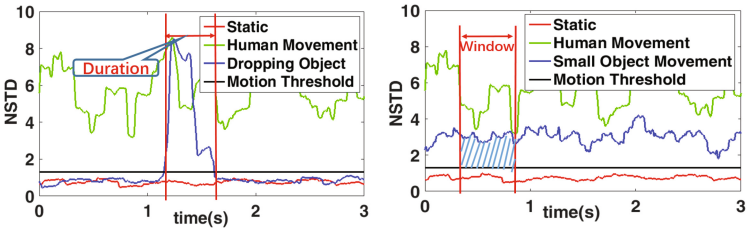
4.4 Intrusion Detection

In this module, we develop two schemes to differentiate the intrusion from object motions in daily life. A duration based filter is used to get rid of very short-term object motions such as dropping objects, while a magnitude based filter is applied to eliminate the interference caused by small moving objects such as pets.

Duration-based Filter. In our daily life, moving objects in the environment could experience a high speed so that a band-pass filter could not filter them out, those objects could be falling coat hangers or dropping boxes. Through empirical study, we notice that these activities only last for a very short time. As shown in Fig. 6(a), the duration of a dropping object usually lasts less than 1 s, while human intrusion often lasts longer, say lasting for at least 2 s at a normal speed. In order to filter out those short-term activities, we measure the duration for $\mu_{now} > \delta_{motion}$. If the duration is less than 1 s, it implies object dropping;

Magnitude-based Filter. In consideration of different families, some may raise a small pet in their home. The motion of small pets not only could reach the same speed as human beings but also last for some time which could not be filtered out by the last steps. However, a small pet has a smaller size which often introduces less number of reflected paths than a human does, so the magnitude of signal fluctuation caused by the small pet movement is smaller than that by human intrusion as shown in Fig. 6(b). Inspired by this observation, we propose an area-based method to differentiate human intrusion from others. First, we calculate the integration when μ_{now} is larger than δ_{motion} in a time window (e.g. 1 s) and then compare the value with the threshold δ_{area} to determine if the motion it is human intrusion, which could be expressed as follows:

$$\begin{cases} \int (\mu_{now} > \delta_{motion})dt > \delta_{area} & Human \quad Intrusion \\ \int (\mu_{now} > \delta_{motion})dt < \delta_{area} & Not \quad Intrusion \end{cases} \tag{5}$$



(a) (b)

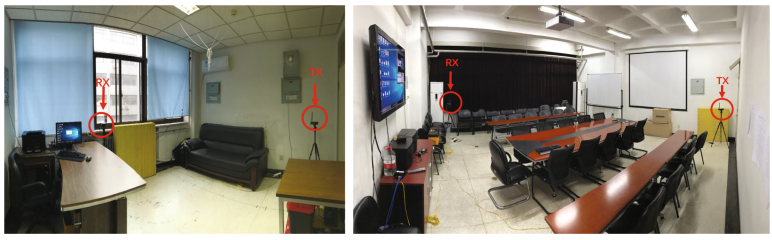
Fig. 6. (a) Dropping object vs intrusion (b) Pet movement vs intrusion

5 Evaluation

In this section, we present the evaluation results of our AR-Alarm system using off-the-shelf WiFi devices. First, we introduce the experiment settings. Then we present the dataset and metrics for evaluation. Finally, we will report our system performance in various scenarios.

5.1 Experimental Setups

Our system only needs one Wi-Fi transmitter and one receiver. We employ two GIGABYTE miniPCs equipped with off-the-shelf Intel 5300 Wi-Fi cards as the transmitter and receiver. The CSI tool [5] developed by Halperin is installed on the miniPCs to collect the CSI from the receiver. The sampling rate of CSI in our experiments is set to 500 Hz to ensure that the human intrusion could be detected without much delay. We conduct experiments in two rooms of different sizes to test our proposed framework as shown in Fig. 7. (office room: 3 m × 4 m, meeting room: 6 m × 6 m).



(a) Office Room (b) Meeting Room

Fig. 7. Test environments

5.2 Dataset and Metrics

Before the system evaluation, we firstly gather CSI data in an office room with and without human motion to learn the system parameters and construct an original static pattern database. Once the thresholds are determined, different indoor multipath environments (changing room or moving furniture) will share the same system parameters. The learning period for system parameters takes about two minutes. Then in the testing stage, four students (three males, one female) perform intrusion activities in the two test rooms over two months. We deploy a camera in each room to record the activities conducted as ground truth. And the metrics for evaluation are given below:

True Detection Rate (TDR) is the probability that the system can detect a human intrusion.

False Positive Rate (FPR) is defined as the proportion that the system generates an alarm when there is no human intrusion.

5.3 System Performance

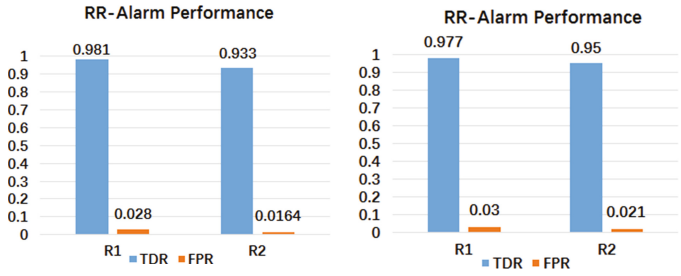
In this section, we present the evaluation performance of our AR-Alarm system from two aspects. As the techniques proposed in previous work [10,13,15] are environment dependent, we first conduct experiments to see if our system can automatically adjust itself to adapt to the environments while achieving comparable results with previous work. Then to further evaluate the robustness of our system, we simulate several daily events which have not been considered in previous work.

5.3.1 Adaptability to the Environment

In order to test the adaptability of our system to the indoor environment changes, we design two challenging situations: (1) Different indoor environments, and (2) Different environment settings.

Adaptability to Different Indoor Environments. We firstly conduct the experiments in two different rooms (R1: Office Room, R2: Meeting Room) just like the prior work [4,10,13,15], the WiFi transmitters are placed at various heights from 1.2 m to 2 m. Diverse TX-RX distances from 2 m to 7 m are tested. Both LOS and NLOS conditions (when the transmitter is blocked by an object) are also evaluated. We divide the entire space into small grids of size 1.5 m × 1.5 m and the intrusion activity takes place in every grid for several times. As shown below in Fig. 8a, our system not only shows consistent performance across different indoor environments but also achieves comparable performance with prior work [4,10,13,15]. Remarkably, in order to achieve such system performance, existing schemes [4,10,13,15] either require labor-intensive calibration or multiple location data collection to suit for a different environment. In contrast, our system is deployed in two environments without change of system parameters. So with its self-adaptive mechanism, it could accommodate different environments with no human efforts.

Adaptability to Environmental Setting Changes. Besides changing the indoor environments for experiments, we also evaluate the system against furniture movement. In each environment, we move big furniture such as bookcases, sofa, tables to different locations in order to simulate the setting changes. It is noted that our system performance is not affected much by the movement of these furniture. Specifically, Fig. 8b shows the performance when the sofa in R1 is moved to the window side and a big table in R2 is moved from the middle to the wall side. In all cases, AR-Alarm system shows excellent adaptability to the multipath environment changes.



(a) R1vsR2 (b) R1vsR2(Move Furniture)

Fig. 8. AR-Alarm performance

5.3.2 Robustness to Daily Events

In this part, we further study the impact of daily events such as dropping object, swinging curtain and small pets' movement on the system performance, to see if we can distinguish human intrusion from these events.

Impact of dropping object. To study the influence of a dropping object to the system performance, we manually drop the object in different positions to simulate the dropping events happening in real life. To isolate the influence of human, volunteers stand firmly and hold the object in hand ahead of time which ensures the change of their posture is as little as possible in the whole dropping process. The influence of dropping event in two test environments is presented in Tables 1 and 2, respectively. In most cases, our system could resist influence of a dropping object. Sometimes, the object drops down and then rolls on the floor for a period of time. In this situation, our system might cause false alarm because of its long-lasting influence.

Impact of swinging curtain. To further test the system robustness, we evaluate the influence of swinging curtain. In the experiment, volunteers wave the curtain manually to simulate the effect of blowing wind. And for sake of excluding the interference from human, the subject is requested to stay outside the room with a cord connected to the curtain. Different waving strengths are applied to simulate different intensity of the wind. Results are shown in Tables 1 and 2, respectively.

Table 1. Confusion matrix of R1

G	P	
	Stationary	Intrusion
Dropping object	96.5%	3.5%
Swinging curtain	99.8%	0.2%
Moving pet	95.2%	4.8%

Table 2. Confusion matrix of R2

G	P	
	Stationary	Intrusion
Dropping object	98%	2%
Swinging curtain	99.5%	0.5%
Moving pet	94.5%	5.5%

The false-alarm rates in two rooms are both lower than 1%, indicating that the system is quite robust to swinging curtain.

Impact of small pets' movement. Considering that many families have pets or sweeping robot kind of things, we study the influence of this kind of small moving object on the system performance. Similarly, volunteers manually pull boxes of three different size ($30 \times 28 \times 30\,\mathrm{cm}^3$, $40 \times 30 \times 37\,\mathrm{cm}^3$, $59 \times 33 \times 44\,\mathrm{cm}^3$) with a cord in different routes to simulate pet movement. What's more, for each route, we repeat several times with different moving speeds. The results are presented in confusion matrix shown below. Among the experiments, the false alarms are mainly caused by the large box which has similar size with a human torso.

6 Conclusion

In this paper, we design and implement an adaptive and robust indoor human intrusion detection system, AR-Alarm. This is the first Wi-Fi based adaptive intrusion detection system which addresses two challenges, i.e., the multipath environment changes and common anomalous scenes in real life. Utilizing the commodity off-the-shelf WiFi devices, our system could achieve a very high detection rate and a low false alarm rate. Experimental results conducted in different multipath environments have demonstrated the adaptability and robustness of our system. It has the potential to become a practical and non-intrusive human intrusion detection system.

Human intrusion detection has long been a research topic in human activity sensing domain. Although we implemented quite an effective human intrusion detector using WiFi devices, the system still has a lot of room for further improvement. Considering that the intruders often break in from windows or doors, we could place transceivers properly to further improve the detection accuracy of our system. If we could take more daily events into account, our system will be further closer to practice. We are working on these questions and expect to deploy the system in real homes in near future.

Acknowledgments. This work is supported by National Key Research and Development Plan under Grant No. 2016YFB1001200.

References

1. Transafety. http://www.usroads.com/journals/p/rej/9710/re971001.htm
2. Bhartia, A., Chen, Y.C., Rallapalli, S., Qiu, L.: Harnessing frequency diversity in wi-fi networks. In: International Conference on Mobile Computing and Networking (MOBICOM 2011), Las Vegas, Nevada, USA, September, pp. 253–264 (2011)
3. Cai, Q., Aggarwal, J.K.: Automatic tracking of human motion in indoor scenes across multiple synchronized video streams. In: International Conference on Computer Vision, pp. 356–362 (1998)
4. Gong, L., Yang, W., Zhou, Z., Man, D., Cai, H., Zhou, X., Yang, Z.: An adaptive wireless passive human detection via fine-grained physical layer information. Ad Hoc Netw. **38**, 38–50 (2016)
5. Halperin, D., Hu, W., Sheth, A., Wetherall, D.: Tool release: gathering 802.11n traces with channel state information. ACM Sigcomm Comput. Commun. Rev. **41**(1), 53 (2011)
6. Iyengar, S.G., Varshney, P.K., Damarla, T.: On the detection of footsteps based on acoustic and seismic sensing. In: Asilomar Conference on Signals, pp. 2248–2252 (2007)
7. Kosba, A.E., Saeed, A., Youssef, M.: Rasid: a robust WLAN device-free passive motion detection system. In: 2012 IEEE International Conference on Pervasive Computing and Communications, pp. 180–189, March 2012
8. Liu, L., Zhang, W., Deng, C., Yin, S., Wei, S.: Briguard: a lightweight indoor intrusion detection system based on infrared light spot displacement. IET Sci. Measur. Technol. **9**(3), 306–314 (2015)
9. Orr, R.J., Abowd, G.D.: The smart floor: a mechanism for natural user identification and tracking. In: CHI 2000 Extended Abstracts on Human Factors in Computing Systems, pp. 275–276 (2000)
10. Qian, K., Wu, C., Yang, Z., Liu, Y., Zhou, Z.: Pads: passive detection of moving targets with dynamic speed using PHY layer information. In: IEEE International Conference on Parallel and Distributed Systems, pp. 1–8 (2014)
11. Wang, H., Zhang, D., Wang, Y., Ma, J., Wang, Y., Li, S.: RT-fall: a real-time and contactless fall detection system with commodity wifi devices. IEEE Trans. Mobile Comput. **PP**(99), 1 (2017)
12. Wang, W., Liu, A.X., Shahzad, M., Ling, K., Lu, S.: Understanding and modeling of wifi signal based human activity recognition. In: International Conference on Mobile Computing and NETWORKING, pp. 65–76 (2015)
13. Wu, C., Yang, Z., Zhou, Z., Liu, X., Liu, Y., Cao, J.: Non-invasive detection of moving and stationary human with wifi. IEEE J. Sel. Areas Commun. **33**(11), 2329–2342 (2015)
14. Wu, K., Xiao, J., Yi, Y., Gao, M., Ni, L.M.: Fila: fine-grained indoor localization. In: INFOCOM, 2012 Proceedings IEEE, pp. 2210–2218 (2012)
15. Xiao, J., Wu, K., Yi, Y., Wang, L., Ni, L.M.: FIMD: fine-grained device-free motion detection. **90**(1), 229–235 (2012)
16. Youssef, M., Mah, M., Agrawala, A.: Challenges: device-free passive localization for wireless environments. In: ACM International Conference on Mobile Computing and NETWORKING, pp. 222–229 (2007)
17. Zhou, Z., Yang, Z., Wu, C., Liu, Y., Ni, L.M.: On multipath link characterization and adaptation for device-free human detection, pp. 389–398 (2015)
18. Zhou, Z., Yang, Z., Wu, C., Shangguan, L.: Towards omnidirectional passive human detection. In: INFOCOM, 2013 Proceedings IEEE, pp. 3057–3065 (2013)