國立臺灣大學電機資訊學院電信工程學研究所

碩士論文

Graduate Institute of Communication Engineering
College of Electrical Engineering and Computer Science
National Taiwan University

Master Thesis

基於 WiFi 通道狀態資訊與功率延遲特徵之入侵偵測與追蹤技術

Intruder Detection and Tracking Based on Power Delay Profile from WiFi CSI

李妍潔

Yen-Chieh Li

指導教授：謝宏昀 博士

Advisor: Hung-Yun Hsieh, Ph.D.

中華民國 112 年 8 月

August 2023

doi:10.6342/NTU202303843

國立臺灣大學碩士學位論文
口試委員會審定書
MASTER'S THESIS ACCEPTANCE CERTIFICATE
NATIONAL TAIWAN UNIVERSITY

基於 WiFi 通道狀態資訊與功率延遲特徵之入侵偵測與追蹤技術

Intruder Detection and Tracking Based on Power Delay Profile from WiFi CSI

本論文係李妍潔（R10942047）在國立臺灣大學電信工程學研究所完成之碩士學位論文，於民國 112 年 7 月 25 日承下列考試委員審查通過及口試及格，特此證明。

The undersigned, appointed by the Graduate Institute of Communication Engineering on 25/7/2023 have examined a Master's thesis entitled above presented by Yen-Chieh Li (R10942047) candidate and hereby certify that it is worthy of acceptance.

口試委員 Oral examination committee:

謝志昀　　黃相軒　　方凱田

（指導教授 Advisor）

系主任/所長 Director: 劉陽夏

致謝

時光流轉，兩年的研究生涯也已進入尾聲，在這期間受到許多人的幫助，伴隨著滿滿的收穫與祝福，即將畢業了。懷抱著五味雜陳的心，仍不忘的是對這一路上支持的無限感恩。

能夠順利完成本論文，首先感謝謝宏昀教授在我迷茫時的指點、懈怠時的督促，並在每一次的報告中激勵我在研究上找到問題的能力。感謝一起畢業的學長同學們，彼此之間相互扶持，有你們的陪伴是我的幸運。感謝實驗室的學弟妹，平時的閒話家常都是都是忙碌日子裡的小確幸。最後感謝我的父母以及家人們，在這段時間裡，每當我需要幫助的時候，都不嫌麻煩的伸出援手；這段旅程很辛苦，你們對我的關心與鼓勵是我心底一直以來最踏實的後盾。時間仍陪著我們漫步前進，這段旅程將成為我難以忘懷的回憶。滿懷著對所有人的感激之情，期許感謝之人都能在自己的道路上一路順遂，保持健康的身體向目標邁進。

最後，謹以此向所有關心我、幫助我的人致上最深的謝意，並將這份研究成果呈現給你們。

2023/08/08 李妍潔 筆

doi:10.6342/NTU202303843

摘要

基於通道狀態信息（CSI）的入侵偵測系統至今已有許多發展。然而，以往的相關研究在入侵者被阻擋或僅於小範圍內活動時會讓表現變差，並且大多數研究僅偵測入侵者的存在。我們認為一個完善的入侵檢測系統應該足夠穩健、對入侵者敏感，並且能夠在一定程度上追蹤入侵者所在的區域。功率延遲特徵（PDP）根據每條路徑的延遲提供近似路徑分量的資訊。眾所周知，當信號向四面八方傳播時，不同的傳播路徑會不同程度地受到入侵者的影響。基於以上觀點，我們設計了一種演算法能夠尋找最能反映入侵者活動的路徑分量以增加檢測概率，並同時利用 PDP 提供的延遲資訊來追蹤入侵者位置。首先，我們必須構建一個入侵檢測系統來評估演算法的性能。在以往研究的基礎上，我們設計了一個基礎系統，並在實驗室和教室進行了測試，其平均偵測率能夠達到 93.69%。然而，對於一些入侵者被遮擋或遠離檢測設備的位置，偵測率僅為 60.77%。經過演算法的增強，遮擋區域的偵測率可以提高到 94.44%，整個系統的平均偵測率也提高到 98.98%。另外，為了驗證 PDP 能否達到追蹤的目的，我們還在模擬器上模擬了實驗室環境。我們控制空間中唯一變量為入侵者，在理想環境下使用 320MHz 頻寬，可以使追蹤誤差小至 0.45m。

doi:10.6342/NTU202303843

ABSTRACT

There have been many developments in intrusion detection systems based on Channel State Information (CSI). However, previous related research performances are limited when intruders are blocked or only move in a small area, and most studies only detect intruders' existence. A sound intrusion detection system should be robust enough, sensitive to intruders, and able to track the area where the intruder is located to a certain extent. Power Delay Profile (PDP) provides approximate path component information based on the delay of each path. It is known that when the signal spreads in all directions, different propagation paths are affected to varying degrees by intruders. Based on the above point of view, we designed an algorithm to find the path component that best reflects the intruder's activities to increase the probability of detection, and at the same time use the delay information provided by the PDP to track the intruder's position. First, we must construct an intrusion detection system to evaluate the algorithm's performance. Based on previous research, we built a basic system and tested it in actual laboratories and classrooms, and its average detection rate has reached 93.69%. However, the detection rate was only 60.77% for some positions where the intruder was obstructed or moved away from the detection devices. After the enhancement of our algorithm, the detection rate of blocked areas could increase to 94.44%, and the average detection rate of the overall system has also risen to 98.98%. Additionally, to verify that PDP can achieve the purpose of tracking, we also simulated the laboratory environment on the simulator. We control the only change in the space is the intruder so that the tracking accuracy can be as small as 0.45m.

doi:10.6342/NTU202303843

TABLE OF CONTENTS

doi:10.6342/NTU202303843

doi:10.6342/NTU202303843

doi:10.6342/NTU202303843

LIST OF TABLES

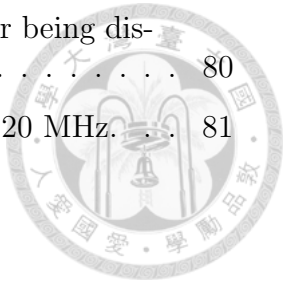
doi:10.6342/NTU202303843

LIST OF FIGURES

doi:10.6342/NTU202303843

doi:10.6342/NTU202303843

doi:10.6342/NTU202303843



doi:10.6342/NTU202303843

CHAPTER 1

INTRODUCTION

In recent years, device-free passive detection technology that does not require any equipment has become popular, and several associated studies and programs have been created to enhance people's experiences. So far, many existing techniques exist to achieve intrusion detection, such as using cameras [9, 10], sensors [11, 12] that need to be worn, received signal strength (RSS) based [13–15], and channel state information (CSI) based methods [16–20]. Our research focuses on detecting the presence or absence of intruders rather than identifying intruders.

Firstly, the camera-based method installs cameras in the target environment and analyzes collected images to identify intruders. Its disadvantage is that it is affected by light and may not accurately detect intruders in darker environments or if obstructed. In addition, there are potential privacy issues with collecting images. The sensor-based method requires users to wear the corresponding sensors. The prerequisite for using this method is confirmation of whether the user is wearing the corresponding sensor. However, this restriction can make users feel inconvenienced and may lose their detection purpose. The above are traditional methods and have specific requirements for basic equipment installation.

With the development of wireless network technology, people also try to use the ubiquitous WiFi signal to detect changes in the surrounding wireless content. This includes intrusion detection, indoor positioning, motion recognition, and gesture or physiological feature recognition. RSS-based methods utilize measured RSS changes to infer the state of a dynamic environment. The RSS signal between the receiver and transmitter is attenuated when a targeted intrusion reaches the monitoring range. Although RSS is convenient and has no privacy concerns, it is not a stable metric due to its sensitivity to environmental noise and coarse-grained signals.

Today, many commercial devices can extract CSI, such as the Atheros AR9580 chipset, PicoScene, and Nexmon, as well as the Intel Wifi Link 5300 NIC. CSI contains measurement information on the magnitude and phase of each Orthogonal Frequency Division Multiplexing (OFDM) subcarrier [2, 3]. This better expresses the different multipath reflections caused by humans. Due to CSI's benefits over RSS, which only offers coarse-grained channel information at the physical layer, researchers have proposed several CSI-based passive detection systems. To this end, we propose an intrusion detection method that utilizes the phase difference

doi:10.6342/NTU202303843

between adjacent antennas, which is more stable than the amplitude. It uses Power Delay Profile (PDP) information to enhance the intrusion message and estimate the approximate location of the intruder to achieve Detection and Tracking Purposes simultaneously.

In contrast to previous intrusion detection systems based on CSI, most are intended to detect random activities carried out inside the building. However, considering that most intruder activities are cautious and concentrated in specific fixed points in a small range, the system design and experiments are specially carried out for this scenario. We found that intrusion detection will affect detection performance because of whether the intruder blocks the device. Its weakening is because it is difficult for the signal to reach the position of the intruder, and it will be weakened due to multiple reflections and diffractions. Here, based on PDP, an intrusion information enhancement method is designed further to improve the average performance of the intrusion system [31]. Since the PDP covers the propagation information of the path, we further track the intruder location by analyzing which path delay components are most affected by the intruder. We organize our contributions as follows:

- Constructing a stable intrusion detection system can effectively compensate for inadequacies and adapt to different environmental changes. There can be an average detection performance of 93.69% against intrusions in the indoor environment.

- Developing a PDP-based method for enhancing intrusion signals. By utilizing the path component information of the PDP, the intrusion signal can be improved when the intruder's position is blocked, thereby affecting the detection effect. An improvement of 98.98% can be achieved in the average performance of the intrusion detection system without increasing the number of false alarms.

- Analyze PDPs to determine the location of the intruder. The main delay components can be identified primarily based on how much the intruder affects the different paths. Intruder tracking maps may be generated by converting the delayed parts into distances. In an ideal environment, the tracking offset using a 320MHz bandwidth can be as small as 0.4481m.

doi:10.6342/NTU202303843

CHAPTER 2

BACKGROUND AND RELATED WORK

2.1 Backgrounds

The presence of unauthorized or malicious individuals in the target indoor space is detected by analyzing channel state information (CSI) in the indoor environment. It is designed to identify intruders or unauthorized individuals who may pose a security threat or compromise user privacy.

In indoor wireless communication systems such as Wi-Fi networks, CSI provides valuable information about wireless channel characteristics and properties, including signal strength, multipath fading, and other channel impairments. CSI measurements are typically obtained from access points or devices deployed in indoor environments.

CSI intruder detection systems in indoor settings utilize CSI measurements to detect anomalies or deviations that may indicate the presence of intruders. Some specific aspects of indoor CSI intruder detection include:

1. Presence Detection: CSI data can be used to detect the presence of individuals within the indoor environment. By analyzing CSI measurements from multiple access points (AP) or devices, changes in signal strengths or multipath profiles caused by an individual can be detected. Unusual or unexpected variations in the CSI patterns can raise alarms for potential intruders.

2. Intruder Tracking: CSI data and localization techniques can track intruder movement within the indoor environment. By analyzing the CSI measurements from different access points or devices, it is possible to estimate the location and trajectory of an intruder. This information can be valuable for security personnel to respond effectively.

3. Integration with Security Systems: CSI intruder detection can be integrated with existing security systems in indoor environments. For example, detecting an intruder through CSI analysis can trigger alarms, send notifications to security personnel, or activate surveillance cameras for visual confirmation.

Various techniques can be employed to perform CSI intruder detection in indoor environments. These include signal processing algorithms, statistical analysis, machine learning, and pattern recognition techniques.

doi:10.6342/NTU202303843

Overall, CSI intruder detection in indoor environments is critical in enhancing wireless communication networks' security and safety. It enables the detection of unauthorized individuals, suspicious activities, and potential security threats within the indoor environment with the help of CSI measurements.

2.2 Multipath Signals

To further understand how CSI information is used, we must first understand what messages CSI contains. First of all, signals spread in all directions when propagating. Line of sight (LoS) and non-line of sight (NLoS) can be distinguished among the many paths from the transmitter to the receiver. LoS means no obstruction between the transmitter and the receiver, which is the shortest path in the signal. NLoS refers to those paths that are reflected or scattered due to obstacles.

The signal is transmitted by OFDM, and multiple symbols are transmitted on different subcarriers simultaneously. The modulated signal has different degrees of delay at the receiver due to the difference in the propagation path, which can be represented by the channel impulse response (CIR). After the signal is demodulated, the information on each subcarrier is restored. The state of the subcarrier at this time is channel state information (CSI). Next, OFDM, CIR, and CSI will be explained below.

2.2.1 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a digital modulation technique widely used in modern wireless communication systems, including Wi-Fi, 4G LTE, and 5G networks. OFDM enables efficient and reliable data transmission over wireless channels by dividing the available frequency spectrum into multiple orthogonal subcarriers [2, 3].

Compared with the previous single-carrier communication system, the advantages of OFDM are manifested in multipath channels. In traditional single-carrier modulation schemes, the entire bandwidth is occupied by a single-carrier signal. However, in OFDM, the available bandwidth is divided into multiple smaller subcarriers, each with a narrower bandwidth. These subcarriers are closely spaced and orthogonal to each other, meaning they do not interfere with one another.

doi:10.6342/NTU202303843

The subcarriers of OFDM satisfy the following orthogonality:

$$\begin{cases} \int_0^{T_s} \cos(2\pi m\Delta f t)\cdot\cos(2\pi n\Delta f t)\,dt = \begin{cases} T_s/2 & , m=n \\ 0 & , m\neq n \end{cases} \\ \int_0^{T_s} \sin(2\pi m\Delta f t)\cdot\sin(2\pi n\Delta f t)\,dt = \begin{cases} T_s/2 & , m=n \\ 0 & , m\neq n \end{cases} \\ \int_0^{T_s} \cos(2\pi m\Delta f t)\cdot\sin(2\pi n\Delta f t)\,dt = 0, \end{cases} \tag{2.1}$$

where $m, n \in \mathbb{Z}$, and T_s is symbol duration. T_s gets $T_s = \frac{1}{\Delta f}$ according to the frequency resolution Δf. It can be known from (2.1) that there will be a value only when m=n. Therefore, although OFDM has overlapping frequency parts, they are not interdependent, as shown in Figure 1.

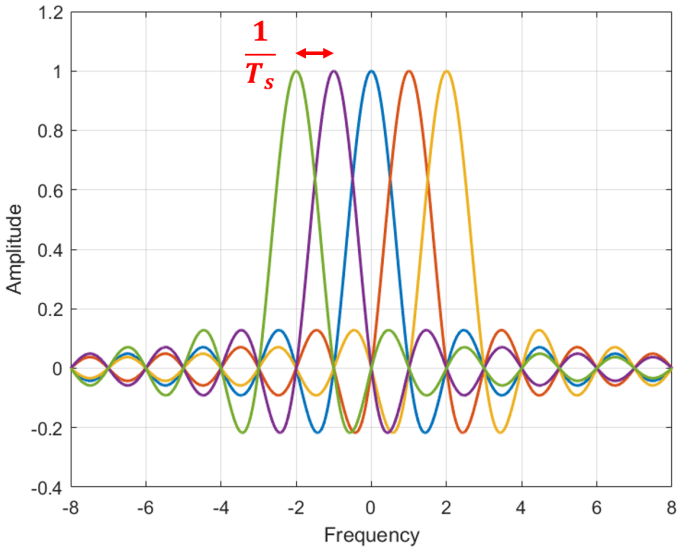


Figure 1: Orthogonality of signal propagation using OFDM.

2.2.2 Channel Impulse Response (CIR)

CIR refers to the response of a communication channel to an impulse input signal. It is a fundamental concept in wireless communication systems and describes the characteristics of the channel in terms of its time-varying amplitude, phase, and delay.

In practical terms, the channel impulse response represents the effect of the wireless channel on a transmitted signal. When an impulse, a short-duration signal, is transmitted through the track, it undergoes various changes due to factors like multipath propagation, fading, interference, and other channel impairments. The CIR captures these changes and provides insight into the behavior of the channel.

doi:10.6342/NTU202303843

The CIR is typically represented as a time-domain sequence, where each sample corresponds to the channel's response at a particular time instant. It characterizes the channel's response over a particular duration, considering the different propagation paths and delays associated with each path.

The CIR at time point t can be expressed as [4, 5]

$$h(t) = \sum_{k=0}^{K} \alpha_k \delta(t - \tau_k) e^{-j\theta_k} + n(t), \tag{2.2}$$

where K represents the total number of paths for signal propagation, and α_k, τ_k, and θ_k represent the amplitude attenuation, delay, and phase offset of the k^{th} path, respectively. Noise is represented by $n(t)$. In more detail, α_k can be expressed as follows [6, 7]:

$$\alpha_k = \frac{W A_k \prod_{i=1}^{r_k} \varepsilon_i}{(d_k)^{\frac{n}{2}}},\ W = \frac{\lambda \sqrt{G_t G_r} Q_{tem} Q_{hum}}{(4\pi)^{\frac{n}{2}}}, \tag{2.3}$$

where λ is the wavelength of the radio signal, G_t and G_r are the gain of the transmitter and receiver antenna, Q_{tem} and Q_{hum} are respective the temperature and humidity quality factor. n, A_k, and r_k represent the loss factor, the shadowing effect, and the number of reflections on the k^{th} path; ε_i is the reflection coefficient of each reflector, which varies according to the material of the i^{th} reflector, between 0 and 1, depending on the material. Multiple reflections lengthen the route; it leads to the product of numerous ε_i values shrinking. Thus, according to (2.3), numerous reflections of the path will significantly reduce α_k.

2.2.3 Channel State Information (CSI)

In the ideal case, CIR may be further transformed by the Fourier transform into channel frequency response (CFR), and the corresponding CFR can be written as [4, 5]:

$$H(f) = \sum_{k=0}^{K} \alpha_k \exp^{-j2\pi f \tau_k + \theta_k} + N(f), \tag{2.4}$$

where $N(f)$ is the noise frequency response and f is the frequency of the radio signal.

However, the ideal Fourier transform cannot be realized in reality, and the fast Fourier transform (FFT) is used instead. It is a method for quickly computing the discrete Fourier transform (DFT) of a sequence [8]. A signal is represented in the frequency domain via Fourier analysis after being transformed from the temporal domain. In other words, CSI is sampling CFR in the frequency domain.

CSI represents the information about the characteristics of the communication channel between a transmitter and a receiver. In the frequency domain, the

doi:10.6342/NTU202303843

wireless channel state can be described as [4, 5]:

$$\mathbf{Y} = \mathbf{HX} + n, \tag{2.5}$$

where n is the additive noise vector and $\mathbf{H}$ is the channel matrix. When a known sequence of $textbf{X}$ is transmitted, the receiver can estimate $textbf{H}$ in the formula above. Each component of $\mathbf{H}$ indicates the signal's attenuation factor along a specific transmission channel. Different variables, such as signal scattering, environmental attenuation, and distance attenuation, might influence the attenuation factors. CSI enables the communication system to adjust to the current channel circumstances by providing information on the channel matrix $\mathbf{H}$. The following is an expression for the estimated $\mathbf{H}$ for N subcarriers:

$$\mathbf{H} = [H_1, H_2, ..., H_n, ..., H_N]^T, \tag{2.6}$$

the CSI of i^{th} is:

$$H_n = |H_n| \, e^{j \sin(\angle H_n)}. \tag{2.7}$$

The amplitude and phase details of the i^{th} subcarrier are represented on the right side of the equation by $|H_i|$ and $\angle H_i$, respectively. Each CSI entry represents sampled CFR can be express by

$$H_n(f) = \sum_{k=0}^{K} \alpha_{n,k} \exp^{-j2\pi f \tau_{n,k} + \theta_{n,k}} + N(f), \tag{2.8}$$

from (2.4). In Wi-Fi, the subcarrier spacing is 312.5 kHz (IEEE 802.11ab/g/n/ac) or 78.125 kHz (IEEE 802.11ax/be), which means that the CFR is sampled at discrete frequency points $f = f_0 + n\Delta f$, where n is the index of the subcarrier and Δf is the subcarrier spacing.

The temporal sequence of CSI matrices characterizes the Multi-Input Multi-Output (MIMO) channel variations across different domains, i.e., time, frequency and spatial. It will be described in more detail in Section 3.2.

2.3 Overview of Intrution Detection

This section reviews some previous work on intrusion detection. Passive intrusion detection, RSS-based, and CSI-based detection methods are the three points of view used. The latter two of them are WiFi-based strategies.

2.3.1 Passive Intrusion Detection

The earliest and most extensively studied techniques rely on pictures taken by cameras and are based on vision technology. For instance, [9] employs image-based algorithms to follow moving subjects while analyzing a series of shots taken

doi:10.6342/NTU202303843

by a camera. However, the most critical issue with these image-based methods is privacy, coupled with the sizeable computational cost required for real-time processing. [10] relies on whether humans block infrared rays to report intrusions, but like the image-based method, it is only applicable to line-of-sight scenarios. When there are obstacles between humans and the detection device, detection is impossible. In addition, information from audio [11] and pressure [12] sensors can also be used for intrusion detection. This is mainly based on noise and floor vibration changes caused by intrusion activities. It should be emphasized, nevertheless, that these signals are easily influenced by other outside sound sources or environmental pressure to cause false alarms.

2.3.2 RSS-based Methods

When an object enters the wireless network area, the link passing through the object will experience shielding loss. Wilson and Patwari calculated the position of people discovered inside a region encompassed by nodes by observing changes in the network's attenuation field [13]. In this study, the system is first calibrated in a static environment, or in which no objects are present in the monitored region.

[14] utilizes radio sensors deployed around (and possibly on top of) built-up areas and has nodes transmitting to each other to make signal-strength measurements of links passing through buildings or areas of interest. The phasor sum of all multipath components at the receiver varies when a moving object alters the amplitude or phase of one or more multipath components over time. There is a higher RSS variance.

Cosba et al. A system named RASID is proposed [15], which also selects RSS sample variance as features, and after that uses non-parametric statistical anomaly and contour updating methods to record environmental changes. RASID is reliable, however, the sampling rate of 1 sample/s is too slow, taking a long time to collect data.

Although the RSS-based system described above can produce particular outcomes, more WiFi sensor nodes must be deployed to minimize multipath effects and increase accuracy.

2.3.3 CSI-based Methods

The CSI can be analyzed from the packets transmitted and received between the two devices. Owing to multi-path transmission, CSI is affected by reflections in the surrounding environment, resulting in changes and disturbances. When intruders show up, the indoor environment changes, affecting CSI transmission paths. It can be reflected in the amplitude and phase, and then analyze these

doi:10.6342/NTU202303843

data to detect intruders.

Having investigated various related studies, we came to the following conclusions. Currently, most intrusion detection studies using CSI must extract signals and perform feature selection first. Some works also perform preprocessing before selecting features to reduce noise impact, enhance signal features, or reduce the amount of data. Finally, a threshold or pre-trained model is used for decision-making.

2.3.3.1 Signal Analysis

[16–18] uses CSI amplitude as the main analysis signal, and [19,20] uses phase difference.

Most studies use amplitude because of its stability. The raw CSI phase displays far more unpredictability than the raw CSI amplitude because of ambient noise and out-of-synch clocks between the transmitter and receiver. The amplitude is mainly affected by the beamforming matrix [21]. Phase is affected by Sampling Frequency Offset (SFO) and Carrier Frequency Offset(CFO) [20]:

$$H_i = \underbrace{\left(\sum_{n}^{N} a_n e^{-j2\pi d_i f/c}\right)}_{\text{Multipath Channel}} \underbrace{e^{-j2\pi\delta_i f}}_{\text{SFO}} \underbrace{e^{-j\beta}}_{\text{CFO}} \underbrace{q_i e^{-j2\pi\zeta_i}}_{\text{Beamforming}}, \tag{2.9}$$

where d_i is the path length from the transmit antenna to receive antenna of the i^{th} path, f stands for the carrier frequency, c for the speed of light, δ_i for SFO, β for CFO, and q_i and ζ_i for the beamforming matrix's amplitude attenuation and phase shift, respectively. Calculating the phase difference between the two antennas can eliminate most SFO and CFO, and the processed phase difference is even more stable than amplitude. It will be introduced in Chapter 3.

2.3.3.2 Feature Extraction

In intrusion detection, feature extraction is crucial. The correct features can streamline data processing while effectively reflecting intrusions' presence.

Wang et al. [16] proposed a Wi-Alarm system, which aims to select simple but robust information as features and does not require preprocessing to speed up system processing. However, although its design can significantly save calculation costs, most of the unprocessed original CSI has non-negligible high-frequency signals, and the extracted features, the CSI amplitude mean and variance, are not accurate enough and are prone to instability due to environmental changes. Under such a design, the CSI data cannot be fully utilized, affecting detection accuracy.

[17] choose to utilize the power spectral density (PSD) of CSI as the detection feature instead of the amplitude and phase information, and it calculates the PSD's

doi:10.6342/NTU202303843

kurtosis as the feature's criteria. More than 99% accuracy in detection is possible. However, this method mainly aims at situations with only a single intruder in the environment. Crowd gathering will result in a signal superposition effect when there are several invaders, making accurate intrusion detection challenging. In addition, its test environment is relatively ideal. High identification accuracy and system reaction speed are difficult to maintain in a complex environment.

By computing the eigenvalues of the phase difference covariance matrix between nearby antenna pairs as fingerprints, the passive intrusion detection system achieves CSI-based passive intrusion detection [20]. Similarly, [18] further extrapolates characteristics from the subcarrier correlation coefficient distribution. The eigenvalue of covariance shows the relationship between subcarriers, while the correlation coefficient illustrates how the Doppler shift of adjacent subcarriers is similar. Although the covariance and correlation coefficient reflect the correlation between two random variables, both values are affected by the subcarrier dimension. Therefore, the matrix cannot be considered a feature directly. [18, 20] use the maximum value and the sum of matrices under certain conditions as the final features. However, when the speed of the intruder changes continuously or stands at a fixed point, the distinction between features becomes blurred, which reduces detection efficiency.

2.3.3.3 Decision Method

Decision-making processes for system infiltration may be loosely classified into two groups: Threshold-based methods set a threshold, and decide whether to intrude according to whether the value exceeds the threshold. Another technique is model-based. The detection model needs to be pre-trained, and the model will judge the intrusion result.

Compared with defining the threshold with a fixed value, most current threshold-based methods are dynamic algorithms. For example, [17] uses the exponential moving average algorithm to define the threshold dynamically. The formula is as follows:

$$TH_t = (1 - \xi)TH_{t-1} + \xi f_t. \tag{2.10}$$

ξ is the coefficient between 0 and 1, f_t is the feature in time t. On the other hand, [19] normalizes the features. The seemingly fixed threshold changes with the collected data. Although this dynamic method seems to be able to adjust as the environment changes, it still has shortcomings. First, when the detection environment changes, it is inevitable to spend a certain amount of time collecting operating environmental data to set the initial threshold. Second, when the coefficient is not appropriately set, the threshold value shifts with time, significantly

doi:10.6342/NTU202303843

reducing detection performance. And this brings us back to the first point. The threshold needs to be redefined.

Training data of the target model are required for the model-based approach. The trained model must be resilient enough to alter with various circumstances. The two significant factors affecting the robustness of the model are whether the extracted features are sufficiently independent of the scene. The other is the method of model selection and adjustment. A shallow machine-learning approach is preferable since intrusion detection requires binary classification. It needs less data and less sophisticated computer power than a deep-learning model. Applications for detection and recognition frequently employ shallow learning techniques like K-Nearest Neighbors (KNN) [22], Random Forest (RF) [23], and Support Vector Machine (SVM) [24].

Although the computational complexity of shallow learning is not high, it still requires a higher upfront cost than threshold-based methods. This is in exchange for the stability of the intrusion detection system. The above methods have their advantages and disadvantages.

2.3.3.4 Comparison

We have summarized the related works mentioned above and organized them in Table 1. Further comparisons for each step and method are shown in Table 2.

Table 1: Comparison of related works.

Name	**CSI Signal**	**Features**	**Decision**
Wi-Alarm [16]	Amplitude	Mean, Variance	Model
RT passive intrusion detection [17]	Amplitude	PSD, kurtosis	Threshold
Adaptive RT indoor intrusion detection [18]	Amplitude	Correlation coefficient	Model
Ar-Alarm [19]	Phase difference	Standard deviation	Threshold
Robust passive intrusion detection [20]	Phase difference	Covariance	Model

Generally speaking, current intruder detection systems still have room for improvement, and most of these systems focus primarily on the dynamic movement of the intruder. As the actual intrusion behavior may be slow and fixed, we also perform related experiments when the intruder is active at a fixed position.

It is important to note that there may be various obstacles in the target space, including pillars, cabinets, etc. When there is obstruction at the location of the

doi:10.6342/NTU202303843

intrusion, it affects signal transmission. We know from (2.3) that the signal will be attenuated a lot after multiple reflections. Because the position is blocked, the path components passing through the position are reduced, and the signal is weakened simultaneously. A general CSI signal is obtained by averaging and summing multiple paths (2.2). We consider increasing the extent to which the intruder affects the CSI by changing the path weight. The approach will be described in Chapter 5.

Table 2: Comparison of Steps for an Intrusion Detection System.

Steps	Items	Advantages	Disadvantages
Signal Analysis	Amplitude	Simple	Unstable
	Phase difference	Stable	Complex
Feature Extraction	Mean, PSD	Simple	scenario-dependent
	CorrCoef, Covariance	scenario-independent	Complex
Decision Method	Threshold	Simple	Shift over time
	Model	robust	High upfront cost

2.4 Overview of Intruder Tracking

Since it is possible to confirm whether an intruder exists in the space through the intrusion detection system, it is expected to further confirm the location of the intruder. The work related to human body tracking or positioning can be divided into methods based on signal feature extraction or machine learning.

2.4.1 Signal Feature Extraction

One of the standard tracking methods is to estimate the speed and direction of the human body, such as [25–28]. However, the disadvantage of this method is that it is easily affected by multipath effects, which leads to estimation deviation and affects the tracking effect. Another method is to estimate the Angle of Arrival (AOA) and Time-of-Flight (TOF): [29] uses the MUSIC algorithm to estimate, which is very sensitive to radio frequency channels and mutual coupling characteristics. [30] uses Kalman The filter builds a model for estimation but requires a lot of calculations and high-frequency accuracy. The Power Delay Profile (PDP) is used to track the position of the human body [31], but it is only used for activity recognition at a fixed position and is easily affected by the LOS component.

The technique used in [25] to determine the radial direction of human motion is the foundation of [8]. The cross-covariance between time-lag subcarrier segments

doi:10.6342/NTU202303843

is computed using this. And refer to [26] to build a model linking CSI dynamics to the path length change rate (PLCR) for speed estimation. WiTrack [29] tracks motion by processing signals from its receiver antennas through TOF Estimation and 3D Localization. Find the TOF of the signal by Frequency-Modulated Carrier Waves (FMCW) [32], and use the ellipse model to track the intruder's location. However, besides restricting the intruder's movement, the above method requires TOF and AOA information. It is much cost to compute these features and often requires additional calibrations. [31] used the PDP to trace the user; the intruder's position was decided by converting the PDP between multi-antenna links into distances and superimposing them. However, the purpose of [31] is mainly to track users needing motion recognition, most of which stand in a fixed position. Therefore, in the design of its algorithm, when the user is moving, the LOS component can easily overwhelm other delay components, resulting in tracking failure.

2.4.2 Machine Learning

Both [33] and [34] divide the target space and let individuals stand in different positions to collect training data. [33] uses the deformed 1-dimensional Convolutional Neural Network (C1D) model; [34] uses KNN. Although the above methods also have a certain positioning effect when the individual is at a fixed point, their disadvantages are that the pre-processing of the training is complicated. When the environment changes, the model needs to be retrained again.

Our goal is to effectively track the intruder regardless of how he behaves, whether static or dynamic. As much as possible, we would like to reduce the costs associated with tracking and the threshold for the use of equipment. For this purpose, we simulate an ideal laboratory environment. An algorithm based on the PDP method is designed to track intruders without requiring any training.

doi:10.6342/NTU202303843

CHAPTER 3

INTRUSION DETECTION SYSTEM

In this chapter, we will introduce the detailed process of our preliminary construction of the intrusion detection system, including the overall structure of the entire system and the details and considerations of each step.

3.1 System Overview

We created the system's process based on empirical analysis, as Figure 2. There are several steps in the system process. These comprise collecting CSI data, signal analysis, data preprocessing, feature extraction, real-time test data, empty training data, and ultimately the detection outcomes attained by the trained model.

Figure 2: System flow of intrusion detection system.

According to the commercial WiFi device used, Lanner LWR-X8460, we initially developed a 1×4 MIMO-based CSI collection system. The IEEE 802.11n protocol has a 2.4GHz frequency spectrum and a 20MHz bandwidth. The setting above is the lowest bandwidth standard commercial Wi-Fi equipment can achieve. Next, we perform signal analysis based on previously collected CSI data, from which the amplitude or phase is derived. The raw amplitude contains many high-frequency components, and the phase contains errors such as sampling frequency offset (SFO) and carrier frequency offset (CFO). Although the phase difference can eliminate most offsets, sometimes there will still be a shift of $/pi$, caused by the limited design of hardware equipment. This requires some preprocessing to restore the original phase difference. We extract target features from the restored CSI, which should be sensitive to human presence and provide a suitable scene-independent index. Based on the extracted features, a SVM model is generated, and individual classifiers are constructed for different receiving antennas. Voting is performed between each classifier to enhance our system's robustness to intruder movement. In what follows, we will describe each step in detail and introduce its related technologies.

doi:10.6342/NTU202303843

3.2 Data Collection

The time series of the CSI matrix illustrates how the MIMO channel varies in terms of time, frequency, and space. The CSI of each packet can be expressed as a three-dimensional matrix $\mathbf{H} \in \mathbb{C}^{M \times N \times K}$, which represents amplitude attenuation and phase shift, as shown in Figure 3 for a MIMO-OFDM channel with M transmitting antennas, N receiving antennas, and K subcarriers. The CSI time series is a four-dimensional sequence with continuous transmission on the time axis.

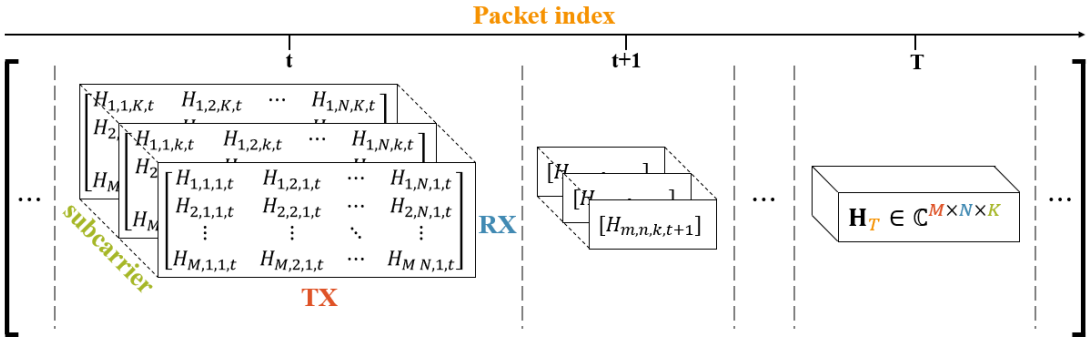


Figure 3: The four-dimensional CSI tensor constructed from the time series of the CSI matrices of the MIMO-OFDM channel.

We built a CSI collection system on Lanner LWR-x8460 based on 1×4 MIMO using the IEEE 802.11n protocol, and the bandwidth is 20MHz. IEEE 802.11n works in the 2.4GHz frequency band. When transmitting on a 20MHz channel, the channel is divided into 64 subcarriers (equal to FFT size). [35] The 4 pilot signals are located at -21, -7, 7, and 21 subcarriers respectively. In Legacy Mode, the signal is transmitted on subcarriers -26 to -1 and 1 to 26 [36], with 0 being the center, Direct Current (DC), carrier. Pilot subcarriers are used for estimation and synchronization, and null subcarriers do not carry anything, including guard bands and DC components. After deducting the empty subcarriers from the original CSI, we use the remaining subcarriers $(64 - 12 = 52)$ for subsequent processing. We use 500Hz to transmit packets. This means a CSI matrix of size $500 \times 1 \times 4 \times 52$ can be collected within one second.

3.3 Signal Analysis and Preprocessing

3.3.1 Amplitude

Next, we observe the raw CSI amplitude in Figure 4, which contains many outliers in high-frequency components. The Hampel filter can eliminate these undesirable elements and guarantee the continuity of quality of service (QoS) in various contexts. It detects and removes outliers from the input signal using Hampel identifiers, proposed by Hampel [37, 38]. He created a breakdown point

doi:10.6342/NTU202303843

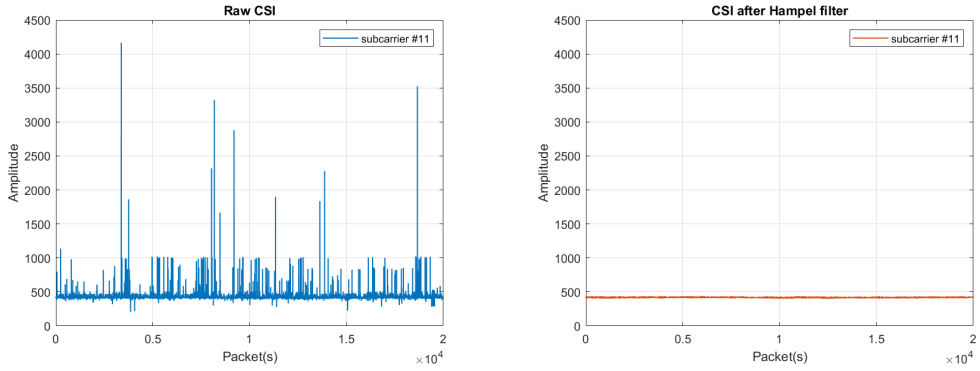
to gauge an estimator's robustness to outliers. He used the median to estimate the data location and used it as a criterion for outlier identification. The standard deviation of the data is calculated using the median absolute deviation (MAD). The approach was further improved by Davies and Gather using a moving window for recognition [39].

Assume there is a sequence $[x_1, x_2, \cdots, x_i, \cdots, x_n]$ of size n and a sliding window of length k, define local median m_i and standard-deviation σ_i as [40]:

$$m_i = median\left(x_{i-k}, x_{i-k+1}, \cdots, x_i, \cdots, x_{i+k-1}, x_{i+k}\right), \tag{3.1}$$

$$\sigma_i = \kappa \cdot median\left(\left|x_{i-k} - m_i\right|, \cdots, \left|x_{i+k} - m_i\right|\right), \tag{3.2}$$

where $\kappa = \frac{1}{\sqrt{2}erfc^{-1}(1/2)} \approx 1.4826$. The quantity σ_i/κ is known as the MAD. For a given threshold n_σ, usually set to 3, a sample x_i is such that $|x_i - m_i| > n_\sigma \sigma_i$ will be declared an outlier and replaces it with m_i. We can see from Figure 4 that the filtered CSI is much cleaner.



(a) (b)

Figure 4: CSI is measured when no individuals are present in the target environment.

3.3.2 Phase Difference

IEEE 802.11n utilizes MIMO technology to achieve higher capacity, range, and reliability through spatial diversity. Commercial off-the-shelf wireless equipment with multiple antennas is standard. According to [41], we combine the phases of several antennas to calculate channel statistics more quickly and are more resistant to environmental changes than amplitudes. We first confirm that the two antenna pair's measured phase difference for successively received data packets is remarkably stable. The CSI measurement provides phase information for each subcarrier, and the following could be used to describe the CSI phase $\hat{\phi}_i$ determined in the i^{th} subcarrier [42]:

doi:10.6342/NTU202303843

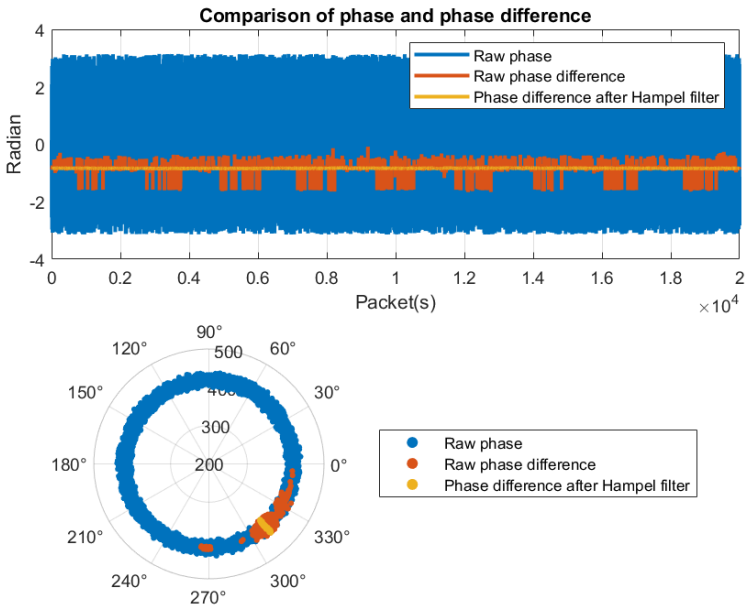


Figure 5: Comparison of raw phase, raw phase difference and phase difference after hampel filter.

$$\hat{\phi}_i = \phi_i - 2\pi \frac{k_i}{N} \delta_i + \beta + Z_i, \tag{3.3}$$

where, respectively, $\hat{\phi}_i$ and ϕ_i represent the measured CSI phase and the actual phase value of the i^{th} subcarrier. The time delay at the receiver induced by SFO is denoted by δ_i, while the phase shift generated by CFO is denoted by β. Measurement noise is Z_i. The index of the i^{th} subcarrier is indicated by k_i, which in IEEE 802.11n ranges from -26 to 26; N is the FFT size, which in IEEE 802.11 a/g/n equals 64. Due to the existence of δ_i, β, and Z_i, actual phase information cannot be obtained directly. We know antennas connected to the same network card share the same downconverter frequency and sample clock [43]. Consequently, the i^{th} subcarrier's observed phase difference is as follows:

$$\Delta\hat{\phi}_i = \Delta\phi_i - 2\pi \frac{k_i}{N} \Delta\delta_i + \Delta\beta + \Delta Z_i, \tag{3.4}$$

where $\Delta\phi_i = \phi_{i,m} - \phi_{i,n}$ and $\Delta\hat{\phi}_i = \hat{\phi_{i,m}} - \hat{\phi_{i,n}}$ are the real phase difference and the measured CSI phase difference values of the i^{th} subcarrier, respectively. m and n represent two different antennas. The time delay difference between the two receiving antennas is $\Delta\delta_i = \delta_{i,m} - \delta_{i,n}$. ΔZ_i is a measurement noise difference, while $\Delta\beta$ is the unknown phase offset difference. Assign the following symbols to their respective values: λ for wavelength, d for antenna spacing, θ for arrival direction, c for light speed, and T_s for receiver sampling interval. We know that reception antennas are positioned half a wavelength apart. Then $\Delta\delta_i$ can be

doi:10.6342/NTU202303843

expressed as:

$$\Delta\delta_i = \frac{\lambda \sin\theta}{2cT_s} \leq \frac{1}{2fT_s}, \tag{3.5}$$

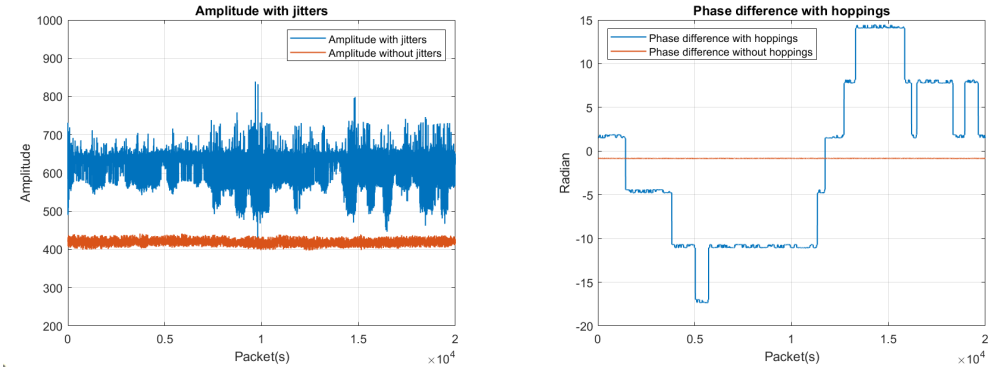
where f is the center frequency, which varies depending on the WiFi network's operational channel, while θ is the angle of arrival and T_s has a bandwidth of 20 MHz, it takes 50 ns. The phase difference resulting from differing timing offsets approaches zero when we select the 2.4 GHz WiFi frequency choice, $-32 \leq k_i \leq 31$, or more precisely, $2\pi\frac{k_i}{N}\Delta\delta_i \in [-0.0131, 0.0127]$, making it insignificant in $\Delta\hat{\phi}_i$. After being omitted, $\Delta\hat{\phi}_i$ is indicated as:

$$\Delta\hat{\phi}_i = \Delta\phi_i + \Delta\beta + \Delta Z_i. \tag{3.6}$$

As for $\Delta\beta$, although we cannot determine the initial phase of each packet and it changes over time, by moving the mean of the phase difference to zero, the $\Delta\beta$ obtained at different times becomes the same. Figure 5 portrays that raw CSI phase data are randomly distributed due to variable δ_i. The phase difference is mainly concentrated around a certain angle. A few outliers located elsewhere can be eliminated using filters.

3.3.3 Preprocessing

Although in Figure 5 we can see that the phase difference is compared to the phase and all its values are concentrated in one place. But there are exceptions: as shown in Figure 6(b), hoppings are in the calculated phase difference, and each hopping is approximately equal to multiple of $\pm\pi$.



(a) (b)

Figure 6: When there is no intrusion in the room, the collected data sometimes have anomalous jitter or hoppings.

These hoppings are caused by the poor design of hardware devices. There is no fixed time for them, and they will appear randomly. It also affects the stability of the amplitude. We can see in Figure 6(a) that when there are no intruders

doi:10.6342/NTU202303843

in the environment, The amplitude should be stable as indicated by the red line. However, the abnormal amplitude we collected is the blue line with apparent jitter as if intruders were in the space. These jitters have no regularity and cannot be eliminated by specific algorithms. Fortunately, as mentioned above, from the perspective of phase difference, each hopping is about a specific value, so we design an Algorithm 1 to eliminate them.

In our devised algorithm, we iteratively unwrap and wrap the phase difference back to 2pi, adding an appropriate Hampel filter between the two motions. As shown in Figure 7(c), the first Hampel filter is not intended to eliminate hopping directly. Instead, it is designed to eliminate outliers that suddenly appear in specific continuous data. When we remove such outliers and wrap the phase difference back in the range of 0 to 2π, comparing Figure 7(d) with Figure 7(a), we can see that the phase difference is much cleaner. We use the second Hampel filter to remove outliers again, which is the hopping we need to eradicate. After re-unwrapping, we can get phase difference data without hopping.

Algorithm 1 Phase difference preprocessing to remove aberrant hoppings.

Input:
CSI phase tensor, $\hat{\phi}$;
Sampled frequency, W;
Output:
CSI phase difference tensor, $\Delta\hat{\phi}$;
set the number of receiver antennas = N;
set the number of subcarriers = K;
for $\forall i, j \in [1, N], i < j$ **do**
  $\Delta\hat{\phi_{i,j}} = unwrap(\hat{\phi}_i - \hat{\phi}_j)$;
  set $w = W/10$;
  for each $k \in [1, K]$ **do**
    set window size = w, threshold $n_\sigma = 0.01$;
    $\Delta\hat{\phi_{i,j,k}} = hampel(\Delta\hat{\phi_{i,j,k}}, w, n_\sigma)$;
  end for
  $\Delta\hat{\phi_{i,j}} = wrapTo2Pi(\Delta\hat{\phi_{i,j}})$;
  set $w = W/5$;
  for each $k \in [1, K]$ **do**
    set window size = w;
    $\Delta\hat{\phi_{i,j,k}} = hampel(\Delta\hat{\phi_{i,j,k}}, w, n_\sigma)$;
  end for
  $\Delta\hat{\phi_{i,j}} = unwrap(\hat{\phi}_i - \hat{\phi}_j)$;
  removed remaining aberrant hoppings with threshold $th = \pi/2$;
end for

doi:10.6342/NTU202303843

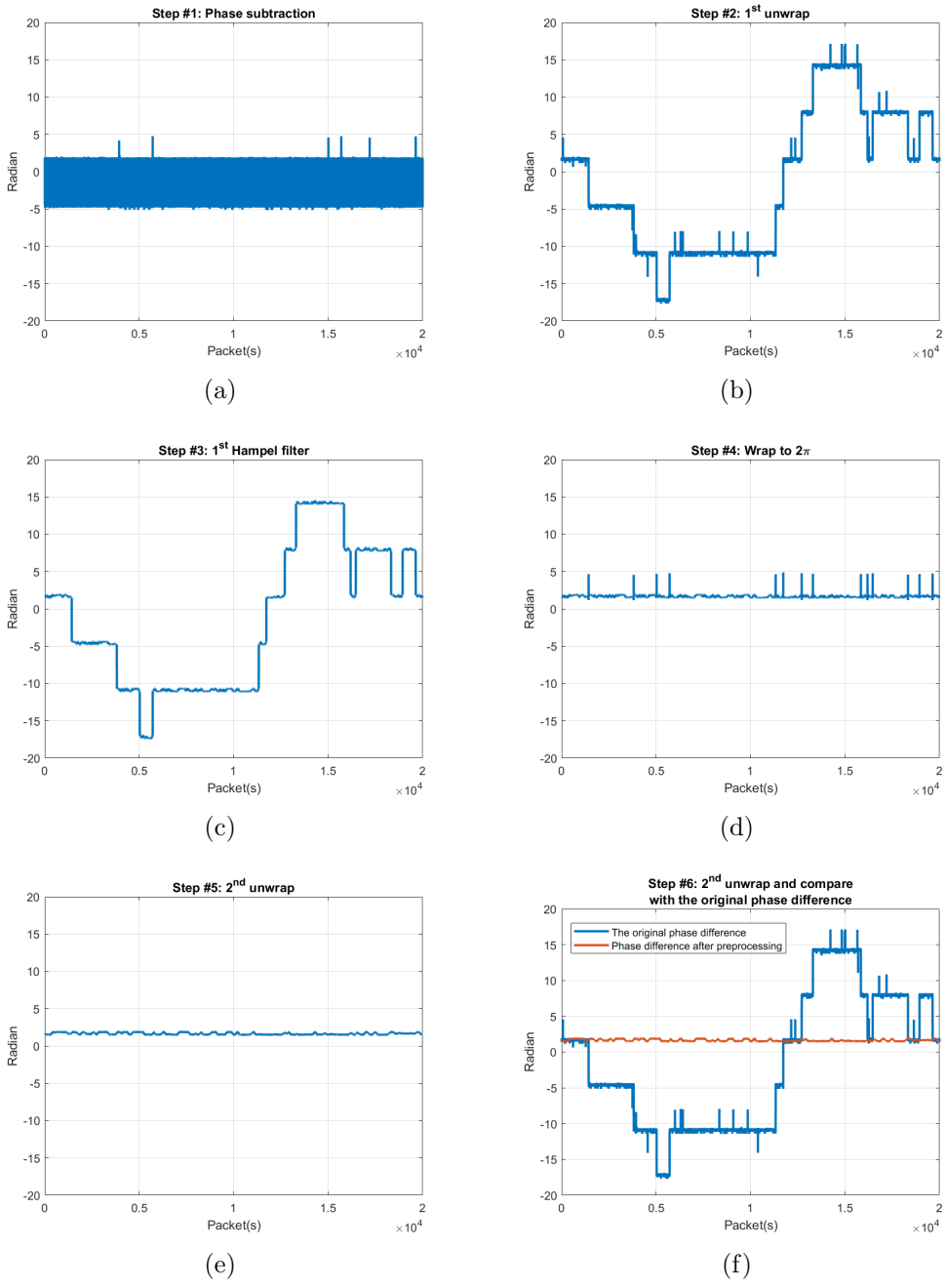


Figure 7: Preprocessing steps for phase difference.

doi:10.6342/NTU202303843

3.4 Feature Extraction

After obtaining the basic CSI signal information, we need to extract the features that best reflect the overall signal. The purpose is not only to eliminate the chaff but also to reduce the computational cost of detecting intruders.

3.4.1 Data Propagation

We first assume that a CSI matrix H_t is obtained at time T_i, and it is known that H_t can retrieve from the FT of CIR in a short amount of time around T_i, as described in (2.2). The wireless channel is affected when an intrusive person gets close to a transmitter or receiver because part of the broadcast signal's propagation routes are altered. Each component of H_t in this instance changes as the invasion progresses. However, the CSI of various subcarriers in H_t must differ due to frequency selective fading effects. The CSI fluctuates more dramatically at some subcarriers than others. We denote the subcarrier with the most intense variation as f_c and take it as a representative. Therefore, according to (2.4) we have

$$H_{T_i}(f_c) = \sum_{k=0}^{K} \alpha_{k,T_i} e^{-j(2\pi f_c \tau_{k,T_i} + \theta_{k,T_i})} + N_{T_i}(f_c), \tag{3.7}$$

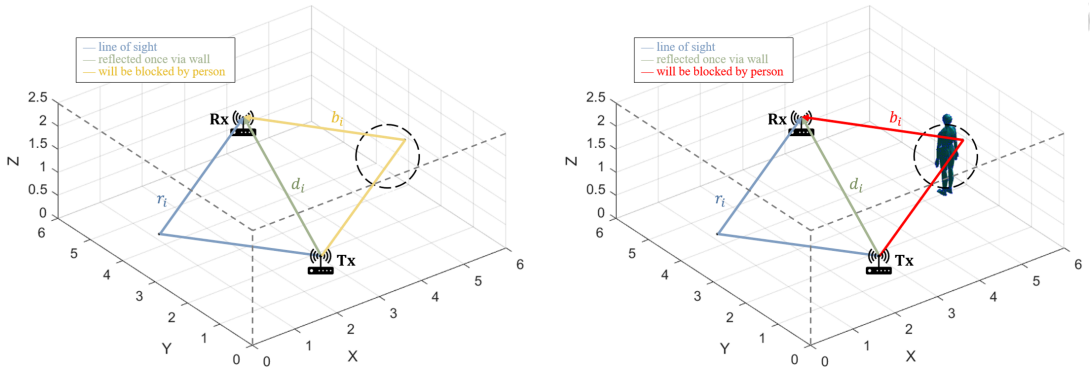
where the amplitude attenuation, propagation delay, and phase offset along the k^{th} path are designated as α_{k,T_i}, τ_{k,T_i}, and θ_{k,T_i}, respectively, during the brief interval between $T_i - t_s$ and T_i. They are nearly constant for such a brief time. The following is how the CIR is stated during this small duration, according to (2.2):

$$h_{T_i}(t) = \sum_{k=0}^{K} \alpha_{k,T_i} \delta(t - \tau_{k,T_i}) e^{-j\theta_{k,T_i}} + n_{T_i}(t). \tag{3.8}$$

Since intruders obstruct some of the sent signals' propagation pathways, their presence should impact CSI. In this case, we assume that the intrusion has not yet passed between the transmitter and receiver even though it is getting closer. As shown in Figure 8(a), assuming that the floor and the wall are composed of the same material, the only thing in the space that influences the propagation path when there is no incursion is the wall. First observe that the propagation path marked $b_1, b_2, \cdots, b_i, \cdots b_{K_b}$ will first directly reach the wall at $x = 6$, experience reflection at the wall, and then reach Rx. However, when an intruder appears in front of this reflection, as shown in Figure 8(b), the path is blocked by the intruder. The human body is around 70% water, and water substantially attenuates electromagnetic signals, making it difficult for invaders to get through these pathways [44]. At the same time, some blocked paths will change the direction of their reflection and refraction. We denote the total number of all blocked paths

doi:10.6342/NTU202303843

as K_b with reflector changes to intruders. The path without any reflection is K_d, and the path that is still the wall without the influence of the intruder is K_r. To simplify our simulations, all reflection paths pass through only one reflection.



(a) (b)

Figure 8: When an intruder is present or absent in the space.

Below we simulate human invasion and divide the propagation paths into three parts. The CIR without intruders at time T_i is:

$$\begin{aligned} h_{T_i} =& h_{T_i,d} + h_{T_i,r} + h_{T_i,b} \\ =& \sum_{d=0}^{K_d} \alpha_{d,T_i} \delta(t - \tau_{d,T_i}) e^{-j\theta_{d,T_i}} + \sum_{r=0}^{K_r} \alpha_{r,T_i} \delta(t - \tau_{r,T_i}) e^{-j\theta_{r,T_i}} + \\ & \sum_{b=0}^{K_b} \alpha_{b,T_i} \delta(t - \tau_{b,T_i}) e^{-j\theta_{b,T_i}}. \end{aligned} \tag{3.9}$$

In (3.9), the noise is almost nonexistent since the WiFi system's noise is often considerably less than the WiFi signal, mainly when the distance between the transmitter and receiver is tiny. According to (2.3), the three separate amplitude attenuation parameters in (3.9) can be further stated as follows:

$$\alpha_{d,T_i} = \frac{WA_{d,T_i}}{(d_{d,T_i})^{\frac{n}{2}}}, \ \alpha_{m,T_i} = \alpha_{r,T_i} = \alpha_{b,T_i} = \frac{WA_{m,T_i}\varepsilon_{wall}}{(d_{m,T_i})^{\frac{n}{2}}}, \tag{3.10}$$

where ε_{wall} is the reflection coefficient of wall, and α_{r,T_i} and α_{b,T_i} are the same. Then, we advance to the time T_{i+1} when the intruder appears, as shown in Figure

doi:10.6342/NTU202303843

8(b). This is how the new CIR is presented:

$$\begin{aligned} h_{T_{i+1}} =& h_{T_{i+1},d} + h_{T_{i+1},r} + h_{T_{i+1},b} \\ =& \sum_{d=0}^{K_d} \alpha_{d,T_{i+1}} \delta(t - \tau_{d,T_{i+1}}) e^{-j\theta_{d,T_{i+1}}} + \sum_{r=0}^{K_r} \alpha_{r,T_{i+1}} \delta(t - \tau_{r,T_{i+1}}) e^{-j\theta_{r,T_{i+1}}} + \\ & \sum_{b=0}^{K_b} \alpha_{b,T_{i+1}} \delta(t - \tau_{b,T_{i+1}}) e^{-j\theta_{b,T_{i+1}}}, \end{aligned} \tag{3.11}$$

and at this time

$$\alpha_{b,T_{i+1}} = \frac{WA_{b,T_{i+1}} \varepsilon_{human}}{(d_{b,T_{i+1}})^{\frac{n}{2}}}, \tag{3.12}$$

where ε_{human} is the reflection coefficient of human. There is no change in the CIR for paths not blocked by intruders. That is to say, $\alpha_{d,T_i} = \alpha_{d,T_{i+1}}$, $\alpha_{r,T_i} = \alpha_{r,T_{i+1}}$. For the paths K_b, the presence of intruders not only affects the amplitude attenuation but also affects the angle of arrival (AoA). This is because the irregular shape of the human body changes the reflection angle. Based on the above, we get the CSI of the environment where there is an intruder according to (2.4):

$$\begin{aligned} H_{T_{i+1}} =& H_{T_{i,d}} + H_{T_{i,r}} + H_{T_{i+1,b}} \\ =& \sum_{d=0}^{K_d} \alpha_{d,T_i} e^{-j(2\pi f_c \tau_{d,T_i} + \theta_{d,T_i})} + \sum_{r=0}^{K_r} \alpha_{r,T_i} e^{-j(2\pi f_c \tau_{r,T_i} + \theta_{r,T_i})} + \\ & \sum_{b=0}^{K_b} \alpha_{b,T_{i+1}} e^{-j(2\pi f_c \tau_{b,T_{i+1}} + \theta_{b,T_{i+1}})}. \end{aligned} \tag{3.13}$$

From the decomposition of the above process, we can know how the intruder affects the path of the signal and then changes its amplitude and phase. The actual intrusion scenario is much more complicated than this simulation, and there are many elements in the environment that will affect the signal. Therefore, we need to extract scenario-independent features to detect intruders.

3.4.2 Sliding Window

In addition to real-time monitoring of intruders in the environment, the intrusion detection system is also very significant to the system in terms of the time point when an intruder is detected and the opportunity to issue an alarm. Therefore, we segment the collected CSI data into multiple data windows with some overlap. More feature sets are acquired in the sample, and the detection sensitivity is increased when the window is smaller. At the same time, the machine learning model's generalization capacity deteriorates, making it more susceptible to overfitting, and the too-small window cannot reflect the intrusion's actions. On the contrary, when the data window becomes larger, although it can better reflect

doi:10.6342/NTU202303843

the changes in the human body's influence on the environment, the features are reduced, and the model becomes underfitted. As a result of the above, we will determine the window and step sizes based on the performance of the recognition. The illustration diagram of the sliding window is shown in Figure 9.

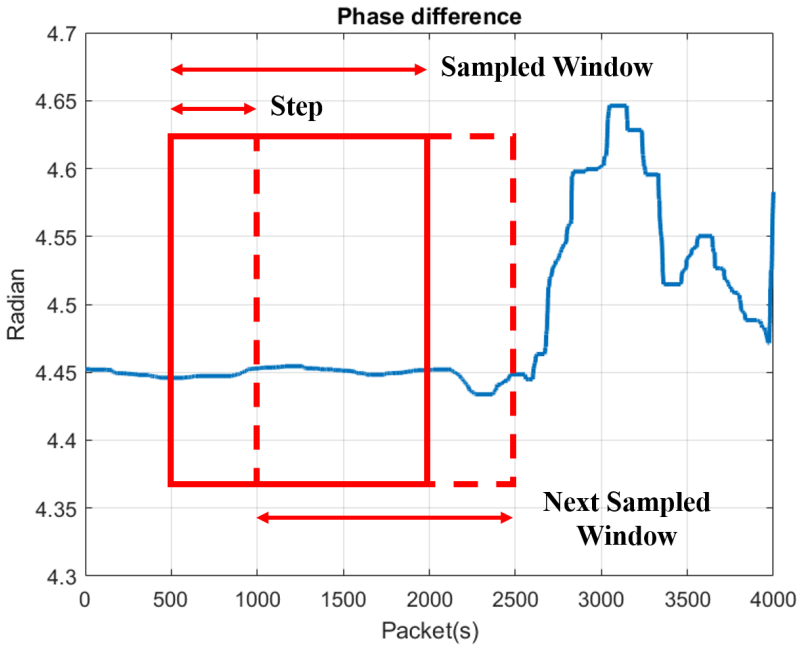


Figure 9: Segmentation using a slided window.

3.4.3 Features

As our goal, an intrusion detection system must accurately detect intruders regardless of the environment. Therefore, the features we extract are the most critical part of the entire system, and they should meet the following conditions:

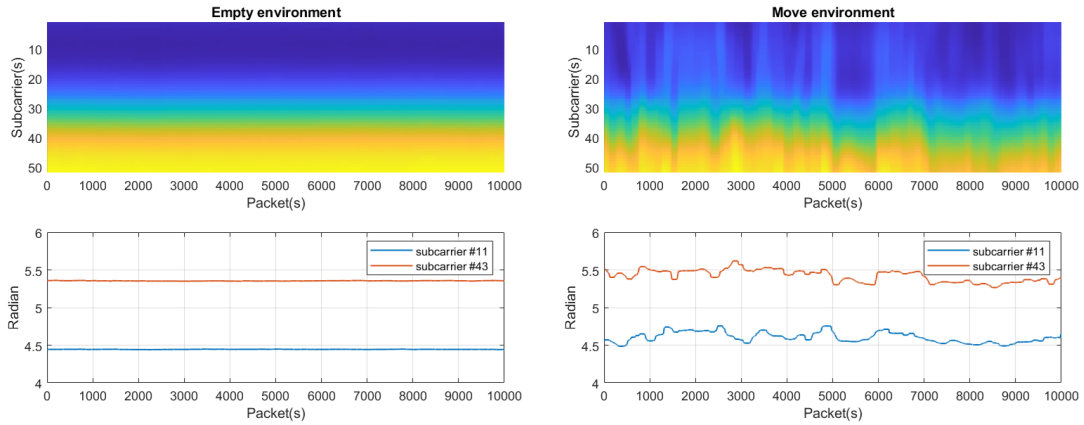
1. Sensitivity. The features retrieved from an empty environment and those extracted from CSI of human motion should differ significantly.

2. Scenario-independent. Considering the different application environments, the features should preferably be relative, and should not change much due to different scenarios.

To decide on the appropriate features, we first have to observe the changes in the intruder's appearance. In subsection 3.4.1, we explained how intruders affect the propagation of CSI signals. Here we visualize the CSI signals more intuitively to observe their differences. We stated in subsection 3.3.3 that the amplitude is more unstable than the phase difference, so choosing to extract features from the phase difference. Figure 10 shows the CSI phase difference with preprocessing

doi:10.6342/NTU202303843

under different scenarios. Among them, **Empty** means that there is no life in the environment, and **Move** means that there are intruders in space and they keep moving.



(a) (b)

Figure 10: Examples of subcarrier fluctuations in Empty and Move environments.

3.4.3.1 Variance

From Figure 10, we can directly observe that the CSI in the case of Move oscillates. Empty is the opposite, the change of CSI is minimal, and the phase difference hardly varies. And the best to show this feature is variance. The level of a random variable's dispersion is described by its variance. This gauges how much a set of numbers deviate from their expected value. It is the expected value of the square of the deviation between the random variable and its sample mean. For the CSI phase difference array $P_i = [p_{i,1}, p_{i,2}, \cdots, p_{i,pkt}, \cdots p_{i,W}]$ of the i^{th} subcarrier with a window size W, the variance is defined as:

$$v_i = Var(P_i) = \frac{1}{W} \sum_{pkt=1}^{W} |p_{i,pkt} - \mu_i|^2 , \tag{3.14}$$

where μ is the expected value of P_i,

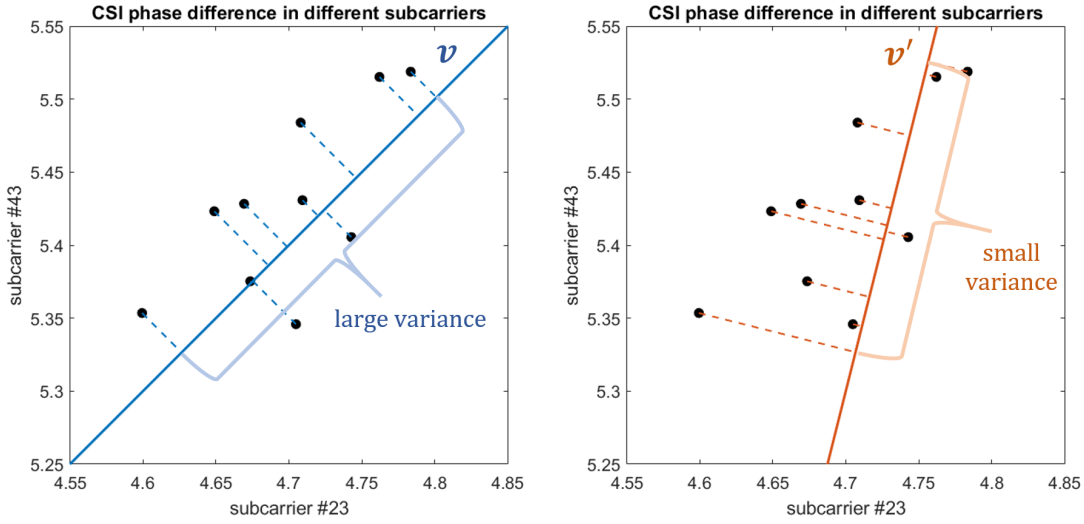
$$\mu = E(P_i) = \frac{1}{W} \sum_{pkt=1}^{W} p_{i,pkt}. \tag{3.15}$$

In the same window, calculate the variance of each subcarrier according to (3.14) to get $V = [v_1, v_2, \cdots, v_i, \cdots, v_K]$. The expected value of V is further calculated, that is, the average variation of each subcarrier, and the feature $f_{var} = E(V)$ can be obtained.

doi:10.6342/NTU202303843

3.4.3.2 Principal Component Analysis (PCA)

In machine learning, PCA [45] is a method that extracts features and reduces the dimensionality of the dataset. The purpose of dimension reduction is to reduce the number of dimensions of the data, but the overall performance will not differ significantly or even improve. The basic assumption of PCA is that the data will be able to find a projection axis (vector) within the feature space. After the projection, the maximum variation of this group of data can be determined. Theoretically, the principal component with higher variance can better represent the data type.



(a) (b)

Figure 11: The difference between the projection of the data on the v and v' vectors and their variance.

Figure 11(a) illustrates the values p_i of the CSI phase difference on two different subcarriers respectively displayed. Suppose there is a vector $\vec{v}$, and the projection vector of each data point on $\vec{v}$ is:

$$\vec{v_{p_i}} = |\vec{p_i}| \cos\theta \times \frac{\vec{v}}{|\vec{v}|} = |\vec{p_i}| \times \frac{\vec{p_i} \cdot \vec{v}}{|\vec{p_i}|\,|\vec{v}|} \times \frac{\vec{v}}{|\vec{v}|} = \frac{\vec{p_i} \cdot \vec{v}}{|\vec{v}|^2}\vec{v}. \tag{3.16}$$

The projected data point is $[v^T p_1, v^T p_2, \cdots, v^T p_i, \cdots, v^T p_n]$. The variance Σ used to measure the importance of PCA needs to be expressed in a matrix like this:

$$\Sigma = \frac{1}{n}\sum_{i=1}^{n}(v^T p_i)(v^T p_i)^T = \frac{1}{n}\sum_{i=1}^{n}(v^T p_i p_i^T v) = v^T\left(\frac{1}{n}\sum_{i=1}^{n} p_i p_i^T\right)v = v^T C v, \tag{3.17}$$

doi:10.6342/NTU202303843

where C is covariance matrix:

$$C = \frac{1}{n}\sum_{i=1}^{n} p_i p_i^T, \quad x_i = \begin{bmatrix} p_i^{(1)} \\ \vdots \\ p_i^{(d)} \end{bmatrix}. \tag{3.18}$$

From the above summary, PCA can be described as an optimization problem, which is to find the projection vector to maximize the variation of the projected data. For the p_i data exemplified earlier, two characteristic components can be extracted by PCA. The projected data is shown in Figure 12, from which we can see that the variation of the principal component (PC) #1 is sufficient to represent the information of this data. This approach can effectively reduce the number of dimensions, but the overall variation has not been reduced too much.

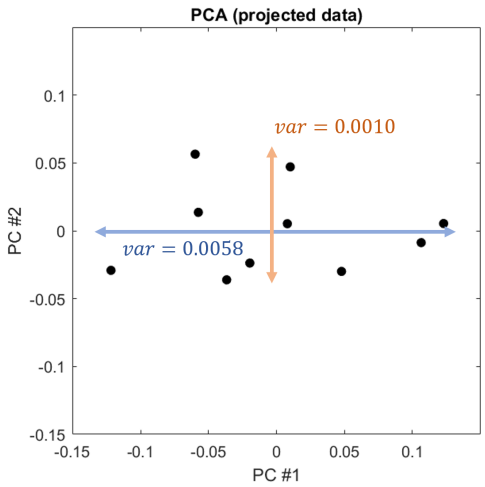


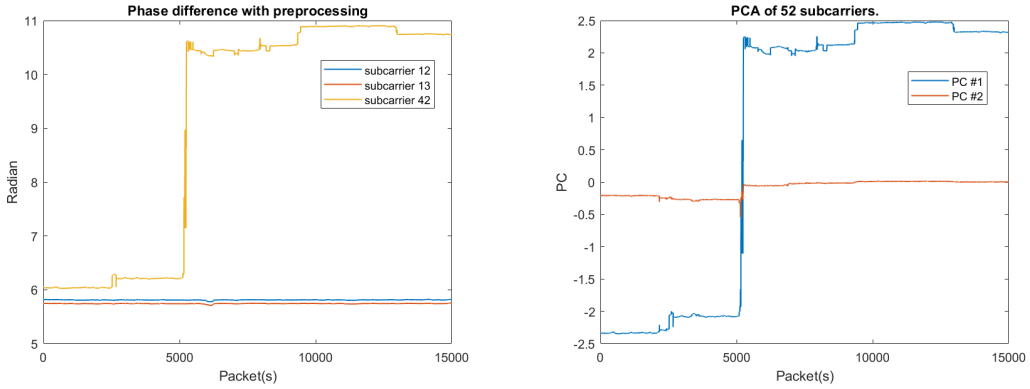
Figure 12: Data after PCA projection.

After we understood the significance of PCA, we decided to use the CSI phase difference data containing 52 subcarriers calculating PCA. In addition to effectively reducing the data dimension, another reason is that we can eliminate most hopping after preprocessing. However, there is still minimal phase difference hopping that may occur in a particular subcarrier. And it cannot be eliminated as subcarrier 42 of Figure 13(a). At this time, if the expected value of the variance of each subcarrier is directly calculated as described in Section 3.4.3.1, for a window containing hopping, it will result in a rapidly increasing variance. And if we choose a suitable principal component, this effect can be reduced.

Usually, the first principal component contains more than 80% of the data information. However, most errors or noise in the data will be included in the calculation. Therefore, compared with PC #1, we are more inclined to choose PC #2 as the data for analyzing variance. It doesn't contain a lot of noise like PC #1,

doi:10.6342/NTU202303843

and it doesn't like the components after PC #3 cannot reflect the characteristics of the original data. See Figure 13(b), PC #2 has obviously reduced hopping errors. Here, the second principal component of the CSI phase difference is expressed as $PC_2 = PCA(\mathbf{P}, 2)$, and the characteristic $f_{PCA} = Var(PC_2)$ is calculated according to (3.14).



(a) (b)

Figure 13: PCA can eliminate the anomalous hopping of the phase difference to a certain degree.

3.4.3.3 Correlation Coefficient

Since the transmission power parameters will be altered for various scenarios and circumstances that depend on the scenario and human motion can result in amplitude interference, the potential features should be independent of the absolute power. So the similarity between subcarriers may be an excellent scene-independent indicator. In statistics, The correlation coefficient is used to assess the degree of linear connection between variables X and Y in two sets of data [46]. Applied to CSI data, what we need to compare is the similarity between each subcarrier. The correlation coefficient between two variables is defined as the product of the covariance of the two variables divided by their standard deviations. The covariance here differs from (3.18). Suppose we are going to calculate the covariance of the CSI phase difference P_i, P_j between subcarriers i and j, and the expected values are $\bar{P}_i, \bar{P}_j$:

$$cov(P_i, P_j) = E[(P_i - \bar{P}_i)(P_j - \bar{P}_j)] = E(P_i \cdot P_j) - \bar{P}_i\bar{P}_j, \tag{3.19}$$

then we can calculate correlation coefficient $\rho_{i,j}$:

$$\rho_{i,j} = \frac{cov(P_i, P_j)}{\sigma_i\sigma_j} = \frac{E(P_i \cdot P_j) - \bar{P}_i\bar{P}_j}{\sigma_i\sigma_j}, \tag{3.20}$$

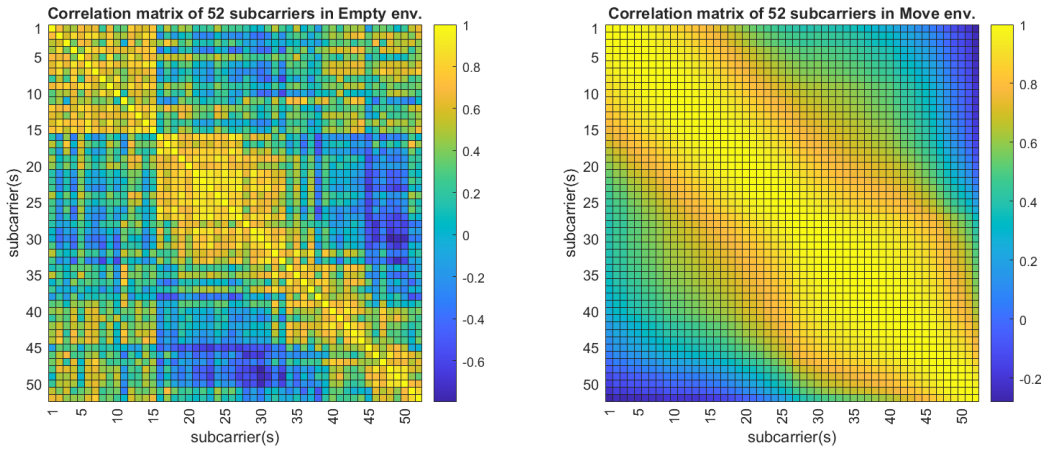
where $\sigma_i\sigma_j$ stand for the P_i and P_j standard deviation. The correlation coefficient matrix of each pair of subcarriers in a fixed window under various environmental

doi:10.6342/NTU202303843

conditions is shown in Figure 14. It is a 52-order symmetric matrix, and the diagonal entity is always 1. Taking a closer look at the characteristics of the two environmental correlation matrices, we find that:

- Empty case: The correlation between adjacent subcarriers is not high, and the correlation between other subcarriers is average.
- Move case: The correlation between adjacent subcarriers is high, and the correlation between subcarriers decreases as the frequency difference increases.

Looking back at the properties of the correlation coefficient, when there are no variables in the environment, the signal transmission path is affected by noise in addition to the environment. Because neither the furnishings of the space nor the environment has changed, the main oscillation of the signal comes from noise, and the correlation between noise is low. When there is an intruder in the environment, some signal transmission paths that pass through the intruder are susceptible to similar fluctuations. Although the signal also has noise, the impact of variations caused by intruders is significantly more than that caused by noise. The correlation between subcarriers should be higher than that of the state without intruders.



(a) (b)

Figure 14: Distribution of subcarrier correlation matrix in Empty and Move environments.

Since the correlation matrix is a 52×52 matrix, it cannot be considered a classification feature. So we decided to focus on the relationship between two adjacent subcarriers. According to the above, we can know that the higher the correlation between the two sub-carriers, the higher the probability of the presence of the intruder. Refer to [18] to extract the detailed part of the correlation matrix,

doi:10.6342/NTU202303843

and the correlation coefficient feature f_{cc} is defined as:

$$f_{cc} = \sum_{i,j=1}^{K} \rho_{i,j}, \quad \forall i, j \in [1, K], j - i = 1, \tag{3.21}$$

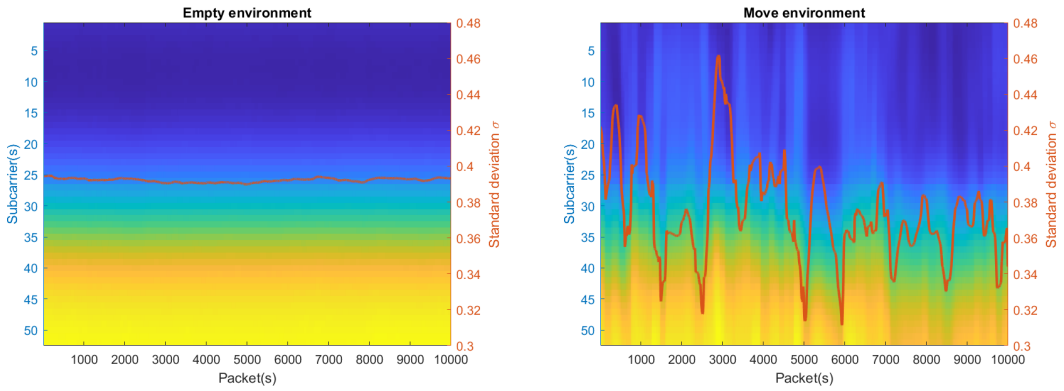
where K is the system's subcarrier count, which in this case is 52. $\rho_{i,j}$ is correlation coefficient from (3.20).

3.4.3.4 Standard Deviation

The majority of the aforementioned features concentrate on how the subcarrier changes in the time domain, while they may also be used to describe how the subcarrier fluctuates with frequency. We utilize the standard deviation in this case because the variance could intensify a subcarrier's fluctuation. The degree of dispersion between subcarriers can be represented concurrently and the units used to measure it are the same. The following is the standard deviation formula [47]:

$$S = \sqrt{\frac{1}{N} \sum_{i=1}^{N} |A_i - \mu|^2}. \tag{3.22}$$

Figure 15 illustrates the fluctuation between subcarriers, and it is clear that the two environments have different features.



(a) (b)

Figure 15: The degree of subcarrier dispersion of each packet can be represented by the standard deviation.

3.5 Model Decision

With the features we extracted, we need to properly classify the preliminary measurements collected from multiple cases. We have mentioned various shallow models in Section 2.3.3.3, among which the most suitable for our system should be the SVM [24] model.

doi:10.6342/NTU202303843

3.5.1 Support Vector Machine (SVM)

SVM is a learning machine for binary classification problems. The machine non-linearly maps input vectors to a very high-dimensional feature space. A decision surface is constructed in this feature space. SVM is one of the most well-liked machine learning methods as a low-cost classification tool. SVMs have been used by several CSI-based detection systems [16, 18, 20, 48–51] to accurately categorize various states. The findings demonstrate that SVM performs better than other machine learning techniques as KNN [22] and RF [23]. To satisfy the system's needs for real-time and high detection accuracy, we apply the SVM algorithm.

SVM is a two-class classification model, to put it simply. With the greatest interval in the feature space determined, its fundamental model is a linear classifier. Maximizing the interval is SVM's learning approach. First, consider a linearly separable training dataset $(X_1, y_1), (X_2, y_2), \cdots, (X_n, y_n)$, where X_i is a column vector containing d elements, that is, $X_i \in \mathbb{R}_d$; y_i is a scalar, $y \in +1, -1$, If $y_i = +1$, then X_i is said to fall under the positive category, and if $y_i = -1$, then X_i is said to fall under the negative category. A boundary is determined by the normal vector W and the intercept b, and its equation is $X^T W + b = 0$. One side directed by the normal vector is of the positive class, while the other side is of the negative class, it may be said. Three parallel boundary lines are shown in Figure 16 with the upper left direction representing the normal direction. We may initially select two parallel borders that divide the two classes of data in order to get the maximum margin boundary. This will guarantee that there is the greatest possible separation between them. The "margin" is the region between these two hyperplanes, and the maximum margin boundary is the line that runs through the center of them. Figure 16 depicts this procedure.

By increasing the distance between the hyperplane and the closest feature vector, SVM can accurately categorize the test data. It can categorize labels and classes that are not linearly separable using kernel functions in addition to linearly separable classes. Given a training dataset (3.23), where x_i is an d-dimensional feature vector, and l_i is the label/class vector to which the feature belongs, the value is 0 or 1. The subsequent optimization issues are resolved using the soft margin SVM method (3.24).

$$T = (x_1, l_1), (x_2, l_2), \cdots, (x_n, l_n), \tag{3.23}$$

$$\underset{w,b,\xi_i}{min} \frac{1}{2} ||w||^2 + C \sum_{i=1}^{n} \xi_i,\ \xi_i \geq 0, \mathbf{s.t.} l_i (w \cdot \Phi(x_i) - b) \geq 1 - \xi_i,\ \forall (x_i, l_i) \in T, \tag{3.24}$$

where C is an adjustable parameter that establishes the trade-off in training between the size of the margin and its level of inaccuracy, and ξ_i quantifies the degree

doi:10.6342/NTU202303843

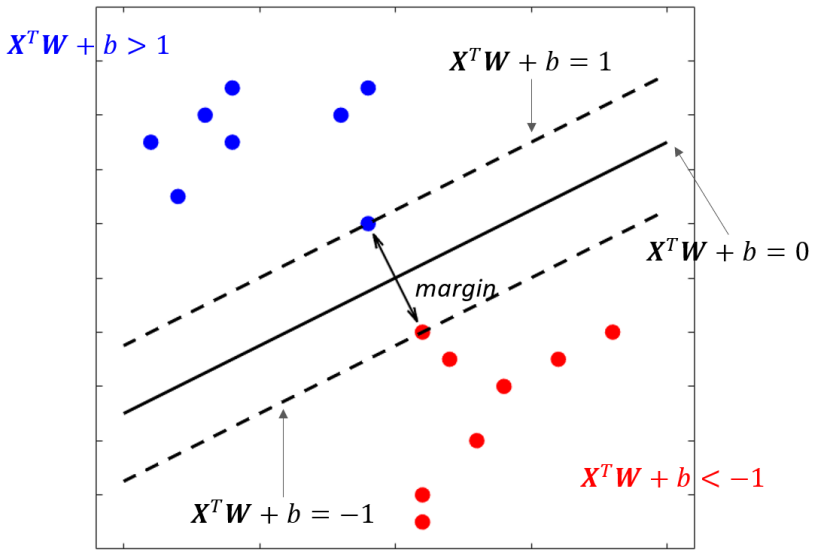


Figure 16: Find the maximum margin to separate two different datasets.

of misclassification. $\Phi(x_i)$ denotes the feature space images of the corresponding patterns in the input space. A nonlinear SVM, which consists of two phases, can be utilized when the classes are not linearly separable:

1. Create a high-dimensional space from the input feature vector so that training data may be separated linearly.

2. Then, as illustrated in Figure 17, the soft margin SVM is utilized to identify the hyperplane with the biggest margin in the new feature space.

Lagrangian multipliers may be used to solve the optimization issue, and by dividing the classes in the dual problem, the optimal hyperplane can be found. The dot product of feature vectors is calculated using the kernel functions as though they had been translated into a higher dimensional space. Without really altering the vectors, this is achieved.

3.5.2 One Class Support Vector Machine (OCSVM)

Although SVM is a low-cost method that can achieve reliable results, considering that we cannot control the actions of intruders, it seems a bit too ideal to use the data collected from simulated intrusion situations for binary classification. Therefore, we turn to One Class Support Vector Machine (OCSVM), which is mostly used for outlier detection.

OCSVM [52] is an unsupervised algorithm. As the name implies, there is only one classification for training data. Learn a decision boundary by using the

doi:10.6342/NTU202303843

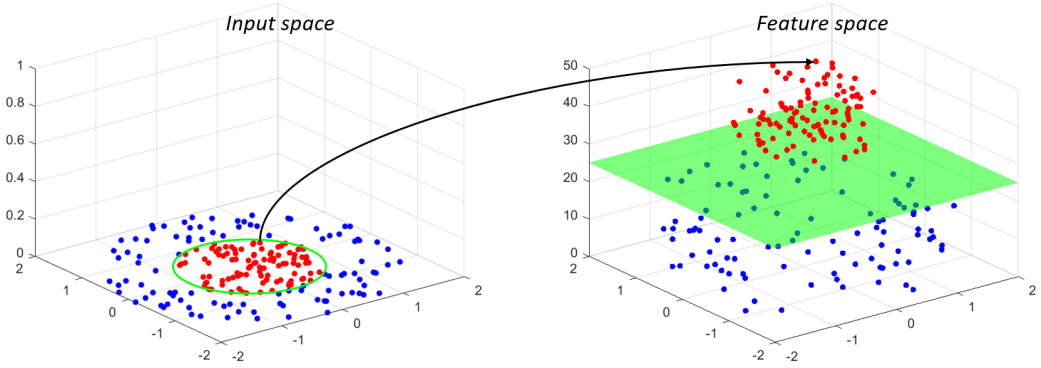


Figure 17: Transform the feature vectors into a higher-dimensional space to find a separable hyperplane.

properties of these normal samples. The freshly produced data point's similarity to the training data may then be determined using this boundary. It is regarded as an outlier if the boundary is crossed. In OCSVM, the data has no label, so we rewrite (3.24) as:

$$\underset{w,\xi_i,\rho}{min}\frac{1}{2}\left|\left|w\right|\right|^2+\frac{1}{vN}\sum_{i=1}^{n}\xi_i-\rho,\ \xi_i\geq 0,\mathbf{s.t.}(w\cdot\Phi(x_i))\geq\rho-\xi_i. \tag{3.25}$$

Here, $v\in(0,1)$ is a parameter. If v approaches 0, the upper bound of the Lagrangian multiplier tends to infinity, i.e. the second inequality constraint in (3.25) becomes invalid. ρ is the offset of slack variable, and N is the number af traing data. The resulting parameters of A can form a set of classification equations:

$$f(x)=sign(w\cdot\Phi(x_i)-\rho). \tag{3.26}$$

For most cases, the non-outlier value brought into this equation will be positive, and the data will be negative if it is an outlier. When there are no intruders in the environment, CSI data is stable. In other words, we can use EMPTY data as training data and construct the required OCSVM model. When an intruder appears in the environment and changes the signal transmission path, CSI becomes unstable and unpredictable. If it leaves the comfort zone, it is marked as abnormal, which means someone has invaded.

The kernel function commonly used in OCSVM is RBF because it fits the training data well to detect outliers. However, for our system, RBF would make our model overfitting. Whenever the target environment changes, the chances of the model detecting outliers increase and false alarms increase. Therefore we use a linear kernel function; although its sensitivity is not as good as RBF, it can significantly reduce false positives. A voting mechanism can make up for insufficient sensitivity issues.

doi:10.6342/NTU202303843

3.5.3 Vote

Because in different environments, the placement of APs is different each time, and the sensitivity of each antenna to intrusion behaviors is different. Therefore, we train individual OCSVM models, which can also be called classifiers, for each pair of phase difference combinations. Let each classifier vote whether the current window should be classified as intrusion behavior. The advantage of this is that when a certain classifier cannot accurately determine the occurrence of an intrusion, there are other classifiers that can detect the intrusion. On the other hand, if only one classifier detects an intrusion, misclassifications occur, but false alarms will not easily be generated.

doi:10.6342/NTU202303843

CHAPTER 4

PRELIMINARY PERFORMANCE OF INTRUSION DETECTION

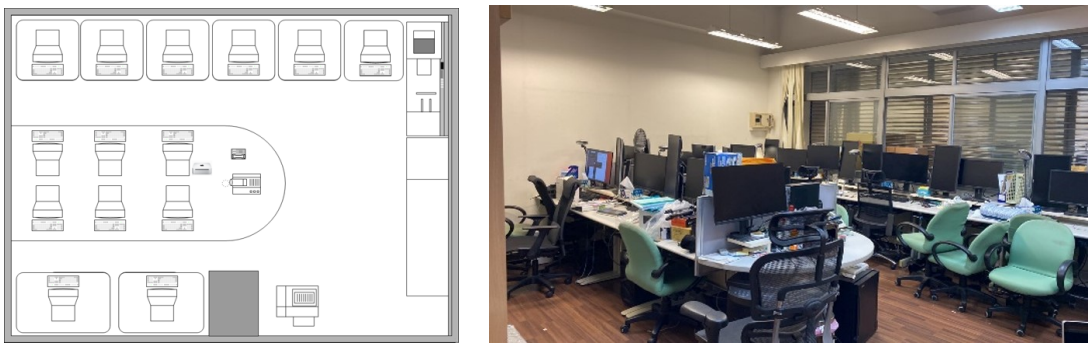
This chapter introduces the experimental evaluation environment and the experimental platform prototype. The effect of settings and scenarios on performance is then covered.

4.1 Setup

We first describe the equipment used and the settings of related parameters, then introduce the experimental field, and finally discuss system performance.

4.1.1 Equipments and Collection Parameters

We use two commercial Wi-Fi devices, Lanner LWR-x8460, to implement our system and test the scenarios to evaluate system performance. The transmitter and receiver utilize the same Wi-Fi AP device, which supports standard IEEE 802.11 a/b/g/n/ac/ax, three frequency bands: 2.4GHz, 5GHz, 6GHz, and 4 internal antennas. In our experiments, we configured the AP to run at 2.4 GHz with a bandwidth of 20 MHz in IEEE 802.11n mode. The purpose is to test the effect of intrusion detection systems under lower performance. The number of antennas used is 1x4. Considering the CSI sample rate is 500 Hz, the AP sends 500 packets every second. Each group's sampling period is set to 60 seconds, making the sample size for each group approximately 30,000 packets. The sliding window



(a) (b)

Figure 18: The floor plan of the laboratory and the pictures of the actual environment.

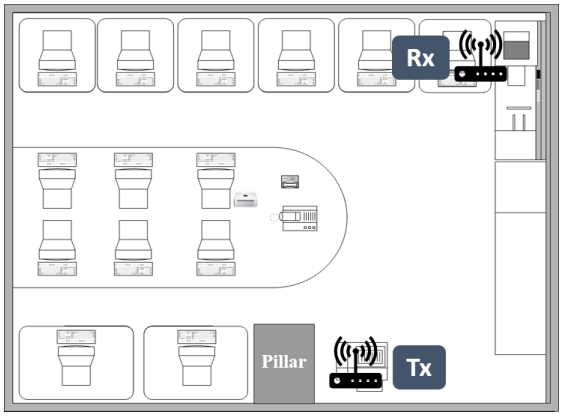
doi:10.6342/NTU202303843

size is set to 1000 packets, about 2 seconds, and the sliding step is 50 packets, about 0.1 seconds. Group collecting was carried out three times. We recorded a temperature of 25°C (77°F) inside the laboratory, and the surroundings outside the laboratory were quiet and devoid of human activity.

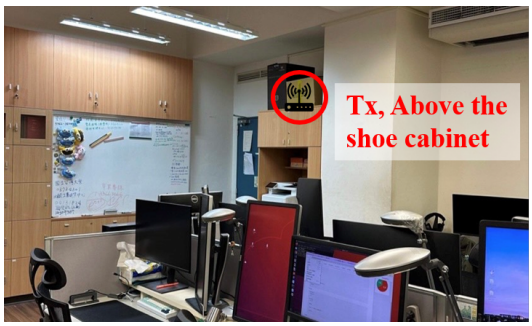
4.1.2 Environment and Experimental Scenarios

To more thoroughly test the robustness of our system, we conduct experiments in three different spaces. Each space is different in size and furnishings. In addition to designing intruders to move in different locations in space, we observe the intrusion system's detection effect on intruders. At the same time, the scene independence of the intrusion detection system is verified by changing the location of the Wi-Fi device and the space.

We also consider that if there are only two devices to detect intruders in ample indoor space, there are more likely to be dead spots in detection. This will result in a reduction in detection performance. Therefore, we also increased the number of devices, including ideal and non-ideal situations. Below we will introduce the three experimental spaces respectively, and the placement of the widgets in each space will additionally be explained together.



(a)



(b)

(c)

Figure 19: The location of the transmitter and receiver.

doi:10.6342/NTU202303843

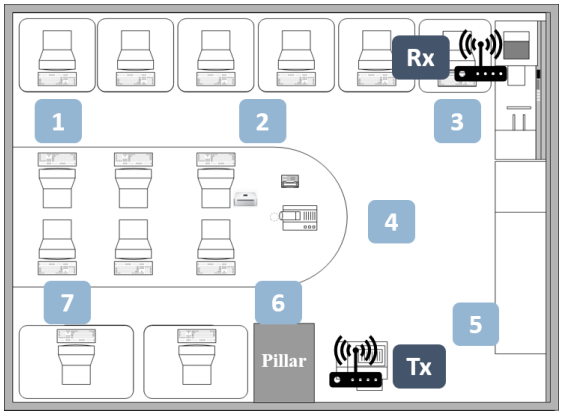


Figure 20: The position and number of intruder activity in the laboratory.

4.1.2.1 Laboratory

Our system's primary purpose is to utilize idle AP devices in the office during off-hours effectively. Therefore, we use two enterprise Wi-Fi devices as our transmitter and receiver.

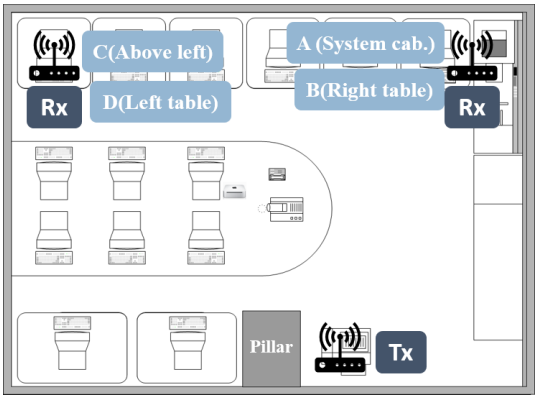
For the first experimental scene, we choose to conduct it in the laboratory. The size is about 6m×6m. There are primarily tables, chairs, and computers in the space. For the overall layout and actual pictures, refer to Figure 18.

The training data for the model also comes from this space. Figure 19(a) shows the transmitter and receiver placement. In addition, we also consider that most of the APs in the actual office are installed close to the ceiling, so we also set up the AP at a height of more than 2m for testing. The actual erection position can be seen in Figure 19. We collected about 40 seconds of empty data in the indoor environment without any intruders. And to enhance the robustness of the model, the empty data that has been preprocessed and contains hoppings are selected as training data. This choice reduces the probability of the system model issuing false alarms due to the selection of imperfect data for training since we cannot control the hopping timing.

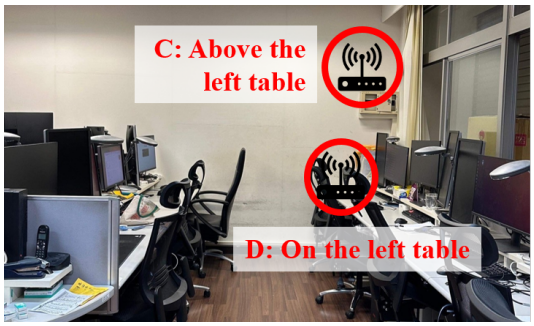
Table 3: The laboratory scenarios I and III are introduced as well as the classroom scenarios.

Case	Intruder position	Intruders	Notes
Empty	Null	Null	No intruders
Move	Laboratory	1-2	No scope of activity specified
Pos$N$	No.N	1	Wave or step

doi:10.6342/NTU202303843



(a)



(b)

(c)

Figure 21: The location of the transmitter and receiver in Scenario II.

The testing data in this space have two different situations, which will be explained in the following paragraphs.

Scenario I

In this scenario, we fix the location of the AP, and the primary variable comes from the intruder. We first let the intruder walk freely in the laboratory without restricting the behavior and location of the intruder. We collected CSI data for this scenario. Next, we start imposing some restrictions on the intruders. The movement range of the intruder is limited to a radius of 1 meter from a certain point. There are no particular restrictions on the movements performed, but most are waving and standing still. It is also necessary to collect empty data similar to training data in this situation.

Figure 20 shows some positions where the intruder is restricted. We organize all intruder activity cases in Table 3.

Scenario II The second scenario is to verify the robustness of the system model. We will move the location of the AP, which will change the primary transmission path of the data to a certain extent. And the high and low positions of the receiver AP are changed respectively. When the AP is at a low height, about one

doi:10.6342/NTU202303843

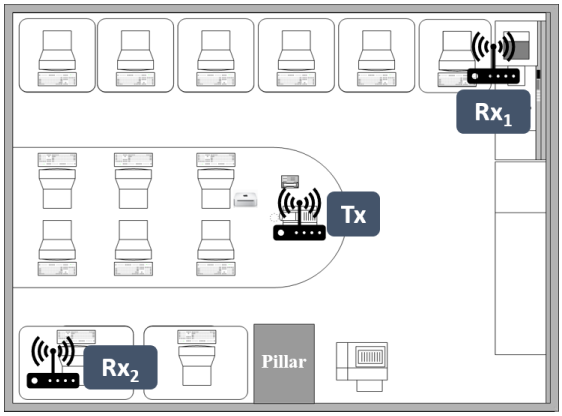
Table 4: Experimental scenarios II in the laboratory.

Case	AP Placement	Intruders	Notes
Empty	No.A	Null	No intruders
	No.B		
	No.C		
	No.D		
Move	No.A	1-2	No scope of activity specified
	No.B		
	No.C		
	No.D		

meter high, signals' propagation will be blocked by obstacles such as desks and computers.

The position of the transmitter AP has not changed. We moved the receiver AP, which was initially placed on the high right side of the laboratory, to the right computer desk. In addition, we have added two receiving APs on the left side. These APs are placed on the computer desk and raised to two meters by several boxes. Figure 21 illustrates the position of APs in this scenario.

Following the above AP placement positions, we collected empty and move

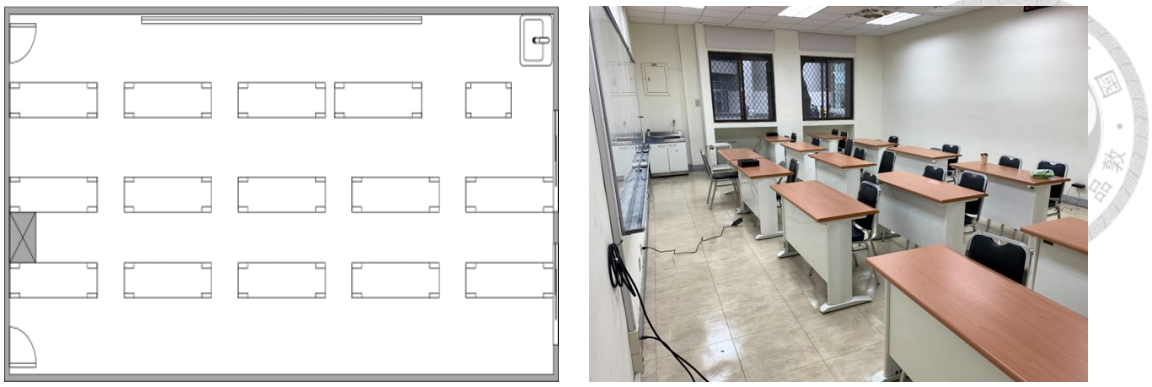


(a)

(b)

Figure 22: The location of the transmitter and receiver in Scenario III.

doi:10.6342/NTU202303843



(a) (b)

Figure 23: The floor plan of the classroom and the pictures of the actual environment.

data. Similarly, there is no intruder in the empty case, and the move case allows intruders to act in the laboratory without restriction.

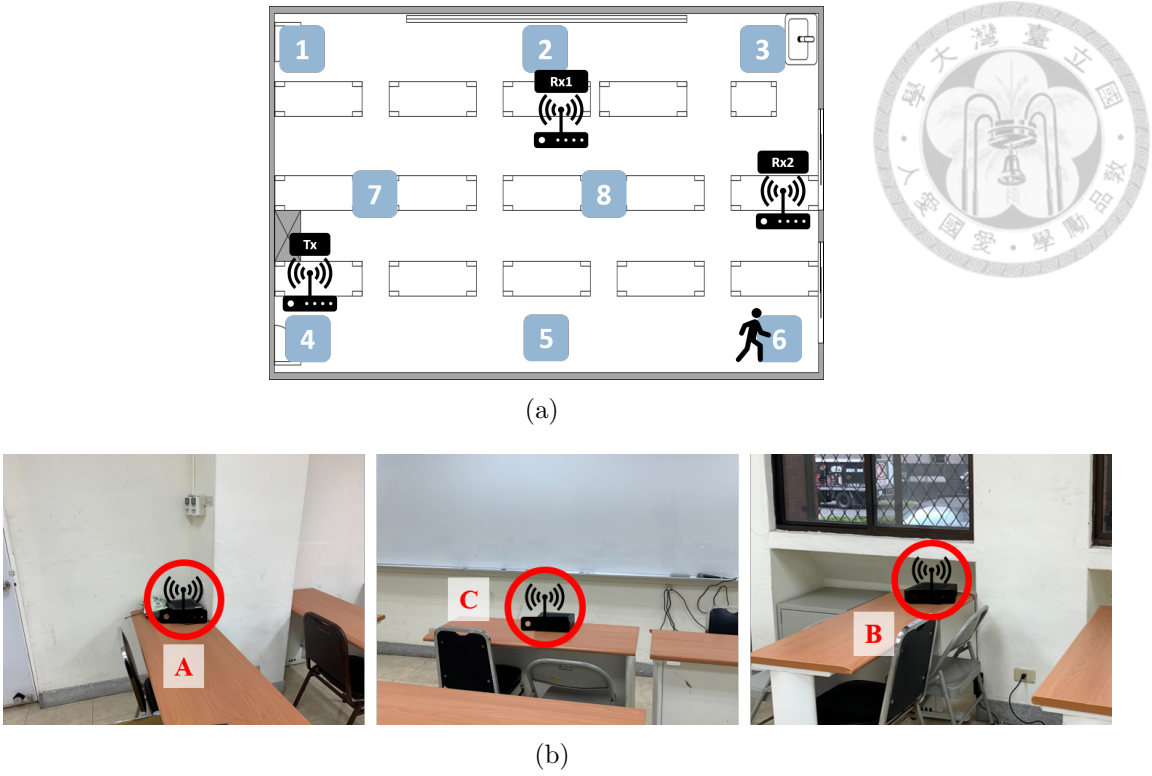
Scenario III It is known that the system uses CSI information for detection, mainly relying on the signal transmitted between two APs so that the detection effect will be affected by the AP placement. For example, detection performance may be reduced if there is an obstacle in the line of sight between the AP and the intruder, such as a pillar. Since the detection effect of using two APs for one transmission path is limited, if the number of APs increases, devices for sensing the environment and detecting intruders are added. It doesn't matter if there is a device that doesn't detect an intruder if one of the devices can sound an intruder alert.

In this scenario, we first consider an ideal situation. The transmitter is placed in the middle of the space and is not blocked by obstacles. The receivers are placed in two corners of the laboratory. The path between the receivers and the transmitter covers the entire space, as shown in Figure 22. All the data collected in cases are the same as in Scenario I, see Table 3. The difference between the two scenarios lies in the location and number of APs.

4.1.2.2 Classroom

We converted the experimental space into a more extensive classroom measuring approximately 8m×12m. The classroom structure is relatively simple, and the furniture placed in the room is tables and chairs. The classroom floor plan and environmental photos are shown in Figure 23. We generally consider that the system cannot control the user to place the AP in the ideal position for classrooms. Most of them will set up the AP at the edge of the space. Same as Scenario III in

doi:10.6342/NTU202303843



(a)

(b)

Figure 24: The position and number of intruder activity, transmitters and receivers in the classroom.

the laboratory, three APs, one transmitter, and two receivers are also used. They are placed in three corners of the classroom. As shown in Figure 24(b), the AP acting as a teleporter is even placed at an angle between the wall and the pillar. This means that when the intruder is at the classroom's front door, there is a pillar between them and the teleporter.

To test the performance of the intruder detection system, the position of the intruder is also specially designed to be located in shelter position 1. This is shown in Figure 24(a). The actual experimental scenarios are the same as those in Table 3; the difference lies in the replacement of the scene and the adjustment of the intruder's position according to the different fields.

4.1.3 Performance Evaluation

We measured a temperature of 25°C (77°F) inside the laboratory, and the surroundings outside the laboratory were quiet and devoid of human activity. The data from the empty environment was collected to train the OCSVM model.

After the OCSVM model is trained, four sorts of output are obtained when we import the test data into the model: True Positive (TP) people are present, and the system reports so, False Positive (FP) no humans are present, but the system reports the presence of an intruder, True Negative (TN) means no humans are

doi:10.6342/NTU202303843

(a) (b)

Figure 25: Intrusion detection performance in laboratory scenario I.

present and the system reports them correctly, False Negative (FN) means people are present but not reported by the system. We pay more attention to TP and FP for an intrusion detection system. The system should have more TP samples and fewer FP samples. The former represents the probability that we can detect an intruder, and the latter represents the probability that the system will send a false alarm. We define the following indicators to more clearly demonstrate system performance:

$$P = \frac{TP}{TP + FN}, \quad FA = \frac{FP}{FP + TN}, \tag{4.1}$$

where Precision (P) represents the percentage of all cases where an intruder was actually detected by the system, while False Alarms (FA) represent how many of the collected empty cases were incorrectly flagged as intruders by the system. As explained in the next sections, we looked at these indicators to assess how well the system performed in various scenarios.

4.2 Perfoemance

The performance evaluation of the intrusion detection system is carried out according to the different field situations of the above design.

4.2.1 Laboratory

4.2.1.1 Scenario I

The training data used to train the OCSVM model is mainly collected in the laboratory. The layout of the transmitter and receiver is shown in Figure 25(b).

doi:10.6342/NTU202303843

Therefore, this scenario focuses primarily on the effect of the pre-trained model.As

(a) (b)

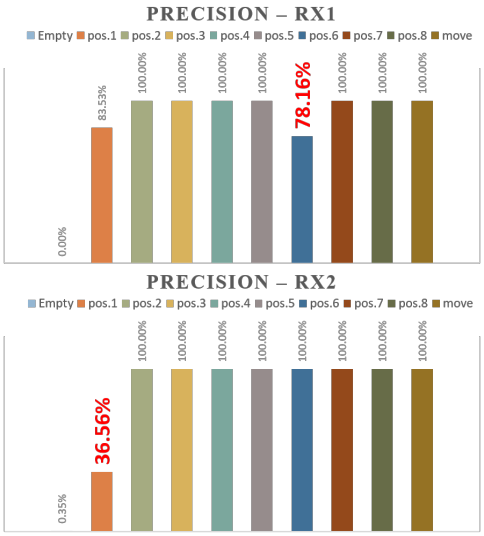
Figure 26: Intrusion detection performance in laboratory scenario II.

shown in Figure 25(a), when the intruder moves irregularly in the laboratory, the detection effect can reach 100.00%. The incidence of FA is also as low as 1.00%. However, when we define the range of activities of intruders, it can be found that the detection effect of position 7 is not as good as that of other positions, only 72.58%. This is due to the pillar blocking between position 7 and the conveyor.

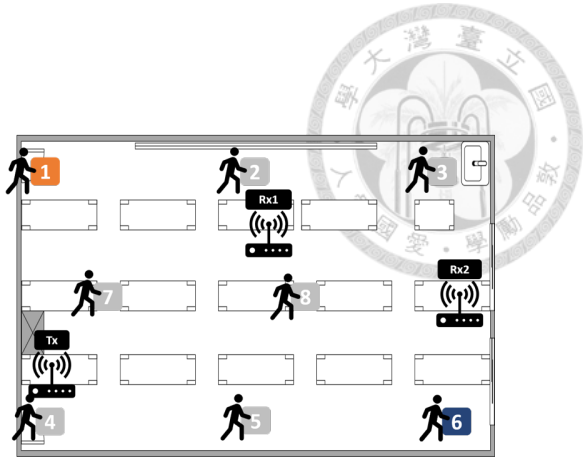
(a) (b)

Figure 27: Intrusion detection performance in laboratory scenario III.

doi:10.6342/NTU202303843



(a)



(b)

Figure 28: Intrusion detection performance in the Classroom.

4.2.1.2 Scenario II

To understand the independence between the pre-trained model and the scenario, we change the spatial layout by moving the receiver to different positions, as Figure 26(b). In this case, there is no regulation on the behavior of the intruder, and the detection performance can reach 100%. With the receiver in position C, although the FA improved slightly, it was still only 4.90%. From this result, it can be seen that the pre-trained model is scenario-independent.

4.2.1.3 Scenario III

In addition to forming a single link from one transmitter and one receiver to monitor intruders, we are also considering increasing performance by adding detection links. The advantage of detecting multiple links simultaneously is that it is considered a successful detection when one of the links detects an intruder. Figure 28 shows the result of this scenario. The performance of link 1 at position 7 is only 58.65%, but link 2 is indeed 100.00%, so the highest detection effect can still reach 100.00%. Same as at position 3.

Besides the above configurations, we also consider the case where the intruder is not moving in this environment. The intruder will stand still at position 2 in the space and only maintain essential breathing. It can be clearly seen that under such conditions the detection rate of the system will drop to only about 50%.

doi:10.6342/NTU202303843

4.2.2 Classroom

Moving the test scene to the classroom not only tests the robustness of the model but also tests the detection effect when the intruder is blocked. When the device is set up as shown in Figure 28(a), it can be seen that position 1 and position 6 are places where the detection effect of link 1 is poor. For link 2, the detection effect of position 1 drops to 36.56%. Although the use of multiple devices can increase detection performance, it is possible that unsatisfactory placement of the devices may result in poor detection in some places in the space due to the user's non-ideal placement.

4.3 Problems

Judging from the above various experimental spaces and the experiments conducted in different environments. The overall average detection precision P_avg can reach 93.69%, and FA is as low as 0.81%. Excluding partially occluded locations that cause poor results, the efficient detection precision P_e can rise to 99.92% on average. However, if only blocked positions are observed, the blocked detection precision P_b is only 60.77%, as shown in Table 5.

Table 5: The precision and false alarm probability of the intrusion detection system, the intruder being blocked will reduce the intrusion precision.

P_{avg}	FA	P_e	P_b
93.69%	0.81%	99.92%	60.77%

Obviously, when the intrusion position is blocked or the intruder keeps static motion, it affects the overall detection performance. Despite the fact that P_{avg} has a positive effect on the current intrusion detection system. However, we intend to further improve P_e in order to achieve a detection effect that encompasses the entire target space.

We will present an overview of power delays in the next chapter. Briefly, the main method is to increase the weight of the path affected by the intruder by analyzing the propagation path of the signal. This is to increase the probability of it being detected.

doi:10.6342/NTU202303843

CHAPTER 5

POWER DELAY PROFILE ANALYSIS

As explained in Chapter 2, CSI is the FT of CIR. CIR also shows the path loss and delay of each path. From the point of view of the time domain, based on the sensitivity of different ways to intruders, we expect to improve detection precision by adjusting the weight of paths. In addition, since the distinction of paths comes from varying delay times, converting the delay to distance can roughly estimate the possible location of the intruder. The above can complete while judging whether there is an intruder.

5.1 Power Delay Profile (PDP)

First, we need to understand the information that PDP can provide. We will explain in detail how the CSI converts to the time domain, propagates through multiple paths, and reaches the receiver and the part distorted by the filter. Due to hardware limitations, CIR cannot fully restore, but fortunately, these incomplete CIR can still provide helpful path information.

5.1.1 Propagation of Signals

We assume here that at time t_0, a packet has a total of K rays. Each ray represents a signal path from the transmitter to the receiver. We use $CIR_{sim,T}$ to represent the simulated emission CIR information, the sum of K paths. And the k^{th} path can be expressed as follows [4, 5]:

$$h_{t_0,k} = \alpha_{t_0,k}\delta(t - \tau_{t_0,k})e^{-j\theta_{t_0,k}}, \tag{5.1}$$

where α represents the amplitude of the path, τ indicates the path delay, depending on the path distance, and θ represents the phase. It is known that from the perspective of the frequency domain, the phase of the i^{th} subcarrier will have an offset due to the frequency:

$$\lambda = c/f_i, \theta_{t_0,k,i} = \frac{2\pi d_k}{\lambda}, \tag{5.2}$$

where *lambda* represents the wavelength, f_i is the frequency of the i^{th} subcarrier, and d_k is the path distance of the k^{th} path. Therefore, according to the i^{th} subcarrier and the time point t_0, CIR_{sim} with total K simulation paths can be expressed

doi:10.6342/NTU202303843

as [4, 5]:

$$h_{t_0,i} = \sum_{k=0}^{K} \alpha_{t_0,k} \delta(t - \tau_{t_0,k}) e^{-j\theta_{t_0,k,i}}. \tag{5.3}$$

After the receiver receives the signals from each path, convert them to the frequency domain to get $CSI = \mathcal{F}(CIR_{sim})$ [8]:

$$H_{t_0}(f_i) = \sum_{k=0}^{K} \alpha_{t_0,k} e^{-j(2\pi f_i \tau_{t_0,k} + \theta_{t_0,k,i})}. \tag{5.4}$$

Assuming that there are I subcarriers in total, the CSI of the collection time point t_0 is:

$$H_{t_0} = [H_{t_0}(f_1), H_{t_0}(f_2), \ldots, H_{t_0}(f_i), \ldots, H_{t_0}(f_I)]. \tag{5.5}$$

This CSI is the data that can be collected in actual experiments. It is also the information that most related research based on CSI will use. And what we want to do is restore CIR information from the collected CSI. In order to distinguish it from the originally simulated CIR_{sim}, the CIR restored from CSI is called CIR_{col}. From the above, we know that $CSI = \mathcal{F}(CIR)$, so we can obtain CIR information through $CIR = \mathcal{F}^{-1}(CSI)$.

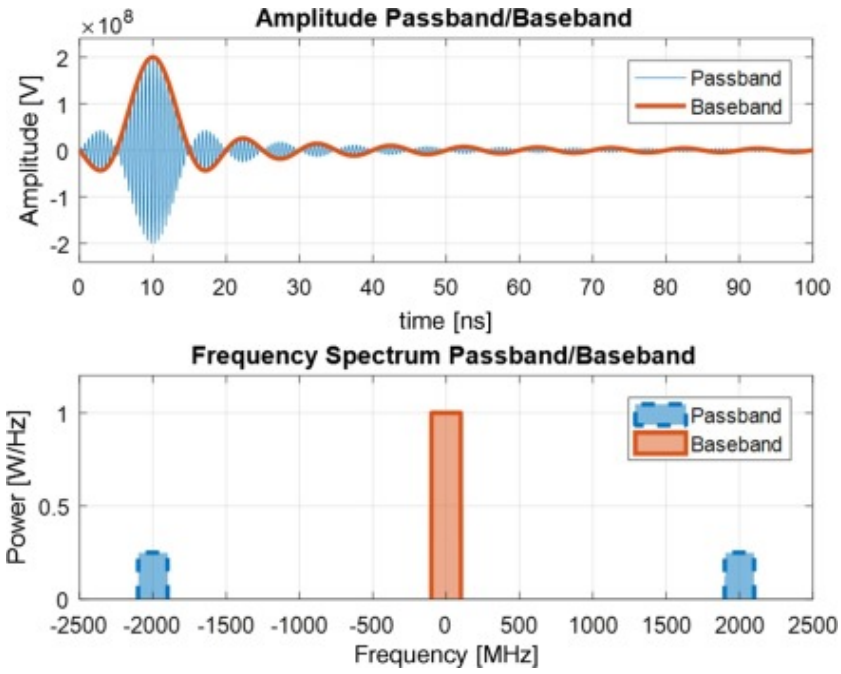


Figure 29: Example of a baseband and passband channel having a carrier frequency of 2000 MHz and a bandwidth of 200 MHz. For ease of comparison in the delay domain, the baseband channel's power is double that of the passband channel [1].

doi:10.6342/NTU202303843

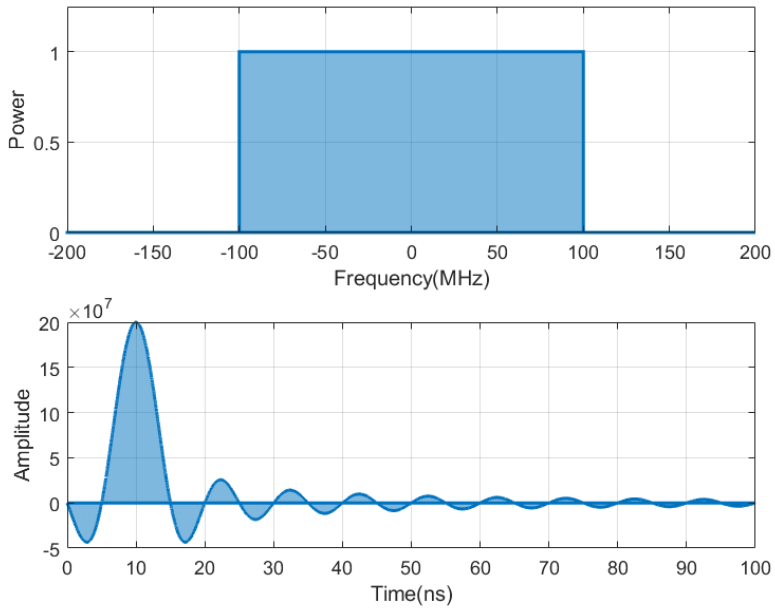


Figure 30: Channel responses for a uniform frequency filter.

5.1.2 Channel Response

As a thoughtful consideration, however, the CIR can ideally be computed from the CFR using an inverse Fourier transform (IFT). However, we are unable to calculate the IFT or fully quantify the CFR in a truly digital system. Instead, we employ CSI, sampling of the CFR, and IFFT, a digital signal processing technique that implements IFT. After periodically expanding the CSI within the bandwidth, computing the IFFT of a CSI is identical to computing the IFFT of a digital signal. Therefore, B, the CSI's bandwidth, plays a significant role in determining how accurate the estimated impulse response is. The computed impulse response's amplitude and phase will be somewhat skewed if the bandwidth is insufficient [53]. Therefore, we will employ various bandwidths to evaluate CIR later. We rely on IFFT to recover CIR by combining the aforementioned [1]:

$$h(t) = \sum_{k=0}^{K} \mathbf{H}(f) e^{\frac{j2\pi kt}{K}}. \tag{5.6}$$

Next, we will illustrate the distortion and sidelobes in the computed impulse response due to frequency-domain, time-domain, and bandpass filter transformations.

The modulation of a continuous wave f_0 around a certain carrier frequency is used for radio data transmission. The bitrate and associated modulation speed are proportional to the applied bandwidth B. The properties of the band-limited filter dictate how an associated channel's impulse response will take shape. A

doi:10.6342/NTU202303843

channel with a uniform bandpass filter and a single multipath delay component, τ_1, serves as an illustration of this [1]:

$$\begin{cases} h(\tau) = \dfrac{B}{2} sinc\left[\pi B(\tau - \tau_1)\right] \cdot \left[exp(i2\pi f_0 t) + exp(-i2\pi f_0 t)\right] \\ H(f) = \begin{cases} 0 \text{ if } |f| > f_0 + \dfrac{B}{2} \text{ and } |f| < f_0 - \dfrac{B}{2} \\ \dfrac{1}{2} \text{ if } |f| < f_0 + \dfrac{B}{2} \text{ and } |f| > f_0 - \dfrac{B}{2}. \end{cases} \end{cases} \tag{5.7}$$

Assume $f_0 = 2\text{GHz}$, $B = 200\text{MHz}$, $\tau_1 = 10\text{ns}$. The corresponding channel response is shown in Figure 29. The carrier frequency f_0 causes rapid $h(\tau)$ oscillations to be seen in the passband. To give a real channel response, positive and negative frequencies of $H(f)$are furthermore required. For ease of explanation, the channel is often stated in baseband, which entails transforming the frequencies to zero mean, so $f' = f - f_0$.

$$\begin{cases} h(\tau) = Bsinc(\pi B(\tau - \tau_1)) \\ H(f') = \begin{cases} 0 \text{ if } |f'| > \dfrac{B}{2} \\ 1 \text{ if } |f'| < \dfrac{B}{2}. \end{cases} \end{cases} \tag{5.8}$$

It is known that $\Delta\tau = 1/B$, so in this example, the time resolution $\Delta\tau = 5ns$. Figure 30 shows the channel response of a uniform frequency filter. We can see that due to the characteristics of the sinc function, at the position of τ_1, the

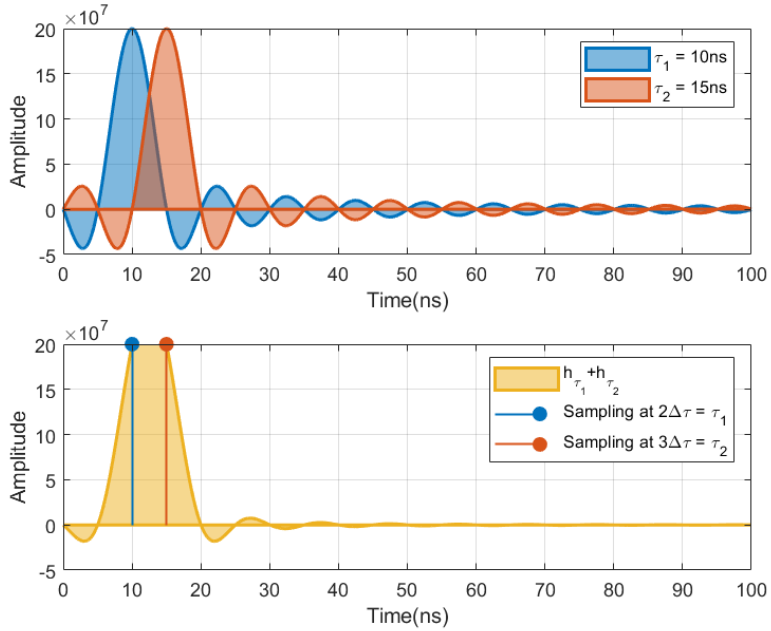


Figure 31: The channel response in the time domain contains two path components, τ_1 and τ_2. Both τ_1 and τ_2 are in $n \cdot \Delta\tau$, ideally well sampled components.

doi:10.6342/NTU202303843

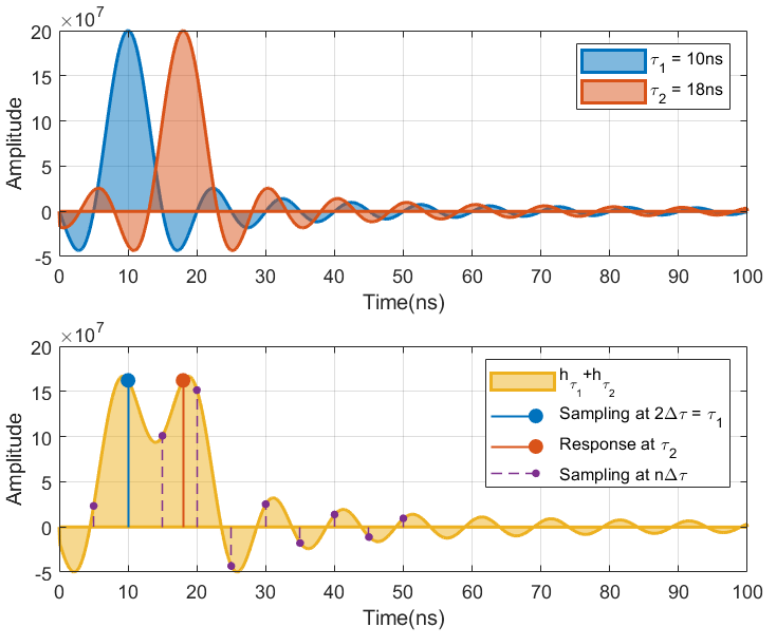


Figure 32: The channel response in the time domain contains two path components, τ_1 and τ_2. As τ_2 is not at the sampling point, the two components interact for the side lobe of *sinc* to be reflected at the sampling point.

amplitude is equal to B. And the position of $n\Delta\tau, n \in \mathbb{Z}$ will be exactly equal to 0. If the delays of the signals are all just on $n\Delta\tau$, the signals can be superimposed without interfering with each other. In fact, signal delays are irregular, and it is almost impossible to obtain a PDP without path interference.

Taking Figure 31 as an example, in addition to the initially assumed τ_1, we added a component with a delay of τ_2 to simulate multipath signals. Assume τ_2 is 15ns, equal to $3 \cdot \Delta\tau$. We can see that the τ_1 and τ_2 components can be analyzed entirely by sampling according to the time resolution of the combined two-component channel response.

Next, we change τ_2 to 18ns, $\tau_2 \neq n\Delta\tau$. Looking at Figure 32, for each $\Delta\tau$, the responses of the two components are superimposed together. It can be seen that the side lobe of the sinc function appears at the sampling point. And the critical thing is that we cannot directly sample the delayed τ_2 component. Instead, we can only rely on the sampling points on both sides of τ_2, that is, $3 \cdot \Delta\tau$ and $4 \cdot \Delta\tau$ to observe the τ_2 component. In addition, it is worth noting that the τ_1 component will also be affected by the τ_2 component. Although τ_1 lies on $n \cdot \Delta\tau$, its amplitude drops compared to the original response.

Now that we have covered possible distortions in the channel response, we return to the possible results for simulated signals. As shown in (5.1), we can represent the delay components of each path in Figure 33(a). Each stem represents a delayed component. At the same time, it also shows the result of each delayed

doi:10.6342/NTU202303843

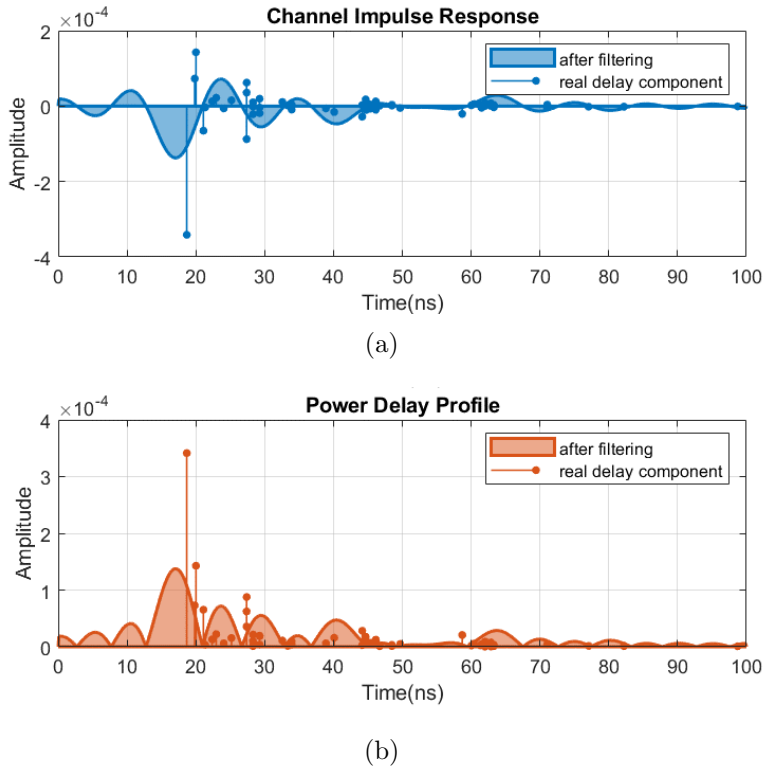


Figure 33: The CIR (a) and power delay curve (b), including the real delay component and the superimposed sinc curve after filtering, $B = 200$MHz.

component being superimposed on each other under the uniform filter of $B = 200$MHz. Figure 33(b) represents the power delay curve, which is the absolute value of the CIR [54].

For the above description, we know that when the bandwidth is infinite, the time resolution $\Delta\tau = -\infty$ can completely separate each path. But it is impossible to achieve infinite bandwidth. Although the restored impulse response is not flawless, it still contains information worth using. Figure 34 shows CIR_{col} and PDP_{col} sampled at $n \cdot \Delta\tau$. If there are multiple paths $|\tau_i - \tau_j| < \Delta\tau$, then τ_i and τ_j are indistinguishable. In other words, all multipaths in PDP_{col} are considered multipath components if their propagation delay difference is smaller than $\frac{1}{B}$. The overall power level of these multipaths is indicated by the matching power level.

According to the above, we know how to obtain PDP by sampling with time resolution. Then we try to calculate CSI with the simulated path, and then convert from CSI to PDP. The result is shown in Figure 35. If the obtained PDP is directly mapped to the positive time axis, in addition to the peak at the beginning, compelling impulse, we will see another peak at the end. This peak is called an invalid impulse, as shown in the red part of Figure 35.

This is actually because of the passband we mentioned earlier. See Figure 29. We know that the total sampling time T_s is related to the frequency resolution

doi:10.6342/NTU202303843

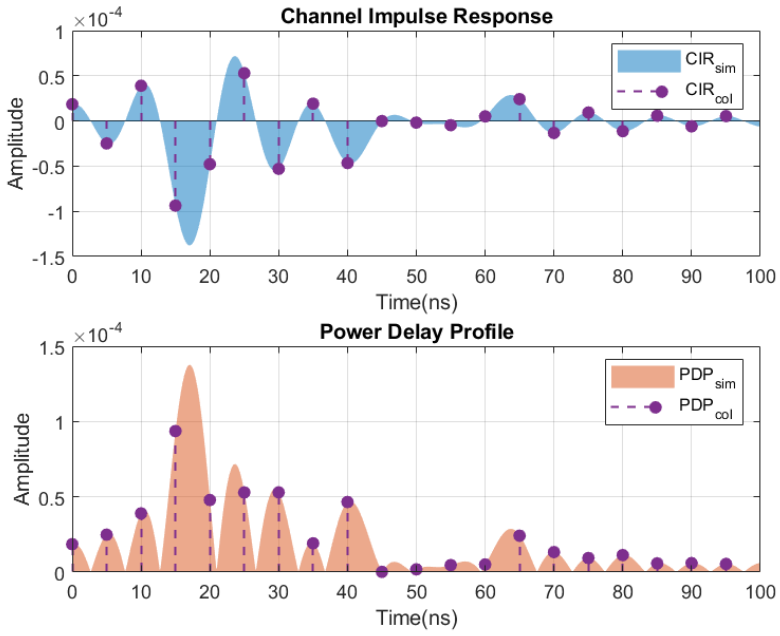


Figure 34: Sampling on $\Delta\tau$, the delay component cannot be completely distinguished. It can only provide an indication of the area where most paths are concentrated.

$\Delta\tau$ [55, 56], the common $\Delta\tau$ is 312.5kHz and 78.125kHz, here we take 312.5kHz as an example, that is, T_s=3200ns. However, due to the actual passband mode, the real sampling period is not in [0,3200]ns, but [-1600, 1600]ns. Therefore, we need to shift the parsed PDP, that is, move the part of [1600, 3200]ns to [-1600, 0]ns, as shown in Figure 35. The invalid impulse mentioned above is actually the channel response from the path where most delays are close to 0ns.

Although T_s can reach 3200ns, the actual effective period is only 1600ns [55,56]. However, most of the signals that can be received by the receiver have a delay of less than 500ns [54], and most of the components that exceed the delay are too weak to reach the receiver due to multiple reflections, diffraction, etc., and what appears is the sidelobes of the sinc function. From the above, it can be concluded that the information after 500ns is actually useless for PDP analysis. There is almost no path component in the extra sampling time.

In order to better understand the effect of PDP on intrusion detection and intruder tracking, we have constructed a simulation environment. We will explain how to obtain critical information from a limited PDP and track intruders in the following section.

doi:10.6342/NTU202303843

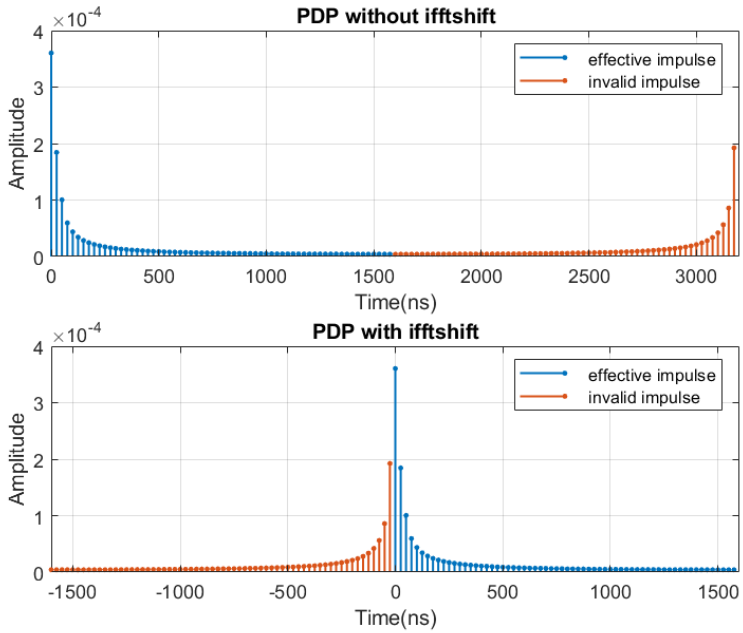


Figure 35: After PDP with ifftshift, the effective pulse time range is [0,1600]ns. Pulses on the negative time axis are invalid.

5.2 Intrusion Information Enhancement

It is known that we can convert CIR from CSI and obtain PDP. Although the PDP contains the information on all the paths, it is also distorted due to interference between the components of each path. Nevertheless, we can still roughly classify all paths by different delays.

According to (5.4), CSI is the uniform sum of all paths. The contribution of each path to CSI differs mainly due to its amplitude. And we know that in space, there are always some among the many paths of signal that are more sensitive to intruders. However, the amplitude may not be as strong as the LoS signal because it has undergone more reflections. Based on the above, we expect to increase the probability of detecting intruders by changing the weight of the path.

5.2.1 Path Component Selection

First, we need to find the delay component most affected by the intruder. The judgment standard is based on the component with the most significant change over a certain period of time W. It is worth noting that the largest variation is not necessarily the largest amplitude component, as shown in Figure 36. Taking the 100th packet as an example, components with larger amplitudes are concentrated at 12.5 ns and 25 ns. However, the most variable component is at 37.5 ns.

doi:10.6342/NTU202303843

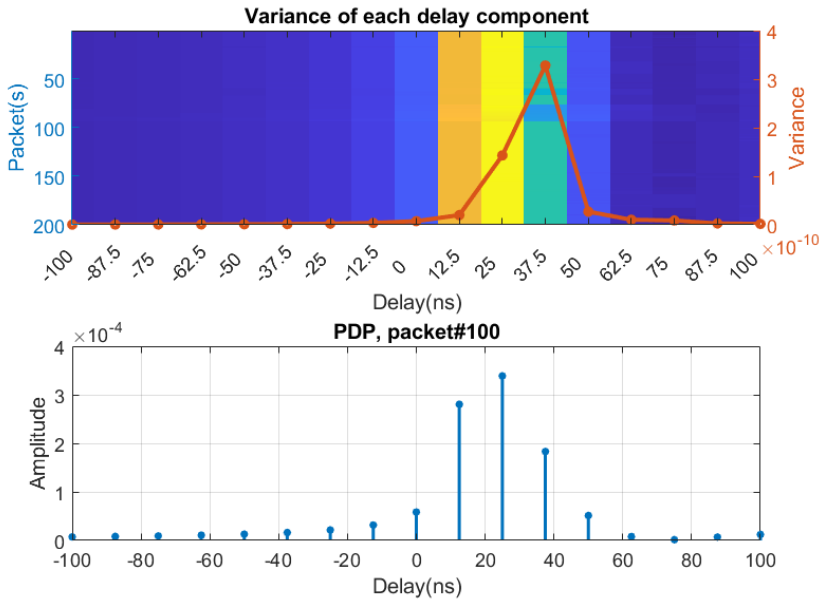


Figure 36: The degree of variation of each delayed component.

The variance is calculated as follows:

$$var(h(\tau)) = \frac{1}{W}\sum_{i=1}^{W}|h_i(\tau) - \mu|^2,\ \mu = \frac{1}{W}\sum_{i=1}^{W}h_i(\tau), \tag{5.9}$$

$h(\tau)$ is a complex matrix, and the variation takes both amplitude and phase into account. Among them, the delay component with the largest variation is the signal we mainly need to enhance.

5.2.2 Weight Changing

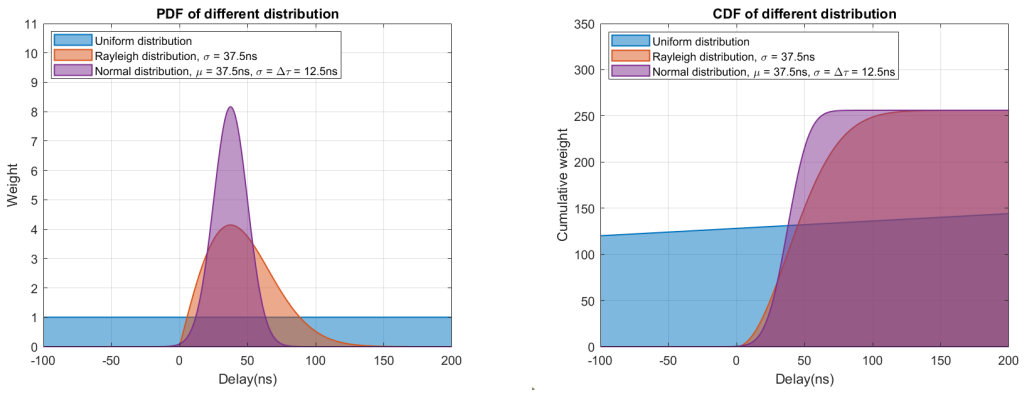
A uniform distribution can be used to represent the general CSI, which is the uniform sum of each path: $f(\tau) = 1$ for $-1600 \leq \tau < 1600$, probability density function (PDF) as shown in Figure 37(a). Here, we take 80MHz, 256 subcarriers as an example. The CSI can be regarded as the sum of 256 path delay component groups, so the endpoint of the cumulative distribution function (CDF) is 256, which is equal to the number of subcarriers.

Consider the scenario where $max(var(h(\tau)))$ is at a delay of 37.5ns, i.e., the delay component weight should be maximized. In order to change the weight distribution method, we consider the Rayleigh distribution and the Normal distribution.

5.2.2.1 Rayleigh Distribution

Rayleigh distribution is a continuous probability distribution for positive-valued random variables. The data can be given by a parameter σ. The PDF of the

doi:10.6342/NTU202303843



(a) (b)

Figure 37: Weights distributed with different probabilities, only display the delay interval of [-100,200]. (i) Uniform distribution, (ii) Rayleigh distribution and (iii) Normal distribution.

Rayleigh distribution is [57, 58]:

$$f(\tau;\sigma) = \frac{\tau}{\sigma^2} e^{-\tau^2/(2\sigma^2)}, \tag{5.10}$$

where σ is the scale parameter of the distribution and also represents the position of the maximum value. Since the distribution starts at 0, the delay components between [-1600,0] will be discarded. But as mentioned in subsection 5.1.2, because the side lobe of the sinc function spreads evenly to both sides, there is still a part of the effective path component in the interval less than 0. In addition, due to its distribution characteristics, when σ is farther away from 0, Rayleigh distribution will become flatter and statistical dispersion will increase.

5.2.2.2 Normal Distribution

Normal distribution (Gaussian distribution) is a type of continuous probability distribution. The general form of its PDF is [59]:

$$f(\tau) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{\tau-\mu}{\sigma}\right)^2}. \tag{5.11}$$

The parameter μ is the mean or expectation of the distribution, while the parameter σ is its standard deviation. We can adjust the degree of weight concentration by controlling the value of the standard deviation. Here we set the standard deviation as $\Delta\tau$. The advantage of the Normal distribution is that it is similar to the characteristic that the side lobe of the sinc function is symmetrically dispersed on both sides. The weight is adjusted forward and backward at the same time. While increasing the target component, it also collects information on both sides of the component. This is similar to restoring the impulse dispersion caused by the sinc function.

doi:10.6342/NTU202303843

Comparing the characteristics of Rayleigh distribution and normal distribution Compared with the requirements of our method, it is more appropriate to adjust the weights according to the normal distribution.

5.2.3 Performance Overview

Compare the original CSI data with the enhanced signal. Figure 38 is illustrated from the simulated CSI signal. In light of the fact that the empty data itself changes very little, even if it is enhanced, it will not adversely affect the original trend of the signal. For data with intruders, emphasizing the path affected by the intruder can greatly increase signal variation. Table 6 simply describes the variance ascension for enhanced signals.

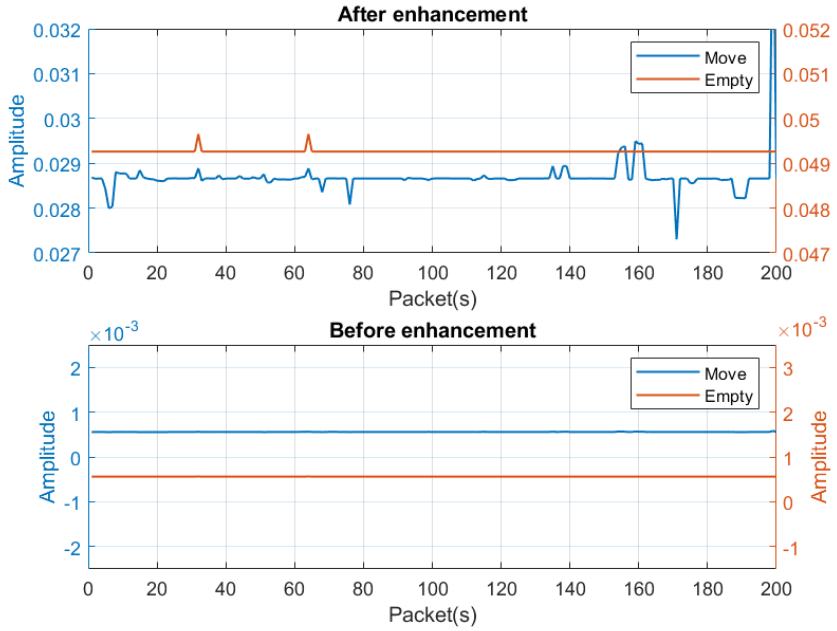


Figure 38: Compare the original CSI data and the enhanced CSI in Amplitude.

Table 6: Comparison of the variances of original CSI and enhanced CSI in amplitude.

	v_{empty}	v_{mov}	v_{mov}/v_{empty}
Original	1.98×10^{-13}	6.92×10^{-12}	**34.9866**
Enhanced	1.52×10^{-9}	2.63×10^{-7}	**172.4844**

Pay attention to v_{mov}/v_{empty}, which represents the gap between empty data and moving data The enhanced signal can effectively increase the ratio of variance of the two scenarios. Performance details will be explained in the next chapter. In

doi:10.6342/NTU202303843

addition to the enhancement of the amplitude, the change in the signal also affects the phase difference. We first verified the effectiveness of this method on simulated signals and then tested it on actual collected intrusion data. The detection effect was significantly improved.

5.3 Intruder Tracking

In terms of the application of PDP, we expect it to be of further benefit in regard to the delay of the signal it can provide. [31] By subtracting the PDP of the empty environment from the PDP of the presence of multiple users, the purpose of tracking users is achieved. In order to obtain as detailed a PDP as possible, the CSI data of multiple channels were spliced together, and 3 receivers were also set up.

We have been inspired by this approach, and the purpose is to achieve a fairly accurate tracking effect while using fewer resources.

5.3.1 Power Delay Profile Difference

Different from obtaining PDP directly, what we will extract is the PDP difference between the empty environment and the intruder environment. The purpose is to know which paths change due to the presence of intruders.

First, before all calculations start, we need to obtain the CSI data of the empty environment, which represents the benchmark for PDP calculations. The next step is to obtain the CSI of the intruder's activities in space. After converting it to PDP, calculate the difference PDP to find the change from the original environment.

Let the CIR obtained from the empty environment be h_{empty}. At time t_0, the intruder is active in the environment, and the collected CIR is h_{hm,t_0}. The PDP difference obtained by subtracting h_{empty} is s_{t_0}, which is calculated as follows:

$$s_{t_0} = abs(h_{empty} - h_{hm,t_0}), \tag{5.12}$$

Figure 39 further illustrates how it works.

We collect packets at different time points along the time axis to obtain discrete PDP differences. Assuming that the total collection time is T, a PDP difference matrix $\mathbf{S}$ with a size of $T \times D$ is obtained. Where D is the total delay time, taking $\Delta f = 312.5$kHz as an example, $D = 1600$ns. So $\mathbf{S}$ can be expressed as:

$$\mathbf{S} = [s_{t_0}, s_{t_1}, \ldots, s_{t_i}, \ldots, s_T]. \tag{5.13}$$

Next, the obtained $\mathbf{S}$ will be processed to track the distance between the intruder and the transmitter and receiver.

doi:10.6342/NTU202303843

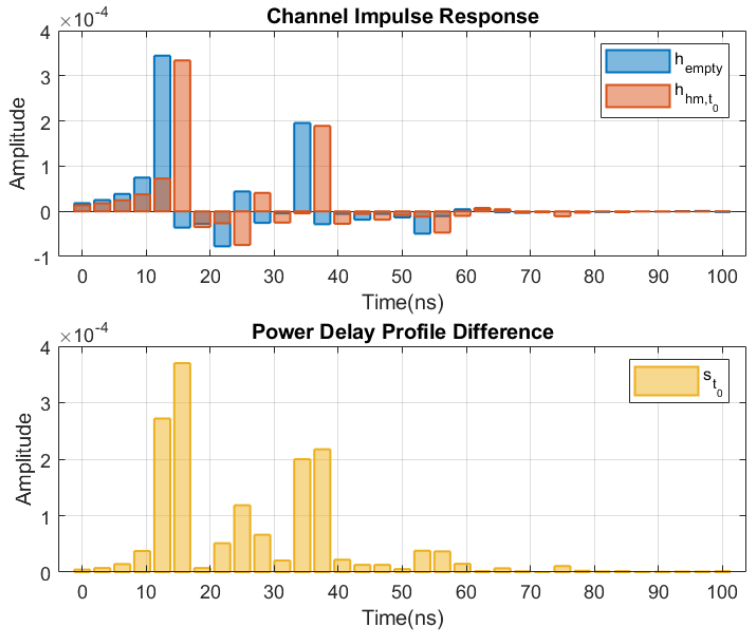


Figure 39: The PDP difference is calculated using the distance between h_{empty} and h_{hm,t_0} on the real part.

We covered a number of features that can be used to detect intruders in Section 3.4. Most features are modified based on variance. This is because the appearance of the intruder itself is the biggest variable in a static environment. Variance is a feature that is simple to calculate but well reflects the changes in the environment. Here again, we choose variance to track the intruders.

We vary $\mathbf{S}$ along the time domain. The purpose is to know which delay component has the largest variation in the time period T. It has nothing to do with the magnitude of the amplitude of $\mathbf{S}$. What matters is the degree of variation, as shown in Figure 40. The obtained variance array is called $\mathbf{V}_T$.

5.3.2 Normalize

Another critical point is that we need to normalize the resulting variance array. This is because, in the case of simulating multiple antennas, the streams of each antenna will be added together to get the final result. Without normalization, one of the streams may be given more weight than other streams, leading to tracking errors. The normalized variance array $\mathbf{V}_{T,norm}$ is represented as follows:

$$\mathbf{V}_{T,norm} = \frac{\mathbf{V}_T - min(\mathbf{V}_T)}{max(\mathbf{V}_T) - min(\mathbf{V}_T)}, \tag{5.14}$$

the results shown in Figure 40 have been normalized. In order to simplify the following description, directly use $\mathbf{V}_T$ to represent $\mathbf{V}_{T,norm}$.

doi:10.6342/NTU202303843

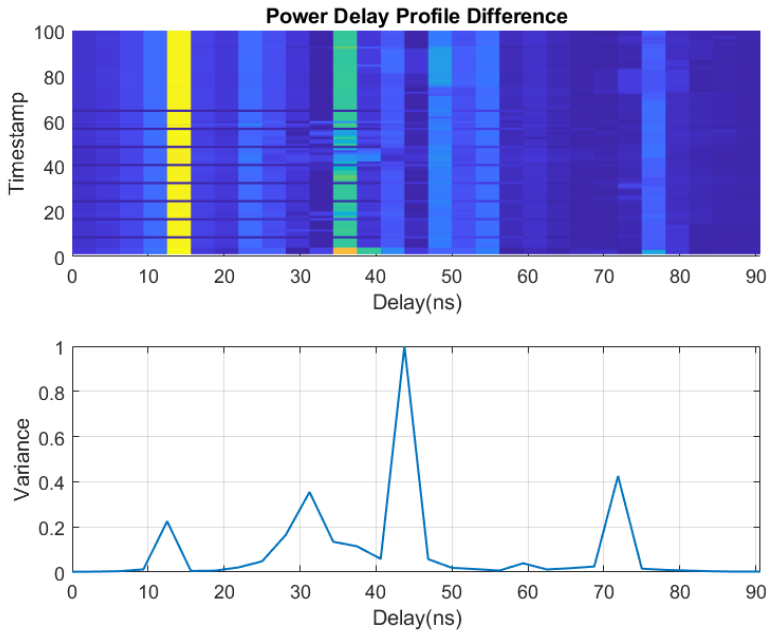


Figure 40: The PDP differences and variance in time domian. The collection time T is 100 timestamps, and the delay interval D is [0,90.625]ns.

5.3.2.1 Effective Delay Interval

Now that the variance of each delayed component in the time domain is obtained, the unreasonable part needs to be dealt with next. We know that due to the side lobe effect of the sinc function, each sampling point will gain more or less. Our purpose is to track the location of the intruder in the target space, so it needs to deal with those components whose delay is less than the LoS delay τ_{LoS}.

$$\tau_{LoS} = \frac{\sqrt{(x_{Tx} - x_{Rx})^2 + (y_{Tx} - y_{Rx})^2}}{c}. \tag{5.15}$$

In fact, it is impossible to have a path shorter than LoS. The reason these unreasonable components exist is due to the relationship between sidelobes and insufficient time resolution. Further thinking, the delay components smaller than τ_{LoS} are mostly composed of sidelobes of τ_{LoS}. In other words, these components are also branches of its components. Therefore, we sum the components smaller than τ_{LoS} and shift the shortest latency to τ_{LoS}. Let the two delayed sampling points closest to τ_{LoS} be τ_l and τ_u, the processed variance array $\mathbf{V}_T = [var(s_{\tau_0}), \ldots, var(s_{\tau_l}), var(s_{\tau_u}), \ldots, var(s_\tau)]$ can be expressed as follows:

$$\mathbf{V}'_T = \left[\sum_{i=0}^{l} var(s_{\tau_i}), var(s_{\tau_u}), \ldots, var(s_\tau)\right]; \tag{5.16}$$

after processing the components of the shortest path, we need to consider the size of the space. Consider the placement of the transmitter and receiver, assuming

doi:10.6342/NTU202303843

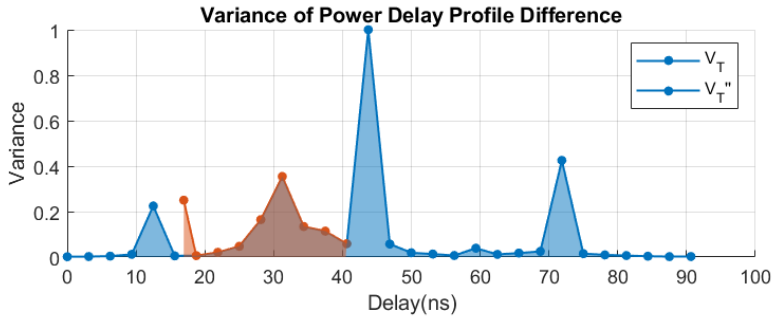


Figure 41: Effective interval of variance array $\mathbf{V}''_T$ of PDP difference.

the farthest distance in space from the devices is d_f, and its delay is τ_f. That is to say, in $\mathbf{V}'_T$, the components whose delay is greater than τ_f can be omitted. Last updated $\mathbf{V}''_T = \left[\sum_{i=0}^{l} var(s_{\tau_i}), var(s_{\tau_u}), \ldots, var(s_{\tau_f})\right]$. The delay interval D is updated as $D = [\tau_{LoS}, \tau_u, \ldots, \tau_f]$, as shown in Figure 41. To simplify the description, the following $\mathbf{V}_T$ all represent $\mathbf{V}''_T$.

5.3.3 Smoothing

It is obviously not an appropriate practice to directly map the delay interval of D to the distance and calculate the intruder's location. First of all, since $\mathbf{V}_T$ is a discrete array analyzed according to time resolution, calculating the distance directly from the delayed sampling point may lead to a large error in determining the location of the intruder. Furthermore, it is better to track the intruder within a certain interval since the intruder is of a certain size. This is because of the intruder's range of activities.

Therefore, we hope that $\mathbf{V}_T$ can be smoothed by some methods, and the intruder's location can be estimated according to its envelope. Time resolution is limited, we need to do difference for $\mathbf{V}_T$. Three different methods were used for testing: Linear, Shape-Preserving Piecewise Cubic Interpolation (Pchip), and Cubic Spline (Spline) interpolation.

5.3.3.1 Linear Interpolation

The linear interpolation of the values at nearby grid points in each individual dimension forms the basis of the interpolated value at a query location [60]. The concatenation of linear interpolants between each pair of data points is what is referred to as linear interpolation on a collection of data points: Linear interpolation on a set of data points $(x_0, y_0), (x_1, y_1), \ldots, (x_n, y_n)$. As a consequence, a continuous curve is produced, which generally has a discontinuous derivative and belongs to the differentiability class $\mathbb{C}^0$.

doi:10.6342/NTU202303843

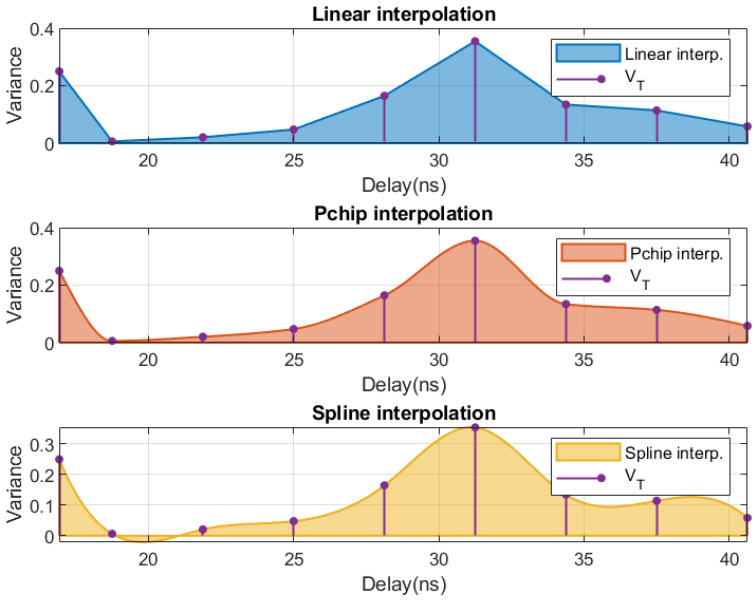


Figure 42: Comparison of $\mathbf{V}_T$ smoothing effects of different interpolation methods.

5.3.3.2 Shape-preserving Piecewise Cubic Interpolation (Pchip)

Pchip interpolation, $\mathbb{C}^1$. The value at a query location is interpolated using a piecewise cubic interpolation that preserves the form of the values at nearby grid points [61]. Using a piecewise cubic polynomial $P(x)$ with the following characteristics, Pchip interpolates:

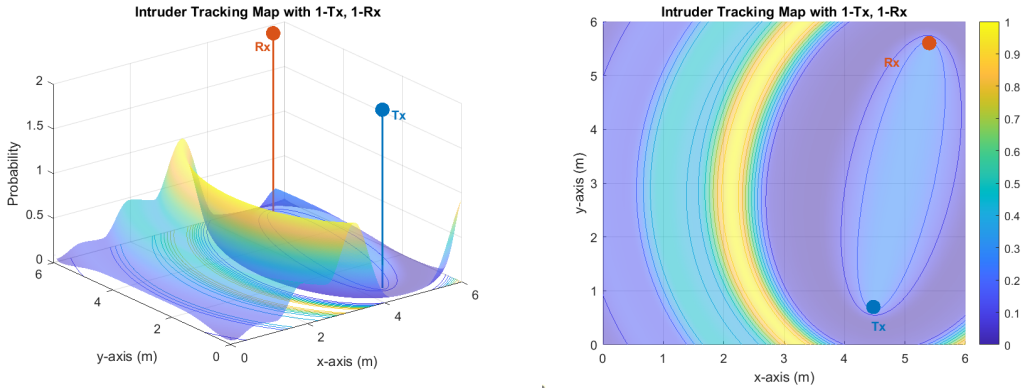
- The polynomial $P(x)$ is a cubic Hermite interpolating polynomial for the provided data points with defined derivatives (slopes) at the interpolation locations for each subinterval $x_k \leq x \leq x_{k+1}$.
- As $P(x)$ interpolates y, the first derivative $\frac{d^2P}{dx^2}$ is continuous and $P(x_j) = y_j$. Jumps at the x_j are probable as the second derivative $fracd2Pdx2$ is probably not continuous.
- The form of the cubic interpolant $P(x)$ is preserved. The slopes at the x_j are selected so that $P(x)$ respects monotonicity and retains the form of the data. As a result, at places where the data has a local extremum, $P(x)$ also has a local extremum on intervals where the data is monotonic.

5.3.3.3 Cubic Spline Interpolation (Spline)

Spline interpolation, $\mathbb{C}^2$, employs not-a-knot end conditions. A cubic interpolation of the values at nearby grid points in each individual dimension serves as

doi:10.6342/NTU202303843

the foundation for the interpolated value at a query location [62]. Similar to how Pchip creates $P(x)$, Spline creates $S(x)$. Spline, on the other hand, selects the slopes at the x_j in a distinctive manner in order to make even $S(x)$ continuous. Here are only three of the implications that this discrepancy has: 1. Splines give results that are smoother and have continuous $S(x)$. 2. If the data consists of values from a smooth function, the spline algorithm delivers a more accurate result. 3. Pchip requires less setup cost.



(a) (b)

Figure 43: Map $\mathbf{V}_T$ to the distance, according to the normalized $\mathbf{V}_T$ represents the probability of the location of the intruder.(a) is the three-dimensional space construction of (b).

After introducing the above three interpolation methods, let us take a look at their respective effects in Figure 42. Obviously, linear interpolation cannot make $\mathbf{V}_T$ continuous. It just connects the points together in a straight line. Both Pchip and Spline have a certain effect on smoothing data. However, the Spline is a bit oversmooth, even showing negative values and unusual peaks. Pchip is smoothed almost along the original $\mathbf{V}_T$ trend.

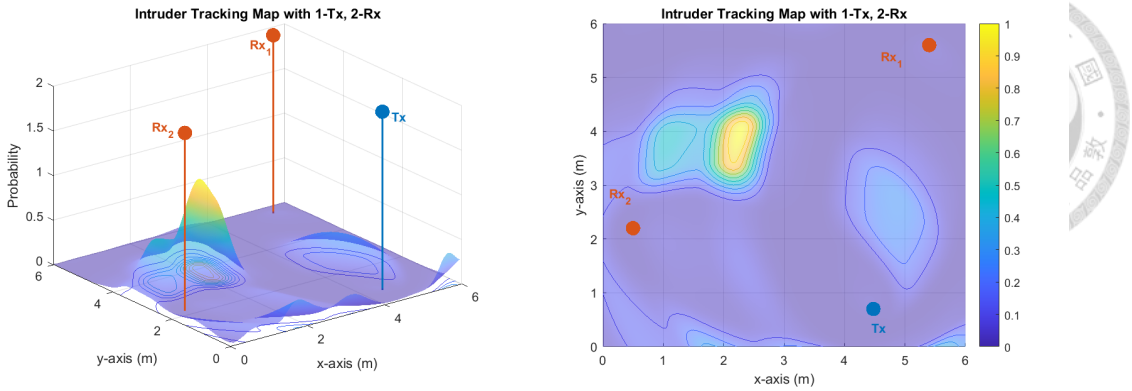
After testing different methods, we finally chose to use the Pchip interpolation method.For the convenience of subsequent description, the smoothed $\mathbf{V}_T$ is still represented by $\mathbf{V}_T$.

5.3.4 Intruder Tracking Map

Based on the information that the intruder's activities affect signaling, we can use $\mathbf{V}_T$ as the probability of how far the intruder is from the transmitter and receiver.

Given the location of the transmitter and receiver, we can calculate the distance between each point in space and the device. We can also convert the delay of $\mathbf{V}_T$ to the distance axis and map it on the map. Assuming a position point (x_0, y_0) in

doi:10.6342/NTU202303843



(a) (b)

Figure 44: Result of intruder tracking with two receivers and one transmitter.(a) is the three-dimensional space construction of (b).

space, the calculation of its distance d_{x_0,y_0} is as follows:

$$d_{x_0,y_0} = \sqrt{(x_{Tx} - x_0)^2 + (y_{Tx} - y_0)^2)} + \sqrt{(x_{Rx} - x_0)^2 + (y_{Rx} - y_0)^2)}. \quad (5.17)$$

For the conversion of $\mathbf{V}_T$ delay and distance, use $d = \tau \times c$, where c is speed of light. The next step is to normalize $\mathbf{V}_T$ again so that the value of $\mathbf{V}_T$ is mapped to the probability, [0,1]. Figure 43 shows the result. We can see that the yellow part represents the range where the intruder is most likely to appear. However, the fly in the ointment is that we cannot track the location of the intruder exactly. The tracking range is a concentric ellipse whose focus is on the transmitter and receiver.

In order to locate the position of the intruder more accurately, we can increase the receiver to get more intruder tracking maps. Add another receiver here, and superimpose the second map on the previous map to get an improved map, as shown in Figure 44. The tracking range of the intruder was obviously reduced from a large circle to a small area.

5.3.5 Algorithm

According to the description of each step above, we write the method of obtaining the intruder tracking map into an algorithm. The input information includes empty environment CSI, intruder environment CSI, transmitter and receiver locations, and target space size. Algorithm 2 will output an intruder tracking map Z of the target space.

In order to better validate our algorithm, we will test it in a simulated environment. In addition to testing the effect of different locations on intruders, experiments are also carried out on hardware device settings, including the use of

doi:10.6342/NTU202303843

different bandwidths and the impact of frequency resolution. The main consideration is to what extent the lack of hardware equipment will affect the tracking effect.

Algorithm 2 Generate intruder tracking map.

Input:
CSI of empty environment, H_{empty};
CSI of intruder environment, H_{hm};
Transmitter Location, (x_{Tx}, yTx);
Receiver Location, (x_{Rx}, yRx);
Target space size, l, w;

Output:
Intruder tracking map, Z;
set bandwidth = B, frequency resolution = Δf;
set number of total streams = N
set the size of $Z = L \times W$;
set delay stamp $\tau = 0 : \frac{1}{B} : \frac{1}{2\Delta f}$;
for $\forall n \in N$ **do**
  $h_{empty,n} = ifft(H_{empty,n})$;
  $h_{hm,n} = ifft(H_{hm,n})$;
  PDP difference $\mathbf{S} = |h_{empty,n} - h_{hm,n}|$;
  Variance $\mathbf{V}_T = normalize(var(\mathbf{S}))$;
  Slice $\mathbf{V}_T$ with delay $\in [\tau_{LoS}, \tau_f]$;
  Smooth $\mathbf{V}_T$;
  for $\forall l \in L$ **do**
    for $\forall w \in W$ **do**
      Calculate the distance between $(x_{l,w}, y_{l,w})$, (x_{Tx}, yTx), (x_{Rx}, yRx), and record the corresponding $\mathbf{V}_T$ in $Z_{l,w,n}$;
    end for
  end for
end for
$Z = \sum_{n=1}^{N} Z_n$;
normalize Z;

doi:10.6342/NTU202303843

CHAPTER 6

PERFORMANCE EVALUATION

First, we will illustrate the performance of the intrusion information enhancement method on a previously constructed detection system. Then we will further introduce the intruder tracking results in the simulated environment.

6.1 Intrusion Information Enhancement Performance

Let us first review the basic detection system. The detection performance will decrease when the intruder is blocked or moves away from the detection device, as shown in position 7 in Figure 20 and position 1 in Figure 24(a). The above situation is mainly because the signal reflecting the intruder is weak, and we can increase the detection rate through appropriate enhancement methods. We will first introduce the difference in features before and after signal enhancement and then further apply the results to the detection system, including model retraining and performance improvement.

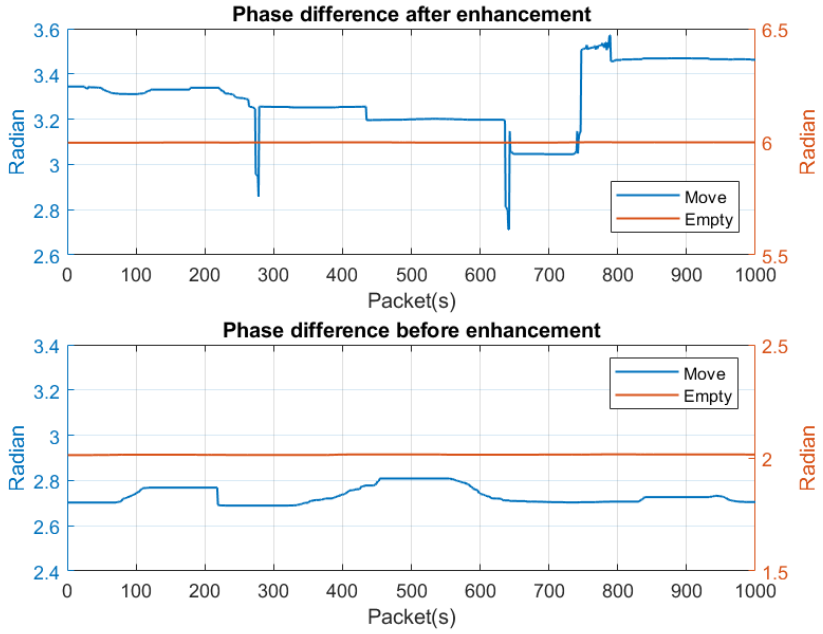


Figure 45: Compare the original and the enhanced phase difference in reality.

doi:10.6342/NTU202303843

Table 7: Comparison of the variances of the original and the enhanced Phase Difference.

	v_{empty}	v_{mov}	v_{mov}/v_{empty}
Original	7.79×10^{-5}	1.26	1.91×10^{4}
Enhanced	1.03×10^{-4}	3.33	5.38×10^{4}

6.1.1 Feature Enhancement

We apply the enhancement method to the intrusion data collected in Section 4.2, and the enhancement effect shows in Figure 45. To better compare the difference before and after enhancement, the Y-axis of Figure 45 has scaled to the same arc range. Move data has noticeable changes after being enhanced, while Empty data maintains a stable trend.

Since the enhancement method cannot identify whether there is an intruder, amplifying the intrusion information will also strengthen the noise, such as the variance features v before and after enhancement in Table 7. However, the degree to which the intruder affects the signal is still far greater than the noise, as we can use the ratio of v_{empty} and v_{mov} to illustrate. If we only compare the v before and after enhancement, we can see that both v_{empty} and v_{mov} have enlarged. But if we compare the value of v_{mov}/v_{empty}, it is evident that the ratio has been magnified by three times, which means that the distance between the empty data and the

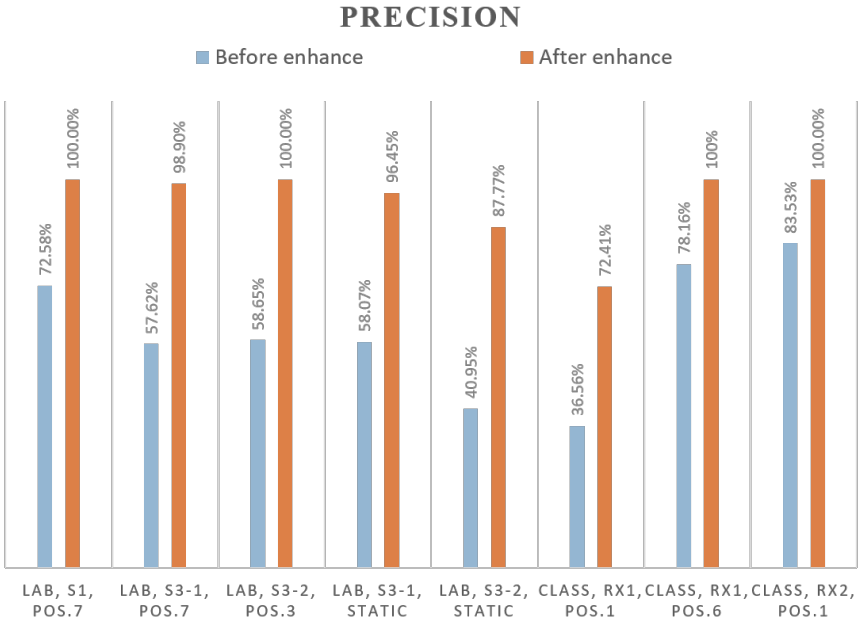


Figure 46: Compare the original and the enhanced intrusion detection performance in blocked position and static intrusion.

doi:10.6342/NTU202303843

Table 8: The precision and false alarm probability of the intrusion detection system, the intruder being blocked will reduce the intrusion precision.

P_{avg}	FA	P_e	P_b
93.69%	0.81%	99.92%	60.77%
98.98%	1.49%	100.00%	94.44%

move data is even greater.

6.1.2 System Performance

We augment all the experimental data and use the new Empty data to train a new OCSVM model. All intrusion detection data judged by the new model significantly improve the detection effect. Since most of the data already have nearly 100% detection accuracy on the primary system, and the same result can achieve after enhancement, only the improved detection performance of those blocked areas showed in Figure 46.

The system's performance before and after enhancement showed in Table 8. The enhancement method can improve the effective area performance from 99.92% to 100% and enhance the average performance on blocked regions to 94.44%. The overall detection rate of the system can increase to about 98.98%.

We compare the system with other studies [16,18,20]. The reason for choosing these systems is that the features used in our system are partially referenced from them, and both use the SVM model for decision-making. The disadvantage of systems using thresholds is that thresholds must be redefined when the environment changes and detection performance will deteriorate over time. Since our method can adapt to different environments and is not affected by the detection time, it is difficult to directly compare with the threshold-based system based on the above differences. So our system only compares with [16,18,20]. The indicators for comparison include system average performance P_{avg}, false alarm FA, fixed-point

Table 9: The precision and false alarm probability of the different intrusion detection systems, the intruder being blocked will reduce the intrusion precision.

	P_{avg}	FA	P_{fixed}	P_{dyn}
Our system	**99.38%**	1.49%	97.87%	100.00%
Wi-Alarm [16]	79.50%	50.31%	91.72%	97.1%
Adaptive RT-IDS [18]	81.89%	25.34%	77.07%	93.94%
Robust P-IDS [20]	72.70%	17.94%	63.20%	88.67%

doi:10.6342/NTU202303843

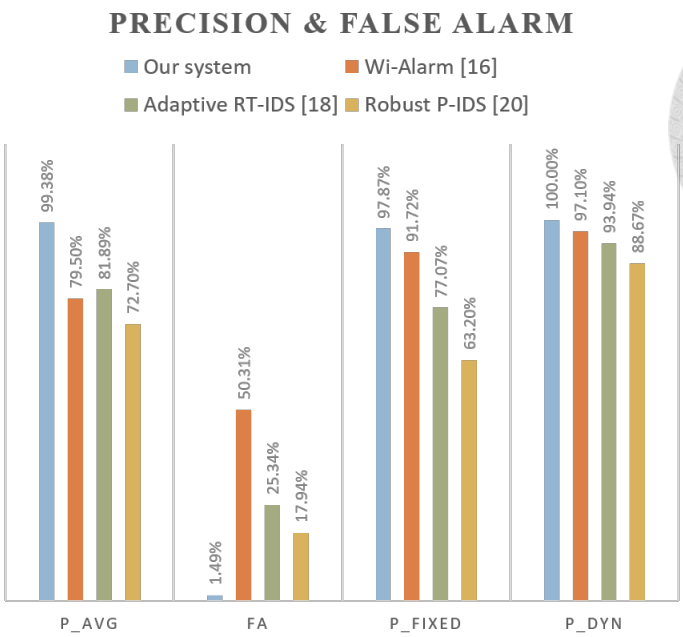


Figure 47: Comparison of detection performance of our system with other studies.

detection performance P_{fixed}, and dynamic motion detection performance P_{dyn}.

It can be seen that the detection rate of all systems can reach more than 88% when intruders are active in a wide range. However, when the intruder is only at a fixed point, and the movement range is small, the detection rates of [16, 18, 20] drop and [20] even drops to 63%. Moreover, the system design of them is prone to false alarms. We found that it is because their systems are not robust enough. Once the environment changes, the chance of false alarms increases a lot.

6.2 Simulator

To prove the feasibility of PDP for our intrusion detection system, we simulate an ideal environment first. It aims to test the effect of different paths on the emergence of intruders.

6.2.1 RayTracing Model

[1] Here we refer to the ray-tracking system constructed based on the RayTracing [63] model in MATLAB. At the same time, it uses STereoLithography (STL) files to build an indoor environment, intruders, and obstacles (such as tables, chairs, etc.) to be observed. RayTracing objects are propagation models that compute propagation paths with 3-D environment geometry [64, 65]. The STL file describes the surface geometry of a three-dimensional object and uses multiple

[1] Thanks to Yi-Hung, Chiang for providing relevant tools to complete the construction of the simulation environment.

doi:10.6342/NTU202303843

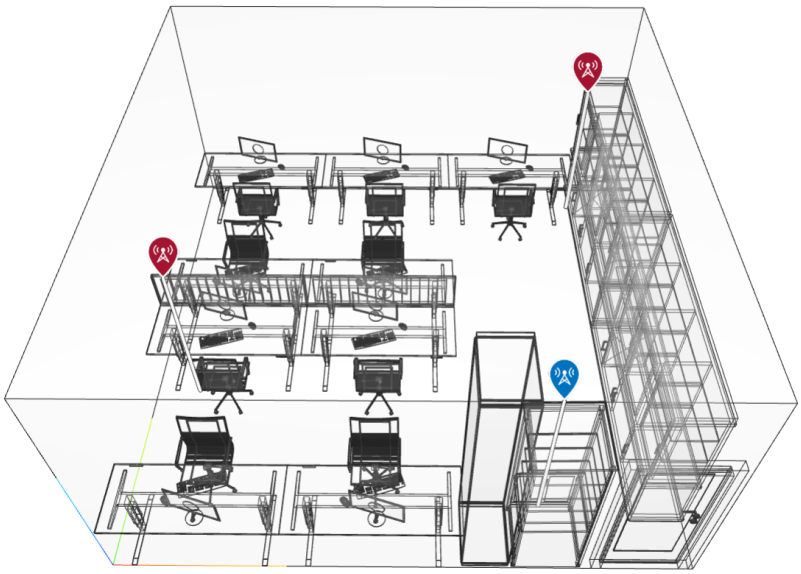


Figure 48: Simulated laboratory environment. The blue mark is the transmitter, and the red marks on the upper right and middle left are receiver 1 and receiver 2 respectively.

triangles to create the target shape.

The entire simulator can roughly divided into three steps: First, you need to use the propagationModel [63] to set the parameters of the signal path to be collected. Next, use RayTracing [63] to generate detailed information for each way. Finally, use comm.RayTracingChannel [66] to adjust the ray according to different channel settings.

6.2.2 Environment and Intruders

The purpose of the simulation is to be able to be applied in the real environment, so the simulated space and the settings for the hardware are all referenced

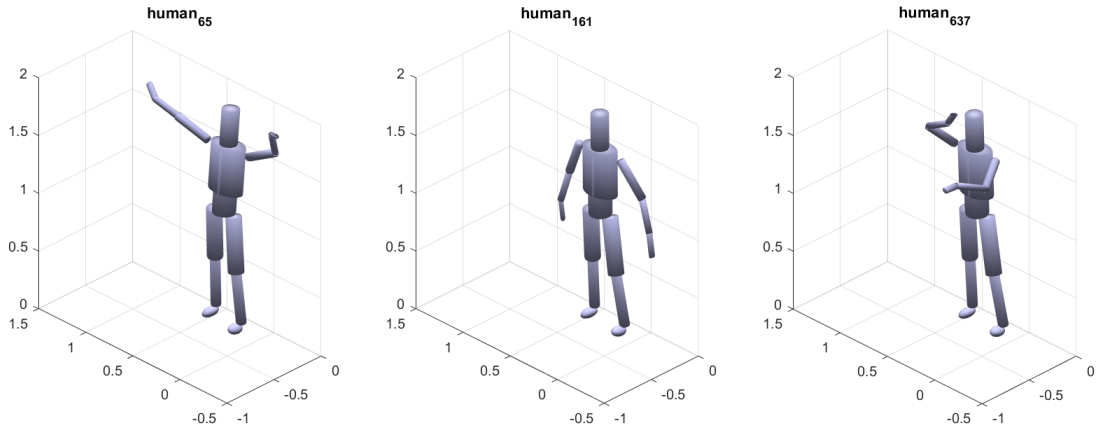
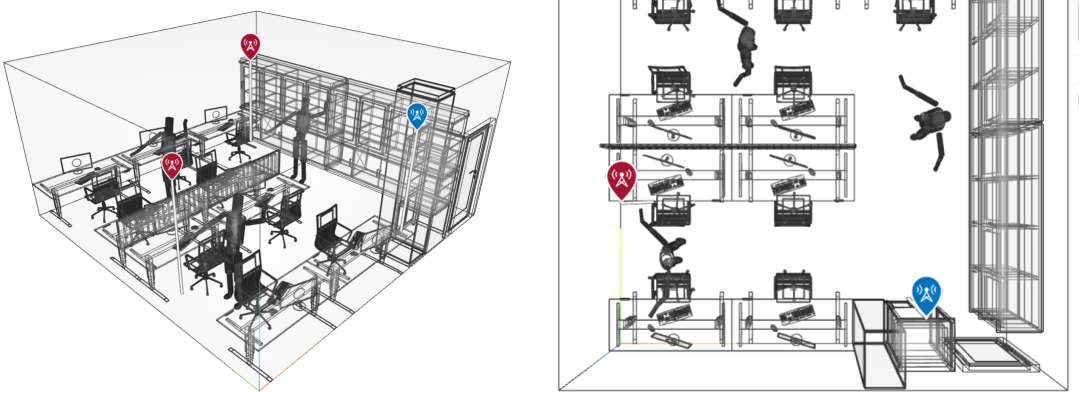


Figure 49: Simulated intruder behavior: waving.

doi:10.6342/NTU202303843



(a) (b)

Figure 50: What the intruder looks like in the simulated space, and the location of the transmitter and receiver.

from the real scene.

According to the space size of the actual laboratory and the placement of objects, we simulated a space with a size of 6m×6m×3m. The door is on the right, there is a shoe cabinet on the left side of the door, the system cabinet is placed on the right side of the space, tables, and chairs are neatly placed in other positions, and there are screens, keyboards and mice on the table.As shown in Figure 48.

We used a transmitter and two receivers to track the intruder. Their placement is shown in Figure 48. The blue mark represents the transmitter, and the red mark is the receiver. Connect the devices according to the placement position, and you can see that their shape is similar to the letter L. The purpose of this arrangement is to maximize the use of the concentric ellipse characteristics of the tracking map. Overlapping two tracking maps perpendicular to each other creates a checkerboard pattern.

After establishing the target space, we need the invaders. The data used to simulate the movements of the attendants came from the KIT Whole-Body Human Motion Database [67]. The requirement for the intruder's action is to be able to perform activities at a fixed location. Finally, he must choose to let the intruder perform a waving action at a designated location. The approximate activity of an intruder is shown in Figure 49. The data collection frequency is 100Hz. The figure shows the intruder's actions at the 65^{th}, 161^{st}, and 637^{th} timestamps respectively.

As for where the intrusions are located in the target space, we designed three distinct locations. Because in the simulated laboratory space, the space in which

doi:10.6342/NTU202303843

the intruder can move is like a letter U rotated 90 degrees. This is symmetrical along the X-axis. The intruders are at three different locations in the space. For two transmitter-receiver pairs, Tx-Rx_1 and Tx-Rx_2, the intruders are located at LoS and nLoS at two different distances from the device pair, respectively. Such a design allows the measurement of the different distances between the two device pairs and the intruder. Figure 50 shows what the intruder looks like in the simulated space, and the location of the transmitter and receiver. The exact coordinates p_1, p_2 and p_3 of the invaders on the map are: (4.55, 3.35), (1.95, 4.45) and (0.85, 1.45).

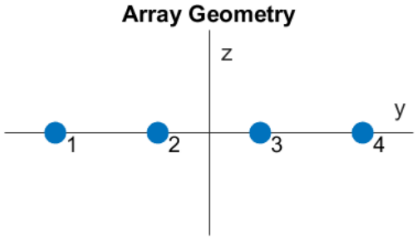
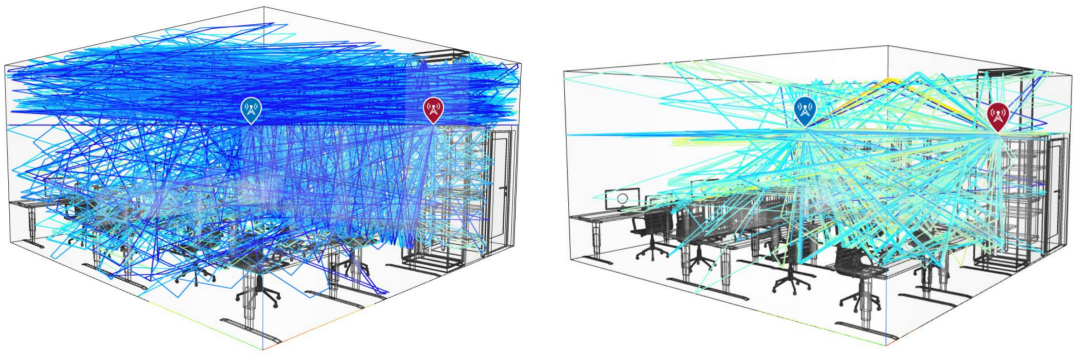


Figure 51: The position of the four antennas of the receiver. The antennas are arranged along the Y-axis.

6.2.3 Settings

In this subsection, the setup of the entire simulation space will be described in more detail. This includes the transmitter and receiver antennas, the used bandwidth, and the number of subcarriers. In addition, the value of the simulated space and intruders, the reflection and diffraction of the simulated path, etc.

First, the transmitter and receiver settings are described: the number of transmitter antennas is set to 1, and the number of receiver antennas is 4, which are



(a) (b)

Figure 52: Rays with different combinations of maximum reflection number and maximum diffraction number in the simulated environment, (a) is (0,10) and (b) is (1,1).

doi:10.6342/NTU202303843

evenly distributed along the Y-axis. This setting refers to the LWR-X8460 device used in the previous chapter. The spacing between the antennas is $\lambda/4$, where λ is the wavelength, $\lambda = \frac{c}{f_c}$, c and f_c represent the speed of light and the center frequency respectively, and the center, f_c, is set at 5GHz. The positions of the 4 antennas of the receiver are shown in Figure 51.

For bandwidth setting, the current commercial AP uses the IEEE 802.11be protocol, which can reach up to 320MHz and 4096 subcarriers. So we set the maximum simulation bandwidth to twice the 320MHz, 640MHz. Considering that the average household may not use such high-level devices, we also checked the effect of low bandwidth.

Regarding the setting of subcarriers, as mentioned in Section 5.1.2, the time resolution of the power delay profile mainly comes from the total bandwidth. Frequency resolution affects the length of delay traceable back. However, components with delays beyond 500ns are useless. Nevertheless, IEEE 802.11be can obtain 4096 subcarriers by shortening Δf to 78.125kHz, but for our goal, the time resolution of 312.5kHz is sufficient. Therefore, the maximum number of subcarriers is set to 1024, and each subcarrier is spaced at 312.5kHz.

Next is a description of the simulated environment. Due to the parameter limits of the propagationModel module, all items in the target space can only be set to the same material. Here we set all materials to concrete, which has a reflectance of about 0.4 [68]. In fact, the reflection coefficient of human skin is about 0.7. It can be seen from (3.10) that if the influence of noise is not considered, only from the perspective of reflection, the simulated path loss will be more than the actual one, that is, the signal attenuation is larger.

The module also provides settings for the maximum number of reflections and the maximum number of diffractions. Before that, we explain AngularSeparation, which is a parameter provided by the module to set the total number of rays emitted. We set this parameter to low, which means that the angle between each ray is relative to the other. According to the documentation, up to a total of 655,362 rays can be emitted. Going back to the description of the maximum

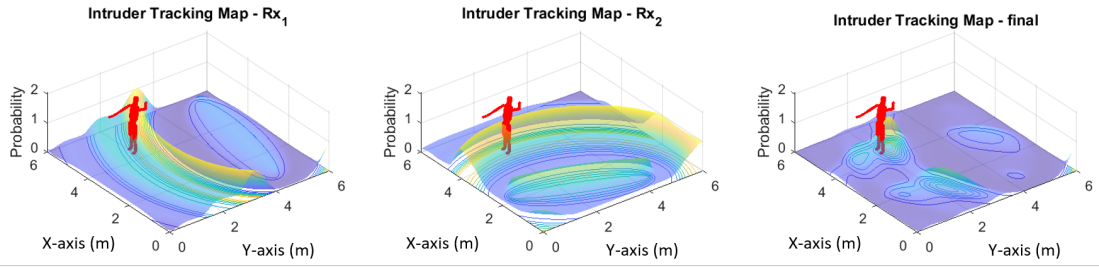


Figure 53: Overlaying two maps to get the final intruder tracking map.

doi:10.6342/NTU202303843

number of reflections, assuming it is n, and when all rays are emitted, those rays with a reflection number greater than n will be discarded. The same applies to the maximum diffraction number. Diffraction is the phenomenon that multiple rays are scattered due to rays passing through the edge of the object. We conduct tests on setting different reflection and diffraction quantities, mainly to find the most suitable combination. This allows the rays to cover the target space more completely. In addition, the time calculation cost–performance ratio is higher.

Explain the two combinations $(r_1, d_1) = (0, 10)$, $(r_2, d_2) = (1, 1)$ of the maximum reflection number and the maximum diffraction number. Case 1 (r_1, d_1) is shown in Figure 52(a), the captured rays cover most of the space, the total number of rays is 637, and the calculation time is 9.935628s. The result of case 2 (r_2, d_2) is shown in Figure 52(b). Compared with case 1, the rays are more concentrated near the transmitter and receiver, the total number of rays is 726, and the calculation time is 1504.157s. Judging from the results, the number of rays obtained by the two cases is almost the same. However, since our purpose is to track the intruder, rays need to cover the target space more comprehensively. The calculation time of case 2 is much longer than that of case 1, so in this simulation, the maximum reflection number and the maximum diffraction number are finally set as $(r, d) = (0, 10)$.

Figure 54: Comparison of scores before and after enhancement between simulated data and experimental data.

doi:10.6342/NTU202303843

6.3 Intrusion Detection in Simulated Environment

Although it has been shown in the previous subsections that our enhancement method can effectively improve the detection precision, here we try to restore the detection scenario of the real scene with the simulator. In addition to testing the detection effect in the simulated environment, it is also to prove the reliability of the signal using the RayTracing model.

6.3.1 Score Perfoemance

First, let us explain the limitation of the simulator on the intrusion detection part: Since rayTracing can only simulate the reflection and diffraction of the path, it cannot simulate the part where the radio wave penetrates the material, so the blocked position in the simulation is not as perfect as in the experiment blocked by pillars. In addition, it is difficult for the simulator to simulate a static case, because the simulated human body objects cannot have slight breathing changes like real humans. If the simulated intruder is set to remain still, it is just an additional obstacle in the space. To sum up the above, the intruder in the simulation cannot be completely blocked, and the static case is not suitable for simulation, so that the intrusion detection accuracy in the simulation will be better than the actual experiment.

In order to restore the actual scene as much as possible, we added AWGN and controlled the SNR at 50 dB, so that the simulated signal could be very close to the experimental data without hardware hopping. Due to the limitations of RayTracing, it is challenging to act further on the hoppings caused by hardware defects. We will not repeat the discussion of the detection effect of the ideal position here but mainly introduce the performance of those slightly blocked locations, and compare the performance of the enhanced intrusion information with the experiment.

Since the simulated situation is difficult to completely restore the difficulties encountered in the experimental environment, even if the intruder is slightly blocked, it can still be detected 100%, so it is inappropriate to directly evaluate the per-

Table 10: Comparison of the average score and score difference before and after enhancement between simulated data and experimental data.

	SCORE_{before}	SCORE_{after}	$\text{SCORE}_{before} - \text{SCORE}_{after}$
Simulation	-3.65×10^{-7}	-6.00×10^{-8}	-3.06×10^{-7}
Experiment	6.73×10^{-13}	-1.00×10^{-12}	-1.67×10^{-12}

doi:10.6342/NTU202303843

Table 11: Bandwidth and corresponding subcarriers, time resolution and distance offset.

Bandwidth	Subcarriers	Time resolution	Distance offset
20MHz	64	50ns	15m
40MHz	128	25ns	7.5m
80MHz	256	12.5ns	3.75m
160MHz	512	6.25ns	1.87m
320MHz	1024	3.125ns	0.94m
640MHz	2048	1.5625ns	0.47m

formance from the detection precision, but we can still observe the enhancement effect from other aspects. When the data is passed through the classifier trained by OCSVM, a score will be obtained. When the score is less than 0, it will be judged as abnormal by the classifier, which means that there is an intruder. We can evaluate the performance of the augmentation method by observing the change of this score.

Looking at Figure 54, the main simulated scene and the intruder's position is position 7 of laboratory Scenario I. Only part of the data is displayed for the convenience of viewing the detection performance. We judged from the 100 packets shown in the figure that the simulated environment scores are very close to 0, but they are still less than 0, and the intruder can be completely detected. The data in the actual environment is not ideal, only 38% are detected. Then compare the scores before and after enhancement, and we can see that the scores of both the simulation and the actual environment have decreased. More intuitively, from the experimental data, the detection rate can be increased to 77% after enhancement. The average score and score difference before and after the enhancement of the two data can be viewed in Table 10.

When the enhancement method is applied to the simulated data, the score drops significantly, proving that it performs well for intrusion signal augmentation.

6.4 Intruder Tracking Performance

In this subsection, we will illustrate the effect of PDP applied to intruder tracking. Since the size of the simulated target space is 6m×6m, if the bandwidth used is below 80MHz, it will be difficult to track the intruder. The time resolutions of bandwidth 20MHz and 40MHz are 50ns and 25ns respectively. These are about

doi:10.6342/NTU202303843

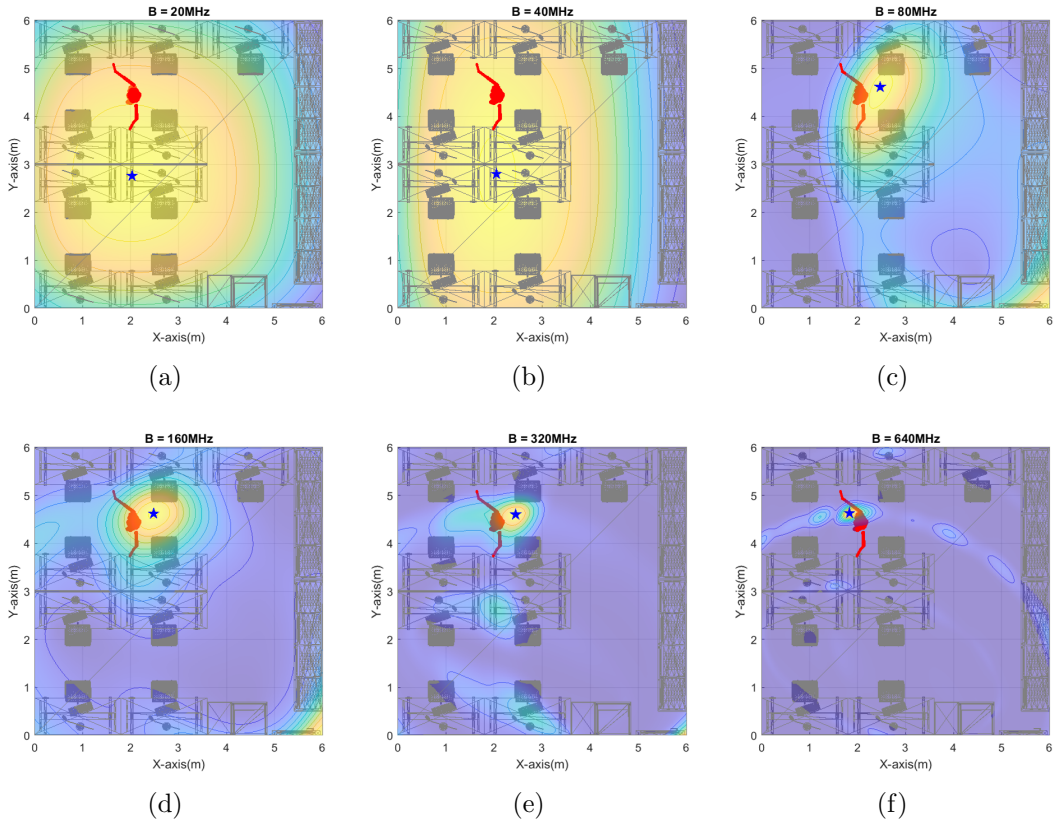


Figure 55: Intruder tracking results using different bandwidths: (a) 20MHz, (b) 40MHz, (c) 80MHz, (d) 160MHz, (e) 320MHz and (f) 640MHz, where $p_{hm} = (1.95, 4.45)$.

15m and 7.5m when converted to distance. Therefore, the effective bandwidths are 80MHz, 160MHz, 320MHz and further 640MHz respectively.

The simulated environment has one transmitter and two receivers. We multiply the tracking maps obtained by the two links to obtain the final intruder tracking map, as shown in Figure 53. For the convenience of viewing, the display of the follow-up results will be displayed in plan view, so that the distance between the tracking position and the intruder can be seen more clearly.

Tracking results will be explained separately for different bandwidths, including the distance between the tracking point and the actual location of the intruder, the tracking range, and so on.

6.4.1 Bandwidth

The number of subcarriers that can be used in varied bandwidths is different. The time resolution is also changed due to the size of the bandwidth, which also affects the tracking offset. We sorted out the information on the number of subcarriers, time resolution, and distance offset under different conditions in Table 11.

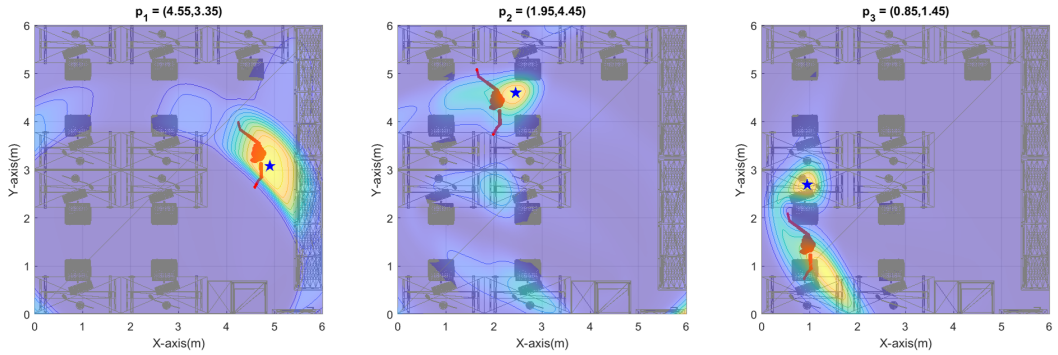
doi:10.6342/NTU202303843

Table 12: Tracking offsets and scores at different bandwidths, $p_{hm} = (1.95, 4.45)$.

BANDWIDTH	$\lvert p_{trk} - p_{hm} \rvert$	SCORE OF p_{hm}	SCORE OF p_{trk}
20MHz	1.6919m	1.0904	1.1323
40MHz	1.6530m	1.1927	1.2211
80MHz	0.5440m	0.6114	3.6457
160MHz	0.5566m	0.1401	5.5614
320MHz	0.5220m	0.0830	12.1040
640MHz	0.2163m	1.0729	49.2084

In the case of no change in the simulated environment, we fixed the movement and position of the intruder. We observed the impact of different bandwidths on tracking performance. The results of the intruder tracking map are shown in Figure 55. The blue pentagram represents the most likely position of the intruder, and the actual position of the intruder $p_{hm} = (1.95, 4.45)$.

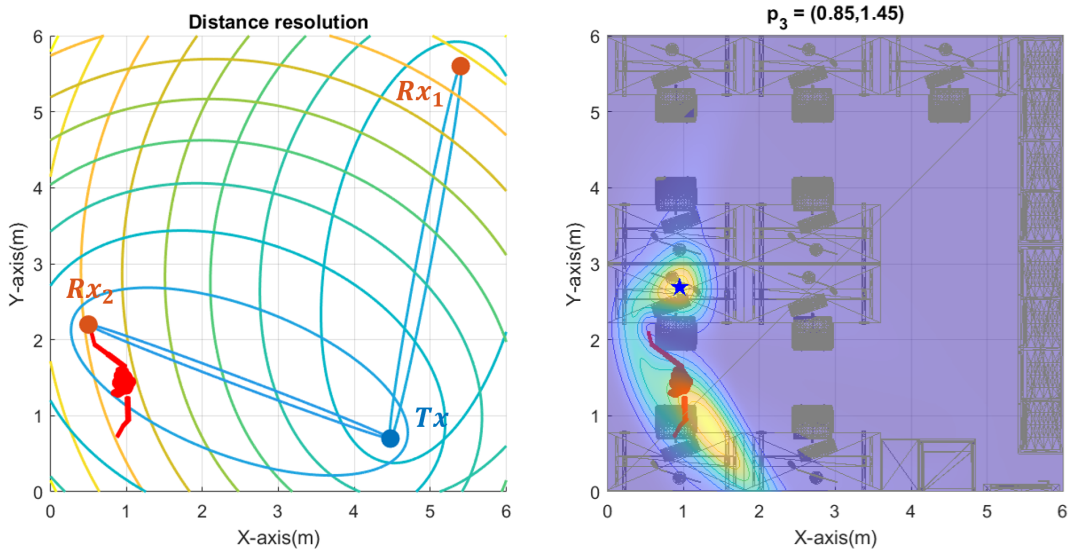
The tracking position is p_{trk}, and the Table 12 shows the deviation between p_{trk} and p_{hm} and the score of p_{hm} on the tracking map. We cut the map in centimeters, and there will be 600 $/times$ 600 points in total, and the total score is 3,600. The higher the score, the more likely the intruder is at that position. Observe Figure 55(c) and Table 12, even if only using 80MHz bandwidth, the tracking offset can still be around 0.5m. But because the given possible range is larger, the score of p_{trk} is only 3.6457. By analogy, the possible range of intruders given by the tracking map will shrink as bandwidth increases. When the bandwidth reaches 640MHz, the score of p_{trk} rises to 49.2084, and the tracking error is also reduced to only about 0.22m.



(a) (b) (c)

Figure 56: Tracking results of intruders at different positions: (a) $p_1 = (4.55, 3.35)$, (b) $p_2 = (1.95, 4.45)$ and (c) $p_3 = (0.85, 1.45)$, where B =1024MHz.

doi:10.6342/NTU202303843



(a) (b)

Figure 57: The distance resolution diverges from the transmitter and receiver as concentric ellipses.

However, if we observe the score difference between p_{trk} and p_{hm}, the wider bandwidth will have a larger score difference. This is because when the time resolution is increased and the focused range is reduced, the score will be densely concentrated on the target point.

6.4.2 Intruder Position

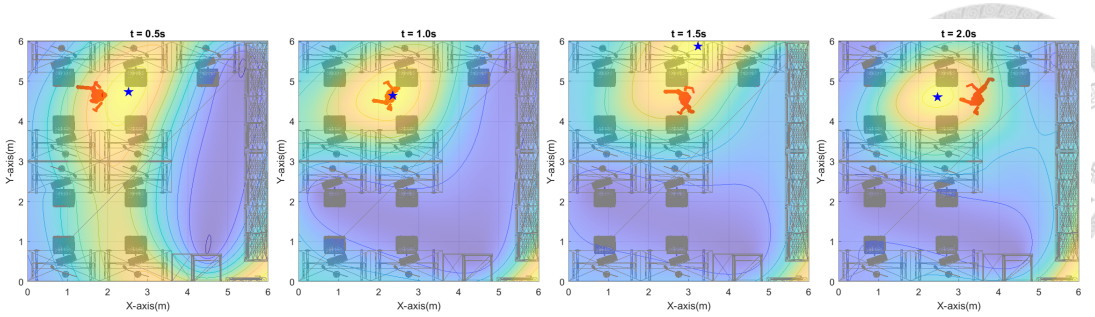
In this subsection, we will test the scenario where the intruder is located at different positions. Select 320 MHz to observe the tracking effect in more detail. Tracking performance is shown in Figure 56.

When the position of the intruder is at p_1 and p_3, even if the bandwidth is set to 320 MHz, the tracking range does not shrink much. This is so that we can determine how far an intruder is from the transmitter and receiver when using our way of tracking them. The distance resolution is a concentric ellipse with the transmitter and receiver as focal points outward, as shown in Figure 57(a). In the

Table 13: Tracking offsets and scores at different positions, B=320MHz.

Position	$\lvert p_{trk} - p_n \rvert$	score of p_n	score of p_{trk}
$p_1 = (4.55, 3.35)$	0.4421m	1.9851	11.8639
$p_2 = (1.95, 4.45)$	0.5220m	0.0830	12.1040
$p_3 = (0.85, 1.45)$	1.2440m	15.0930	15.9578

doi:10.6342/NTU202303843



(a) (b) (c) (d)

Figure 58: Intruder walks with time in 80 MHz, t = (a) 0.5s, (b) 1.0s, (c) 1.5s and (d) 2.0s.

range closer to the transmitter and receiver, blue ellipse, the distance difference along the normal is longer than yellow ellipse, which is farther from the device. Therefore, when an intruder approaches the LoS between devices, the tracking range expands, and there is also a large tracking offset.

Table 13 shows the distance offset between p_{trk} and the actual intruder position $p_n, n \in [1, 3]$ and the tracking score of p_n. Although the distance between p_3 and p_{trk} has the largest deviation, the tracking score of the intruder's location is as highest.

6.4.3 Walking Intruder

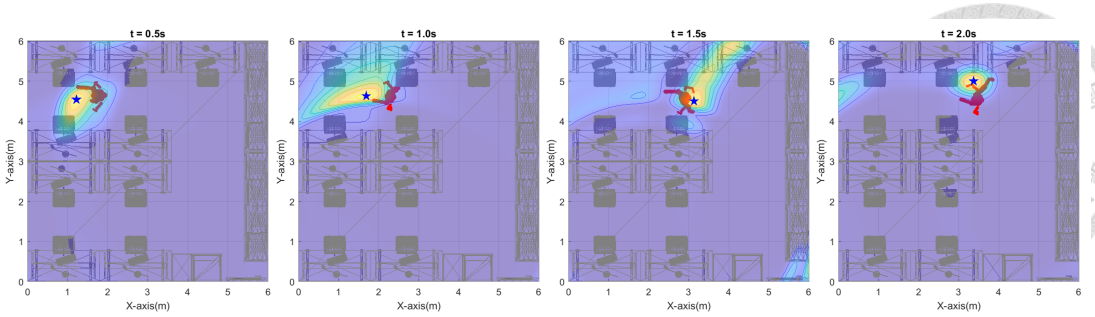
The intruder tracking map is further applied to continuously moving intruders. Using a sliding window, we take about 1 second of data to determine the intruder's position. Since the intruder constantly moves and changes the target position during the sampling interval, the tracking range is sometimes more extensive than if the intruder is stationary. This is shown in Figures 59(b) and 59(c).

Evaluating tracking offset requires the exact location of the intruder. We set the intruder position at the midpoint of the sampling time as p_{hm}. That is to say, when the sampling time is [0.0,1.0]s, then p_{hm} is the intruder's position at t =0.5s. In this test, the average tracking offset using the 80 MHZ bandwidth is 0.7987m; the average tracking offset using the 320 MHZ bandwidth is 0.4481m, and the minimum and maximum offsets are shown in the Table 14 as shown. Even if the

Table 14: The average, minimum and maximum tracking offset of the intruder while walking.

$\lvert p_{trk} - p_n \rvert$	Average	Maximum	minimum
80 MHz	0.7987m	1.3256m	0.1077m
320 MHz	0.4481m	0.5608m	0.2973m

doi:10.6342/NTU202303843



(a) (b) (c) (d)

Figure 59: Intruder walks with time in 320 MHz, t = (a) 0.5s, (b) 1.0s, (c) 1.5s and (d) 2.0s.

device's bandwidth cannot be used to 320 MHz, the tracking offset will not be too large with only 80 MHz.

6.4.4 Noise

To be closer to the actual environment, we add Additive white Gaussian noise (AWGN) to the simulated ideal CSI signal and set the Signal-to-noise ratio (SNR) to 15 dB. This level of SNR is the standard lower limit for the smooth transmission of signals, and even a small SNR will lead to poor signal communication. The CSI disturbed by the noise is shown in Figure 60, and the amplitude and the phase are influenced to a certain extent.

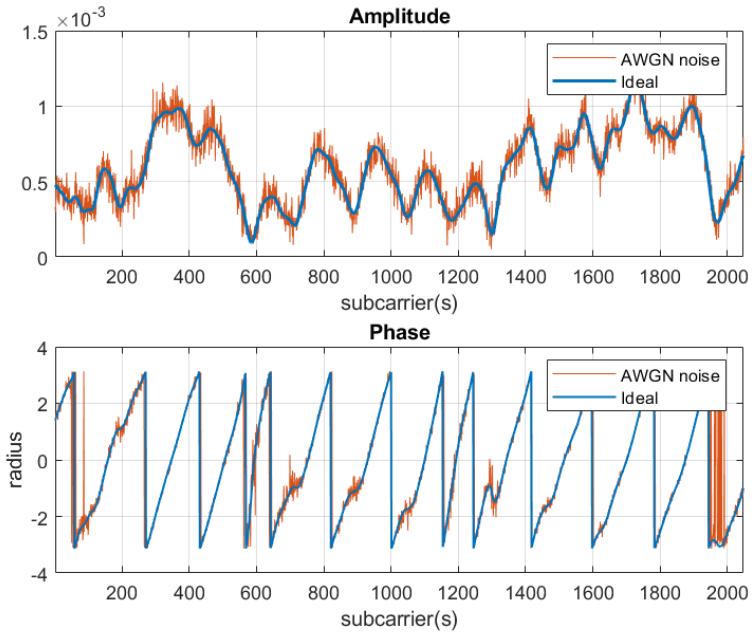


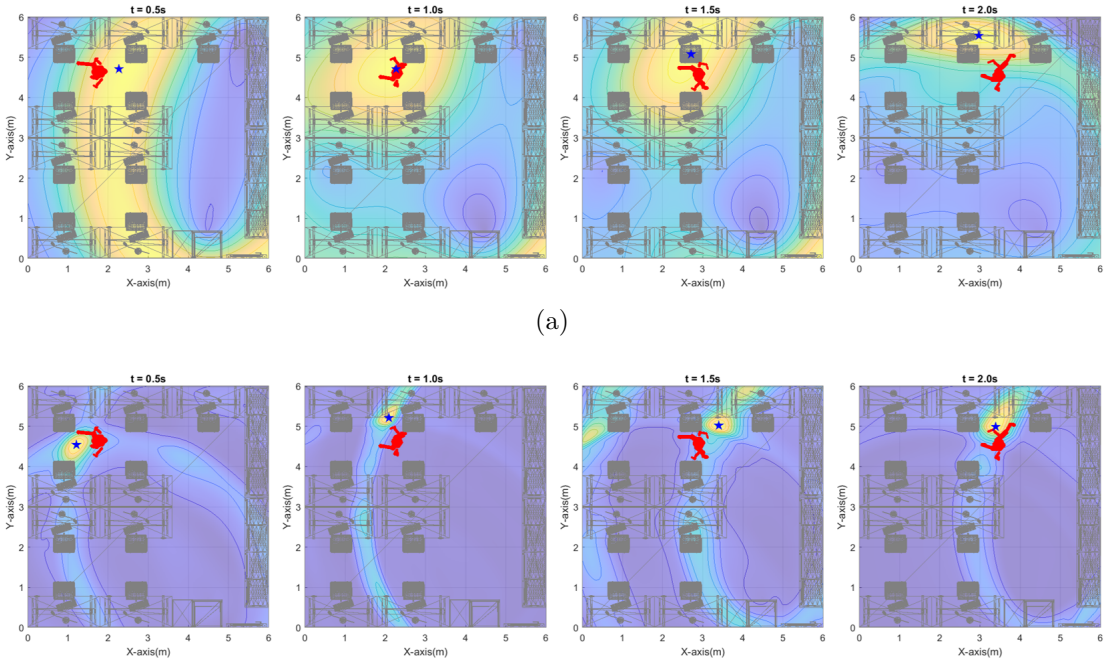
Figure 60: Amplitude and phase changes of the simulated CSI after being disturbed by AWGN.

doi:10.6342/NTU202303843

Table 15: The average, maximum, and minimum tracking offsets after adding AWGN to the CSI data of walking intruders.

Bandwidth	$\lvert p_{trk} - p_n \rvert$	AVERAGE	MAXIMUM	MINIMUM
80 MHz	Ideal	0.7987m	1.3256m	0.1077m
	AWGN	0.8808m	1.2436m	0.1112m
320 MHz	Ideal	0.4481m	0.5608m	0.2973m
	AWGN	0.5641m	0.6920m	0.4401m

The simulation results can be seen in Table 15. At 80 MHz bandwidth, the average tracking offset is 0.8808m; at 320 MHz bandwidth is 0.5641m. The offset of the tracking point calculated by the current algorithm is slightly increased, but it is all controlled at about 10cm. From [54] we can know the phase error which affects the PDP the most, but even if AWGN is added to the simulated phase, the error is still far from the error of the actual environment. The reason is that the most critical influence on the phase is the delay from the SFO, which will make the phase of the entire signal very random. Further calibration for the CSI phase is required to apply the algorithm to practical experiments.



(a)

(b)

Figure 61: Intruder walks with AWGN, $B =$ (a) 80 Mhz and (b) 320 MHz.

Overall, the performance of our algorithm in an ideal environment using the existing maximum bandwidth can make the average tracking error as small as 0.45m, and compared with other studies, the computational complexity and CSI

doi:10.6342/NTU202303843

information requirements are relatively much lower.

doi:10.6342/NTU202303843

CHAPTER 7

CONCLUSION AND FUTURE WORK

The information explosion makes People increasingly concerned about their privacy and security. In contrast, the user may not be willing to install a monitor to prevent intruders from entering their personal space because of privacy concerns. CSI is an excellent source of information. Wi-Fi is everywhere, in homes, offices, and mass transit. When people do not turn off the Wi-Fi when they leave the house, we can take advantage of the still-running AP. In addition to improving environmental security, it also increases AP use value.

7.1 Intrusion Detection System

After we read many kinds of research on intruder detection, we found some flaws in the existing research, such as the detection effect will drop when the intruder is occluded or only performing static activities. And some systems are not accurate enough for CSI feature selection, which makes the system easily invalidated due to environmental changes. Test results show that even if some systems effectively detect fixed-point intruders, the probability of false alarms is as high as 50%. Overdetection is not how a sound system should behave.

We selected more powerful features based on common intrusion system architectures, which are sensitive to the presence and activity of intruders, and are also stable in an empty environment. In addition, we also performed some preprocessing on the CSI signal, so that the phase difference can compensate for the lack and instability on the hardware more than the amplitude, which is opposite to the amplitude usually used in most studies. Considering the difficulty of executing the system, we choose OCSVM as the intrusion decision model. The model is less expensive to train and more resistant to different intruder behaviors.

The detection effect of the model constructed based on the above method is better than that of most systems, but we found that there is still room for improvement in the performance of the occlusion position, so we further use the information of the PDP to enhance the detection effect. When the signal spreads in all directions, due to the space's complexity, some positions must be blocked, making it difficult for the signal to reach. Multiple reflections often make These signals prone to significant amplitude attenuation. The same is true when the intruder is in static activity, because the range of the intruder's activities is reduced,

doi:10.6342/NTU202303843

so the paths that can reflect its behavior are reduced.

The PDP gives us path information, allowing us to find the delay component that best reflects the intruder. We modify the weights of different paths to make the restored CSI easier to detect intruders. Applying the same enhancement method to the air environment data, although it will increase the noise signal, its effect will not raise the false alarm excessively. After enhanced algorithm adjustment, our system can adapt to different environments and intruder behaviors, and the average detection accuracy is as high as 99.38%, and the false alarm is only 1.49%.

7.2 Intruder Tracking Map

After detecting an intruder in the target space, further tracking is expected. We exploit the PDP difference between the empty and intruder environments for intruder tracking. The calculated PDP difference can represent the most likely location by the degree of change in the influence of the intruder. Convert the delay information provided by the PDP to distance and map it to the target environment map. A map of concentric ellipses is formed by the transmitter's and receiver's distance to each location in space. By multiplying and superimposing the ellipse maps formed by at least two receivers, the range where the intruder is most likely to exist can be found.

Since the delay resolution of PDP is mainly affected by the bandwidth, for our hypothetical target environment, 6m×6m, a bandwidth of at least 80 MHz is needed to track intruders more accurately. In addition, when the intruder is close to the LOS, the tracking range will be expanded, mainly due to the method of tracking map generation.

Our method tracks intruders by collecting CSI over some time, rather than using a single packet to make a decision. In addition to the intruder's activity at a fixed point, we tested the intruder's continuous movement. Our tracking map can change over time even if the intruder keeps changing location. In an ideal environment, the tracking displacement can be as small as 0.45m using 320 MHz bandwidth, and only 0.79m even at 80 MHz. The signal is added to AWGN for testing, and the tracking displacement is still controlled below 10 cm even though it has increased.

Overall, the performance of our algorithm in an ideal environment using the existing maximum bandwidth can make the average tracking error as small as 0.45m, and compared with other studies, the computational complexity and CSI information requirements are relatively much lower.

doi:10.6342/NTU202303843

7.3 Future work

The possible future developments of the intrusion detection system and the intruder tracking method are discussed below.

7.3.1 Intrusion Detection and Identification

Our intrusion detection system relies only on 20MHz, 64 subcarrier information. However, Wi-Fi bandwidth can reach 320 MHz and 4096 subcarriers. Since the features used in our system look at subcarriers from a macro perspective and preprocessing has reduced noise. Therefore, when the number of sub-carriers increases, we do not need to make any other adjustments except to retrain the pre-trained model according to the number of sub-carriers.

In addition to detecting human presence, intrusion detection also focuses on identifying intruders. The purpose is to distinguish whether there are illegal intruders in the environment. To distinguish different individuals, the system will need more features that can reflect subtle changes, and it will also need to establish a database for legitimate individuals. In addition, a further goal may be to distinguish which one is an illegal intruder when there are multiple individuals. The technology is more complex and involves a multi-person detection system.

7.3.2 Combination of Intruder Tracking and Detection

We use simulated environments to verify the effectiveness of our proposed method when tracking intruders. But there are many more environmental variables in the real world than in the simulated environment, especially for phase effects. Even if we try to get closer to the actual situation by adding AWGN, the degree of its influence on the signal is much smaller than the time delay caused by SFO. In addition, we can only simulate the reflection and diffraction of signals, and the propagation of electromagnetic waves in reality also includes scattering and refraction. Further signal processing is required to apply the intruder tracking algorithm using PDP to the actual environment, and hardware, environment, etc. need to be adjusted.

In addition, we are also thinking about whether we can combine the detection and tracking of intruders. In our proposed system, the detection and tracking were initially regarded as two steps, that is, the intruder's presence is detected first and then tracked. However, The PDP difference used by the intruder tracking map can provide the gap between the current and empty environments. Further analysis of the values of these differences may be used to distinguish the presence of intruders. Another possible approach is to consider the scope of the intruder's activities. For example, if the potential scope of tracking is too concentrated on

doi:10.6342/NTU202303843

a certain point, it usually is abnormal and unreliable. Conversely, if the possible range is so extensive that the tracking effect is lost, there may also be no intruders in the space at all. Still, it is also necessary to consider whether the bandwidth used is not large enough.

Based on the above, many issues can be pondered in the development of CSI applied to intruders. After all, the privacy and security issues of physical or digital property will only be paid more and more attention.

doi:10.6342/NTU202303843

REFERENCES

[1] A. Zaidi, F. Athley, J. Medbo, U. Gustavsson, G. Durisi, and X. Chen, "Chapter 3 - propagation & channel modeling," in *5G Physical Layer*, A. Zaidi, F. Athley, J. Medbo, U. Gustavsson, G. Durisi, and X. Chen, Eds. Academic Press, 2018, pp. 35–85.

[2] R. v. Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, 1st ed. USA: Artech House, Inc., 2000.

[3] L. Hanzo, W. T. Webb, and T. Keller, "Single- and multi-carrier quadrature amplitude modulation : Principles and applications for personal communications, wlans and broadcasting," 2000.

[4] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[5] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[6] D. M. Pozar, *Microwave Engineering*. Wiley, 1998.

[7] L. Gui, W. Yuan, and F. Xiao, "Csi-based passive intrusion detection bound estimation in indoor nlos scenario," *Fundamental Research*, 2022.

[8] C. Van Loan, *Computational Frameworks for the Fast Fourier Transform*. USA: Society for Industrial and Applied Mathematics, 1992.

[9] Q. Cai and J. Aggarwal, "Automatic tracking of human motion in indoor scenes across multiple synchronized video streams," in *Sixth International Conference on Computer Vision (IEEE Cat. No.98CH36271)*, 1998, pp. 356–362.

[10] L. Liu, W. Zhang, C. Deng, S. Yin, and S. Wei, "Briguard: a lightweight indoor intrusion detection system based on infrared light spot displacement," *IET Science, Measurement & Technology*, vol. 9, no. 3, pp. 306–314, 2015.

[11] S. G. Iyengar, P. K. Varshney, and T. Damarla, "On the detection of footsteps based on acoustic and seismic sensing," in *2007 Conference Record of the Forty-First Asilomar Conference on Signals, Systems and Computers*, 2007, pp. 2248–2252.

[12] R. J. Orr and G. D. Abowd, "The smart floor: a mechanism for natural user identification and tracking," *CHI '00 Extended Abstracts on Human Factors in Computing Systems*, 2000.

[13] J. Wilson and N. Patwari, "Radio tomographic imaging with wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 5, pp. 621–632, 2010.

doi:10.6342/NTU202303843

[14] J. Wilson and N. Patwari, "See-through walls: Motion tracking using variance-based radio tomography networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 05, pp. 612–621, may 2011.

[15] A. E. Kosba, A. Saeed, and M. Youssef, "Rasid: A robust wlan device-free passive motion detection system," in *2012 IEEE International Conference on Pervasive Computing and Communications*, 2012, pp. 180–189.

[16] T. Wang, D. Yang, S. Zhang, Y. Wu, and S. Xu, "Wi-alarm: Low-cost passive intrusion detection using wifi," *Sensors*, vol. 19, no. 10, 2019.

[17] X. Wang, Y. Wang, and D. Wang, "A real-time csi-based passive intrusion detection method," in *2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, 2020, pp. 1091–1098.

[18] W. Zhuang, Y. Shen, L. Li, C. Gao, and D. Dai, "Develop an adaptive real-time indoor intrusion detection system based on empirical analysis of ofdm subcarriers," *Sensors (Basel, Switzerland)*, vol. 21, 2021.

[19] S. Li, X. Li, K. Niu, H. Wang, Y. Zhang, and D. Zhang, "Ar-alarm: An adaptive and robust intrusion detection system leveraging csi from commodity wi-fi," in *Enhanced Quality of Life and Smart Living*, M. Mokhtari, B. Abdulrazak, and H. Aloulou, Eds. Cham: Springer International Publishing, 2017, pp. 211–223.

[20] E. Ding, X. Li, T. Zhao, L. Zhang, and Y. Hu, "A robust passive intrusion detection system with commodity wifi devices," *Journal of Sensors*, vol. 2018, pp. 1–12, 06 2018.

[21] Y. Ma, G. Zhou, and S. Wang, "Wifi sensing with channel state information: A survey," *ACM Comput. Surv.*, vol. 52, no. 3, jun 2019.

[22] N. S. Altman, "An introduction to kernel and nearest-neighbor nonparametric regression," *The American Statistician*, vol. 46, no. 3, pp. 175–185, 1992.

[23] T. K. Ho, "Random decision forests," in *Proceedings of 3rd International Conference on Document Analysis and Recognition*, vol. 1, 1995, pp. 278–282 vol.1.

[24] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, p. 273–297, sep 1995.

[25] D. Wu, D. Zhang, C. Xu, Y. Wang, and H. Wang, "Widir: Walking direction estimation using wireless signals," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 351–362.

doi:10.6342/NTU202303843

[26] K. Qian, C. Wu, Z. Yang, Y. Liu, and K. Jamieson, "Widar: Decimeter-level passive tracking via velocity monitoring with commodity wi-fi," in *Proceedings of the 18th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. Mobihoc '17. New York, NY, USA: Association for Computing Machinery, 2017.

[27] Y. Jin, Z. Tian, Y. Li, Z. Li, and Z. Zhang, "A novel device-free tracking system using wifi: Turning fading channel from foe to friend," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[28] D. Wu, Y. Zeng, R. Gao, S. Li, Y. Li, R. C. Shah, H. Lu, and D. Zhang, "Witraj: Robust indoor motion tracking with wifi signals," *IEEE Transactions on Mobile Computing*, vol. 22, no. 5, pp. 3062–3078, 2023.

[29] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller, "3d tracking via body radio reflections," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. Seattle, WA: USENIX Association, Apr. 2014, pp. 317–329.

[30] X. Zuo, Z. Tian, Y. Jin, Z. Li, and M. Zhou, "Passive human tracking based on imm kalman filter using wifi signal," in *2022 IEEE 10th Asia-Pacific Conference on Antennas and Propagation (APCAP)*, 2022, pp. 1–2.

[31] S. Tan, L. Zhang, Z. Wang, and J. Yang, "Multitrack: Multi-user tracking and activity recognition using commodity wifi," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–12.

[32] B. R. Mahafza, *Radar Systems Analysis and Design Using MATLAB*. USA: CRC Press, Inc., 2000.

[33] F. Wang, J. Feng, Y. Zhao, X. Zhang, S. Zhang, and J. Han, "Joint activity recognition and indoor localization with wifi fingerprints," *IEEE Access*, vol. 7, pp. 80 058–80 068, 2019.

[34] J. Huang, B. Liu, H. Jin, and N. Yu, "Wilay: A two-layer human localization and activity recognition system using wifi," in *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*, 2021, pp. 1–6.

[35] M. S. Gast, "Chapter 2. the phy," in *802.11ac: A Survival Guide*. O'Reilly Media, Inc., Aug. 2013, online; accessed Dec 2021.

[36] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Predictable 802.11 packet delivery from wireless channel measurements," vol. 40, no. 4, p. 159–170, aug 2010.

[37] F. R. Hampel, "A General Qualitative Definition of Robustness," *The Annals of Mathematical Statistics*, vol. 42, no. 6, pp. 1887 – 1896, 1971.

[38] "The influence curve and its role in robust estimation," *Journal of the American Statistical Association*, vol. 69, no. 346, pp. 383–393, 1974.

doi:10.6342/NTU202303843

[39] L. Davies and U. Gather, "The identification of multiple outliers," *Journal of the American Statistical Association*, vol. 88, no. 423, pp. 782–792, 1993.

[40] "On-line outlier detection and data cleaning," *Computers and Chemical Engineering*, vol. 28, no. 9, pp. 1635–1647, 2004.

[41] C. Wu, Z. Yang, Z. Zhou, K. Qian, Y. Liu, and M. Liu, "Phaseu: Real-time los identification with wifi," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, 2015, pp. 2038–2046.

[42] M. Speth, S. Fechtel, G. Fock, and H. Meyr, "Optimum receiver design for wireless broad-band systems using ofdm. i," *IEEE Transactions on Communications*, vol. 47, no. 11, pp. 1668–1677, 1999.

[43] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson, "Phaser: Enabling phased array signal processing on commodity wifi access points," ser. MobiCom '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 153–164.

[44] L. Wang, L. Liu, C. Hu, and M. Q. Meng, "A novel RF-based propagation model with tissue absorption for location of the GI tract," *Annu Int Conf IEEE Eng Med Biol Soc*, vol. 2010, pp. 654–657, 2010.

[45] K. P. F.R.S., "Liii. on lines and planes of closest fit to systems of points in space," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 2, no. 11, pp. 559–572, 1901.

[46] J. L. Rodgers and W. A. Nicewander, "Thirteen ways to look at the correlation coefficient," *The American Statistician*, vol. 42, no. 1, pp. 59–66, 1988.

[47] J. M. Bland and D. G. Altman, "Statistics notes: Measurement error proportional to the mean," *BMJ*, vol. 313, no. 7049, p. 106, 1996.

[48] K. Qian, C. Wu, Z. Yang, Y. Liu, and Z. Zhou, "Pads: Passive detection of moving targets with dynamic speed using phy layer information," in *2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS)*, 2014, pp. 1–8.

[49] T. Yoshida and Kindai, "Estimating the number of people using existing wifi access point in indoor environment," 2015.

[50] M. A. A. Al-qaness, F. Li, X. Ma, Y. Zhang, and G. Liu, "Device-free indoor activity recognition system," *Applied Sciences*, vol. 6, no. 11, 2016.

[51] R. Zhou, X. Lu, P. Zhao, and J. Chen, "Device-free presence detection and localization with svm and csi fingerprinting," *IEEE Sensors Journal*, vol. 17, no. 23, pp. 7990–7999, 2017.

[52] B. Schölkopf, R. C. Williamson, A. Smola, J. Shawe-Taylor, and J. Platt, "Support vector method for novelty detection," in *Advances in Neural Information Processing Systems*, S. Solla, T. Leen, and K. Müller, Eds., vol. 12. MIT Press, 1999.

doi:10.6342/NTU202303843

[53] A. V. Oppenheim, *Discrete-time signal processing*. Pearson Education India, 1999.

[54] Y. Xie, Z. Li, and M. Li, "Precise power delay profiling with commodity wi-fi," *IEEE Transactions on Mobile Computing*, vol. 18, no. 6, pp. 1342–1355, 2019.

[55] J. Montojo and J. Damnjanovic, *Carrier Aggregation*. John Wiley and Sons, Ltd, 2011, ch. 28, pp. 623–650.

[56] A. Gorokhov, A. Farajidana, K. Bhattad, X. Luo, and S. Geirhofer, *Multiple Antenna Techniques for LTE-Advanced*. John Wiley and Sons, Ltd, 2011, ch. 29, pp. 651–672.

[57] "Chapter 4 - the mathematics of failure and reliability," in *Reliability and Failure of Electronic Materials and Devices*, M. Ohring, Ed. San Diego: Academic Press, 1998, pp. 175–236.

[58] A. Papoulis and S. Pillai, *Probability, Random Variables and Stochastic Processes*. McGraw-Hill Education, 2001.

[59] G. Casella and R. L. Berger, *Statistical Inference, 2/e*. Duxbury, 2001.

[60] E. Meijering, "A chronology of interpolation: From ancient astronomy to modern signal and image processing," *Proceedings of the IEEE*, vol. 90, no. 3, pp. 319–342, 2002.

[61] L. Yang and Z. Huiyan, "Shape preserving piecewise cubic interpolation," *Applied Mathematics*, vol. 11, no. 4, pp. 419–424, Dec 1996.

[62] C. A. Hall and W. Meyer, "Optimal error bounds for cubic spline interpolation," *Journal of Approximation Theory*, vol. 16, no. 2, pp. 105–122, 1976.

[63] I. The MathWorks, *Antenna Toolbox*, Natick, Massachusetts, United State, 2023.

[64] "Ray tracing for radio propagation modeling: Principles and applications," *IEEE Access*, vol. 3, pp. 1089–1100, 2015.

[65] K. Schaubach, N. Davis, and T. Rappaport, "A ray tracing method for predicting path loss and delay spread in microcellular environments," 06 1992, pp. 932 – 935 vol.2.

[66] I. The MathWorks, *Communications Toolbox*, Natick, Massachusetts, United State, 2023.

[67] C. Mandery, O. Terlemez, M. Do, N. Vahrenkamp, and T. Asfour, "The kit whole-body human motion database," in *International Conference on Advanced Robotics (ICAR)*, 2015, pp. 329–336.

[68] R. Zajicek and J. Vrba, "Broadband complex permittivity determination for biomedical applications," in *Advanced Microwave Circuits and Systems*, V. Zhurbenko, Ed. Rijeka: IntechOpen, 2010, ch. 17.

doi:10.6342/NTU202303843