

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Citation: Y. Yao, Y. Li and T. Zhu, "Interference-Negligible Privacy-Preserved Shield for RF sensing," in *IEEE Transactions on Mobile Computing*, doi: 10.1109/TMC.2023.3276930.

DOI: <https://doi.org/10.1109/TMC.2023.3276930>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

#### **Please provide feedback**

Please support the ScholarWorks@UMBC repository by emailing [scholarworks-group@umbc.edu](mailto:scholarworks-group@umbc.edu) and telling us what having access to this work means to you and why it's important to you. Thank you.

# Interference-Negligible Privacy-Preserved Shield for RF sensing

Yao Yao, Yan Li, and Ting Zhu

**Abstract**—Researchers have demonstrated the feasibility of detecting human motion behind the wall with radio frequency (RF) sensing techniques. With these techniques, an eavesdropper can monitor people's behavior from outside of the room without the need to access the room. This introduces a severe privacy-leakage issue. To address this issue, we propose Aegis, an interference-negligible RF sensing shield that i) incapacitates the RF sensing of eavesdroppers that work on any WiFi frequency bands and at any unknown locations outside of the protected area; ii) has minimum interference to the on-going WiFi communication; and iii) preserves authorized RF sensing inside the private region. Our extensive evaluation shows that when Aegis is activated, the accuracy of legitimate sensing system only decreases by 0.08, while the accuracy of the illegitimate sensing system is as low as 0.04. Moreover, the on-going data communication throughput is even increased by 10MB/s on 2.4GHz WiFi band and 5MB/s on 5GHz WiFi band.

**Index Terms**—RF sensing, activity recognition, human tracking, preserve privacy.

## 1 INTRODUCTION

Radio frequency (RF) sensing techniques can leverage the RF signals reflected from a human body for tracking people [15], [14] and recognizing their activities [2], [16] and gestures [19], [3]. Although radio signals can be attenuated and reflected by obstacles, researchers proposed sensing systems that can sense human activities even behind the wall [4], [30]. Although most RF sensing systems rely on the patterns obtained by machine training, [36] shows that the training result through the wall can be applied to another room, which means the eavesdropper might not have to train in the target room before listening. Therefore, these RF sensing techniques also introduce serious privacy leakage issues. As shown in Figure 1(a): Alice (a WiFi access point) is sending WiFi packets to Bob (a smartphone). The signal transmitted by Alice is reflected by a person's body and utilized by Carol (a private RF sensing system) that is conducting legitimate human tracking and activity recognition for applications (e.g., smart homes) in the *private region* (i.e., a private home). However, Eve (eavesdropper) can also perform illegitimate RF sensing outside of the private region by analyzing the WiFi signal bounced from the human body. As demonstrated in [2], [16], Eve can spy on his/her neighbors' activities and decipher password based on keystroke [5]. This is a serious privacy leakage issue.

This issue can be solved by covering the private region with electromagnetic shielding (similar to the Faraday cage). However, this approach is very expensive and sometimes unfeasible due to the geographic limitations. Moreover, Carol can not conduct the legitimate human tracking and activity recognition inside the shielded private region because Alice's signal is blocked (shown in Figure 1(b)).

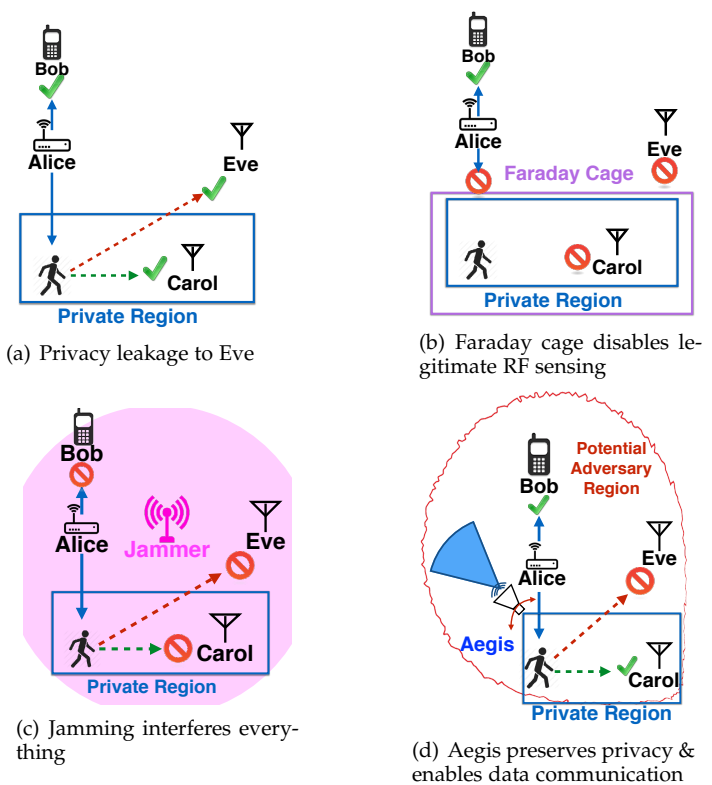


Fig. 1: Difference between Aegis and other approaches.

Another approach is to use a jammer that distorts the information so that Eve cannot derive the human location and activities from the reflected signal. However, jamming may also introduce a severe interference to Carol's legitimate human tracking and activity recognition system and the communication between Alice and Bob (Figure 1(c)).

Different from the above approaches, we present Aegis, a novel interference-negligible RF sensing shield. As shown in Figure 1(d), Aegis reflects the received signal from Alice by changing its amplitude, delay, and doppler shift. By using the directional antenna and rotating the antenna, Aegis can

- University of Maryland Baltimore County Department of Computer Science and Electrical Engineering, 1000 Hilltop Circle, ITE 325, Baltimore, Maryland 21250  
E-mail: yaoyaoumbc@umbc.edu, bhyanli@gmail.com, zt@umbc.edu

cover all of the potential adversary regions where Eve may reside in. Our design goals are i) preventing Eve from eavesdropping the human location and activities information at any potential adversary regions and **using any WiFi frequency bands**; ii) introducing negligible interference to the ongoing wireless data communication from Alice to Bob; and iii) protecting Carol's legitimate RF sensing system in the private region. To achieve these three design goals, we need to address the following two design challenges:

- **How to identify and cover the potential adversary region?** To be more effective, ideally, we want to point the directional antenna to Eve but not Carol. However, in order to track the human movement, Eve only needs to act as a silent receiver, which is very difficult to localize because Eve does not generate any signals. Therefore, instead of localizing Eve, we propose to identify the potential adversary region based on the location of the sender (i.e., Alice), which can be estimated based on existing approaches (such as the received signal strength, time-of-arrival, angle-of-arrival). Then, based on the identified potential adversary region, we can rotate the directional antennas to obfuscate the human motion information inside the whole region.

- **How to prevent the eavesdropping while maintaining legitimate communication and sensing?** It is impossible to tell who is the eavesdropper. For example, Eve may act as another Bob (a legitimate communication node). Therefore, the signal reflected by Aegis should only interfere the human motion information but not the data communication. Since RF sensing techniques use three physical layer features (i.e., signal amplitude gain, delay, and Doppler shift) to track human movement and identify human activities, the design goal of Aegis is to distort all these three features in the potential adversary region while introducing negligible interference to the on-going data communication. Specifically, Aegis changes i) the signal amplitude with a combination of amplifiers; ii) the Doppler shift by controlling the speed of a fan attached to the mouth of its directional horn antenna; and iii) the delay by rotating the directional antenna. By carefully controlling the transmission directions and transmission power of directional antenna, the data communication signals received by legitimate receivers (such as Bob) is not noticeably interfered by the signals reflected by Aegis.

In summary, our main contributions are as follows:

- We build a novel hardware platform that can simultaneously change amplitude, delay, and Doppler shift of the wireless signals so that eavesdroppers cannot identify the human motions based on the reflected signal. Moreover, by rotating the directional antennas, our hardware platform can cover any area within the potential adversary region.
- We design a novel scheme to estimate the potential adversary region under two different threat models (i.e., passive eavesdroppers and active adversaries). We also develop a new metrics (i.e., signature entropy) to identify the boundary of the potential adversary region.
- We optimize the control of the RF sensing shield (Aegis) to change the signal amplitude, delay, and Doppler shift so that Aegis can prevent various types of eavesdroppers. In the meantime, the changes of the signal are optimized so that Aegis only obfuscates human motion information but leaves the data communication content unaffected.
- We evaluated our design extensively in real-world settings.

Our experimental results show that Aegis can effectively prevent the eavesdropper. For example, when Aegis is activated, the accuracy of legitimate sensing system only decreases by 0.08, while the accuracy of the illegitimate sensing system is as low as 0.04. Since Aegis elevated the amplitude of the overall received signal, the throughput of the data communication is increased by 10MB/s on 2.4GHz WiFi band and 5MB/s on 5GHz WiFi band. Thus the interference to communication is negligible.

## 2 RELATED WORK

Lots of approaches have been proposed to conduct RF-based human tracking and activity recognition. These approaches can be categorized into the following three categories:

**I) RSS-based.** Received signal strength (RSS)-based methods mainly monitor the signal strength at the receiver side to achieve human tracking and activity recognition. In the field of human tracking, lot of works have been done to conduct single person tracking [15], [14], [32] and multiple targets tracking [18]. In the field of activity recognition, harmony achieves up to 90% activity recognition accuracy [7]. Although RSS has been known as a coarse-grained measurement, several approaches are even able to recognize gestures [22], [2]. Moreover, as presented in [16], RSS can be used to monitor respiration.

**II) CSI-based.** Compared with RSS-based methods, channel state information (CSI) has been considered as a fine-grained measurement. Besides the signal strength information, CSI also provides more detailed information including phases of the received signal [33], [26]. By leveraging CSI information, researchers have developed a fall detection system [12] with 87% detection accuracy, and an activity recognition system [28] to recognize 9 activities. Even under radio frequency interference, it is still possible to conduct human activity recognition. In addition, CSI-based approaches have also been developed to identify individuals [34], hear human talks [24], and recognize keystrokes [5].

On the privacy preserving side, the most related work is PhyCloak [20]. However, Aegis is different from PhyCloak in three aspects: i) Aegis *simultaneously* incapacitates adversaries in all the WiFi bands within 2.4 GHz and 5 GHz; ii) Aegis is independent of the legitimate sensing systems since it does not require complex signal processing scheme; and iii) the rotating directional antenna in Aegis makes the MIMO adversaries hard to separate the obfuscating signal from the original signal.

## 3 UNDERSTANDING RF SENSING

### 3.1 Principle of RF sensing

RF sensing systems leverage the wireless signals bouncing back off the human body. As shown in Figure 2: the signal from the transmitter reaches the receiver via multiple propagation paths. The signal that propagates directly from the transmitter to the receiver takes the line-of-sight (LoS) path,  $P_l$ . The signal that is reflected by the static obstacle takes the non-line-of-sight (NLoS) path,  $P_{nl}$ . The signal bounced off the human body also creates a path,  $P_h$ . When the human is moving or performing activities,  $P_h$  would become  $P'_h$ , which has a different length comparing to  $P_h$ . Since paths  $P_l$  and  $P_{nl}$  are relatively stable, the human activities that cause the transition from  $P_h$  to  $P'_h$  can be

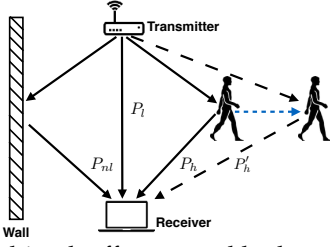


Fig. 2: Multipath effect caused by human motion

derived based on measurable features of the received signal, such as amplitude, delay, and Doppler shift.

When the person moves, the received signal amplitude (i.e., RSS or CSI values) fluctuates. Consequently, the RSS values contain a unique pattern, which is the basis of RSS-based localization and tracking [35], [5], [7].

When the person moves away from the transmitter and receiver, the signal bounced off the human body will take a longer path to reach the receiver, which requires more propagation time. Thus the delay of the received signal can also be used to conduct localization [10] and tracking [31].

Doppler shift is introduced by the relative speed between the human body and the receiver [17]. Different human gestures introduces distinguishable patterns in the Doppler shift that can be used for gesture recognition [19].

### 3.2 Formal analysis

Most of the RF based human motion sensing systems build on top of the measurements of RSS, delay, and Doppler shift. The changes in these three features can be represented by the complex value channel frequency response (CFR) [27]. CFR can be denoted as  $H(f, t)$ , which can be calculated using the following Equation:

$$H(f, t) = e^{-j2\pi\Delta f t} \sum_{k=1}^N a_k(f, t) e^{-j2\pi f \tau_k(t)} \quad (1)$$

where  $f$  is the frequency of a wireless channel,  $t$  is time.  $a_k(f, t)$  is the amplitude attenuation.  $\tau_k(t)$  is the delay.  $\Delta f$  is the Doppler shift. Given the transmitted signal  $X(t)$ , the received signal  $Y(t)$  can be written as  $Y(t) = H(f, t) \times X(t)$ .

Therefore, in order to make sure that Eve cannot derive a valid human activity, our system needs to randomize human activity information embedded in the amplitude, delay and Doppler shift outside of the private region. In this way, Aegis does not need to know details about Eve, such as Eve's communication protocols or sensing algorithms.

## 4 ASSUMPTIONS AND THREAT MODEL

### 4.1 Assumptions

We assume that there exist multiple WiFi access points that work in different frequency bands (e.g., 2.4 GHz and 5 GHz) in the environment. As shown in Figure 1(a), Carol is deployed in the private region and Eve is outside of the private region. We assume that the private region is isolated from other areas by walls or doors or non-transparent windows. The private region can be an office room or a private home. Eve cannot visually observe the human activities inside the private region. However, Eve can use any state-of-the-art RF sensing techniques to conduct the human activity and gesture recognition.

### 4.2 Threat Model

We address two commonly considered radio-equipped adversaries: passive eavesdroppers and active adversaries.

#### 4.2.1 Passive eavesdroppers

As shown in Figure 1(a), an adversary (Eve) eavesdrops on the wireless medium and records the RF signals transmitted by Alice and reflected by the human body. Based on the recorded RF signals, Eve applies different RF sensing techniques [7], [29], [17] to recognize human activities and gestures. In other words, Eve can leverage the human activity information embedded in any combinations of the three components (i.e., signal amplitude, delay, and Doppler shift) to derive human activities and gestures. Since our system can randomize human activity information embedded in the amplitude, delay, and Doppler shift outside of the private region, we ensure that the adversary cannot recognize any activities or gestures inside the private region.

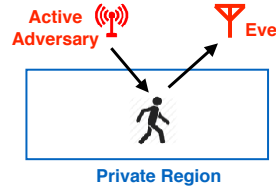


Fig. 3: Threat model with the active adversary

#### 4.2.2 Active eavesdropper

As shown in Figure 3, such an adversary pretends to be a benign WiFi user and actively sends out RF signals, which can be at any WiFi frequency bands (e.g., 2.4 GHz or 5 GHz). By applying RF sensing techniques on the received signals, which are originally generated by the adversary and reflected by the human body inside the private region, the adversary's receiver (Eve) can recognize the human activities and gestures inside the private region. Since our system directly reflects and randomizes human activity information embedded in the amplitude, delay and Doppler shift of the received signals at the physical layer in any frequency band, we can obfuscate the adversary's sensing.

## 5 SYSTEM OVERVIEW

The design goals of our system are i) incapacitating the RF sensing of eavesdroppers that work on any WiFi frequency band and are deployed at any unknown location outside of the private area; ii) minimizing interference to the ongoing WiFi communication; and iii) preserving authorized RF sensing inside the private region. To achieve this design goal, we propose Aegis system (shown in Figure 4) which contains two parts: hardware platform and middleware.

**Hardware platform**, which contains five main components: i) an omni-directional receiving (Rx) antenna that receives the RF signals from the environment; ii) an amplification circuit, which changes the amplitude of the received signals; iii) a directional transmitting (Tx) antenna, which transmits the distorted RF signals; iv) a fan, which is attached to the mouth of the Tx antenna and can be used to introduce Doppler shift to the RF signals; and v) a stepper motor, which is mounted underneath the Tx antenna. The stepper motor can be used to rotate and change the orientation of the directional Tx antenna. The rotation of the Tx antenna can introduce randomized delay. With these components, the hardware platform can change the amplitude, delay and Doppler shift of the signal in all of the WiFi bands.

**Middleware**, which controls the hardware platform for generating the distorted signals to cover the potential adversary



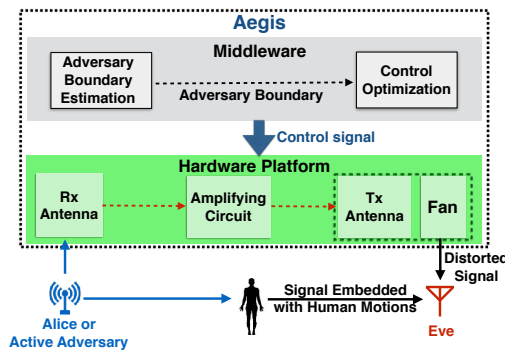


Fig. 4: System Overview of Aegis

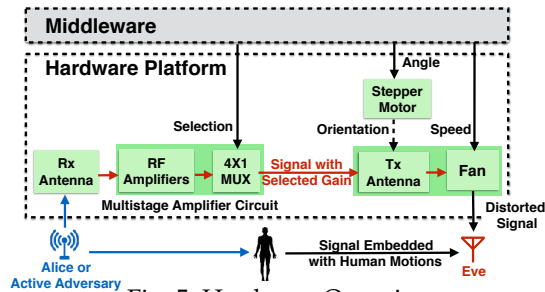


Fig. 5: Hardware Overview

region. Specifically, the middleware has two functions: i) estimating the boundary of the potential adversary region based on the estimated location and transmission power of the WiFi transmitter. The result of this estimation is used to decide the rotation angle of the Tx antenna; ii) calculating the control parameters, including the speed of the fan, the gain of the amplifier circuit, and the speed of the motor, so that the output signal can obfuscate the human motion information. With the estimated boundary and the parameters, the middleware controls the hardware to block illegitimate sensing in the potential adversary region.

## 6 HARDWARE DESIGN

The design goals of Aegis' hardware platform are i) distorting the human motions embedded in amplitude, delay and Doppler shift of the signals in all of the WiFi bands (i.e., both 2.4 GHz and 5 GHz); and ii) controlling the distorted signals outside of the private region. Existing full-duplex systems [13], [37], [6] i) cannot provide the distorted signals over multiple frequency bands; and ii) cannot ensure the full coverage of privacy preserving within the private region. Therefore, to achieve these design goals, we propose a simple but effective hardware platform (shown in Figure 5) that leverages commercial-off-the-shelf (COTS) components. Specifically, our hardware platform uses i) an amplifier circuit to change the amplitude of received RF signals; ii) a fan to change the Doppler shift; and iii) a motor to rotate the Tx antenna so that the signal propagation delays can be changed. After making the above changes, the signal reflected by our hardware platform can obfuscate the human motion information in the potential adversary regions. In the meanwhile, our hardware system can also minimize the interference to the on-going WiFi communications and preserve the authorized human activity and gesture recognition inside the private region.

### 6.1 Distorting Reflected Signal's Amplitudes

In order to distort the human movement information embedded in the reflected signal amplitude, our hardware

platform needs to change the received signal's amplitude and immediately rebroadcast the changed signal so that the changed signal can not be filtered out by Eve. We cannot rely on a traditional and costly system that goes through down-conversion, digitization, analog regeneration, and up-conversion. Such a system causes detectable signal delays and can be filtered out by Eve as a separate signal.

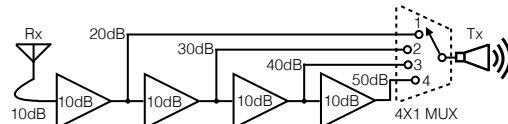


Fig. 6: A Simplified Multistage Amplifier Circuit Diagram

To address this challenge, we need a multistage amplifier that reflects the signals immediately without decoding any data. However, existing amplifier has very limited amplification gain, which does not meet our requirement. Therefore, we designed a multistage amplifier circuit.

#### 6.1.1 Amplifier circuit

As shown in Figure 6, the amplifier circuit contains four RF amplifiers (with 10 dB gain) and a multiplexer (MUX). After the signal is received, it is amplified for 10 dB by the receiving circuit. Then, the signal goes through the multistage amplifier circuit. By connecting the transmitting (Tx) antenna to different input of the MUX, we can get different amplification gain. For the sake of clarity, the impedance matching circuit is not shown in Figure 6.

#### 6.1.2 Parameter selection

In order to distort the human motion information at the potential adversary region while preserving the data communication and RF sensing at the private region, we need to make sure the amplification gains are sufficient enough and not interfere with legitimate data communication and RF sensing. With a typical high gain +10 dB omni-directional gain antenna and low noise +10 dB amplifier (LNA), the typical received signal strength is -35 dBm at 3 meters with -50 dB of RF propagation loss. The reflect coefficient of a human body is around 0.6 [21]. Therefore, to obfuscate the human movements, the reflected signal requirement is a minimum of  $-35 \text{ dBm} \times 0.6 = -21 \text{ dBm}$ . Therefore, we should reflect back a minimum of 14 dB gain. To make sure that we can defend against an eavesdropper with a sensitive receiver, in the circuit, we connect 4 RF 10 dB amplifiers and a 4X1 MUX. After the first amplified of 10 dB by the receiving antenna, the MUX has 4 gain values {20 dB, 30 dB, 40 dB, 50 dB} as inputs. By randomly switching among these 4 values, we can distort the reflected signals' amplitude. We note that our multistage amplifier circuit design is generic. It can be extended to support more number of amplification gains. On the other hand, our evaluation results demonstrated that our current 4 gain values are sufficient to distort the human motion information at the potential adversary region.

### 6.2 Distorting Reflected Signal's Doppler Shifts

In order to distort the human motion information embedded in the Doppler shifts, we need to create frequency shifts in the same frequency band as human movements and transmit the distorted signals. To meet this requirement, we place a fan at the mouth of the Aegis's transmitting directional horn antenna [1]. By randomizing the fan's rotating speed, we introduce randomized Doppler shifts, which can defend

against an eavesdropper that senses human motion via the Doppler shift.

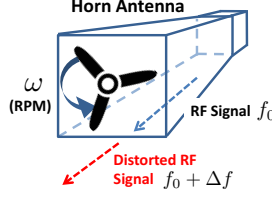


Fig. 7: A fan distorted the Doppler shift caused by human movements

### 6.2.1 Principles of Doppler Shift

Doppler shift is the change in frequency of a wave for an observer moving relative to its source [8]. In our system, the source moving speed relative to the medium is  $v_s = 0$ . The observer (i.e., fan blades) moving speed relative to the medium is  $v_f = \omega r$ . Where,  $\omega$  is the angular speed and  $r$  is the fan radius (here  $r = 50\text{mm}$ ). The rotational speed of the fan can be calculated by using the following equation:

$$\omega_f = \frac{60 \cdot \omega}{2\pi} \quad (2)$$

Thus, we can estimate the Doppler shift  $\Delta f$  created by the fan using the following equation:

$$\Delta f = \frac{v_f - v_s}{c} f_0 = \frac{\omega r}{c} f_0 = \frac{2\pi \omega_f r}{60 \cdot c} f_0 \quad (3)$$

where,  $f_0$  is the frequency of the originally received signal by our hardware. In order to distort the human motion information embedded in the Doppler shifts, we need to determine the fan's rotational speed range.

### 6.2.2 Parameters from Empirical Study

From our empirical study, when a person is walking at 1-2 m/s, the Doppler shift created by his/her movement is around 10 Hz. Falling limbs at 10 m/s can introduce around 80 Hz Doppler shift. Thus, from Equation 3, we can estimate the corresponding rotational speed range is from 240 rounds per minute (RPM) to 2,000 RPM. In our system, our fan rotational speed can change from 0 to 4,000 RPM. Therefore, by randomly changing the rotational speed of the fan, we can create the Doppler shift that can obfuscate the human motion information in the potential adversary region.

A practical concern is that would the fans on other everyday apparatus (such as air conditioner, i.e., AC) affect the sensing system and Aegis. The fans on every apparatus could affect the RF signal. However, those fans work at a constant speed for a long period of time (10 minutes to hours), which would span across multiple human activities. Therefore, the fan rotation would be recognized as a constant environmental noise. On the other hand, the fan of Aegis would change speed randomly in the time span of one activity. From the above analysis, the fans of everyday apparatus would not be a major concern of Aegis.

## 6.3 Distorting Delay and Ensuring Coverage

Traditionally, signal delays can be introduced by using an expensive device. However, if the delay is too long, Eve can easily filter out the delayed signal. Therefore, we need to leverage the multipath effect to generate delayed signals. In our Aegis hardware platform, we mount our directional antenna on a stepper motor, which can change the orientation and rotating speed of the directional antenna.

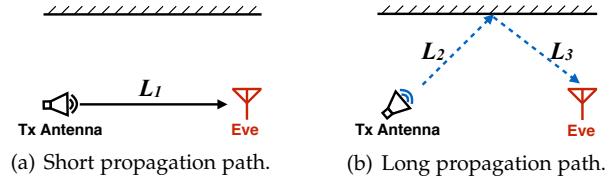


Fig. 8: Distort delay by rotating a directional antenna

### 6.3.1 Changing Delay by Rotating the Antenna

Figure 8 shows why rotating the directional antenna can create the delay. In Figure 8(a), originally, the Tx antenna is pointing at Eve. Therefore, the signal propagation path length is  $L_1$ . After some time, Tx antenna is rotated to the position shown in Figure 8(b). In this case, the signal propagation path length is changed to be  $L_2 + L_3$ . Since  $L_2 + L_3$  is longer than  $L_1$ , the signal's delay is also increased. By randomize the rotating speed of the stepper motors, we can randomize the delay introduced in the signal. Therefore, we defend the adversaries using the signal delay to recognize human activities.

## 7 MIDDLEWARE DESIGN

The design goal of the middleware is to achieve the full coverage of the potential adversary region with distorted signal. Our middleware contains two modules (shown in Figure 9): human motion obfuscation module and motor controller module.

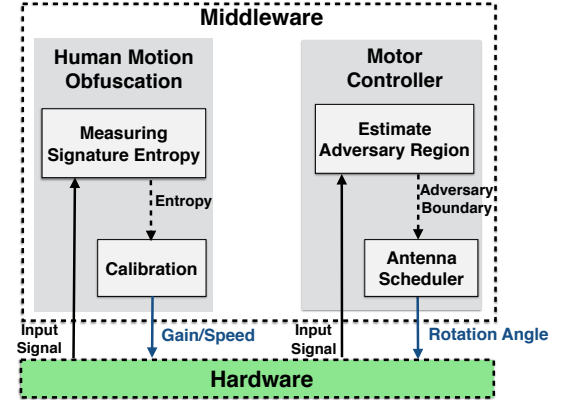


Fig. 9: Middleware Architecture

- **Human Motion Obfuscation Module:** This module obfuscates the human motion information by distorting the physical layer features (i.e., amplitude, Doppler shift, and delay). Since we do not know which feature the eavesdropper uses for recognizing human motion, we need to distort all these three features when generating the distorted signal. To evaluate the effectiveness of our approach, we propose a new metric (i.e., **signature entropy**), which fuses the three features together to indicate how much human motion information is embedded in the distorted signal. Then we use the hill climbing algorithm to maximize the correlation signature entropy in the distorted signal.
- **Motor Controller Module:** This module controls the Tx directional antenna to cover the potential adversary region with the distorted signal. The potential adversary region can be marked by its boundary, which we define as the **adversary boundary**. However, multiple active adversaries can work on the same frequency alternatively, which causes the adversary boundary to change over time. On the other hand, multiple active adversaries can also work in different

frequency bands at the same time, which creates overlapping adversary boundaries. The motor controller module estimates the adversary boundaries by considering all the active adversaries, and dynamically change the range of rotation to cover the potential adversary region.

## 7.1 Control Optimization

The key idea of Aegis is to feed the eavesdropper with invalid human motion information. To achieve that, we need to quantify the human motion information, which could be done by analyzing the real human motion signal. Then we will obfuscate that information and send it to the eavesdropper. In the meantime, we need to make sure the obfuscating signal would not jeopardize the data communication.

In this section, we first introduce the signature entropy, which indicates how much human motion information is embedded in the signal. Then, we show how to tune signature entropy of the signal received at a certain location with the distorted signal. In the end, we show that the distorted signal will not jeopardize wireless data communication.

### 7.1.1 Signature Entropy

In order to minimize the human motion information obtained by the eavesdropper, we need a metric to measure the amount of information. Entropy is usually used to measure the amount of information in the signal. However, classical entropy model targets the communication information instead of human motion information. To solve this issue, we leverage the observation that information is embedded in the fluctuation of the signal features. For example, the amplitude modulation (AM) radio embeds information in the fluctuation of signal amplitudes. Similarly, the human motion information is embedded in the fluctuation of amplitude, Doppler shift, and delay. These features can be unified by using the following equation:

$$s = \sum_{i=0}^K a_i(t_i) e^{-j2\pi f_D T_i(t_i)} \quad (4)$$

Where  $K$  is the number of signal samples collected between the start and the end of the human motion.  $a_i$  is the instantaneous amplitude change.  $f_D$  is the Doppler shift.  $T_i(t_i)$  is the delay at time  $t_i$ .  $s$  is the human motion signature that describes the pattern caused by human motion.

The human motion signature is essentially the frequency domain representation of a time series. The signal received by the sensing system can also be transformed into the frequency domain with the same form. Thus if the signal "looks like" the human motion signature, it was affected by the same human motion. Cross correlation [11] tells the probability of one series contains the pattern of another series. Specifically, the cross correlation  $C_{sg}$  between a human motion signature  $s$  and the received signal  $g$  can be calculated using the following equation:

$$C_{sg} = \sum_{m=0}^N s^*[m]g[m+n] \quad (5)$$

Where, the cross correlation  $C_{sg}$  is the probability of signal  $g$  containing human motion signature  $s$ . In real implementation, the cross-correlation should be normalized. We define the conditional signature entropy  $H_k(Co_i|Cf_k)$  as:

$$H_k(Co_i|Cf_k) = \sum p(co_i, cf_k) \log \frac{p(co_i)}{p(co_i, cf_k)} \quad (6)$$

The conditional signature entropy describes the ability to predict the correct activity given the observed signatures and signals when Aegis is activated.

### 7.1.2 Calibration

To maximize signature entropy for the adversary while minimizing the signature entropy of authorized receivers, we calibrate Aegis by defining the search space in for gain, fan speed, and antenna direction placement. We define entropy measured by the illegitimate receiver (i.e., adversary) as follow:

$$Adv_{i,k,x,y} = H|Gain_i, Fan_k, \theta_j \quad (7)$$

where  $Gain_i$  is the  $i$ th array of gain level to test.  $Fan_k$  the  $k$ th fan speed to test,  $\theta_j$  is the  $j$ th antenna angle to test.

Similarly, we can define entropy measured by the legitimate (authorized) receiver as follow:

$$Auth_{i,k,x,y} = H_n|Gain_i, Fan_k, \theta_j \quad (8)$$

Thus the goal of the calibration process is to maximize  $Adv_{i,k,x,y} - Auth_{i,k,x,y}$ .

We use the hill climbing to maximize the difference between the signature entropy measured by the legitimate sensing system and that measured by the illegitimate sensing system. Specifically, we try every combination of the parameters to find the maximum entropy difference.

### 7.1.3 Impact on Communication

In this section, we discuss interference robustness of the most common communication schemes under Aegis.

•**Impact of amplification** Simply amplifying and rebroadcasting the received signal might affect the data transmission. However, the Channel State Information (CSI) is decided in the packet level. Hence if the signal amplitude changes abruptly in one packet, the data transmission would be affected. But if the signal amplitude changes between two packets, the data transmission would be intact. The goal of Aegis is the obfuscate human motion, which usually takes more than 0.1 second. In the meantime, a WiFi packet takes hundreds of microseconds. Thus Aegis would change the signal amplitude far slower than the packet rate. This would cause multiple packets shares the same level of SNR, and the data communication is unaffected.

•**Impact of frequency shift** We model multipath and Doppler shifts on a sine RF signals as follows:

$$(A \pm A_m) e^{j2\pi[f_c(t+T_m)+f_d(t+T_m)]} \quad (9)$$

Where  $A$  is the amplitude of the signal sent,  $A_m$  is the multipath and propagated amplitude of the signal.  $f_c$  is the frequency of the original signal.  $f_d$  is the Doppler shifted frequency bounced off on a body.  $t$  is the transmit, time and  $T_m$  is the propagation and multipath time.

Therefore, we can define coherence of time as  $T_c$  and the range of frequency drifts defined as  $B_d$ .

$$T_c = \frac{1}{B_d} \quad (10)$$

Since human motions usually introduce frequency shift under 150Hz,  $B_d$  has a range of 1 ~ 150Hz. For a wireless communication receiver to recover from the Doppler Effect interference, it must sample more than  $T_c/2$  samples, which can be fulfilled by most communication devices.

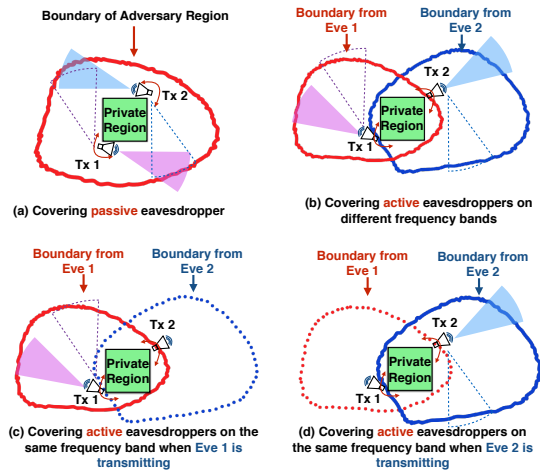


Fig. 10: Two elemental scenarios of antenna deployment.

• **Impact of Delay** To recover from multipath delays, protocols must allow for a guard interval between each symbol. Therefore, depending on the level of channel interference, a wireless communication system must have a guard interval used in Orthogonal frequency-division multiplexing (OFDM), fast enough digitizer, propagation diversity such as multiple-input and multiple-output (MIMO), and enough spread between carrier frequencies. With these mechanisms, the communication systems can avoid suffering from multipath delay. Therefore, the delay introduced by Aegis would not affect the communication.

## 7.2 Motor Controller Module

In this section, we first demonstrate how to cover the potential adversary region when the adversary is passive. Then we discuss the case of active adversaries.

### 7.2.1 Covering Multiple Passive Adversaries

Ideally, Aegis should point the Tx directional antenna to the adversary. But a passive adversary is hard to locate since it does not transmit any signal. However, a passive adversary needs to stay relatively close to the transmitter to sense human motion. If the adversary is far from the transmitter, the signature entropy of the signal would be high since the signal fades drastically. Therefore, the adversary has to stay in the region where the signature entropy is low enough for sensing human motions. We name this region as the **potential adversary region**. As long as Aegis covers the potential adversary region with the distorted signal, there would be no space for the adversary to sense human motion.

To cover the potential adversary region, we need to know its location and shape. The center of the potential adversary region is the location of the transmitter, and the shape should be a circle in an ideal environment. However, due to the multipath effect, the center could be slightly shifted, and the shape would be distorted. Thus we need the entropy map of the area to find the boundary of the potential adversary region. The entropy map can be obtained by scanning the area with a sensor that measures the entropy.

With the boundary of the potential adversary region, we still have to answer three questions to cover the region: **I)** how many directional antennas should be deployed, **II)** where to deploy the antennas, and **III)** what is the range of angle each antenna should cover?

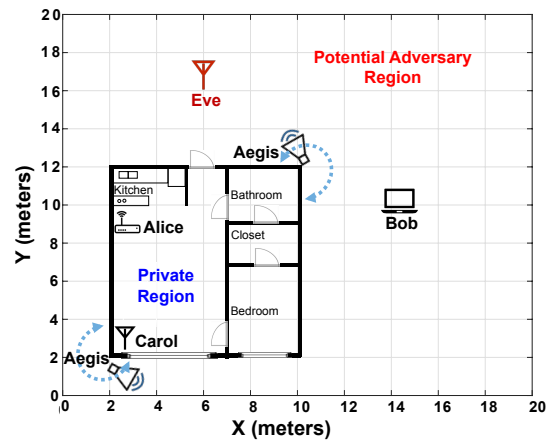


Fig. 11: The deployment of Aegis, Alice (WiFi access point), Bob (legitimate communication device), Carol (legitimate sensing system) and Eve (illegitimate sensing system) .

Figure 10(a) shows how we cover the potential adversary region. We deploy 2 Tx directional antennas (Tx 1 and Tx 2) at two opposite corners of the private region. With the help of the motors, each antenna covers approximately  $270^\circ$ . Although the potential adversary is distorted, this configuration is enough to cover it.

In the meantime, we need to figure out how fast the antenna should rotate. Since most human activities can be performed in  $1 \sim 2$  seconds, the antenna only needs to cover the area in those time. Furthermore, the directional antenna might only need to cover the whole area in  $1 \sim 2$  seconds. This is because we only need to obfuscate part of the human activity information to block the eavesdropper.

Note that the adversary may not be continuously covered by a rotating Tx directional antenna, thus can obtain correct information about human motion discontinuously. However, human motion is a continuous process that usually takes seconds, which is enough for the directional antenna to scan the region multiple times. Thus the adversary would get a mixture of correct and incorrect results, which is still far away from the actual human motion pattern. And since the adversary cannot distinguish real multipath signal from the interference signal, the actual human motion trace cannot be recovered.

### 7.2.2 Covering Multiple Active Adversaries

An active adversary can also hide itself by deploying its Tx antenna and Rx antenna at different locations. Thus Aegis still need to cover the potential adversary region. However, multiple active adversaries could introduce complex potential adversary region. As shown in Figure 10(b), Eve 1 works on the  $2.4GHz$  band, while Eve 2 works on the  $5GHz$  band. The adversary regions created by two active adversaries can be merged as one. In this case, Aegis uses both Tx 1 and Tx 2 to cover the merged adversary region with distorted signal on both  $2.4GHz$  and  $5GHz$  bands.

Eve 1 and Eve 2 can also share the same frequency band by alternatively transmitting signal. As shown in Figure 10(c), Eve 1 and Eve 2 adopt Carrier Sense Multiple Access (CSMA) to avoid the collision. When Eve 1 is transmitting signal, Aegis only uses Tx 1 to cover the adversary region brought by Eve 1. When Eve 2 is transmitting as shown in Figure 10(d), Aegis only uses Tx 2.



## 8 IMPLEMENTATION & DEPLOYMENT

### 8.1 System Implementation

The hardware platform of Aegis is implemented as follow: we use multiple amplifiers (ZJL-6G) and a MUX (NI-2591) to build the amplifying circuit. The input of the circuit is connected to an omni-directional antenna. The output of the circuit is connected to two directional antennas (QRG-218/A). Each directional antenna is attached to a stepper motor (NMB P14329-ND), which is controlled by the motor driver (TRINAMIC TCMC-1311). To create Doppler shift in the distorted signal, we attached a fan (DELTA EFB1324SHE-EP) to the front of the directional antenna. The hardwares can be seen in Figure 12.

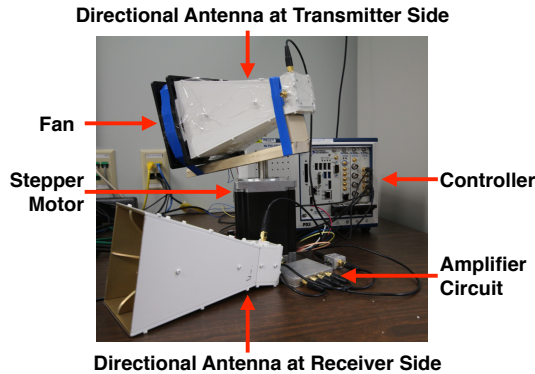


Fig. 12: The hardware implementation of Aegis

To control the hardware platform, we implemented the middleware of Aegis on a NI RF testbed. The testbed directly controls the amplifying circuit, the motor drivers and the fans of the hardware platform.

### 8.2 System Deployment

The system deployment is shown in Figure 11. We perform the experiment in an  $8m \times 10m$  single house. The house contains apparatus for everyday life, including those use AC. We use the house as the private region and the yard around the house as the potential adversary region. The two regions are separated by 30cm thick walls. The private region contains the target human, Carol (legitimate sensing system), and multiple static objects, such as tables and chairs. The potential adversary region contains Aegis, Alice (WiFi access point), Bob (communication device), and Eve (illegitimate sensing system). The directional antennas of Aegis are deployed at the northeast corner and the southwest corner of the private region. We have obtained IRB to conduct the experiments.

### 8.3 Sensing System Implementation

We also build two identical sensing systems. One of them works as Carol (legitimate sensing system), and the other one works as Eve (illegitimate sensing system). Each sensing system consists of a signal digitizer (PXIe-5622), a signal generator (PXIe-5652), a down-converter (PXIe-5601) and an up-converter (PXIe-5450).

## 9 EVALUATION ON ACTIVITY RECOGNITION

We evaluate Aegis' impact on activity recognition in two steps: i) We empirically verify that Aegis is able to incapacitate illegitimate sensing systems with negligible interference to legitimate sensing and communication on all the WiFi bands; and that Aegis successfully achieves its design goals. Specifically, we show that the spatial distribution of signature entropy is consistent with the experiment result.

Activities	Explanation	Notation
Arm push	Right arm push forward	AP
Arm wave1	Right arm waves to the right	AW1
Arm wave2	Right arm waves to the left	AW2
Arm wave3	Wave both arms	AW3
Leg Kick1	Right leg kicks forward	LK1
Leg Kick2	Right leg kicks back	LK2
Leg Kick3	Right leg kicks right	LK3
Sit on the Chair	Walks then sit on the chair	SC
Sit on the Ground	Walks then sit on the ground	SG
Body Twist	Move upper body left and right	BT
Walking	Walks through the room	WK
Empty Room	Empty room	ER

TABLE 1: Activities Dataset

### 9.1 Evaluation Setup & Metrics

We use the following metrics to evaluate Aegis' impact on activity recognition systems and communication systems:

- Accuracy of Activity Recognition:** The accuracy of activity recognition is the ratio between the number of correctly classified activities and the total number of performed activities. This metric depicts whether the human activity recognition systems (Carol and Eve) deliver valid results.
- Communication Throughput:** The throughput is the received megabytes per second (MB/s) measured by Bob. The throughput would drop drastically if Aegis blocks the communication.

### 9.2 Empirical Results of Activity Recognition

With Carol and Eve sensing on the 2.4GHz WiFi band, we have 9 volunteers performed 11 types of activities in the private region. Every volunteer repeats each type of activity for 10 times when Aegis is deactivated, and another 10 times when Aegis is activated. The same process is taken when Carol and Eve are sensing on the 5GHz WiFi band. Thus we obtained around 2,000 activity samples in total. The activities are listed in Table 1.

To show Aegis' impact on activity recognition, we plot the heat maps of frequency offset for each activity in Figure 13. (To save space, we only show the recognition result on 2.4GHz WiFi band. In addition, since the result from Eve is similar with Carol when Aegis is deactivated, we just show Carol's result and list it as the control group.) When Aegis is activated, the heat map of the signal received by Eve contains lots of noise, which obfuscates the patterns of human activities. On the other hand, the signal received by Carol contains much less noise thus shows clear patterns of human activities.

Figure 14 shows the confusion matrices for activity recognition when Aegis is activated. On the 2.4GHz band, the overall recognition accuracy of Carol is 81.8% while that of Eve is 14.17%. On the 5GHz band, Carol has an overall recognition accuracy of 74.3% while Eve only has an accuracy of 7.91%, which is even lower than a random guessing. Notice that the recognition accuracy is higher on 2.4GHz, this is because the attenuation and propagation loss of 5GHz signal are higher than those of 2.4GHz signal.

To show the quantized result, we plot the recognition accuracy of Carol and Eve on 2.4GHz WiFi band in Figure 15. When Aegis is deactivated, both Carol and Eve achieve similar recognition accuracy. However, when Aegis is activated, the recognition accuracy of Eve drops dramatically while the accuracy of Carol only decreases by 0.08, which



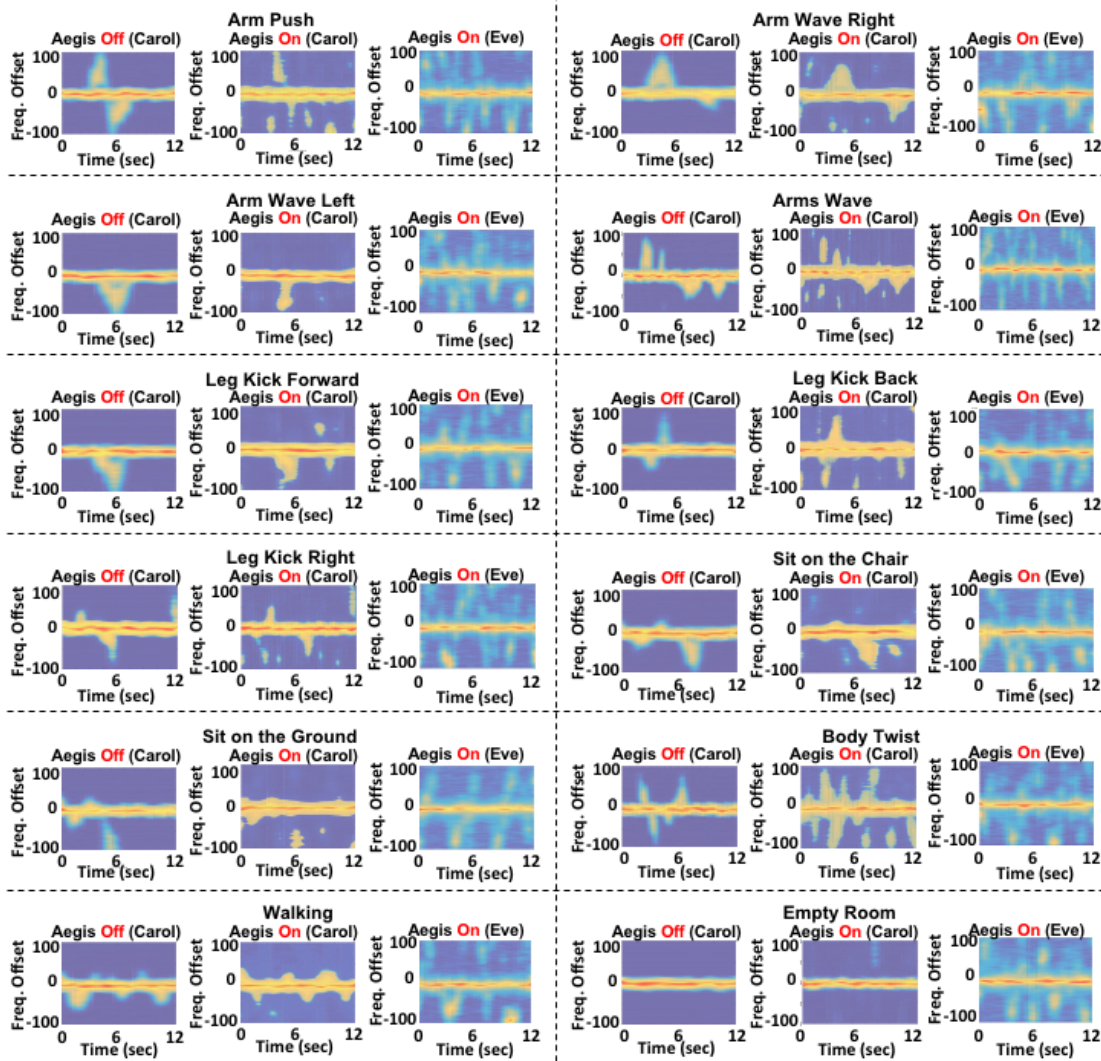


Fig. 13: Heat maps of frequency offset for each type of activity on 2.4 GHz WiFi band. When Aegis is activated, Eve receives signal with obfuscated patterns, but Carol can still get valid patterns.

		Recognized Activity (Carol—2.4 GHz)											
Ground Truth		AP	AW	AW	AW	LK	LK	LK	SC	SG	BT	WK	ER
	AP	0.85	0.03	0.01	0.03	0.02	0	0.01	0	0.04	0	0.01	0
	AW	0.03	0.82	0	0.03	0.01	0.02	0.03	0	0.02	0.02	0.02	0
	AW	0.01	0	0.89	0.03	0.01	0.02	0	0.02	0.02	0	0	0
	AW	0.03	0.03	0.03	0.82	0.02	0.02	0.02	0.01	0.01	0	0	0.01
	LK1	0.02	0.01	0.01	0.02	0.73	0.06	0.09	0.03	0.02	0.01	0	0
	LK2	0	0.02	0.02	0.02	0.06	0.71	0.09	0	0.02	0.03	0.03	0
	LK3	0.01	0.03	0	0.02	0.09	0.09	0.7	0.01	0.03	0.01	0.01	0
	SC	0	0	0.02	0.01	0.03	0	0.01	0.82	0.03	0.05	0.01	0.02
	SG	0.04	0.02	0.02	0.01	0.02	0.02	0.03	0.03	0.79	0	0	0.02
	BT	0	0.02	0	0	0.01	0.03	0.01	0.05	0	0.85	0.03	0
	WK	0.02	0	0	0	0.03	0.01	0.01	0	0.03	0.01	0.89	0
	ER	0	0	0	0.01	0	0	0	0.02	0.02	0	0	0.95

		Recognized Activity (Eve—2.4 GHz)											
Ground Truth		AP	AW	AW	AW	LK	LK	LK	SC	SG	BT	WK	ER
	AP	0.14	0.07	0.07	0.09	0.08	0.08	0.08	0.08	0.06	0.08	0.08	0.09
	AW	0.07	0.13	0.09	0.08	0.07	0.07	0.07	0.08	0.09	0.08	0.08	0.09
	AW	0.07	0.09	0.16	0.08	0.07	0.08	0.07	0.08	0.08	0.07	0.08	0.07
	AW	0.09	0.08	0.08	0.14	0.08	0.08	0.08	0.08	0.07	0.08	0.07	0.08
	LK1	0.08	0.07	0.07	0.08	0.15	0.08	0.08	0.08	0.07	0.08	0.08	0.08
	LK2	0.08	0.07	0.08	0.08	0.08	0.16	0.08	0.07	0.07	0.08	0.08	0.07
	LK3	0.08	0.07	0.07	0.08	0.08	0.18	0.13	0.08	0.07	0.09	0.09	0.08
	SC	0.08	0.08	0.08	0.07	0.08	0.07	0.08	0.15	0.08	0.07	0.09	0.07
	SG	0.08	0.09	0.08	0.08	0.07	0.07	0.07	0.08	0.17	0.07	0.07	0.07
	BT	0.06	0.08	0.07	0.07	0.08	0.08	0.09	0.07	0.07	0.16	0.08	0.09
	WK	0.08	0.08	0.07	0.08	0.08	0.16	0.09	0.07	0.08	0.09	0.04	0
	ER	0.09	0.09	0.07	0.08	0.08	0.07	0.08	0.07	0.07	0.09	0.04	0.17

		Recognized Activity (Carol—5 GHz)											
Ground Truth		AP	AW	AW	AW	LK	LK	LK	SC	SG	BT	WK	ER
	AP	0.74	0.03	0.05	0.06	0.02	0	0.02	0	0	0.03	0.03	0.02
	AW	0.03	0.67	0.2	0.03	0.01	0	0.02	0	0	0.01	0	0.03
	AW	0.05	0.2	0.69	0	0.03	0.02	0	0	0.01	0	0	0
	AW	0.06	0.03	0	0.74	0.03	0.03	0.03	0.02	0.01	0.02	0.03	0
	LK1	0.02	0.01	0.03	0.03	0.7	0.05	0.06	0	0.01	0.07	0.02	0
	LK2	0	0	0.02	0.03	0.05	0.69	0.07	0.06	0.03	0.03	0.02	0
	LK3	0.02	0.02	0	0.03	0.06	0.07	0.6	0.08	0.05	0.03	0.04	0
	SC	0	0	0	0.02	0	0.06	0.08	0.77	0.02	0.01	0.01	0.03
	SG	0	0	0.01	0.01	0.01	0.03	0.05	0.02	0.82	0.02	0.01	0.02
	BT	0.03	0.01	0	0.02	0.07	0.03	0.03	0.01	0.02	0.78	0	0
	WK	0	0	0.03	0.02	0.02	0.04	0.01	0.01	0	0.03	0.83	0.01
	ER	0.02	0.03	0	0	0	0	0	0.03	0.02	0	0.01	0.89

		Recognized Activity (Eve—5 GHz)											
Ground Truth		AP	AW	AW	AW	LK	LK	LK	SC	SG	BT	WK	ER
	AP	0.08	0.09	0.08	0.07	0.07	0.08	0.08	0.08	0.08	0.1	0.09	0.09
	AW	0.09	0.08	0.09	0.08	0.07	0.07	0.08	0.08	0.09	0.08	0.1	0.09
	AW	0.08	0.09	0.09	0.09	0.07	0.08	0.07	0.1	0.08	0.09	0.08	0.08
	AW	0.07	0.08	0.09	0.08	0.08	0.09	0.08	0.08	0.09	0.09	0.09	0.08
	LK1	0.07	0.07	0.07	0.08	0.09	0.1	0.08	0.08	0.09	0.1	0.09	0.08
	LK2	0.08	0.07	0.08	0.09	0.1	0.08	0.09	0.07	0.09	0.08	0.08	0.09
	LK3	0.09	0.08	0.07	0.08	0.08	0.09	0.09	0.08	0.07	0.1	0.09	0.08
	SC	0.08	0.08	0.1	0.09	0.08	0.07	0.08	0.08	0.08	0.08	0.09	0.09
	SG	0.08	0.09	0.08	0.08	0.09	0.09	0.07	0.08	0.07	0.1	0.08	0.09
	BT	0.1	0.08	0.09	0.09	0.1	0.08	0.1	0.08	0.1	0.05	0.06	0.07
	WK	0.1	0.08	0.09	0.09	0.08	0.09	0.09	0.08	0.06	0.09	0.06	0.09
	ER	0.09	0.09	0.08	0.08	0.08	0.09	0.08	0.09	0.09	0.07	0.0	0.1

Fig. 14: Confusion Matrices of Activity Classification on 2.4GHz and 5GHz WiFi Bands with Aegis activated.

is still high enough for legitimate activity recognition. The case of  $5GHz$  is similar.

To show the fan attached to the directional antenna does affect the signature entropy, we show the empirical results in Figure 18. We can see the entropy increases with fan speed and gain.

To testify that Aegis does not disturb communication, we use a laptop (Dell XPS 15) as Bob and install Wireshark on it to monitor its communication throughput. Figure 16 shows the throughput on the  $2.4GHz$  and  $5GHz$  bands with Aegis deactivated and activated. Contrary to our expectation, the throughputs are improved by Aegis. This is because the relayed signal enhances the signal received by Bob. With the above results, we claim that Aegis is able to preserve communication while incapacitating illegitimate sensing.

### 9.3 System Insight Analysis

To prove that Aegis achieves its design goals, we need to explain the empirical experiment result with the theoretical model of Aegis. Specifically, since Aegis obfuscates human motion information by raising the signature entropy in the signal, we need to show that the signature entropy of the signal received in the potential adversary region is relatively high while the signature entropy of the signal received in the private region is relatively low. For this purpose, we measure the spatial distribution of the entropy in our experimental environment as follow: with Aegis activated, we use the sensing system to scan the whole area with a step length of  $1m$ . For each point, we measure the entropy for 10 times with different random status of Aegis, which gives us 10 sets of entropy. Then we perform interpolation on each set of data. As the final step, we plot the average value of the 10 set entropy data. The location of each sampling point is shown in Figure 17(a).

The distribution of the signature entropy is shown in Figure 17(b): the entropy is high in the potential adversary region, which causes the obfuscated patterns in Figure 13. In the private region, the entropy is relatively low, which matches the fact that the signal received by Carol contains much less noise. To be more precise, we show the relationship between the signature entropy and the classification correctness in Figure 17(c): when the entropy is high (1.0), the correctness is less than 10%. As the entropy decreases to 0.14, the correctness raises to 83%. There are two phenomenon worth noticing in Figure 17(c): Firstly, the volunteers performed actions in the region that the entropy is equal or lower than 0.2 to get the result. Secondly, the

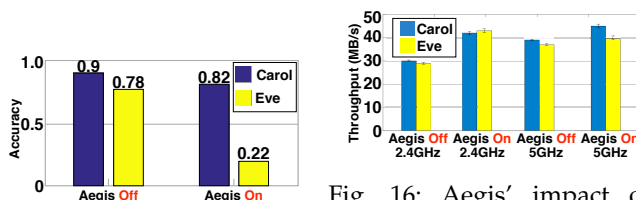


Fig. 15: Recognition accuracy of Carol and Eve with Aegis deactivated and activated on  $2.4GHz$  WiFi band.

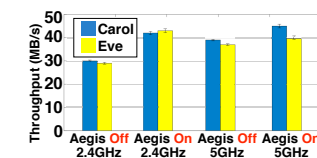


Fig. 16: Aegis' impact on the throughput of Bob (legitimate communication device) on  $2.4GHz$  and  $5GHz$  bands. The throughput is improved because the relayed signal enhances the overall received signal.

entropy and the tracking correctness is not linearly mapped to each other. This is because the randomness introduced by Aegis and the machine learning technology we used for activity recognition.

## 10 EVALUATION ON TRACKING

In this experiment, our volunteers walk along a predefined path in the private region and our sensing systems sense the trajectories of our volunteers every  $0.2s$ . As shown in Figure 19(a), the path is a broken line with multiple turning points. The horizontal span is  $2m$  and the vertical span is  $6m$ . The total length of the path is  $16.5m$ .

In the rest of this section, we first introduce the scheme of our tracking system. Then we demonstrate how we measure the accuracy of the tracking result. After that, we show the sensed trajectory and the tracking accuracy with Aegis deactivated and activated. At last, we analyze the result to show the system insight.

### 10.1 Evaluation Metric

To get a metric that depicts the difference between the tracking result and the ground truth, we leverage the fact that the sensed trajectory consists of multiple sensed locations with timestamps. Assuming the human is moving at a constant speed, we can get the actual location of the human at the time-stamped. Formally speaking, given a time point  $t$ , the tracking system gives a function  $f(t) = (x_s, y_s)$ , where  $(x_s, y_s)$  is the sensed coordination of the human. The ground truth gives another function  $g(v, t) = (x, y)$ , where  $v$  is the speed of the moving human, and  $(x, y)$  is the actual coordination of the human. We define the **tracking error distance**  $d_{err}$  between  $(x, y)$  and  $(x_s, y_s)$  as:

$$d_{err} = \sqrt{(x - x_s)^2 + (y - y_s)^2} \quad (11)$$

For two trajectories, we can get multiple tracking error distances for the sensed locations. Then we use the cumulative distribution function (CDF) [9] of the tracking error distances to depict the difference between the tracking result and the ground truth. We measured ground truth by marking the absolute locations in the house and relating WiFi packets receive and human movement global time during the experiment.

### 10.2 Empirical Results of Tracking

To save space, we only show the tracking result from one of our volunteers on the  $2.4GHz$  WiFi band. Figure 19(b) depicts the trajectories sensed by Carol and Eve when Aegis is deactivated. There are 66 data points on each trajectory (sampled every  $0.2s$  by Carol and Eve). As shown in the figure, both Carol and Eve are able to perform tracking with high accuracy. Figure 20 supports this observation with the corresponding CDF of distance errors. The tracking accuracy of Carol is slightly higher than that of Eve. For example, 80% of Carol's tracking error distance is lower than  $0.5m$  while 80% of Eve's tracking error distance is lower than  $0.85m$ , which is close to the state of art [23], [25]. This is because Carol is closer to the volunteer thus the human motion pattern is more clear.

Figure 19(c) plots the trajectories of the same volunteer when Aegis is activated. The number of data points on each trajectory is still 66 (sampled every  $0.2s$  by Carol and Eve). As shown in this figure, the trajectory sensed by Eve is drastically randomized thus cannot give any valid

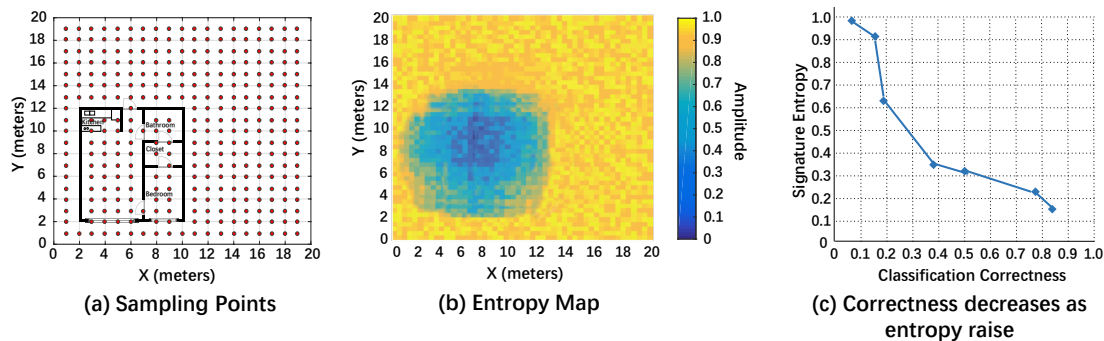


Fig. 17: The distribution of signature entropy. The entropy in the potential adversary region is significantly higher than that in the private region.

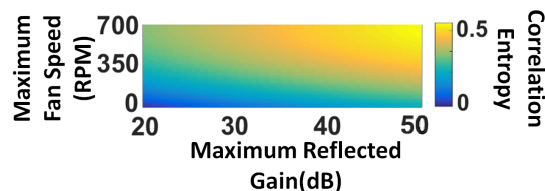


Fig. 18: The distribution of signature entropy with various fan speed and gain.

information about human motion. On the other hand, the trajectory sensed by Carol is barely affected. This observation is also supported by Figure 20. When Aegis is activated, the minimum tracking error distance of Eve is larger than 2m and the median tracking error distance is about 2.35m. On the other hand, the median error distance of Carol is 0.5m, which is at the same level as state of art [23], [25] and is enough to maintain an acceptable accuracy.

**Summary:** *Aegis disturbs the trajectory sensed by Eve but barely affects Carol on all the WiFi bands.*

### 10.3 System Insight Analysis

To explain the results of tracking with the entropy map in Figure 17(b), we need to prove that Aegis raises the signature entropy to the same level no matter the entropy is calculated based on RSS, CSI or delay. Failing to prove that means Aegis cannot incapacitate different types of illegitimate sensing systems with the same performance. For example, if the entropy raises less when calculated based on RSS than delay, the illegitimate sensing systems based on RSS would have better accuracy than the ones based on delay.

We measure the entropy in the signal based on RSS, CSI and delay, respectively. The results are shown in Figure 21: When Aegis is deactivated, the entropy measured by Carol and Eve are at the same level. When Aegis is activated, the entropy measured by Carol raise slightly, but the measured by Eve based on RSS, CSI and delay are all close to 1. Thus we get the following insight:

**Insight:** *Aegis has the same impact on sensing systems that measure RSS, CSI or delay, thus achieves its design goals regardless of the type of eavesdroppers.*

## 11 CONCLUSION

To address the privacy leakage issue in RF sensing, we introduce Aegis, a novel system that i) defends against both passive eavesdroppers and active adversaries; ii) preserves the legitimate RF sensing in the private region; and iii) has minimum interference to the on-going WiFi communication.

Our extensive evaluations in real-world settings demonstrate the effectiveness of our system in both 2.4 GHz and 5 GHz WiFi bands. For example, when Aegis is activated, the accuracy of legitimate sensing system only decreases by 0.08, while the accuracy of the illegitimate sensing system is as low as 0.04. In the meantime, the data communication is not affected.

This work is supported by NSF grants CNS-1652669 and CNS-1539047.

## REFERENCES

- [1] Doppler fan. <https://physics.wvu.edu/doppler-fan>.
- [2] Heba Abdelnasser, Moustafa Youssef, and Khaled A Harras. Wigset: A ubiquitous wifi-based gesture recognition system. In *INFOCOM*, 2015.
- [3] Fadel Adib, Chen-Yu Hsu, Hongzi Mao, Dina Katabi, and Frédo Durand. Capturing the human figure through a wall. In *TOG*, 2015.
- [4] Fadel Adib and Dina Katabi. See through walls with wifi! In *SIGCOMM*, 2013.
- [5] Kamran Ali, Alex X Liu, Wei Wang, and Muhammad Shahzad. Keystroke recognition using wifi signals. In *MobiCom*, 2015.
- [6] Dinesh Bharadia and Sachin Katti. Fastforward: Fast and constructive full duplex relays. In *SIGCOMM*, 2014.
- [7] Zicheng Chi, Yao Yao, Tiantian Xie, Zhichuan Huang, Michael Hammond, and Ting Zhu. Harmony: Exploiting coarse-grained received signal strength from iot devices for human activity recognition. In *ICNP*, 2016.
- [8] Robert Martin Eisberg, Robert Resnick, Susan M Lea, and John Robert Burke. *Modern Physics*. New York: John Wiley and Sons, 1961.
- [9] J.E. Gentle. *Computational Statistics*. Springer, 2009.
- [10] Jon Gjengset, Jie Xiong, Graeme McPhillips, and Kyle Jamieson. Phaser: Enabling phased array signal processing on commodity wifi access points. In *MobiCom* 2014.
- [11] Geoffrey Grimmett and David Stirzaker. *Probability and random processes*. Oxford university press, 2001.
- [12] Chunmei Han, Kaishun Wu, Yuxi Wang, and Lionel M Ni. Wifall: Device-free fall detection by wireless networks. In *INFOCOM*, 2014.
- [13] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. Securing rfids by randomizing the modulation and channel. In *USENIX*, 2015.
- [14] Feng Hong, Yongtuo Zhang, Zhao Zhang, Meiyu Wei, Yuan Feng, and Zhongwen Guo. Wap: Indoor localization and tracking using wifi-assisted particle filter. In *IEEE LCN*, 2014.
- [15] Mohd Nizam Husen and Sukhan Lee. Indoor human localization with orientation using wifi fingerprinting. In *ICUIMC*, 2014.
- [16] Ossi Johannes Kaltiokallio, Hüseyin Yigitler, Riku Jäntti, and Neal Patwari. Non-invasive respiration rate monitoring using a single cots tx-rx pair. In *IPSN*, 2014.
- [17] Youngwook Kim and Hao Ling. Human activity classification based on micro-doppler signatures using a support vector machine. In *IEEE TGRS*, 2009.
- [18] Santosh Nannuru, Yunpeng Li, Mark Coates, and Bo Yang. Multi-target device-free tracking using radio frequency tomography. In *ISSNIP*, 2011.



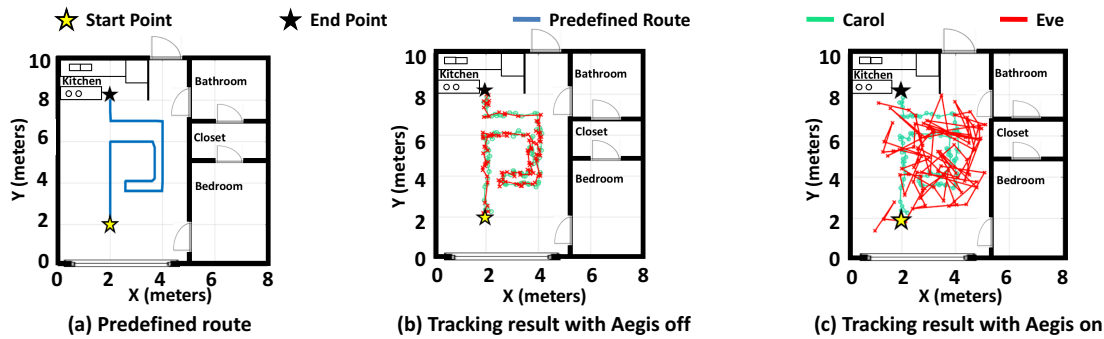


Fig. 19: The predefined route and the tracking result from one of our volunteers. Aegis prevents Eve from tracking human while Carol can still achieve high tracking accuracy.

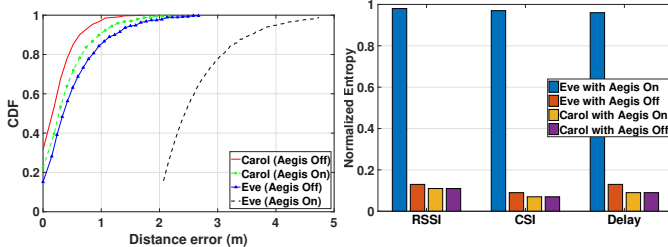


Fig. 20: The CDF of tracking error distance measured by Eve gets close to 1 when Aegis is activated. Eve and Carol with Aegis activated and deactivated.

Fig. 21: Signature entropy Eve gets close to 1 when Aegis is activated. It does not matter Eve uses RSS, CSI or delay.

- [19] Qifan Pu, Sidhant Gupta, Shyamnath Gollakota, and Shwetak Patel. Whole-home gesture recognition using wireless signals. In *MobiCom*, 2013.
- [20] Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. Phycloak: Obfuscating sensing from communication signals. In *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, NSDI'16, pages 685–699, Berkeley, CA, USA, 2016. USENIX Association.
- [21] G Radha Rani and GSN Raju. Transmission and reflection characteristics of electromagnetic energy in biological tissues. *International Journal of Electronics and Communication Engineering*, 6(1):119–129, 2013.
- [22] Stephan Sigg, Ulf Blanke, and Gerhard Troster. The telepathic phone: Frictionless activity recognition from wifi-rssi. In *PerCom*, 2014.
- [23] Deepak Vasisht, Swarun Kumar, and Dina Katabi. Decimeter-level localization with a single wifi access point. In *Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation*, NSDI'16, pages 165–178, Berkeley, CA, USA, 2016. USENIX Association.
- [24] Guanhua Wang, Yongpan Zou, Zimu Zhou, Kaishun Wu, and Lionel M Ni. We can hear you with wi-fi! In *MobiCom*, 2014.
- [25] Ju Wang, Hongbo Jiang, Jie Xiong, Kyle Jamieson, Xiaojang Chen, Dingyi Fang, and Binbin Xie. Lifs: Low human-effort, device-free localization with fine-grained subcarrier information. In *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking*, *MobiCom '16*, pages 243–256, New York, NY, USA, 2016. ACM.
- [26] Wei Wang, Alex X Liu, Muhammad Shahzad, Kang Ling, and Sanglu Lu. Understanding and modeling of wifi signal based human activity recognition. In *MobiCom*, 2015.
- [27] Wei Wang, Alex X. Liu, Muhammad Shahzad, Kang Ling, and Sanglu Lu. Understanding and modeling of wifi signal based human activity recognition. In *MobiCom*, 2015.
- [28] Yan Wang, Jian Liu, Yingying Chen, Marco Gruteser, Jie Yang, and Hongbo Liu. E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures. In *MobiCom*, 2015.
- [29] Yi Wang, Xinli Jiang, Rongyu Cao, and Xiyang Wang. Robust indoor human activity recognition using wireless signals. In *Sensors*, 2015.

- [30] Joey Wilson and Neal Patwari. Through-wall tracking using variance-based radio tomography networks. In *arXiv*, 2009.
- [31] Jie Xiong and Kyle Jamieson. Arraytrack: A fine-grained indoor location system. In *NSDI*, 2013.
- [32] Chenren Xu, Bernhard Firner, Yanyong Zhang, Richard Howard, and Jun Li. Exploiting human mobility trajectory information in indoor device-free passive tracking. In *IPSN*, 2012.
- [33] Zheng Yang, Zimu Zhou, and Yunhao Liu. From rssi to csi: Indoor localization via channel response. In *CSUR*, 2013.
- [34] Jin Zhang, Bo Wei, Wen Hu, and Salil S Kanhere. Wifi-id: Human identification using wifi signal. In *IEEE DCOSS*, 2016.
- [35] Qingquan Zhang, Wei Xu, Zhichuan Huang, Ziqiao Zhou, Ping Yi, Ting Zhu, and Sheng Xiao. Context-centric target localization with optimal anchor deployments. In *ICNP*, 2015.
- [36] Mingmin Zhao, Tianhong Li, Mohammad Abu Alsheikh, Yonglong Tian, Hang Zhao, Antonio Torralba, and Dina Katabi. Through-wall human pose estimation using radio signals. In *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2018.
- [37] Gan Zheng, Ioannis Krikidis, Jiangyuan Li, Athina P Petropulu, and Björn Ottersten. Improving physical layer secrecy using full-duplex jamming receivers. In *SP*, 2013.



**Yao Yao Yao** Yao Yao is a Ph.D. student in the Department of Computer Science and Electrical Engineering (CSEE), UMBC. He has published multiple papers in top conferences. His research areas include Big Data, Embedded Systems, Cyber-Physical Systems, Mobile Systems, Distributed Systems, Operating Systems, Renewable and Sustainable Energies, Internet of Things, Wireless and Sensor Networks, Network Protocols, Social Networks, and Security.



**Yan Li** Dr. Li is a researcher at UMBC. He believes that disruptive innovations derive from experiments that characterize diverse disciplines phenomena. His approach to research in software, biomedical, and Radio Frequency (RF) engineering involves developing testbed platforms measuring the performance of novel ideas. He develops and implements signal processing systems applied to network and wireless communication systems focused on the physical layer.



**Ting Zhu** Dr. Zhu is an associate professor in the Department of Computer Science and Electrical Engineering (CSEE), UMBC. He has received NSF CAREER award in 2017. His research areas include Big Data, Embedded Systems, Cyber-Physical Systems, Mobile Systems, Distributed Systems, Operating Systems, Renewable and Sustainable Energies, Internet of Things, Wireless and Sensor Networks, Network Protocols, Social Networks, and Security.