Aegis: An Interference-Negligible RF Sensing Shield

Yao Yao, Yan Li, Xin Liu, Zicheng Chi, Wei Wang, Tiantian Xie, Ting Zhu
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County
Email: yaoyaoumbc@umbc.edu, bhyanli@gmail.com, {xinliu1, zicheng1, ax29092, xtiant1, zt}@umbc.edu

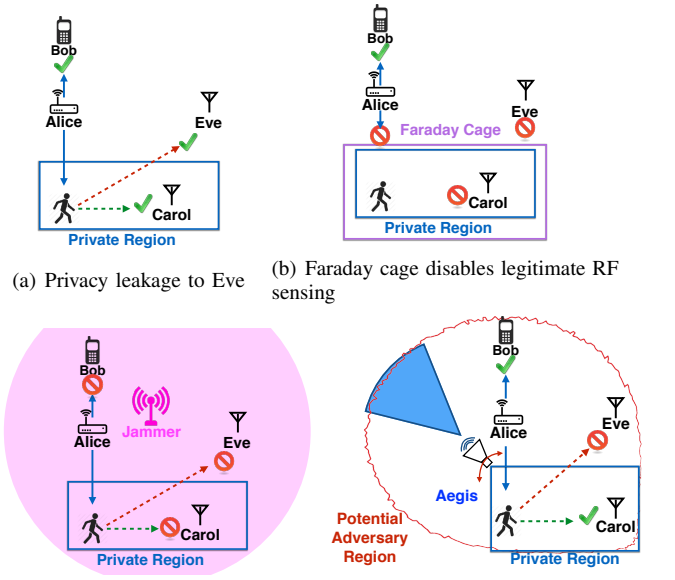
***Abstract*—Researchers have demonstrated the feasibility of detecting human motion behind the wall with radio frequency (RF) sensing techniques. With these techniques, an eavesdropper can monitor people's behavior from outside of the room without the need to access the room. This introduces a severe 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 ongoing WiFi communication; and iii) preserves authorized RF sensing inside the private region. Our extensive evaluation shows that when Aegis is activated, it i) has a negligible impact on the legitimate sensing system; ii) effectively prevents the illegitimate sensing system from sensing human motions. Moreover, the ongoing data communication throughput is even increased in both $2.4GHz$ and $5GHz$ WiFi bands.**

I. Introduction

Radio frequency (RF) sensing techniques leverage the RF signals reflected from a human body for tracking people [1], [2] and recognizing their activities [3], [4] and gestures [5], [6] even behind the wall [7], [8]. These 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) to conduct legitimate human tracking and activity recognition for applications (e.g., smart homes) in the ***private region*** (i.e., a private home). However, Eve (an eavesdropper) could conduct illegitimate RF sensing outside of the private region by analyzing the WiFi signal that bounced off the human body, which means Eve can spy on its neighbors' activities [3], [4] and decipher their password based on keystroke [9].

This privacy leakage issue can be solved by covering the private region with electromagnetic shielding (similar to the Faraday cage) as shown in Figure 1(b). However, this approach is very expensive and would block Alice's signal, which means Carol cannot perform tracking or activity recognition inside the shielded private region. We could use a jammer that distorts the information embedded in the reflected signal everywhere to incapacitate Eve (as shown in Figure 1(c)). However, jamming would also incapacitate Carol, and blocks the ongoing communication between Alice and Bob.

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, Doppler shift, and delay. By rotating the directional antenna while transmitting signal, Aegis can cover all of the potential adversary regions where Eve



(a) Privacy leakage to Eve
(b) Faraday cage disables legitimate RF sensing
(c) Jamming interferes everything
(d) Aegis preserves privacy & enables data communication

Fig. 1. Difference between Aegis and other approaches.

may reside in. Our design goals are i) preventing Eve from acquiring the human location and activities at any potential adversary regions when **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. However, in order to achieve these three design goals, we need to address the following two design challenges:

• **How to identify and cover the potential adversary region?** 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 since Eve does not send 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, and angle-of-arrival). With 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 in the adversary region. 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, Doppler shift, and delay) 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 ongoing 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 amplitude, Doppler shift, and delay of the signal reflected by Aegis, the data communication signal is not noticeably interfered.

In summary, our main contributions are as follows:

• We build a novel hardware platform that can simultaneously change amplitude, Doppler shift, and delay 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: **passive eavesdroppers** and **active adversaries**. We also develop a new metrics, i.e., **signature entropy**, to measure the amount of human motion information embedded in the signal.

• We optimize the control of the RF sensing shield (Aegis) to change the signal amplitude, Doppler shift, and delay to prevent various types of eavesdroppers. In the meantime, the changed signal would only obfuscate 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 the legitimate sensing system only has a negligible decrease, while the illegitimate sensing system is incapacitated. Since Aegis elevated the amplitude of the overall received signal, the throughput of the data communication is increased in both $2.4GHz$ and $5GHz$ WiFi band. Thus the interference to communication is negligible and actually benign.

II. Related Work

We categorize the proposed RF-based human tracking and activity recognition approaches as follow:

I) RSS-based. Received signal strength (RSS)-based methods monitor the signal strength at the receiver side to perform sensing. Researchers have conducted single target tracking [1], [2] and multi-targets tracking [10]. For activity recognition, harmony achieves up to 90% accuracy [11]. Although RSS has been known as a coarse-grained measurement, several approaches are able to recognize gestures [12], [3]. Moreover, RSS can even be used to monitor respiration [4].

II) CSI-based. Channel state information (CSI) is a fine-grained measurement that provides the signal strength as well as the phases of the received signal [13]. Based on CSI, researchers have developed a fall detection system [14] with 87% detection accuracy, and an activity recognition system [15] to recognize 9 activities. In addition, CSI-based approaches have also been developed to identify individuals [16], hear human talks [17], and recognize keystrokes [9].

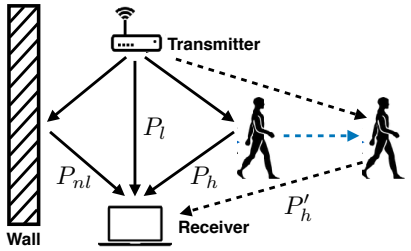


Fig. 2. Multipath effect caused by human motion

Different from the above works, our work addresses the privacy leakage issue due to the RF sensing. The most related work is PhyCloak [18]. However, Aegis is different from PhyCloak in two aspects: **i)** Aegis *simultaneously* incapacitates adversaries in all the WiFi bands within 2.4 GHz and 5 GHz; and **ii)** Aegis is independent of the legitimate sensing systems since it does not require complex signal processing scheme.

III. Understanding RF Sensing

In this section, we introduce the principle of RF-based human motion sensing (i.e., RF sensing), which is also the design basis of Aegis. 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 follows another path, P_h. When the human is moving or performing activities, P_h would become P'_h, which has a different length.

The transition from P_h to P'_h caused by human motion would affect the signal more obviously than fixed paths P_l and P_{nl}. This influence can be detected by measuring three features of the signal: **i) amplitude** (i.e., RSS or CSI values) fluctuates as the human moves. Consequently, the RSS values collected from multiple receivers contains a unique pattern when the human is at a certain location, which enables RSS-based localization and tracking [19]. Through time-frequency analysis, the RSS sequence shows a pattern that matches the movement range and speed of the human activity [9], [11], which enables the activity recognition; **ii) Doppler shift** is introduced by the relative speed between the human body and the receiver [20]. Different human gestures introduce distinguishable patterns in the Doppler shift of RF signals, thus can be used for gesture recognition [5]; **iii) delay** varies with the length of the propagation path since RF signal travels at a constant speed. A longer propagation path brought by human motion would introduce a longer delay, and a shorter path introduces shorter delay. Thus the delay of the received signal could be used to conduct localization [21] and tracking [22].

Most of the RF based human motion sensing systems are built on top of the measurements of RSS, Doppler shift, and delay. The changes in these three features can be represented

by the complex value channel frequency response (CFR) [23]. We denote CFR as $H(f,t)$ and calculate it as follow :

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

where f is the frequency of a wireless channel, t is time. $a_k(f,t)$ is the amplitude attenuation. Δf is the Doppler shift. $\tau_k(t)$ is the delay. 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 motion information embedded in the amplitude, delay and Doppler shift of the signal 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.

IV. Assumptions and Threat Model

In this section, we introduce the assumptions and detailed threat models which reflect real-life scenarios.

A. Assumptions

We assume that there are multiple WiFi access points that work in different frequency bands (e.g., 2.4 GHz and 5 GHz). As shown in Figure 1(a), Carol is in the private region while Eve **can be anywhere outside**. The private region can be an office room or a private house. We assume that the private region is isolated from other areas by walls or non-transparent windows, thus Eve cannot visually peek into it. However, Eve can use any state-of-the-art RF sensing techniques to conduct tracking and human activity recognition.

B. Threat Model

We address two classes of radio-equipped adversaries: passive eavesdroppers and active adversaries.

(a) Passive eavesdroppers: As shown in Figure 1(a), an adversary (Eve) records the RF signals transmitted by Alice and reflected by the human body. Based on the recorded RF signals, Eve can leverage the human activity information embedded in any combination of the three components (i.e., signal amplitude, Doppler shift, and delay) to derive human location and activity [11], [24], [20]. Since our system can distort human motion information embedded in the three components, we ensure that the adversary cannot track people inside the private region or sense his/her activity.

(b) Active adversaries: Such an adversary pretends to be a benign WiFi user and actively sends out RF signals in any WiFi frequency bands (e.g., 2.4 GHz or 5 GHz). The signal sent by the adversary and reflected by the human body inside the private region can be used by the adversary's receiver (Eve) to sense human location and activities. Since Aegis randomizes human motion information embedded in the amplitude, Doppler shift, and delay of the received signals in any frequency band, we can disrupt the adversary's sensing.

Both of the passive eavesdroppers and active adversaries may be in any location outside of the private region. We assume both of the two types of adversaries use omnidirectional antennas. If the adversaries use directional antennas, it would be hard to decide the orientation of the antennas since they cannot visually peek into the private region.

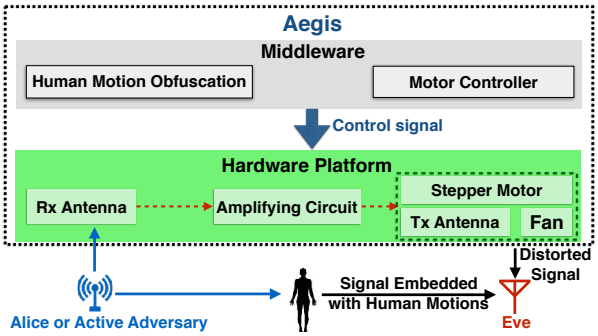


Fig. 3. System Overview of Aegis

V. System Overview

The design goals of Aegis are i) incapacitate the eavesdroppers that work on any WiFi frequency band and at any unknown location outside of the private region; ii) minimize interference to the ongoing WiFi communication; and iii) preserve authorized RF sensing inside the private region. To achieve these goals, Aegis (shown in Figure 3) consists of two parts: hardware platform and middleware.

Hardware platform, which changes the amplitude, delay and Doppler shift of the received RF signals in all of the WiFi bands. The hardware platform contains five main components: **i)** an omnidirectional receiving (Rx) antenna that receives the signal from the environment; **ii)** an amplifying circuit, which amplifies the received signal to distort the human activity information; **iii)** a directional transmitting (Tx) antenna, which transmits the distorted signal; **iv)** a fan, which is attached to the mouth of the Tx antenna to introduce Doppler shift; and **v)** a stepper motor, to which the Tx directional antenna is mounted. The stepper motor can change the orientation of the antenna, which introduces randomized delay.

Middleware, which controls the hardware to generate the distorted signals and cover the potential adversary region. Specifically, the middleware has two parts: **i)** the Human Motion Obfuscation module calculates the speed of the fan, the gain of the amplifying circuit, and the speed of the motor, so that the output signal can obfuscate the human motion information; **ii)** the Motor Controller module estimates the boundary of the potential adversary region based on the estimated location and transmission power of the WiFi transmitter, then calculates the motor's rotation range to cover the adversary region.

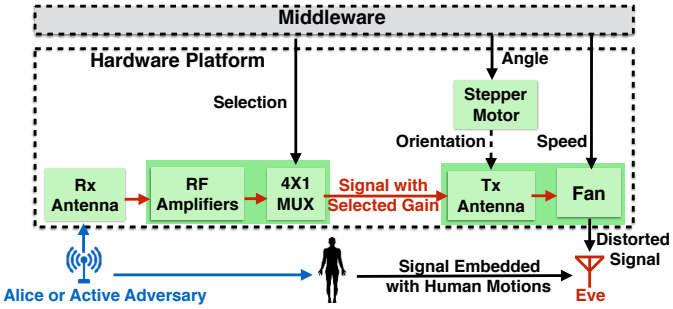


Fig. 4. Hardware Overview

VI. Hardware Design

The design goals of Aegis' hardware platform (shown in Figure 4) are: **i)** distort the human motions embedded in

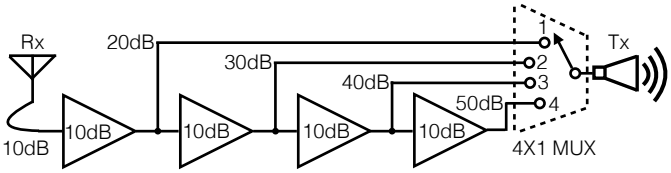


Fig. 5. A Simplified Multistage Amplifier Circuit Diagram

amplitude with the amplifiers; **ii)** distort the human motions embedded in phase with the fan attached to the Tx antenna; and **iii)** distort the human motions embedded in delay by randomizing the rotation speed of the Tx antenna. Aegis changes the signals in all of the WiFi bands (i.e., both 2.4 GHz and 5 GHz). Furthermore, Aegis changes signal rapidly so that Eve cannot filter out the distorted signal.

A. Distorting Reflected Signal's Amplitudes

In order to distort the human motion information embedded in the amplitude of reflected signal, we have to immediately rebroadcast the changed signal. Otherwise, the changed signal could be filtered out by Eve. Traditional systems that relay signal through down-conversion, digitization, analog regeneration, and up-conversion would introduce a delay that can be detected by Eve. To change the amplitude and rebroadcast the signal fast enough, we use the amplifier that amplifies the signal without decoding data. However, a single amplifier has a very limited gain. Thus we designed the multistage amplifier circuit as shown in Figure 5. For the sake of clarity, the impedance matching circuit is not shown.

The circuit contains four RF amplifiers (each with $+10dB$ gain) and a multiplexer (MUX). The received signal is amplified for 10 dB by the receiving circuit, which guarantees that the reflected signal has enough amplitude to disrupt the illegitimate sensing. With a typical high gain $+10dB$ omnidirectional antenna and low noise $+10dB$ amplifier (LNA), the received signal strength is $-35dBm$ at 3 meters with $-50dB$ of RF propagation loss. The reflect coefficient of a human body is around 0.6 [25]. Therefore, to obfuscate the human movements, the reflected signal requires a minimum gain of $-35\ dBm * 0.6 = -21\ dBm$. Thus we should amplify the reflected signal with a minimum gain of $14dB$. The $+10dB$ initial amplification would make sure the reflected signal has enough amplitude after going through the rest of the circuit.

After the initial amplification, we connect four $+10dB$ amplifiers and a 4×1 MUX. The MUX can choose among $20dB, 30dB, 40dB, 50dB$ gains. By randomly switching among these 4 gains, we distort the human movement information embedded in the reflected signal's amplitude. Our evaluation results show that the current 4 gain values are sufficient to distort the human motion information.

B. Distorting Reflected Signal's Doppler Shift

In order to distort the human motion information embedded in the Doppler shift, we place a fan at the mouth of the Tx directional antenna to create random Doppler shift. Doppler shift is the frequency change of a wave when an observer moving relative to the source of the wave [26]. In our system, the source's moving speed is $v_s = 0$, the observer's (i.e., fan blades) moving speed is $v_f = \omega r$, where ω is the angular speed, and r is the fan radius (here $r = 50mm$). The rotational speed of the fan is $\omega_f = \frac{60 \cdot \omega}{2\pi}$. Hence the estimated the Doppler shift Δf created by the fan is:

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

where f_0 is the frequency of the originally received signal.

By randomizing the fan's speed, we introduce randomized Doppler shift to defend against eavesdroppers that utilize the Doppler shift. Our empirical study shows that human motions introduce around $10 \sim 80$ Hz Doppler shift. Thus, from Equation 2, we can estimate the corresponding speed range is from $240 \sim 2,000$ rounds per minute (RPM).

C. Distorting Delay

If we used traditional systems to delay the signal, the delay could be long enough for Eve to filter out the reflected signal. To introduce a delay that is both short and capable of obfuscating human motion information, we leverage the multipath effect. Specifically, we mount the Tx directional antenna to a stepper motor, which can rotate at designated speed. By rotating the directional antenna, we create n propagation paths with different lengths of $L_1, L_2, \ldots, L_i, \ldots, L_j, \ldots, L_n$. Since the RF signal travels at a constant speed, and $L_i \neq L_j$, the delay of the signal changes as the directional antenna rotates. Therefore, by randomizing the rotation speed of the stepper motors, we can introduce random delay into the signal to incapacitate the adversaries.

VII. Middleware Design

As shown in Figure 6, the middleware of Aegis contains two modules:

•Human Motion Obfuscation Module: This module controls the hardware platform (i.e., the MUX, the fan speed, and the motor speed) to distort the physical layer features (i.e., amplitude, Doppler shift, and delay) of the signal. We distort all the three features to defend from unknown eavesdroppers, which could leverage any feature on any WiFi band. To choose appropriate control parameters, we propose **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 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. We mark the potential adversary region with its boundary, which is defined as the **adversary boundary**. However, the adversary boundary could change over time when multiple active adversaries work on the same frequency alternatively. On the other hand, adversary boundaries could overlap when multiple active adversaries work in different frequency bands at the same time. 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.

A. Human Motion Obfuscation Module

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.

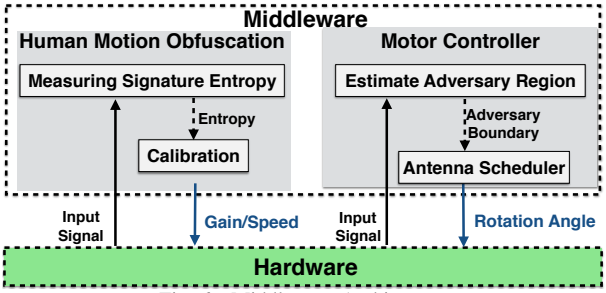


Fig. 6. Middleware Architecture

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. We leverage the observation the human motion information is embedded in the fluctuation of amplitude, Doppler shift, and delay. These features can be unified as:

$$s = \sum_{i=0}^{K} a_i(t_i) e^{-j2\pi f_D T_i(t_i)} \tag{3}$$

where K is the number of signal samples collected during 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. We name s as the human motion signature, which describes the pattern in the signal caused by human motion.

The human motion signature takes a form similar to frequency domain representation of signal. If the frequency domain representation of the received signal "looks like" the human motion signature, the signal contains human motion information. The cross correlation C_{sg} between a human motion signature s and the received signal g tells their similarity [27]:

$$C_{sg} = \sum_{m=0}^{N} s^*[m] g[m+n] \tag{4}$$

where C_{sg} is the probability of signal g containing human motion signature s. We define the correlation signature entropy $H_k(Co_i|Cf_k)$ as:

$$H_k(Co_i|Cf_k) = \sum p(co_i, cf_k) \log \frac{p(co_i)}{p(co_i, cf_k)} \tag{5}$$

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

2) Calibration: To maximize signature entropy of the adversary while minimizing that of authorized receivers, we calibrate Aegis by defining the range of tuning gain, fan speed, and antenna rotation. We define entropy measured by the illegitimate receiver (i.e., adversary) as follow:

$$Adv_{i,k,x,y} = H|Gain_i, Fan_k, \theta_j \tag{6}$$

where $Gain_i$ is the ith array of gain level to test. Fan_k the kth fan speed to test, θ_j is the jth antenna angle to test.

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

$$Auth_{i,k,x,y} = H_n|Gain_i, Fan_k, \theta_j \tag{7}$$

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 algorithm to accomplish this goal. Specifically, we try every combination of the parameters to find the maximum entropy difference.

3) Impact on Communication: In this section, we discuss interference robustness of the most common communication schemes under Aegis. Since the amplitude modulation is deprecated due to multipath effect, we only discuss the phase and frequency modulation methods. We model multipath and Doppler shifts on a sine RF signals as follows:

$$(A \pm A_m)\, e^{j2\pi[f_c(t+T_m)+f_d(t+T_m)]} \tag{8}$$

where A is the amplitude of the sent signal, 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 time of the NLoS path.

Therefore, we can define coherence of time as T_c and the range of frequency drifts defined as B_d.We get that $T_c = \frac{1}{B_d}$.

For a receiver to recover from the Doppler Effect interference, it must sample $T_c/2$ samples. 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 fast enough digitizer, propagation diversity such as multiple-input and multiple-output (MIMO), and enough spread between carrier frequencies.

B. Motor Controller Module

In this section, we demonstrate how Aegis covers the potential adversary region.

1) Covering Passive Adversaries:

A passive adversary is hard to locate since it stays silent while sensing, but it needs to stay relatively close to the transmitter. Otherwise, the signal would fade drastically and the signature entropy would be too high. 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, the adversary can not sense human motion.

To cover the potential adversary region, we need to know its location and shape. Ideally, the center of the potential adversary region is the transmitter, and the shape should be a circle. 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 entropy map, 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 **ii)** what is the range of rotation angle of each antenna?

Figure 7(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°, which contains the distorted potential adversary region.

Note that the adversary may not be continuously covered by the rotating Tx directional antenna, thus can obtain fractions of correct human motion information. However, human motions

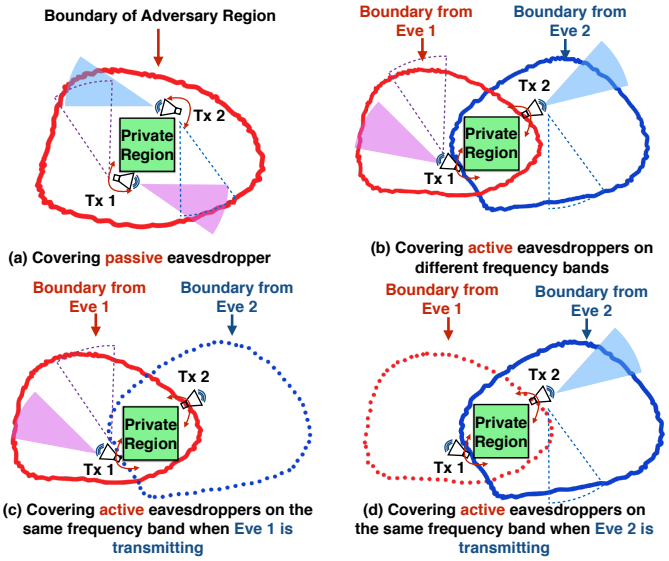


Fig. 7. Antenna deployment and schedule with passive and active adversaries.

usually take seconds, which is long enough for the directional antenna to scan the region multiple times. Thus the adversary would not get fully correct results.

2) Covering Active Adversaries: Aegis can incapacitate an active adversary by covering the potential adversary region since the Rx antenna of the active adversary also has to stay in the region. However, multiple active adversaries could introduce a complex region. As shown in Figure 7(b), Eve 1 works on the $2.4GHz$ band while Eve 2 works on the $5GHz$ band. Their adversary regions can be merged as one. Thus Aegis uses both antennas 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 band by adopting Carrier Sense Multiple Access (CSMA) to avoid the collision. Aegis activates Tx 1 when Eve 1 is transmitting as shown in Figure 7(c) and activates Tx 2 when Eve 2 is transmitting as shown in Figure 7(d) to cover all the adversary regions.

Summary: *Aegis dynamically controls the Tx directional antennas to incapacitate hidden adversaries on different frequency bands.*

VIII. Implementation & Deployment

In this section, we introduce the implementation and deployment of our experimental platform.

A. System Implementation

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 omnidirectional 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 TMCM-1311). We attached a fan (DELTA EFB1324SHE-EP) to the front of the directional antenna. We implemented the middleware of Aegis on a NI RF testbed.

B. System Deployment

We perform the experiment in an $8m \times 10m$ single house. 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. As shown in Figure 8, the private region contains the target human, Carol (legitimate sensing system), and multiple static objects. 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 and the southwest corner of the private region.

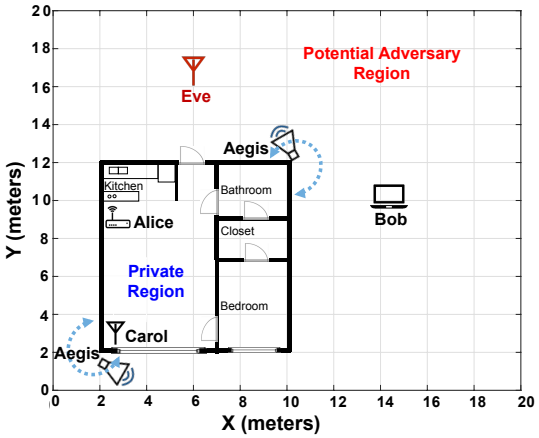


Fig. 8. The deployment of Aegis, Alice (WiFi access point), Bob(legitimate communication device), Carol (legitimate sensing system) and Eve (illegitimate sensing system) .

C. Sensing System Implementation

To test the performance of Aegis, we also build two identical sensing systems that work as Carol (legitimate sensing system) and Eve (illegitimate sensing system) respectively. Each sensing system consists of a signal digitizer (PXIe-5622), a signal generator (PXIe-5652), a down-converter (PXIe-5601) and an upconverter (PXIe-5450).

The sensing systems measure RSS, CSI, and delay. To get clear patterns of human motions, we preprocess the data as follow: **i) RSS:** We performed band-pass filtering on the RSS data to enhance fast fading caused by human movements. **ii) Delay:** We measured the delay times using cross-correlation. **iii) CSI:** To determine Doppler shift in CSI, we performed long-integration of Fourier transforms on the CSI values, and then applied a notch filter without frequency shifts.

The sensing systems apply the Bayesian optimization and estimation [28] on the RSS data for tracking, and support vector machine (SVM) [29] to classify the signature extracted from Doppler shift for activity recognition. The systems also measure the signature entropy based on RSS, CSI or delay.

IX. Evaluation on Activity Recognition

In this section, we verify that Aegis can prevent illegitimate activity recognition without blocking communication.

A. Evaluation Setup & Metrics

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

Activities	Explanation	Notation
Arm Wave Left	Right arm waves to the left	AW1
Arm Wave Right	Right arm waves to the right	AW2
Arms Wave	Wave both arms	AW3
Leg Kick Forward	Right leg kicks forward	LK1
Leg Kick Back	Right leg kicks back	LK2
Leg Kick Right	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
Walking	Walks through the room	WK
Empty Room	Empty room	ER

TABLE I
Activities Dataset

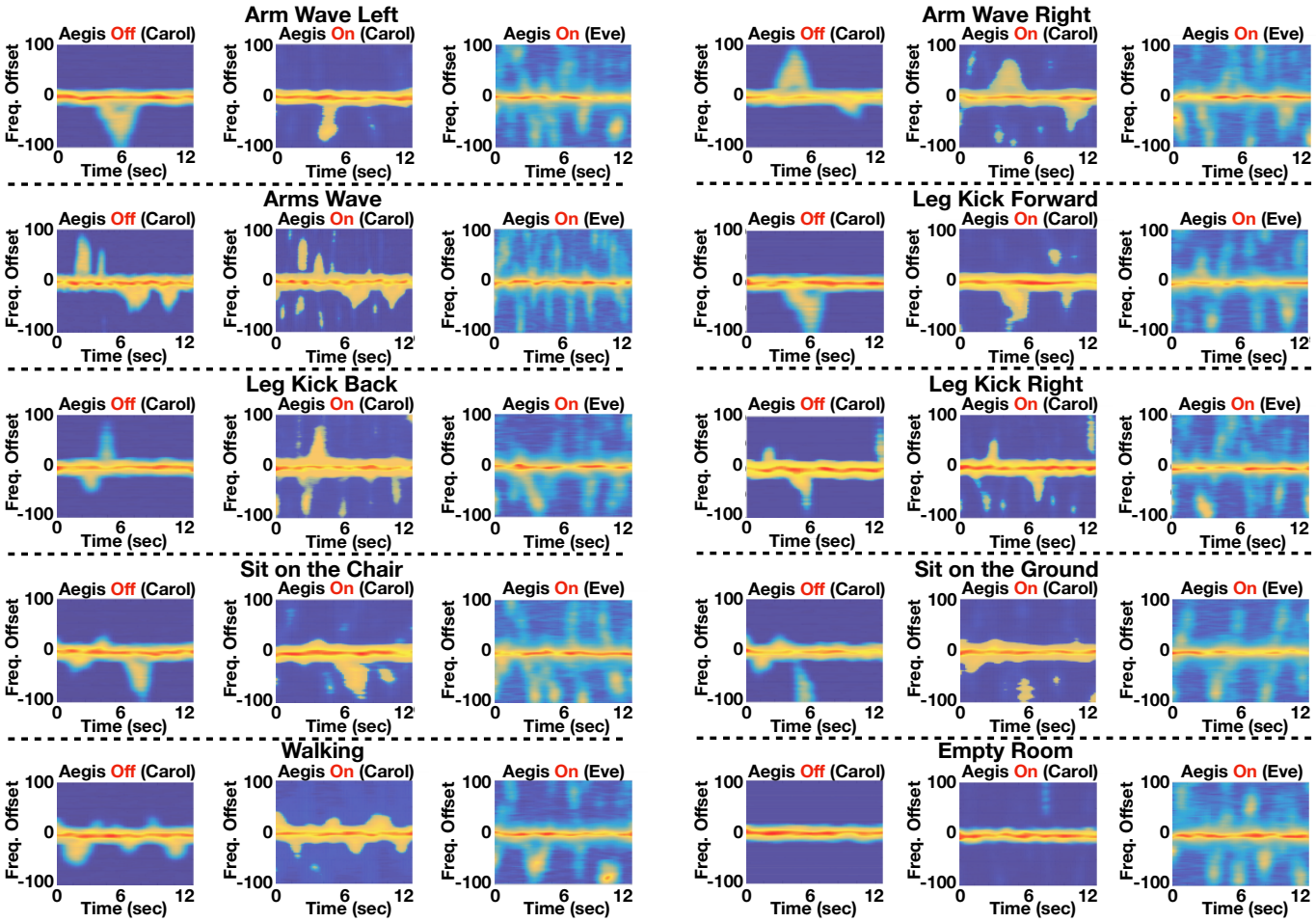


Fig. 9. Heat maps of frequency offset for each type of activity on 2.4 GHz WiFi band. When Aegis is activated, Eve receives signal with obfuscated patterns, but Carol can still get valid patterns.

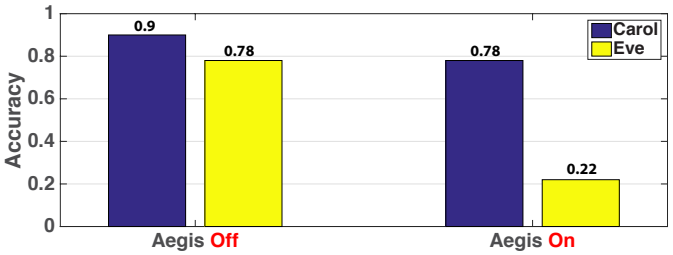


Fig. 10. Recognition accuracy of Carol and Eve with Aegis deactivated and activated on $2.4GHz$ WiFi band.

•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.

•Communication Throughput: The unit of throughput is the received megabytes per second (MB/s).

B. Empirical Results of Activity Recognition

With Carol and Eve sensing on $2.4GHz$ and $5GHz$ WiFi band, we have 9 volunteers performed 10 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. Thus we obtained $3,600$ activity samples. The activities are listed in Table I.

Figure 9 shows the heat maps of frequency offset for each activity. (To save space, we only show the results on $2.4GHz$ WiFi band. We also omit Eve's results when Aegis is deactivated since they are similar to Carol's.) When Aegis is activated, Eve's received signal contains lots of noise, which obfuscates the patterns of human activities. On the other hand, Carol's received signal contains patterns of human activities as clear as when Aegis is deactivated.

To show Aegis' impact on recognition accuracy, we plot the recognition accuracy of Carol and Eve on $2.4GHz$ WiFi band in Figure 10. 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. We omit the similar results on the $5GHz$ band to save space.

Figure 11 shows the confusion matrices when Aegis is activated. On the $2.4GHz$ band, the accuracy of Carol is 78.2% while that of Eve is 22.4%. On the $5GHz$ band, Carol has an overall recognition accuracy of 69.2% while Eve only has an accuracy of 11%, which is close to a random guessing. The recognition accuracy is higher on $2.4GHz$ since the attenuation and propagation loss are lower in this band.

To testify that Aegis preserves communication, we measure the throughput of Carol and Eve. Figure 12 shows the throughput on the $2.4GHz$ and $5GHz$ bands with Aegis deactivated and activated. The result shows the throughput is improved by Aegis. This is because the relayed signal enhances the signal

Recognized Activity (Carol—2.4 GHz)

Ground Truth	AW1	AW2	AW3	LK1	LK2	LK3	SC	SG	WK	ER
AW1	**0.82**	0.03	0.02	0	0.01	0.01	0.05	0.03	0.01	0.02
AW2	0.03	**0.86**	0.02	0.02	0.02	0.02	0.01	0	0	0.02
AW3	0.02	0.02	**0.92**	0.02	0	0.02	0	0	0	0
LK1	0	0.02	0.02	**0.73**	0.09	0.06	0.03	0.03	0.02	0
LK2	0.01	0.02	0	0.09	**0.73**	0.09	0.03	0.02	0.01	0
LK3	0.01	0.02	0.02	0.06	0.09	**0.77**	0.01	0.02	0	0
SC	0.05	0.01	0	0.03	0.03	0.01	**0.52**	0.32	0.03	0
SG	0.03	0	0	0.03	0.02	0.02	0.32	**0.58**	0	0
WK	0.01	0	0	0.02	0.01	0	0.03	0	**0.93**	0
ER	0.02	0	0	0	0	0	0.02	0	0	**0.96**

Recognized Activity (Eve—2.4 GHz)

Ground Truth	AW1	AW2	AW3	LK1	LK2	LK3	SC	SG	WK	ER
AW1	**0.2**	0.1	0.08	0.07	0.1	0.11	0.09	0.09	0.08	0.08
AW2	0.1	**0.21**	0.05	0.08	0.09	0.08	0.1	0.1	0.09	0.1
AW3	0.08	0.05	**0.29**	0.1	0.1	0.08	0.06	0.09	0.07	0.08
LK1	0.07	0.08	0.1	**0.19**	0.09	0.11	0.08	0.07	0.11	0.1
LK2	0.1	0.09	0.1	0.09	**0.19**	0.11	0.08	0.09	0.08	0.07
LK3	0.11	0.08	0.08	0.11	0.11	**0.21**	0.08	0.07	0.08	0.07
SC	0.09	0.1	0.06	0.08	0.08	0.08	**0.21**	0.18	0.08	0.04
SG	0.09	0.1	0.09	0.07	0.09	0.07	0.18	**0.17**	0.05	0.09
WK	0.08	0.09	0.07	0.11	0.08	0.08	0.08	0.05	**0.28**	0.08
ER	0.08	0.1	0.08	0.1	0.07	0.07	0.04	0.09	0.08	**0.29**

Recognized Activity (Carol—5 GHz)

Ground Truth	AW1	AW2	AW3	LK1	LK2	LK3	SC	SG	WK	ER
AW1	**0.73**	0.02	0.05	0.05	0.07	0.03	0.01	0.01	0.01	0
AW2	0.02	**0.8**	0.01	0.03	0.03	0.03	0.02	0.03	0.01	0.02
AW3	0.05	0.01	**0.7**	0.08	0.1	0.03	0.03	0	0	0
LK1	0.05	0.03	0.08	**0.65**	0.05	0.05	0.03	0.04	0.02	0
LK2	0.07	0.03	0.1	0.05	**0.58**	0.06	0.03	0.04	0.04	0
LK3	0.03	0.03	0.03	0.05	0.06	**0.7**	0.07	0.03	0	0
SC	0.01	0.02	0.03	0.03	0.03	0.07	**0.48**	0.32	0	0.01
SG	0.01	0.03	0	0.04	0.04	0.03	0.32	**0.49**	0.03	0.01
WK	0.01	0.01	0	0.02	0.04	0	0	0.03	**0.86**	0.03
ER	0	0.02	0	0	0	0	0.01	0.01	0.03	**0.93**

Recognized Activity (Eve—5 GHz)

Ground Truth	AW1	AW2	AW3	LK1	LK2	LK3	SC	SG	WK	ER
AW1	**0.11**	0.1	0.1	0.1	0.1	0.11	0.09	0.11	0.1	0.08
AW2	0.1	**0.1**	0.12	0.11	0.11	0.09	0.1	0.1	0.08	0.09
AW3	0.1	0.12	**0.11**	0.1	0.1	0.1	0.1	0.08	0.09	0.1
LK1	0.1	0.11	0.1	**0.12**	0.09	0.11	0.1	0.09	0.09	0.09
LK2	0.1	0.11	0.1	0.09	**0.11**	0.09	0.09	0.11	0.11	0.09
LK3	0.11	0.09	0.1	0.11	0.09	**0.1**	0.11	0.09	0.1	0.1
SC	0.09	0.1	0.1	0.1	0.09	0.11	**0.1**	0.11	0.1	0.1
SG	0.11	0.1	0.08	0.09	0.11	0.09	0.11	**0.11**	0.1	0.1
WK	0.1	0.08	0.09	0.09	0.11	0.1	0.1	0.1	**0.11**	0.12
ER	0.08	0.09	0.1	0.09	0.09	0.1	0.1	0.1	0.12	**0.13**

Fig. 11. Confusion matrices of activity classification on $2.4GHz$ and $5GHz$ WiFi bands with Aegis activated.

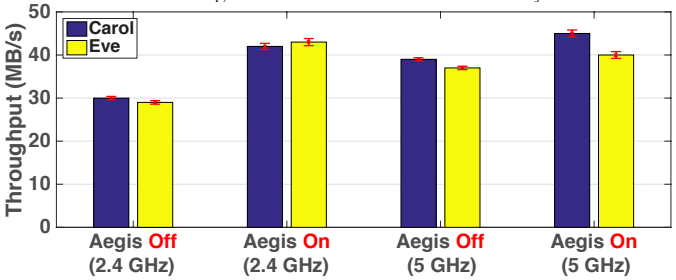


Fig. 12. Aegis improves the throughput on $2.4GHz$ and $5GHz$ bands.

received by Bob.

Summary: *Empirical experiments show that Aegis incapacitates illegitimate sensing systems while preserving legitimate sensing and data communication on all the WiFi bands.*

C. System Insight Analysis

Since Aegis obfuscates human motion information by raising the signature entropy in the signal, we need to testify that the signature entropy measured in the potential adversary region is higher than that measured in the private region. For this purpose, we use the sensing system to scan the whole area with a step length of $1m$ while measuring the signature entropy at every sampling point. The distribution of the signature entropy is shown in Figure 13(a): the entropy is high in the potential adversary region, which causes the obfuscated patterns in Figure 9. The entropy is low in the private region, which matches the clear patterns in Carol's received signal.

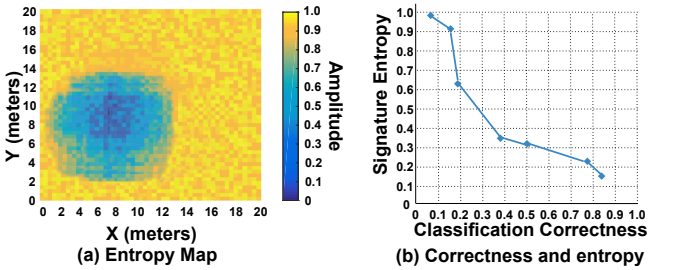


Fig. 13. The entropy in the potential adversary region is significantly higher than that in the private region. High entropy means low classification correctness.

To be more precise, we show the relationship between the signature entropy and the classification correctness in Figure 13(b): 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%. Thus we get an insight of Aegis:

Insight: *Aegis elevates the signature entropy of the signal received in the potential adversary region, but barely affects the signature entropy of the signal received in the private region. Thus Aegis can block Eve at any unknown location in the potential adversary region while not affecting Carol.*

X. Evaluation on Tracking

In this experiment, our volunteers walk along a predefined path in the private region and our sensing systems sense the human's location every $0.2s$. As shown in Figure 14(a), the path is a $16.5m$ broken line with multiple turning points. The horizontal span is $2m$ and the vertical span is $6m$.

A. Evaluation Metric

Assuming the speed of the human is constant, we can get the actual location of the human via time. 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:

$$d_{err} = \sqrt{(x - x_s)^2 + (y - y_s)^2} \quad (9)$$

For two trajectories, we can get multiple tracking error distances. Then we use the cumulative distribution function (CDF) [30] of the tracking error distances to depict the difference between the tracking result and the ground truth.

B. Empirical Results of Tracking

To save space, we only show the tracking result of one volunteers in the $2.4GHz$ WiFi band. Figure 14(a) shows the trajectories sensed by Carol and Eve when Aegis is deactivated. There are 66 points on each trajectory. As shown in the figure, both Carol and Eve are able to perform tracking with high accuracy. Figure 15 supports this observation with the corresponding CDF of distance errors. The tracking accuracy of Carol is slightly higher than that of Eve.

Figure 14(b) plots the trajectories of the same volunteer when Aegis is activated. The trajectory sensed by Eve is drastically randomized, but the trajectory sensed by Carol is barely affected. This observation is also supported by Figure 15. When Aegis is activated, the minimum tracking error distance of Eve is larger than $2m$ and the median tracking

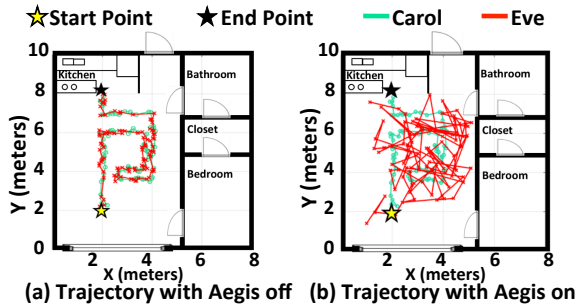


Fig. 14. The predefined route and the tracking result from one of our volunteers. Aegis prevents Eve from tracking human while Carol can still achieve high tracking accuracy.

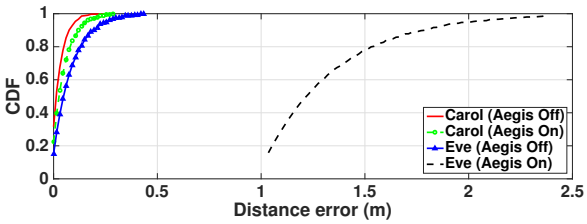


Fig. 15. The CDF of tracking error distance measured by Eve and Carol with Aegis activated and deactivated.

error distance is about $2.35m$. However, the median error distance of Carol is $0.05m$, which is an acceptable accuracy.

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

C. System Insight Analysis

To explain the results of tracking with the entropy map in Figure 13(b), we need to testify that Aegis raises the signature entropy to the same level no matter if the entropy is calculated based on RSS, CSI or delay, which means Aegis incapacitates different types of adversaries with the same performance.

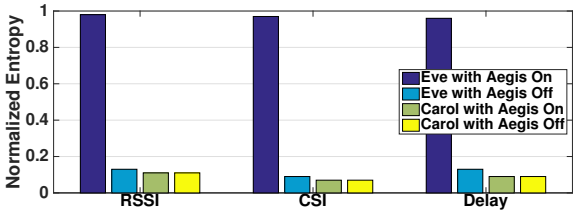


Fig. 16. Signature entropy measured by Eve gets close to 1 when Aegis is activated. It does not matter if Eve uses RSS, CSI or delay.

We measure the entropy in the signal based on RSS, CSI, and delay, respectively. The results are shown in Figure 16. 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 raises slightly, but the entropy 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.*

XI. 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 ongoing 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.

References

[1] M. N. Husen and S. Lee, "Indoor human localization with orientation using wifi fingerprinting," in ICUIMC, 2014.

[2] F. Hong, Y. Zhang, Z. Zhang, M. Wei, Y. Feng, and Z. Guo, "Wap: Indoor localization and tracking using wifi-assisted particle filter," in IEEE LCN, 2014.

[3] H. Abdelnasser, M. Youssef, and K. A. Harras, "Wigest: A ubiquitous wifi-based gesture recognition system," in INFOCOM, 2015.

[4] O. J. Kaltiokallio, H. Yigitler, R. Jäntti, and N. Patwari, "Non-invasive respiration rate monitoring using a single cots tx-rx pair," in IPSN, 2014.

[5] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Whole-home gesture recognition using wireless signals," in MobiCom, 2013.

[6] F. Adib, C.-Y. Hsu, H. Mao, D. Katabi, and F. Durand, "Capturing the human figure through a wall," in TOG, 2015.

[7] F. Adib and D. Katabi, "See through walls with wifi!" in SIGCOMM, 2013.

[8] J. Wilson and N. Patwari, "Through-wall tracking using variance-based radio tomography networks," in arXiv, 2009.

[9] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using wifi signals," in MobiCom, 2015.

[10] S. Nannuru, Y. Li, M. Coates, and B. Yang, "Multi-target device-free tracking using radio frequency tomography," in ISSNIP, 2011.

[11] Z. Chi, Y. Yao, T. Xie, Z. Huang, M. Hammond, and T. Zhu, "Harmony: Exploiting coarse-grained received signal strength from iot devices for human activity recognition," in ICNP, 2016.

[12] S. Sigg, U. Blanke, and G. Troster, "The telepathic phone: Frictionless activity recognition from wifi-rssi," in PerCom, 2014.

[13] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of wifi signal based human activity recognition," in MobiCom, 2015.

[14] C. Han, K. Wu, Y. Wang, and L. M. Ni, "Wifall: Device-free fall detection by wireless networks," in INFOCOM, 2014.

[15] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: device-free location-oriented activity identification using fine-grained wifi signatures," in MobiCom, 2015.

[16] J. Zhang, B. Wei, W. Hu, and S. S. Kanhere, "Wifi-id: Human identification using wifi signal," in IEEE DCOSS, 2016.

[17] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with wi-fi!" in MobiCom, 2014.

[18] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "Phycloak: Obfuscating sensing from communication signals." in NSDI, 2016.

[19] Q. Zhang, W. Xu, Z. Huang, Z. Zhou, P. Yi, T. Zhu, and S. Xiao, "Context-centric target localization with optimal anchor deployments," in ICNP, 2015.

[20] Y. Kim and H. Ling, "Human activity classification based on micro-doppler signatures using a support vector machine," in IEEE TGRS, 2009.

[21] J. Gjengset, J. Xiong, G. McPhillips, and K. Jamieson, "Phaser: Enabling phased array signal processing on commodity wifi access points," in MobiCom 2014.

[22] J. Xiong and K. Jamieson, "Arraytrack: A fine-grained indoor location system." in NSDI 2013.

[23] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of wifi signal based human activity recognition," in MobiCom, 2015.

[24] Y. Wang, X. Jiang, R. Cao, and X. Wang, "Robust indoor human activity recognition using wireless signals," in Sensors, 2015.

[25] G. R. Rani and G. Raju, "Transmission and reflection characteristics of electromagnetic energy in biological tissues," IJECE, vol. 6, no. 1, pp. 119–129, 2013.

[26] R. M. Eisberg, R. Resnick, S. M. Lea, and J. R. Burke, Modern Physics. New York: John Wiley and Sons, 1961.

[27] G. Grimmett and D. Stirzaker, Probability and random processes. Oxford university press, 2001.

[28] G. V. Zàruba, M. Huber, F. A. Kamangar, and I. Chlamtac, "Indoor location tracking using rssi readings from a single wi-fi access point," in Wireless Network, 2007.

[29] J. Y. Chang, K. Y. Lee, K. C. J. Lin, and W. Hsu, "Wifi action recognition via vision-based methods," in ICASSP, 2016.

[30] J. Gentle, Computational Statistics. Springer, 2009.