IS-WARS: Intelligent and Stealthy Adversarial Attack to Wi-Fi-Based Human Activity Recognition Systems

Pei Huang, *Student Member, IEEE*, Xiaonan Zhang, *Member, IEEE*, Sihan Yu, *Student Member, IEEE*, and Linke Guo, *Senior Member, IEEE*

Abstract—The non-intrusive human activity recognition has been envisioned as a key enabler for many emerging applications requiring interactions between humans and computing systems. To accurately recognize different human behaviors, ubiquitous wireless signals are widely adopted, e.g., Wi-Fi signals, whose Channel State Information (CSI) can precisely reflect human movements. Unfortunately, nearly all Wi-Fi-based recognition systems assume a clean wireless environment, i.e., no interference will compromise the developed algorithms, which, apparently, is not feasible in practice. Even worse, for systems using Wi-Fi 2.4GHz signals, the widely existing interference from coexisting protocols, such as ZigBee, Bluetooth, and LTE-Unlicensed, can easily compromise the recognition process, posing a hard limit on further enhancing the accuracy. Therefore, this work uncovers a new signal adversarial attack against Wi-Fi-based human activity recognition systems, by intentionally injecting interference using coexisting protocol signals. The contaminated Wi-Fi signal will distort CSI estimation and finally output a false recognition result. Different from traditional jamming attacks, this new adversarial attack is intelligent and stealthy in terms of avoiding being detected from traffic analysis. Along with both theoretical analysis and extensive real-world experiments, we have shown this newly-identified attack can easily compromise many existing Wi-Fi-based human recognition systems while still bypassing existing schemes for malicious signal detection.

Index Terms—Wireless adversarial example, cross-technology interference, channel state information, human activity recognition

1 Introduction

HUMAN activity recognition, a branch of smart human sensing, has become increasingly vital in advanced human-computer interaction [1] and has been widely integrated with Virtual Reality technology, health monitoring, smart homes, safe driving, security surveillance, etc. The ubiquitousness of human activity recognition applications persuades both academic and industrial communities to explore the ability of non-intrusive sensing. As such, leveraging changes of invisible wireless signals to capture unique activity characteristics becomes a good candidate for further expanding the methodology of human sensing. Among all the commonly accessible signals, the Wi-Fi signal is the handiest one due to its rich information and wide deployment. Most existing Wi-Fi-based human activity recognition systems extract Channel State Information (CSI) for deriving high-accuracy human activities. In particular, the CSI, originally used as a metric to estimate the channel condition, can reflect many regular activities because of its sensitivity to human movements occurred in the transmission paths [2].

In practice, wireless transmissions are vulnerable to the dynamic and complex environments. This vulnerability becomes even more severe when multiple wireless protocols share the same spectrum. These coexisting signals interfere with each other and worsen the transmission environment. Though many works have put efforts in designing advanced de-noising schemes for CSI sequences and lowering the negative effects of environments, existing recognition systems can still get compromised by powerful attackers. For example, a common wireless jammer can take advantage of the MAC-layer protocol, e.g., Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA), to maliciously congest the entire transmission link by adding noises. However, this type of jamming attack is highly perceptible by the transmission pair because it will jeopardize the expected Wi-Fi transmissions. Hence, in this paper we discover a new type of powerful and inconspicuous attack, *IS-WARS*, to compromise the Wi-Fi-based activity recognition system without impacting normal Wi-Fi transmissions. We take advantages of the cross-technology signals to craft a Wi-Fi adversarial example to stealthily compromise the CSI, in order to misclassify the corresponding activities. Compared with the traditional jamming attack, this new attack is more serious in terms of its stealthiness and potential consequences. Taking the smart health monitoring as an example, an abnormal behavior (e.g., falling) can be misclassified as common activities for elderlies living alone,

- *Pei Huang, Sihan Yu, and Linke Guo are with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634 USA. E-mail: {peih, sihany, linkeg}@clemson.edu.*
- *Xiaonan Zhang is with the Department of Computer Science, Florida State University, Tallahassee, FL 32306 USA. E-mail: xzhang@cs.fsu.edu.*

Manuscript received 26 January 2021; revised 19 July 2021; accepted 27 August 2021. Date of publication 8 September 2021; date of current version 11 November 2022.
(Corresponding author: Linke Guo.)
Digital Object Identifier no. 10.1109/TDSC.2021.3110480

resulting in the missing of emergency calls and first aids. To successfully craft the adversarial signals, there are several critical challenges to be considered,

- *Added noises should be imperceptible.* The Wi-Fi MAC-layer protocols will immediately detect the increasing level of noises and drop the crafted adversarial signals.
- *Added noises should bypass the de-noising scheme.* To cause the misclassification of received adversarial example, the level of noises cannot be too small to be removed by de-noising schemes adopted in the recognition system.

The above contradicting requirements cannot be easily fulfilled by simply adding noises for generating the adversarial example. To address these challenges, we apply the cross-technology interference (CTI) on overlapped frequency bands for crafting. The attacker sends controllable noises to intentionally cause the CTI, which will finally contaminate the received CSI sequences. In practice, many overlapping protocols, such as ZigBee and Bluetooth, can cause severe CTI to Wi-Fi traffic over ISM 2.4GHz bands [3], [4], [5]. While most of the previous studies try to avoid CTI to enhance communication performances [6], [7], [8] and some works show that the CSI amplitudes influenced by CTI can be leveraged for cross-technology communication [9], [10], they use machine learning models to handle the features of CTI-interfered CSI as a black box so the detailed and quantified effect of how CTI will impact the CSI remains underexplored. Therefore, for this paper, we will first discuss the principles of state-of-the-art human activity recognition systems, then provide a thorough study on how CTI can modify the CSI sequence, and finally, demonstrate the attacking process of stealthy attacks using the CTI. Our main contributions are listed as follows,

- This paper provides a comprehensive study on quantifying the impact of CTI on normal Wi-Fi transmissions.
- This work identifies a new intelligent and stealthy adversarial attack on many Wi-Fi-based human activity monitoring systems using received CSI sequences and demonstrates the difficulty in mitigating the CTI-based attack.
- Extensive real-world experiments demonstrate the existence and feasibility of the attack.

The rest of this paper is organized as follows. Section 2 gives preliminaries about Wi-Fi-based activity recognition. Section 3 provides an overview of our attack IS-WARS, followed by a feasibility analysis in Section 4. Section 5 shows the detailed design of IS-WARS. Section 6 thoroughly evaluates attack performance. Section 7 discusses related works and Section 8 concludes the paper.

2 Preliminaries

2.1 CSI in Wi-Fi-Based Recognition

Compared to other usable channel properties (e.g., Received Signal Strength (RSS), phases) for activity recognition, CSI, which is a widely used metric in multiple-input/multiple-output (MIMO) radio systems [11] to estimate the channel condition of transmission links, contains more fine-grained information than RSS and is less vulnerable to noises than phase information alone.

Suppose a MIMO communication system has N_{T_X} transmitter antennas and N_{R_X} receiver antennas. $\boldsymbol{x}$ is the sent signal and $\boldsymbol{n}$ denotes the noise. The received signal can be modeled as

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{n},$$

where $\boldsymbol{H}$ is the CSI matrix. $\boldsymbol{H}(f,t)$, which is the CSI matrix measuring channel frequency response in different subcarriers with center frequency f at time t, can be calculated at the receiver side by solving a set of equations using a known transmitted/received signal pair via $\boldsymbol{H}(f,t) = Y(f,t)/X(f,t)$

$$\boldsymbol{H}(f,t) = \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1N_{\mathrm{T_x}}} \\ h_{21} & h_{22} & \cdots & h_{2N_{\mathrm{T_x}}} \\ \vdots & \vdots & \ddots & \vdots \\ h_{N_{\mathrm{R_x}}1} & h_{N_{\mathrm{R_x}}2} & \cdots & h_{N_{\mathrm{R_x}}N_{\mathrm{T_x}}} \end{bmatrix}, \tag{1}$$

where h_{mn} is the complex transmission coefficient from the transmitter's antenna m to the receiver's antenna n. Most of the human behavior recognition systems leverage the changes incurred in h_{mn} and other derived metrics, e.g., Doppler shift, to determine the corresponding activities.

2.2 CTI in Heterogeneous Environment

Due to the wireless coexistence in the 2.4GHz ISM band, CSI can be easily contaminated by interferences from devices using not only traditional Wi-Fi protocols (e.g., 802.11 b/g/n/ac) but also other wireless standards in the overlapped spectrum, such as IEEE 802.15.1 Bluetooth and IEEE 802.15.4, i.e., ZigBee, WirelessHART, and ISA100. The latter, known as Cross-Technology Interference, could bring a detrimental impact to the reliability of Wi-Fi communication, e.g., significant packet loss in a highly crowded heterogeneous environment. Existing works have demonstrated that the preambles of Wi-Fi packets can be impacted and the CSI amplitudes will be greatly altered by on-going ZigBee packets during Wi-Fi transmission when Wi-Fi traffic is not backoff [9].

2.3 Signal De-Noising and Threats

Despite that CTI's interference to CSI has been proved, we have to take the broad spectrum of de-noising approaches into consideration, such as smooth filter [12], low-pass filter [13], principal component analysis (PCA) [14], linear interpolation fitting [15], Kalman filter [16], and wavelet transform [17]. Most of them have been employed in the Wi-Fi-based recognition system to discard unavoidable noises and further capture more accurate human activities. Unfortunately, these de-noising schemes can only help remove the out-band noise. The noise caused by CTI cannot be easily detected and eliminated, which will inevitably contaminate CSI [18]. If no adequate de-noising approaches specifically for CTI noise, it is highly possible that sending malicious cross-technology wireless signals can impact the CSI and further compromise Wi-Fi-based recognition systems.

Recently, there are some noise detecting methods specifically designed for CTI. For example, authors in [10]

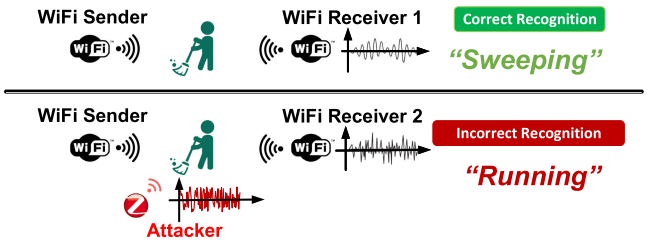


Fig. 1. IS-WARS attack overview.

proposed cyclostationarity analysis that uses the distinct repeating patterns shown by different signals to differentiate between Wi-Fi signals and CTI. They compute the Spectral Correlation Function (SCF) in the frequency domain on each subcarriers. For the subcarriers whose amplitude and phase information are distorted by CTI, some peaks are sufficiently visible on corresponding SCF, while SCF without interference does not exhibit any peak. However, it can only detect the CTI that distributing on a small range of frequencies and tries to recover the interfered subcarriers. It is efficient for detecting unintended CTI but not that useful if the CTI is carefully distributed over a bunch of subcarriers.

3 System Overview and Assumptions

3.1 Problem Definition

We consider a device-free indoor Wi-Fi-based human activity recognition system as described in Fig. 1. When there is a human subject moving around, the Wi-Fi signals sent from Wi-Fi senders are interfered with human body's reflection, so the signals received contain specific and unique changes incurred by different types of human activity. The goal of the recognition system is to find features in each set of numerical changes and map them to the designated activities. The idea of our attack is to deploy a cross-technology signal source, e.g., a ZigBee device, to intentionally send a malicious signal, expecting to create an adversarial example to change CSI at the receiver side and finally cause incorrectly identification of the recognized activity. For example, the uncompromised Wi-Fi receiver 1 can correctly recognize the user's behavior as "sweeping the floor", while the Wi-Fi device 2 suffering the CTI from a nearby ZigBee attacker fails to output the correct behavior.

To design this new attack, named as **I**ntelligent and **S**tealthy adversarial attack to **W**i-Fi-based Human **A**ctivity **R**ecognition **S**ystem (IS-WARS), we mainly consider two different mechanisms in current literature, 1) *Classification-based Approach.* A large quantity of data with known activity labels is collected. Their patterns are learned via clustering, machine learning methods, etc. and further used for classifying unknown ones [19], [20], [21], [22], [23]; 2) *Model-based Recognition.* They theoretically model the relationship between channel properties and human activities, such as Fresnel zone model and velocity model. Common quantities include Angle of Arrival (AoA), Time of Flight (ToF), speed, distance, Doppler shift, and phase [24], [25], [26], [27].

3.2 IS-WARS Attacker Model

A complete IS-WARS attack process includes three steps, 1) sense and observe wireless environment (e.g., sniff Wi-Fi packet), 2) generate interference, and 3) bypass de-noising and cause classifications. Based on the challenges discussed in Section 1, an IS-WARS attacker needs to achieve the following three objectives:

Objective 1. *Before launching an attack, an attacker can obtain preliminary knowledge about the system through sensing and observing. Here, we demonstrate two levels of abilities an attack has.*

- Basic: *Obtain superficial knowledge about the recognition system, such as the frequency band that Wi-Fi senders/receivers are working on, the average statistics of CSI sequences, by sensing and observing the wireless environment. The attacker must know the information of the channel that the Wi-Fi packets are transmitted on. The attacker can sniff CSI multiple times to measure the impact of interference due to the low cost of sensing the system's small-scale, indoor environment.*
- Advanced: *To launch a strong attacker, the attacker may be able to acquire some more advanced information about the system. For example, the attacker may know the deployed locations of Wi-Fi senders/receivers in some cases, such as when the system is deployed in a public indoor area. If the attacker spends enough time sniffing, they can even know how CSI sequences impacted by human activities may look like. The attacker is not necessarily to be very close to the scene when sniffing. The CSI characteristics, including the distinct variances caused by human movements, are detectable even if there is a wall between the sniffer and the receiver [28]. The technical details that cannot be sensed or observed easily, e.g., how the system processes the signals, may not be known to the attacker.*

Objective 2. *The IS-WARS attack has to "*intelligently*" adapt to different wireless environments and device settings based on the acquired knowledge about the recognition system. Meanwhile, the attack should be "*stealthy*" enough to prevent the Wi-Fi receiver from knowing that the malicious interference has been embedded in the received signal. The generated interference should be high enough to incur CSI changes but relatively low to not impact normal Wi-Fi transmission and decoding.*

Objective 3. *The generated malicious CTI noises should survive after the de-noising schemes deployed both by the Wi-Fi receiver and by the recognition system.*

4 Feasibility Study

4.1 Theoretical Analysis of CTI Impact on CSI

The Wi-Fi receiver can overhear ZigBee transmission on designated subcarriers overlapped with ZigBee communication channels. However, most commodity Wi-Fi devices are not capable of understanding cross-technology messages and only hear ZigBee signal as an added power on the original Wi-Fi signal, which is reflected on CSI as a part of channel status.

4.1.1 Effects to Signal-to-Interference-Plus-Noise Ratio

Assuming the WiFi receiver W_i has one single antenna and is in the transmission range of the ZigBee transmitter Z_j, Z_j

is working on the spectrum overlapped with W_i, the received signal $\boldsymbol{y}_k$ at the kth timestamp can be reformulated as

$$\boldsymbol{y}_k = \left(\boldsymbol{h}_k + \sum_j \boldsymbol{h}_k^{Z_j}\right)\boldsymbol{x}_k + \boldsymbol{n}_k,$$

where $\boldsymbol{h}_k$ is the CSI without CTI, $\boldsymbol{h}_k^{Z_j}$ is the CTI perturbation caused by Z_j, $\boldsymbol{x}_k$ is the transmitted signal, and $\boldsymbol{n}_k$ is the noise.

The Wi-Fi packets will not back-off if the Signal-to-Interference-plus-Noise Ratio (SINR) detected in Wi-Fi transmission is qualified, while the CTI is still affecting the estimated CSI. Therefore, the ground truth SINR η_k and the SINR from system's view η_k' can be derived as follows:

$$\eta_k = \frac{|\boldsymbol{h}_k|^2 p_k}{p_k^n + \sum_j |\boldsymbol{h}_k^{Z_j}|^2 p_k}, \eta_k' = \frac{|\boldsymbol{h}_k|^2 p_k + \sum_j |\boldsymbol{h}_k^{Z_j}|^2 p_k}{p_k^n}, \quad (2)$$

where p_k the signal power at kth timestamp and p_k^n is the noise power complying to a normal distribution.

4.1.2 Factors in CTI-Enabled CSI Perturbation

We try to find out why CSI can be perturbed by the presence of ZigBee signals from the aspect of signal propagation, which is often described by the path loss. Suppose that $P_{i,j}^r$ is the power of signal emitted from Z_j and received at W_i, denoted as $|\boldsymbol{h}_k^{Z_j}|^2 p_k$ in Equation (2). The relationship between $P_{i,j}^r$ and the power of the transmitted signal by Z_j, i.e., P_j^t, is as follows if free space path loss is considered

$$P_L(d_{i,j}) = 10\log\frac{P_j^t}{P_{i,j}^r} = P_L(d_i) + 10\nu\log\left(\frac{d_{i,j}}{d_i}\right) + \phi_j, \quad (3)$$

where $P_L(\cdot)$ is the path loss, d_i is the close-in reference distance, $d_{i,j}$ is the distance between W_i and Z_j, ν is the path loss exponent, and ϕ_j is the shadow fading factor with a normal distribution $\mathcal{N}(0, \sigma_\phi^2)$.

From Equation (3), it is clear that $P_L(d_{i,j})$ is determined by $d_{i,j}$ and $P_L(d_{i,j}) - P_L(d_i)$ follows a normal distribution:

$$P_L(d_{i,j}) - P_L(d_i) \sim \mathcal{N}\left(10\nu\log\left(\frac{d_{i,j}}{d_i}\right), \sigma_\phi^2\right).$$

The transmit power P_j^t is another dominant factor for $P_{i,j}^r$, and thus, also for the CSI $|\boldsymbol{h}_k^{Z_j}|^2$.

4.1.3 Why Using CTI

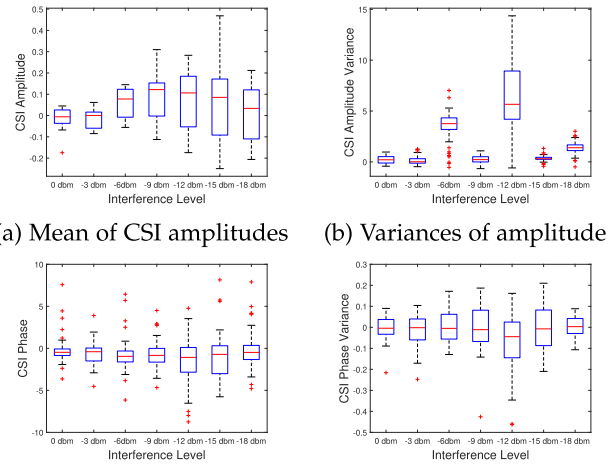
In our work, we will focus on ZigBee-Wi-Fi interference. The advantages of using ZigBee-Wi-Fi CTI come in four folds.

First, compared to other noise addition schemes, CTI is more controllable and fine-tuned by adjusting the above deterministic factors, e.g., P_j^t and $d_{i,j}$.

Second, it is possible to achieve "*stealthiness*" described in Objective 2 if CTI-impacted SINR successfully deceives the Wi-Fi receiver. Devices that can generate CTI, e.g., ZigBee pads, can be small enough to be unnoticeable. They are handier and cheaper than Software-defined Radios like USRP, which allows a wider application of IS-WARS attacks.

Third, ZigBee transmission power can be as low as 1mw (two orders of magnitude lower than Wi-Fi's), making the CTI-based attack less detectable and the possibility of triggering collision avoidance during interference lower, while its transmission range (10–100 meters) is sufficient for attacking a small-scale Wi-Fi-based system.

Last but not least, deploying ZigBee protocol in our attack is free from modification on protocol design. It does not offer complex interference avoidance features like the adaptive frequency hopping technique used in Bluetooth. Moreover, the data rate of ZigBee is comparatively slower than other wireless protocols in the 2.4GHz spectrum. Without manually putting constraints on data rate, the travel time of a ZigBee packet is long enough to cover the entire transmitting Wi-Fi packets, which makes it more difficult for legitimate receivers to discover and mitigate interference. Hence, attacking with ZigBee signals is more reliable than other coexisting protocols.



(a) Mean of CSI amplitudes (b) Variances of amplitude

(c) Mean of CSI phases (d) Variances of phase ratios

Fig. 2. Ratio of interfered signals versus clean signals.

4.2 Empirical Study on CTI-Impacted CSI

We conduct an empirical study to evaluate CSI statistics and show that CTI is capable of interfering with CSI in practice.

4.2.1 Experiment Setting

We set a pair of Wi-Fi transceivers (1m to each other) and a ZigBee source locating in the middle to generate interference at different transmission powers. For each interference level, we collect 10 CSI sequences from received Wi-Fi traffic with a time duration of 20 seconds.

4.2.2 Performance Evaluation

The means and variances of amplitudes and phases, which are represented as the ratios of the differences between contaminated CSI sequences' statistics and clean samples' statistics to clean samples' statistics, are shown in Fig. 2. In Fig. 2a, when the interference level is -15 dBm, though sometimes the ratio is below 0 due to random fluctuations, the average ratio is approximately 0.1, which means that the average amplitude of interfered signals is around 1.1 times

TABLE 1
A Summary of Recognition Systems and Their Vulnerabilities

	Existing Works	Used Quantities or Models	Vulnerabilities
Mathematical Profiles	Wang *et al.* [2]	Location velocity profile	CSI amplitude and phase
	Widar 3.0 [24]	Body-coordinate velocity profile	CSI phase and Doppler Frequency Shift
	Widar 2.0 [25]	Multi-dimensional signal parameters	AoA, ToF, Doppler shifts
Fresnel Zone Model	Zhang *et al.* [29]	Phase shifts in Fresnel zones	CSI amplitude and phase
	Wang *et al.* [26]		
	Wu *et al.* [27]		
Black-box Classification	Jiang *et al.* [21]	CNN	Everything in CSI
	Gu *et al.* [20]	Classification tree	RSS fingerprint
	Wang *et al.* [22]	Kernel SVM	Everything in CSI
	Ordóñez *et al.* [23]	DeepConvLSTM	Everything in CSI

the amplitude of clean signals. We can tell that the averages of amplitudes in Fig. 2a are larger than those of clean samples, and are increasing with the interference level (from -18dBm to -9dBm). If the interference level exceeds a threshold (-9 dBm in our cases), the interference reflected by amplitudes becomes smaller because the Wi-Fi transmitter backoffs in response to the existence of noises or the Wi-Fi receiver discards highly-contaminated, corrupted packets. The large variances of interfered amplitudes may lead to inaccurate recognition. From Fig. 2c, the differences between average phases between interfered signals and clean signals are much smaller than those of amplitudes. However, the ranges of phases are significantly expanded with an increased number of outliers and large variances. Therefore, we can confidently deduce that the robustness of CSI-based recognition systems will be jeopardized by the interference and the abnormality of attacks may be more unnoticeable from phase statistic monitoring.

4.3 Existing Recognition Systems and Their Vulnerabilities

Existing approaches are either domain-related or domain-free, where domain is a pair of activity and the corresponding environment factors, such as location and orientation. We summarize them into three categories: Mathematically derived profiles, Fresnel zone model, and black-box classification as in Table 1 and explore their vulnerabilities as below.

4.3.1 Mathematical Profiles

In [2], Wang *et al*. model the *domain-related velocity profile* from multi-path length changes and rewrite $H(f,t)$ as a summation of responses on multiple travel paths. They divide the power of CSI $|H(f,t)|^2$ into dynamic portion $|H_d(f)|^2$ and static portion $|H_s(f)|^2$. $|H(f,t)|^2$ holds the speed v_k of human subject moving on kth path as follows:

$$|H_s(f)a_k(f,t)|\cos\left(\frac{2\pi v_k t}{\lambda}+\frac{2\pi d_k(0)}{\lambda}+\phi_{sk}\right),$$

where $a_k(f,t)$ is the attenuation, λ is the wavelength, $d_k(0)$ is the initial path length on kth path, and ϕ_{sk} is an initial phase offset.

CTI creates perturbations $a_k^{Z_j}(f,t)$ on $a_k(f,t)$. So, compared to the ground truth v_k, the CTI-interfered velocity profile v_k' derived has an error of

$$\arccos\left\{\frac{a_k(f,t)}{a_k(f,t)+\sum_j a_k^{Z_j}(f,t)}\cos\left[\frac{2\pi v_k t}{\lambda}+\frac{2\pi d_k(0)}{\lambda}+\phi_{sk}\right]\right\}.$$

Widar 3.0 [24] works on another velocity profile, *body-coordinate velocity profile (BVP)*. It is a domain-free quantity that describes the velocities at different body parts involved in the gesture movements. It first estimates a human subject's location and orientation via ToF, AoA, and Doppler Frequency Shift (DFS) D in the dynamic portion of CSI, and then derives BVP from DFS without domain impacts. The CSI representation of BVP is similar to that of velocity profile. Therefore, though the static portion is fully ignored, dynamic DFS D can still be mistaken with perturbed CSI and results in wrong BVP. The location and orientation inference could also be obfuscated from AoA and ToF, which leads to wrong base points when discarding domain effects. Specifically, the signal phase of the l-the path, ith packet, jth subcarrier and kth sensor [25] is

$$f_{\tau_l}(i,j,k)\approx f_c\tau_l+\Delta f_j\tau_l+f_c\boldsymbol{\Delta s_k}\cdot\boldsymbol{\phi_l}-f_{D_l}\Delta t_i,$$

where τ_l, $\boldsymbol{\phi_l}$, and f_{D_l} are the ToF, AoA, and DFS of the lth path. For a contaminated phase with CTI-introduced error $\sum_j f_l^{Z_j}$, the error is distributed among ToF, AoA, and DFS.

4.3.2 Fresnel Zone Model

Fresnel zone is a series of concentric ellipsoids representing the signal strength of propagation in free space. When a human object is moving, they cross zone boundaries and introduce phase shifts, leading to constructive or destructive interference in the received signal. In [29], they model the sum of dynamic part and static part in a slightly different way

$$|H(f,\theta)|^2=|H_s(f)|^2+|H_d(f)|^2+2|H_s(f)||H_d(f)|\cos\theta,$$

where θ is the phase difference between the static vector and dynamic vector. In their model, they assume that the amplitude of the dynamic vector is stable.

The contaminated phase difference between the static vector and dynamic vector become $\theta'=\theta+\sum_j\theta^{Z_j}$. The path-length difference between direct path and reflected path as $\Delta d:=\frac{c\Delta\theta}{2\pi\Delta f}$ is derived for classification, where $\Delta\theta$ is the difference between θs of two subcarriers and Δf is the

subcarrier spacing. The contaminated $\Delta' d$ is $\Delta'\theta/\Delta\theta$ times of the ground true Δd.

4.3.3 Black-Box Classification

A black-box approach in [21] uses Convolution Neural Networks (CNNs) to train and classify activity data with two labels, domains and ground truth, to remove domain-specific quantities. The quantity extracted from CSI is represented as $\boldsymbol{V} = \mathrm{Softplus}(\boldsymbol{W_z}\boldsymbol{Z} + \boldsymbol{b_z})$, where $\boldsymbol{W_z}$ and $\boldsymbol{b_z}$ are parameters to be learned and the softplus function is an activation function to introduce linearity, $\boldsymbol{Z}$ is the output of feature extractor. Another softmax layer obtains the probability vector $\boldsymbol{y_i}$ of activities of mapped feature representation $\boldsymbol{H}_i$ and output the activity label with the highest probability. Here, everything in CSI may lead to misclassification. The attacking goal turns into how to make the unclassified data cross CNN's decision boundaries. This is impossible to be analyzed from formulation due to the complexity of neural networks. We will show how IS-WARS attack performs against neural networks by experiments later.

4.4 De-Noising Performance Against CTI

A majority of de-noising schemes used in Wi-Fi-based recognition systems are originated from eigenvalue-based methods, such as Principal Component Analysis (PCA), which works more effectively than filters [30]. The basic idea of PCA is to perform eigen-decomposition on the correlation matrix of CSI to calculate the eigenvectors and then eliminate out-band noises and quasi-static offsets by reconstructing the principal components from eigenvectors. The CSI is orthogonally transformed into a new coordinate systems such that the greatest variance, i.e., noise, of the data is projected on the first coordinate, which is called the first principal component. The interfered phase on kth path

$$\cos\left\{\frac{2\pi d_k(t)}{\lambda} + \phi_k + \sum_j \left[\phi_s^{Z_j}(t) - \phi_k^{Z_j}(t)\right]\right\},$$

is decomposed into

$$\cos(\phi_k')\cos\left[\frac{2\pi\Delta_k(t)}{\lambda}\right], -\sin(\phi_k')\sin\left[\frac{2\pi\Delta_k(t)}{\lambda}\right],$$

where ϕ_k' is $\frac{2\pi d_k(0)}{\lambda} + \phi_k + \sum_j \left[\phi_s^{Z_j}(t) - \phi_k^{Z_j}(t)\right]$ and $\Delta_k(t)$ is the length of the path changes between time 0 and t. The first PCA component is discarded for de-noising. Due to the orthogonality of PCA components, the discarded one is either $\cos$ part or $\sin$ part. Obviously, the error introduced by CTI, $\sum_j \left[\phi_s^{Z_j}(t) - \phi_k^{Z_j}(t)\right]$, still remains in other components. Therefore, the de-noising scheme will not effectively work against CTI noises, for which Objective 3 will be satisfied.

As for the cyclostationary analysis [10], it locates the subset of stained subcarriers by finding the spiked peak/valley of CSI amplitudes over all subcarriers. When the level of CTI is carefully controlled and widely spread, the peaks are not significant for detection.

5 Design of IS-WARS

5.1 Wi-Fi Packet Sniffing

In correspondence with the aforementioned adversarial model and analysis, the attacker is assumed to have a sniffer to sense the Wi-Fi environment and a ZigBee device to generate CTI. The sniffer can be deployed near the scene within desired period of time before launching the attack in order to retrieve rich background information, including average CSI amplitudes, which can be used to pre-analyze different CSI patterns. The attacker can use this background information to determine suboptimal settings $\boldsymbol{I_s}^0$ for their initial attack. For example, to decide an initial CTI power level, the attacker will jointly consider a set of distance and transmit power to ensure that the CTI power received at the Wi-Fi's side meets the expectation of attack after suffering from path loss (Equation (3)). Moreover, the attacker may choose to attack the Wi-Fi device with the highest received packet power because it allows more intense CTI while preserving normal traffic. Theoretically, the *Objective 1* is always fulfilled regardless of other settings. Under this objective, the attacker has freedom to change interference given the analysis in Section 4.1.

5.2 Malicious CTI Generation

In North America, the 2.4 GHz Wi-Fi works on 2401 MHz to 2473 MHz. Though the bandwidth of ZigBee channels is only 2 MHz (1/10 of Wi-Fi channel's bandwidth), ZigBee channels can cover a frequency range from 2402 MHz to 2480 MHz. Thus, it is sufficient for ZigBee devices to affect as many WiFi channels and subcarriers as wishes. To meet the *Objective 2*, it is of great importance to ensure the generated CTI could be adequate enough to invoke wrong recognition but without impacting normal Wi-Fi transmissions. For the IS-WARS attacker, changing the perturbation on CSI can be easily achieved by increasing the power of interference level, while the *stealthiness* can only be fulfilled by jointly considering the normal symbol decoding at the receiver side. The CSI can be estimated from the received symbols $\boldsymbol{y}_k = \left(\boldsymbol{h}_k + \sum_j \boldsymbol{h}_k^{Z_j}\right)\boldsymbol{x}_k + \boldsymbol{n}_k$ with known ground truth symbols in Section 4.1.1, which is usually transmitted on pilot subcarriers

$$\hat{\boldsymbol{h}}_k = \boldsymbol{y}_k\boldsymbol{x}_k^* = \left(\boldsymbol{h}_k + \sum_j \boldsymbol{h}_k^{Z_j}\right)|\boldsymbol{x}_k| + \boldsymbol{n}_k\boldsymbol{x}_k^*. \tag{4}$$

Given the estimated channel status, Maximum Likelihood (ML) detector is more frequently used way to find the optimal transmitted symbols from the received signals, where the receiver finds the optimally transmitted signal vector $\hat{\boldsymbol{x}}$ via Maximum Likelihood criterion that minimizes the euclidean distance to the received signal vector $\boldsymbol{y}$ and perform an exhaustive search across all valid sequences for the transmitted symbol as $\hat{\boldsymbol{x}} = \arg\min||\boldsymbol{y} - \hat{\boldsymbol{H}}\boldsymbol{x}||^2$. It is impractical to give a mathematical constraint on $\hat{\boldsymbol{H}}$ for stealthiness or compute solutions every time, so our idea is to lower the sensitivity of CSI estimation to noise in order to reduce the possibility of decoding failure.

The sensitivity of the solution to small changes in the input data is measured by condition number $\kappa(\hat{H})$ of $\hat{\boldsymbol{H}}$,

which evaluates how much error in the output results from an error in the input and gives a bound on how inaccurate the message decoding will be. The condition number is defined as

$$\frac{||\Delta \boldsymbol{x}||}{||\boldsymbol{x}+\Delta \boldsymbol{x}||} \leq \kappa(\hat{\boldsymbol{H}}) \frac{||\Delta \boldsymbol{y}||}{||\boldsymbol{y}||}, \tag{5}$$

and formulated as

$$\kappa\big(\hat{\boldsymbol{H}}'\big) = \frac{\sigma_{\max}\big(\hat{\boldsymbol{H}}'\big)}{\sigma_{\min}\big(\hat{\boldsymbol{H}}'\big)}, \tag{6}$$

where $||\cdot||$ is the matrix norm. If the condition number is large, a small change in the transmitted signal will generate larger perturbations in $\boldsymbol{y}$, which indicates low reliability and higher probability of solution finding failure. $\sigma_{\max}(\hat{\boldsymbol{H}}')$ and $\sigma_{\min}(\hat{\boldsymbol{H}}')$ are maximal and minimal singular values of $\hat{\boldsymbol{H}}'$, respectively.

Therefore, from Equation (5), the attacker, who has the ability of Wi-Fi packet sniffing, has to minimize the condition number $\kappa(\hat{\boldsymbol{H}})$. Along with decreasing $\kappa(\hat{\boldsymbol{H}})$ to avoid the decoding failure, the attacker has to ensure that the perturbation triggered is large enough to cause misrecognition. The problem turns into as follows:

$$\begin{aligned} \min \quad & \kappa\big(\hat{\boldsymbol{H}}'\big) \\ \text{s.t.} \quad & \Omega\Big(\Big[\hat{\boldsymbol{h}}_i', \ldots, \hat{\boldsymbol{h}}_j'\Big]\Big) - \Omega\Big(\Big[\hat{\boldsymbol{h}}_i, \ldots, \hat{\boldsymbol{h}}_j\Big]\Big) \geq T_\Omega, \end{aligned} \tag{7}$$

where $\Omega([\hat{\boldsymbol{h}}_i', \ldots, \hat{\boldsymbol{h}}_j'])$ is the quantities derived from a set of perturbed CSI readings for recognition and T_Ω is the minimum difference between noisy quantities and clean ones that can lead to misclassification.

Finding the optimal solution for $\kappa(\hat{\boldsymbol{H}}')$ is an NP hard problem due to the nonlinear and non-convex nature of singular values, but it can be changed into a convex optimization problem with existing relaxation methods. For example, authors in [31] relax the nonconvex problem of controlling singular values in to a set of optimization problems on convex subsets. Then, we can find the optimal solution on the convex problem $K(\sigma_{\max}(\hat{\boldsymbol{H}}'), \sigma_{\min}(\hat{\boldsymbol{H}}'))$ converted from $(\hat{\boldsymbol{H}}')$.

5.3 Iterative Optimal Solution Finding

We propose to find the optimal interference on the converted convex problem in an iterative way by observing the resulting noisy CSI matrix $\hat{\boldsymbol{H}}'$ from interference. At the very beginning, the attacker holds a vector of parameters $\boldsymbol{I_s}$ with attacker-chosen factors that can change the interference posed on CSI. The possible candidates include the transmit power level of Z_j, the frequency range that Z_j works on, the location of the attacker (loc_x, loc_y, loc_z), and the distance $d_{i,j}$ to the system sensor W_i.

To improve the suboptimal initial attack settings and find the optimal solutions of $\boldsymbol{I_s}$, a function $f(\boldsymbol{I_s})$ is derived from Equation (7), which is formulated by combining the constraint and minimization goal together

$$f(\boldsymbol{I_s}) = K\big(\sigma_{\max}\big(\hat{\boldsymbol{H}}'\big), \sigma_{\min}\big(\hat{\boldsymbol{H}}'\big)\big)\hat{\boldsymbol{H}}'(\boldsymbol{I_s}) + \delta(\boldsymbol{I_s}), \tag{8}$$

where $\hat{\boldsymbol{H}}'(\boldsymbol{I_s})$ is CSI matrix interfered by $\boldsymbol{I_s}$ and $\delta(\boldsymbol{I_s})$ is

$$\max\left(\log\left(\frac{\Omega([\hat{\boldsymbol{h}}(\boldsymbol{I_s})_i', \ldots, \hat{\boldsymbol{h}}(\boldsymbol{I_s})_j'])}{\Omega([\hat{\boldsymbol{h}}(\boldsymbol{I_s})_i, \ldots, \hat{\boldsymbol{h}}(\boldsymbol{I_s})_j]}\right), -\log(T_\Omega)\right). \tag{9}$$

Then, we apply a method similar to Zeroth Order Stochastic Descent [32]. If the optimal is not reached, an interference setting $\boldsymbol{I_{s_k}}$ is randomly picked in $\boldsymbol{I_s}$ to be updated by subtracting a small amount computed from the approximate gradient g_i and Hessian estimate S_i

$$g_i :\approx \frac{f(\boldsymbol{I_s} + \epsilon \boldsymbol{e_i}) - f(\boldsymbol{I_s} - \epsilon \boldsymbol{e_i})}{2\epsilon}, \tag{10}$$

$$S_i :\approx \frac{f(\boldsymbol{I_s} + \epsilon \boldsymbol{e_i}) - 2f(\boldsymbol{I_s}) + f(\boldsymbol{I_s} - \epsilon \boldsymbol{e_i})}{\epsilon^2}, \tag{11}$$

where ϵ is a small constant and $\boldsymbol{e_i}$ is a standard basis vector with only the ith component as 1. $\boldsymbol{I_{s_k}}$ is modified based on the values of g_i and S_i.

Optimal $\boldsymbol{I_{s_k}}$ is located when the newly updated $\boldsymbol{I_{s_k}}$ is similar to the old one, which is equivalent to that the approximated gradient is almost zero as summarized in Algorithm 1. Therefore, the resulting $\boldsymbol{I_{s_k}}$ and $\boldsymbol{I_s}$ find a balance between stealthiness and effectiveness. After deciding the optimal $\boldsymbol{I_s}$, the attacker finds the optimal location (distance), transmit power, etc., and may leave the device at the spot for a continuous attack. The computation complexity of this optimization depends linearly on the dimensionality [33].

Algorithm 1. Basic IS-WARS Attack

Result: Optimal $\boldsymbol{I_s}$
Sense Wi-Fi environment;
Initialize a suboptimal attacking profile ${\boldsymbol{I_s}}^0$;
while *The incurred interference does not meet the attacker's expectation* **do**
  Obtain the CSI sequences $\hat{\boldsymbol{H}}'({\boldsymbol{I_s}}^i)$ under current attacking profile ${\boldsymbol{I_s}}^i$;
  Compute $f(\boldsymbol{I_s})$;
  Pick an interference setting ${\boldsymbol{I_{s_j}}}^i$ in ${\boldsymbol{I_s}}^i$;
  Choose a small constant ϵ and a standard basis vector $\boldsymbol{e_i}$ with only the jth component as 1 ;
  Slightly modify ${\boldsymbol{I_{s_j}}}^i$ by computing gradient g_i and Hessian estimate S_i;
  Choose a scaling factor η;
  if $S_i \leq 0$ **then**
    ${\boldsymbol{I_{s_j}}}^{i+1} = {\boldsymbol{I_{s_j}}}^i - \eta g_i$;
  else
    ${\boldsymbol{I_{s_j}}}^{i+1} = {\boldsymbol{I_{s_j}}}^i - \eta g_i / S_i$;
  end
  Monitor the newly incurred interference on CSI;
end

5.4 Advanced Scheme

The *stealthiness* property in the basic scheme is not as desired in the sense that the attacking device will stay at its optimal location. Moreover, based on the analysis in Section 4, existing recognition systems rely more on dynamic portions and frequency domain properties of CSI. A stable attacker affects more from the aspect of CSI amplitudes but

(a) Floorplan (b) Environment Setup

Fig. 3. Experimental settings.

produces less perturbation in the frequency domain. To generate a more untraceable and powerful interference, we add a dynamic property to the IS-WARS attack, e.g, the attacking device is moving at a certain speed. If the interference source is moving, its signal arouses Doppler shift from the view of Wi-Fi receiver W_i as

$$\Delta^{Z_j} f = \frac{\Delta v}{c} f_0, \tag{12}$$

where Δv is the relative velocity to W_i.

Not only will it directly affect the Doppler-shift-related profiles for recognition (e.g., the DFS profile, D, used in BVP), Δf also creates a Carrier Frequency Offset (CFO) in signals, which deviates the CSI phase $\phi(t)$ by $2\pi\Delta f t$ with time t and further affects the CSI power/amplitudes and thus, resulting in a new $\hat{\boldsymbol{H}}'$. Based on the fact that Δf is positive when the source and the receiver are moving towards each other, the attacker is able to control the constructive or destructive effect of dynamic adversarial property on CSI sequences. By including the relative velocity Δv in $\boldsymbol{I_s}$, the strategy is optimized in the same fashion as Algorithm 1.

6 Performance Evaluation

In this section, we analyze the attacking performance on profiles and then implement our attack on a real system.

6.1 Evaluation Settings

6.1.1 Attacker Setting

To verify that our attack is feasible in the most constrained situation, we only consider an attacker that can achieve *Objective 1-Basic* in Section 3.2 instead of *Objective 1-Advanced*. Thus, the sensing and observation ability of the attacker is limited to sensing the frequency band that Wi-Fi senders/receivers are working on and extracting the CSI from sensed packets. Their attacking profiles only consists of the transmit power level, the location of the attacker, and their moving speed.

6.1.2 Environmental Setting

The experiment is done in a $3\,m \times 5\,m$ room as shown in Fig. 3a. The distance between the Wi-Fi sender and the Wi-Fi receiver is 1.5 meters. We choose Nexus 5 smartphones as the WiFi devices, which are installed with Nexmon [34], a C-based firmware patching framework enabling raw Wi-Fi signal transmission and CSI extraction. The Wi-Fi transmission happens in 2.4GHz and on single antenna. The interference sources are ZigBee devices setting on different frequency bands, TI SimpleLink Multi-Standard CC26x2R Wireless MCU LaunchPads. The devices used are shown in Fig. 3b, where the human subject is waving.

6.1.3 Experimental Settings

Wi-Fi devices are set to work on Wi-Fi Channel 1 (2401 MHz-2423 MHz with center frequency 2412 MHz) and the ZigBee interference sources can work on a combination of ZigBee Channel 11 (center frequency 2405 MHz), Channel 12 (center frequency 2410 MHz), Channel 13 (center frequency 2415 MHz), or Channle 14 (center frequency 2420 MHz) to cover as many as Wi-Fi subcarriers as they want. Two activities categories are designed for experiments. The first one is *gentle* movements, including resting in bed, waving, clap, and push and pull, during which the human subject stays at the same location. The second category is *vigorous* activities involving location changes, including walking, sitting down, entering and leaving the room. In total, twenty volunteers were recruited for data collection.

For the basic attack scenario, the attacker's location is fixed. In the advanced scheme, the attacker walks with relative speed to the Wi-Fi receiver. Under each set of settings, 2-3 CSI sequences with a monitoring time of 20 seconds are recorded.

6.2 Throughput Analysis

We first monitor the wireless environment when a ZigBee device, 1.5 meters away from the Wi-Fi receiver, is emitting interference signals. The Wi-Fi sender sends 8×800 packets under 8 different levels of CTI. This process is repeated for 10 times. We have verified that all captured packets can be correctly decoded. The numbers of packets received by Wi-Fi receiver are recorded and the packet success transmission rates, as well as network throughputs, are evaluated as shown in Table 2. We can tell that CTI will not greatly affect throughput and thus, it is hard to distinguish an attacker from the network performance perspective, which verifies the objective of achieving *stealthiness*. When the CTI level is -18 dBm, the ZigBee interference sensed by the Wi-Fi receiver is so low that it does not affect the network performance at all. However, slight drops in performance are observed when CTI level is -9 dBm, -12 dBm, and -15 dBm, which is in correspondence with the change of CSI amplitudes in Fig. 2a.

6.3 Attacking Mathematical Profiles

Next, we break down the interfered CSI sequences and analyze how the derived profiles affected by interference. The attack effectiveness is directly reflected by profiles because the basic principle of real systems is matching profiles with the closest known label. If the statistics of an interfered sample becomes closer to a wrong class than the correct one, it definitely leads to incorrect classification. The reason for comparing the distance changes between labeled and unlabeled profiles instead of comparing against a certain threshold is that reliable recognition systems rarely set thresholds manually and instead, their thresholds/decision boundaries are learned from data. We will not talk about Fresnel zone model because it is directly related to CSI amplitudes and phases, which have been proven to be influenceable by CTI.

TABLE 2
Network Performance Under Different Levels of CTI

	0 dBm	-3 dBm	-6 dBm	-9 dBm	-12 dBm	-15 dBm	-18 dBm	clean
# of Received Packets	682	684	686	663	632	652	706	701
Successful Transmission Ratio	85.25%	85.5%	85.75%	82.88%	79%	81.5%	88.25%	87.63%
Throughput (kbps)	38.74	40.57	39.54	37.81	36.04	37.26	40.26	40.65

6.3.1 Location Velocity Profile

After PCA de-noising, authors in [2] apply Discrete Wavelet Transform (DWT) to decompose the first five PCA components into 12 levels and average the results to capture the movement information presented in different PCA components. The recognition is done by calculating the likelihood of each activity's hidden Markov model. Therefore, we extract DWT-decomposed coefficients of interfered samples and compare them with coefficients of clean samples. We set the decomposition level to 6 because our data experience boundary effects if the level is 12. The average distances of coefficients between two classes of activities are shown in Fig. 4, where M1 and M2 are two different *gentle* motion types, while M3 and M4 are *vigorous*.

In Fig. 4, we measure four types of distances: Between coefficients of clean samples from M1 and clean samples from M2, between coefficients of clean samples in M1, between coefficients of noisy samples in M1 and clean samples in M2, and between coefficients of noisy samples in M1 and clean samples in M2. Intuitively, the distances between clean samples from two different motion classes are larger than those from the same class. After experiencing the attack, however, not only the distances between noisy samples to samples in its actual class become larger, but also we witness an increase in the distances between noisy samples and samples from a wrong class. Moreover, for 5 out of 6 coefficients, the gap between the distances of noisy samples to M1 and M2 is smaller. All aforementioned results indicate that our attack successfully blurs the boundary between M1 and M2 for interfered CSI, so the system will more likely guess a random class to fit noisy CSI in. For vigorous activities, the differences between classes are larger, but the coefficient changes still suffer from the attack.

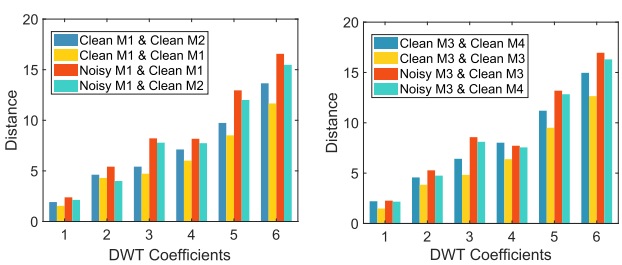
6.3.2 BVP

BVP in [24] is estimated as an l_0-optimization problem from the Doppler spectrum, which is derived from CSI amplitudes and phases after basic PCA de-noising. We use the authors' open-source codes to compute Doppler spectrum and visualize some examples in Fig. 5, where Motion 1 is push/pull and Motion 2 is clap.

In Fig. 5, more peaks show up in interfered Doppler spectrum of Motion 1 while a featured peak in the clean spectrum of Motion 2 is replaced by a bunch of small peaks. Moreover, the spectrum apart from the peaks in Fig. 5d is changed by the interference and becomes similar to that in Fig. 5b. Visually, the interfered Motion 2's Doppler spectrum is closer to the spectrum of the other class. To verify this observation, we calculated the *correlation coefficients* between spectrum matrices. The correlation between clean Motion 1 and clean Motion 2 is 0.1616, demonstrating their distinctiveness, but there is a sharp increase in the correlation between interfered Motion 2 and clean Motion 1, which is 0.6509, while the correlation between interfered Motion 2 and clean Motion 2 is only 0.3651. Thus, it is highly possible for the system to classify the interfered Motion 2 CSI as Motion 1. Though the correlation between interfered Motion 1 and clean Motion 1 is slightly higher than the correlation between interfered Motion 1 and clean Motion 2 (0.4994 compared to 0.4341), the advantage of correct classification over misclassification is so subtle that the expected classification accuracy will certainly be downgraded by IS-WARS attack. This result also applies to the average spectrum matrices of all other activities.

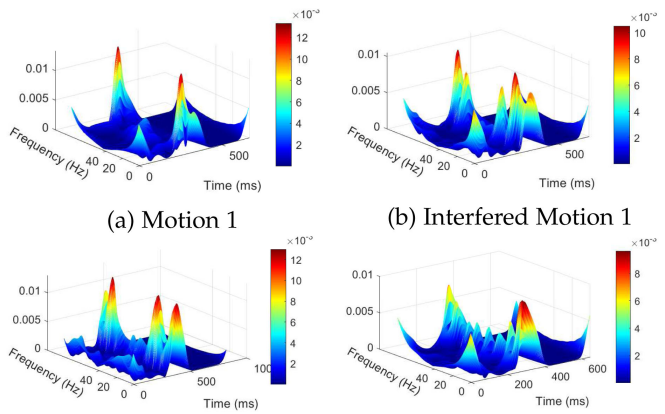
6.4 Improvement With Advanced Attacking Scheme

In an advanced attack, the attacker is moving at a speed of 0.02 m/s. We introduce an additional setting, whether the transmission path of the interference signal to the Wi-Fi receiver is Non-Line-of-Sight (NLOS), into the performance analysis, where NLOS is modeled by placing the source behind the door. The performance under NLOS is measured



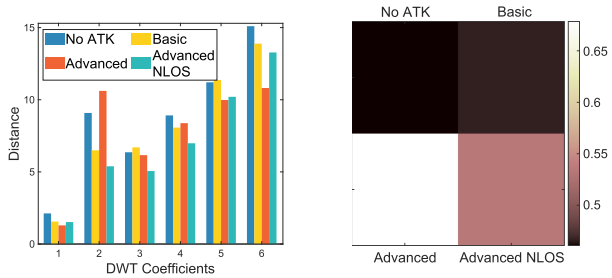
(a) Gentle (b) Vigorous

Fig. 4. DWT coefficient distances.



(a) Motion 1 (b) Interfered Motion 1
(c) Motion 2 (d) Interfered Motion 2

Fig. 5. Doppler spectrum of detected motions.



(a) Location velocity profiles (b) BVP

Fig. 6. Invoked changes in profiles.

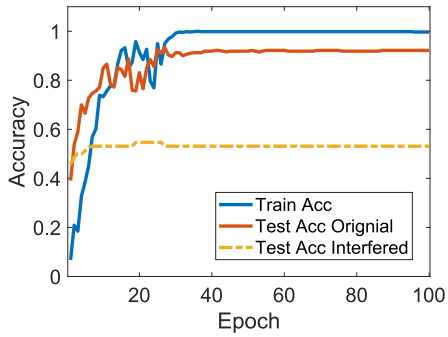


Fig. 7. Effect on CLDNN-based system's accuracy.

in advanced attacks because it is possible for the interference source to be occasionally blocked by obstacles during moving, but the effects of NLOS are also valid on basic attacks.

The performance of advanced attack on mathematical profiles is illustrated in Fig. 6. The y-axis in Fig. 6a are distances between a class A to be attacked and another class B that the interfered samples for A are much easier to be misclassified into. Distances are averaged over all possible classes A. From Fig. 6a, the advanced attacker is more powerful than the basic one as 4 out of 6 interfered coefficients move closer to class B. The advanced attack under NLOS setting is worse than the LOS one, but still outperforms the basic one. Fig. 6b shows the correlation coefficients between clean class A samples (no attack exists) and class B samples, class A samples under basic attack and class B samples, class A samples under advanced attack and class B samples, and class A samples under advanced NLOS attack and class B samples. The results are aligned with what in Fig. 6a, i.e., the interfered A samples under advanced attack, whose coefficient is approximately 0.7, is the closest one to the B samples. The NLOS setting brings negative effects to attack performance, but the basic one is still the worst. The effectiveness of advanced attack is proved.

6.5 Attacking a Real System

6.5.1 System Settings

As mentioned in Section 4, we implement our attack on a real learning-based recognition system built on Convolutional, long short-term memory, fully connected Deep Neural Networks (CLDNN) [35], which is a combination of Convolutional Neural Network (CNN) layers, Long Short-Term Memory (LSTM) layers, and Deep Neural Networks layers. We recruit 10 volunteers to perform each motion for 5 times with a time duration of 100 seconds to collect enough CSI data. In all, 25,000 seconds of samples are stored for 5 activity labels. 80% of these CSI sequences are clean ones labeled with activities for training, 10% of them are unlabeled, clean samples for testing, and the remaining are unlabeled, IS-WARS-attacked samples for testing.

6.5.2 Attack Performance

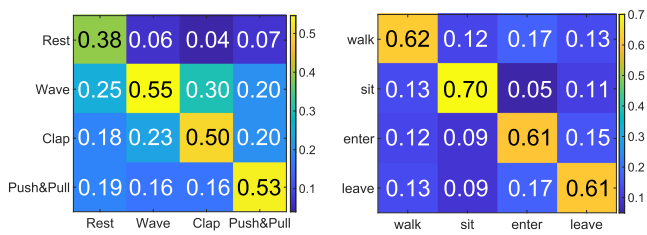
The accuracy of training and testing are illustrated in Fig. 7. From the converged training accuracy (close to 100%) and original testing accuracy (approximately 93%), we can tell that this model is well-trained. However, the accuracy after attack dropped to around 53%, which is close to random guess. This huge drop proves the effectiveness of IS-WARS on learning-based systems.

Next, we analyze the accuracy w.r.t. activity categories, which is shown in the confusion matrices for *gentle* and *vigorous* activities, respectively, in Fig. 8. For the movements in the gentle activity category, samples with ground truth "rest" are likely to be misclassified into other categories with a probability of 61.25%, while samples with other three ground truth labels have a misclassification rate less than 50%. Thus, "rest" tends to be more vulnerable to the attack compared to the other three activities because "rest" creates less distinct turbulences on CSI sequences while IS-WARS attack adds perturbation to make CSI sequences to be more like CSI from activities involving hand movements. It also explains why it is less possible for CSI sequences to be misclassified as "rest". Vigorous activities are slightly more difficult to be attacked because they contain more dynamic features. Nevertheless, there is still a chance to fool the recognition because the spatial information, which is used to distinguish walking, entering the room, and leaving the room, can be blurred under CTI.

6.5.3 Compare With Random Interference

To further validate the practicability and effectiveness of both the activity recognition system and our attack, we bring up several additional experimental scenarios featured with random noises. The new designs are as below. All devices are working on frequencies that overlap with the frequencies used by recognition systems.

1) *Random background noises from other types of source:* Some Wi-Fi devices are downloading data on the 2.4 GHz spectrum at a place at the scene.
2) *Random background noises from the same type of source:* Some benign ZigBee devices are producing ZigBee traffics.



(a) Gentle (b) Vigorous

Fig. 8. Confusion matrix.

TABLE 3
Performance Under Random ZigBee Interference

	Success Transmission	Accuracy
Clean	87.63%	93%
One Benign	49.11%	76%
One Attacker	84.10%	53%
Benign & Attacker	47.42%	59%

In the previous experimental scenario, experiments are done in an apartment building with ongoing 2.4GHz Wi-Fi traffics on all channels in the background. We have also collected each activity multiple times to include the randomness of human activities. From the performance mentioned above, we can tell that our attack is way more harmful than random Wi-Fi interference. Therefore, we focus on the second scenario.

In the previous experimental environment, the attacking device was initially placed at a random place. Here, we replace the attacking device with a benign ZigBee device. The benign ZigBee is transmitting on ZigBee Channel 13 with a transmission level chosen from -21 dBm to 10 dBm. This channel overlaps with Wi-Fi Channel 1 but will not affect the attacker working on ZigBee Channel 11. Unlike the attacker, the benign ZigBee will always stay at its initial place and not change its initial transmission level. The impacts of the benign ZigBee device with different power levels are averaged. Table 3 shows the average effects of random ZigBee interference and attacker. Since the benign ZigBee device is placed at a fixed position near the Wi-Fi transceiver, more Wi-Fi packets are held back from the transmission or received as corrupted, which results in a huge drop in the average ratio of successfully received packets. On the contrary, the packets that survived interference are mostly those experiencing a low level of ZigBee CTI and less perturbed. Thus, they produce more accurate recognition compared to packets interfered with by our attack. Then, we add the attacking device back to the scene and let the attack and the transmission of benign ZigBee packets happen simultaneously. The success transmission ratio does not change much. The impact on recognition accuracy is almost the same as when there is only one attacker at the spot and is much lower than there is only one benign ZigBee device. Despite how much noise is in the background, the attacker's goal is still to try to minimize the extra packet loss caused by malicious interference and maximize the drop in accuracy of recognizing activities using successfully received packets.

6.6 De-Noising Performance versus Interference

We evaluate whether interference from other wireless sources will be discarded. Along with the aforementioned discussion, the de-noising scheme considered here is based on PCA. Since humans cannot precisely control their activities and it is hard to synchronize the timestamps of different CSI samples, we leverage another technique, Dynamic Time Warping (DTW) [36], to measure how far the unlabeled signals are from their ground truth. The euclidean distances between interfered signals and the ground truth clean signals are divided by the average amplitudes of ground truth clean sequences, denoted as "distance ratio". We compute the average distance ratios before and after de-noising applied to both interfered ones and clean ones. Surprisingly, the average distance ratio after de-noising is almost 10 times more than the ratio before. The resulting sequence is drifting farther away than the ground truth, so the de-noising approach cannot discard interference without harming the recognition accuracy.

7 Potential Defenses

Generally, a wireless human activity recognition system has at least three components: Signal preprocessing, feature extraction, and activity recognition. This section briefly provides some insights into how to defend against our proposed attack in these three steps.

Defense During Signal Preprocessing. In the IS-WARS, the attacker can cover all Wi-Fi subcarriers with CTI. If most CTI can be removed from the signal, the possibility of a successful attack will be significantly reduced. Thus, one possible defense is to recover the fully contaminated signal.

Defense During Feature Extraction. The recognition results are directly influenced by the values of features. Current features used in recognition systems, such as amplitudes and phases, are very sensitive to noises. If less sensitive features are explored, this could undermine the impact of CTI.

Defense During Activity Recognition. Lastly, the recognition scheme can be made more robust. For example, if machine learning techniques are used for recognition, techniques like deliberately training the model with CTI-interfered signals should raise the model's robustness against CTI.

8 Related Work

8.1 Applications of Human Activity Recognition

Two major application scenarios of wireless human activity recognition are healthcare monitoring and gesture recognition. The recognition of healthcare applications involves dangerous motions and emergent vital signal monitoring. Dangerous motion recognition often utilizes the deployed in-home wireless transceivers. One representative work is WiFall [37], which uses CSI as an indicator of falling and enables accurate alert of potential injuries. Vital signs, including heartbeat, respiration, blood volume, etc., bring displacement of body surface to be detected by wireless signal characteristics. In [38], authors build testbeds for respiration monitoring based on commodity devices and prove the effectiveness of wireless monitoring. Gesture recognition is a more general-purpose application, which has been widely applied in Virtual Reality and human-computer interaction. In [39], authors achieve contact-less gesture recognition via Commercial-Off-The-Shelf (COTS) RFID as a tag array, benefiting users' daily life in time-saving. However, the consequences brought by successfully attacking these vital applications are severe.

8.2 Wireless Signal Interference

Because of spectrum overlapping, wireless signals are always facing the threats of unexpected interference from other signal sources. Existing works mostly focus on

detection [18], mitigating [8], achieving coexistence [3], or exploiting the interference. However, these works analyze from plain metrics, such as packet loss, to estimate interference, without providing detailed analysis and cannot reduce the loss caused by interference but bring heavier burdens of assessing and hopping. In [9], Guo *et al.* use SVM to classify Wi-Fi packets that are contaminated by ZigBee packets. Wi-Fi packets are symboled as 0 and 1 in terms of whether being contaminated or not. Then, they use 0s and 1s to represent messages that both Wi-Fi and ZigBee receivers can decode. The authors use CTI to fulfill cross-technology communication (CTC), but the experiments cannot provide any generalized conclusion.

8.3 Attacks to Wireless Systems

8.3.1 Jamming Attack and Countermeasures

Wireless jamming is a common attack to compromise the service of wireless systems. The main objective of the jamming device is to ensure that the legitimate nodes cannot use the network by purposefully interfering with the physical transmission and reception of wireless communications. As summarized in [40], there are four kinds of jammers: Constant jammer, deceptive hammer, random jammer, and reactive jammer, in which the deceptive jammer is similar to our attacker. A deceptive jammer emits a legitimate bit sequence which gives the network an impression of the presence of a legitimate node. This impersonation makes deceptive jammers more effective than constant jammers. In [41], authors deploy deceptive jammer to confuse information acquisition without arousing the awareness of the hostile radar. Although this kind of jammer is intelligent, their packets can be easily identified in CSI-based recognition due to environmental differences and unique location profiles. They do not have the same objective as our attack and are not stealthy enough to achieve a long-term negative effect.

There are some works in countering the wireless jamming attack, especially cross-technology jamming. In [42], a ZigBee device will assume that it is suffering from a jamming attack if there are too many failed attempts of transmission when sensing channels, and it will force transmission in busy channels. Suppose the ZigBee packet is transmitted but corrupted due to cross-technology interference. In that case, the authors apply a band stop filter to isolate slower rate Wi-Fi subcarriers, reduce total interference, and then compensate the distorted ZigBee signals with the Direct Sequence Spread Spectrum (DSSS) scheme. However, it is difficult to do these steps vice versa. The filter cannot completely remove the impact of CTI, and Wi-Fi signals cannot be compensated by DSSS because DSSS only available in old version 801.11b and low data rates in 801.11g. The attacker in our attack can cover a Wi-Fi channel with as many ZigBee channels as they desire, which makes it very challenging for the receiver to recover corrupted subcarriers using the information in clean subcarriers,

8.3.2 Illegitimate RF Sensing and Existing Countermeasures

Illegitimate RF sensing is a kind of attack where attackers sensing and analyzing the Wi-Fi signal that bounced off the human body to detect human activity for malicious purposes, e.g., detect if there is anyone at home to prepare for an illegal break-in. The basic principle of protecting against illegitimate RF sensing is obfuscating the wireless signal characteristics used for human activity recognition, such as amplitude gain, delay, Doppler shift, etc.

In [43], the adversary uses a single-antenna receiver to sniff the wireless transmission. They place a reflector near the legal wireless receiver. The reflector can receive and transmit signals and modify the reflected packet copies by controlling three multipath components: Amplitude gain, delay, and Doppler shift, before relaying copies to the legitimate receiver. Their scheme preserves the normal data communication, but since any features that reveal physical information are distorted, the legal wireless receiver cannot recognize human activity from the received signal as well.

To enable simultaneous protection and legitimate human activity sensing, authors in [44] define a term named "adversary region", which is the place that adversaries can perform attack without being visually noticed. In their scheme, the reflector is placed outside the legitimate sensing region. The reflector is equipped with a directional antenna to scan the adversary region, broadcast modified copies, and avoid sending the modified copies to the legitimate receiver. This scheme has several limitations. First, knowing the location and shape of the potential adversary region are required to make this scheme work and the reflector has to be placed in the adversary region, which leaves the indoor area unprotected and increases the chance of being noticed by the attacker, as well as the chance of failed protection. Second, there is a huge decrease in recognition accuracy shown in evaluation results. The recognition accuracy of legitimate sensors drops from 0.9 to 0.78. Though this accuracy is still much higher than the one suffered from our attack, it is definitely incredible harm to system performance. Lastly, since the reflector is using a directional antenna to scan the region, it is not guaranteed that the reflector can obfuscate all copies sensed by the adversary, as claimed by the authors. Receiving partially corrupted results may block adversaries from successfully sensing human activities, but it is possible for an attacker to separate obfuscated packets from clear ones through analysis. Moreover, our attacker does not need the fully correct copies of human-activity-interfered signals to perform attacks. Our purposed attack remains threatening to existing systems.

9 Conclusion

Benefiting from ubiquitous wireless device deployments, human activity recognition systems can achieve non-intrusiveness and high accuracy at the same time leveraging the rich channel information embedded in Wi-Fi signals. However, Wi-Fi-based recognition systems are vulnerable to wireless attacks. In this work, we discover an intelligent but stealthy attack on human activity recognition systems by leveraging wireless signal interference. "Intelligence" is to find optimal interference that can incur misrecognition while preserving normal packet decoding, while "stealth" means the attack remains unnoticeable because it does not harm the function of systems. We thoroughly analyze this new attack from both theoretical and experimental

perspective, and demonstrate the feasibility of the attack on real profiles and systems. To the best of our knowledge, we are the first one to quantitatively analyze the influence of wireless interference and demonstrate effectiveness in real-world experiments.

ACKNOWLEDGMENTS

The work of L. Guo was partially supported by U.S. National Science Foundation under Grants CNS-2008049 and IIS-1949640.

REFERENCES

[1] Z. Liu, X. Liu, J. Zhang, and K. Li, "Opportunities and challenges of wireless human sensing for the smart IoT world: A survey," *IEEE Netw.*, vol. 33, no. 5, pp. 104–110, Sep./Oct. 2019.

[2] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of WiFi signal based human activity recognition," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw.*, 2015, pp. 65–76.

[3] C.-J. M. Liang, N. B. Priyantha, J. Liu, and A. Terzis, "Surviving Wi-Fi interference in low power ZigBee networks," in *Proc. 8th ACM Conf. Embedded Netw. Sensor Syst.*, 2010, pp. 309–322.

[4] J.-H. Hauer, V. Handziski, and A. Wolisz, "Experimental study of the impact of WLAN interference on IEEE 802.15. 4 body area networks," in *Proc. Eur. Conf. Wireless Sensor Netw.*, 2009, pp. 17–32.

[5] A. Hithnawi, H. Shafagh, and S. Duquennoy, "Understanding the impact of cross technology interference on IEEE 802.15. 4," in *Proc. 9th ACM Int. Workshop Wireless Netw. Testbeds Exp. Eval. Characterization*, 2014, pp. 49–56.

[6] J. Elias, S. Paris, and M. Krunz, "Cross-technology interference mitigation in body area networks: An optimization approach," *IEEE Tran. Veh. Technol.*, vol. 64, no. 9, pp. 4144–4157, Sep. 2015.

[7] A. Hithnawi, S. Li, H. Shafagh, J. Gross, and S. Duquennoy, "CrossZig: Combating cross-technology interference in low-power wireless networks," in *Proc. 15th Int. Conf. Inf. Process. Sensor Netw.*, 2016, Art. no. 10.

[8] A. Hithnawi, H. Shafagh, and S. Duquennoy, "TIIM: Technology-independent interference mitigation for low-power wireless networks," in *Proc. 14th Int. Conf. Inf. Process. Sensor Netw.*, 2015, pp. 1–12.

[9] X. Guo, Y. He, X. Zheng, L. Yu, and O. Gnawali, "ZigFi: Harnessing channel state information for cross-technology communication," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, 2018, pp. 360–368.

[10] Y. Zheng *et al.*, "Combating cross-technology interference for robust wireless sensing with cots WiFi," in *Proc. 27th Int. Conf. Comput. Commun. Netw.*, 2018, pp. 1–9.

[11] J.-P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, Aug. 2002.

[12] J. S. Simonoff, *Smoothing Methods in Statistics*. Berlin, Germany: Springer, 2012.

[13] I. W. Selesnick, H. L. Graber, D. S. Pfeil, and R. L. Barbour, "Simultaneous low-pass filtering and total variation denoising," *IEEE Trans. Signal Process.*, vol. 62, no. 5, pp. 1109–1124, Mar. 2014.

[14] G. Chen and S.-E. Qian, "Denoising of hyperspectral imagery using principal component analysis and wavelet shrinkage," *IEEE Trans. Geosci. Remote Sens.*, vol. 49, no. 3, pp. 973–980, Mar. 2011.

[15] G. Hennenfent and F. J. Herrmann, "Seismic denoising with non-uniformly sampled curvelets," *Comput. Sci. Eng.*, vol. 8, no. 3, 2006, Art. no. 16.

[16] G. Welch *et al.*, "An introduction to the Kalman filter," Chapel Hill, NC, USA, 1995.

[17] I. Daubechies, "The wavelet transform, time-frequency localization and signal analysis," *IEEE Trans. Inf. Theory*, vol. 36, no. 5, pp. 961–1005, Sep. 1990.

[18] G. Chen, W. Dong, Z. Zhao, and T. Gu, "Towards accurate corruption estimation in ZigBee under cross-technology interference," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst.*, 2017, pp. 425–435.

[19] S. Yousefi, H. Narui, S. Dayal, S. Ermon, and S. Valaee, "A survey on behavior recognition using WiFi channel state information," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 98–104, Oct. 2017.

[20] Y. Gu, F. Ren, and J. Li, "PAWS: Passive human activity recognition based on WiFi ambient signals," *IEEE Internet of Things J.*, vol. 3, no. 5, pp. 796–805, Oct. 2016.

[21] W. Jiang *et al.*, "Towards environment independent device free human activity recognition," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, 2018, pp. 289–304.

[22] Y. Wang, X. Jiang, R. Cao, and X. Wang, "Robust indoor human activity recognition using wireless signals," *Sensors*, vol. 15, no. 7, pp. 17 195–17 208, 2015.

[23] F. J. Ordóñez and D. Roggen, "Deep convolutional and LSTM recurrent neural networks for multimodal wearable activity recognition," *Sensors*, vol. 16, no. 1, 2016, Art. no. 115.

[24] Y. Zheng *et al.*, "Zero-effort cross-domain gesture recognition with Wi-Fi," in *Proc. 17th Annu. Int. Conf. Mobile Syst. Appl. Services*, 2019, pp. 313–325.

[25] K. Qian, C. Wu, Y. Zhang, G. Zhang, Z. Yang, and Y. Liu, "Widar2.0: Passive human tracking with a single Wi-Fi link," in *Proc. 16th Annu. Int. Conf. Mobile Syst. Appl. Services*, 2018, pp. 350–361.

[26] H. Wang *et al.*, "Human respiration detection with commodity WiFi devices: Do user location and body orientation matter?," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, 2016, pp. 25–36.

[27] D. Wu, D. Zhang, C. Xu, H. Wang, and X. Li, "Device-free WiFi human sensing: From pattern-based to model-based approaches," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 91–97, Oct. 2017.

[28] Y. Zhu *et al.*, "Adversarial WiFi sensing using a single smartphone," 2018, *arXiv:Cryptography and Security*.

[29] D. Zhang, H. Wang, and D. Wu, "Toward centimeter-scale human activity sensing with Wi-Fi signals," *Computer*, vol. 50, no. 1, pp. 48–57, 2017.

[30] S. Tan and J. Yang, "WiFinger: Leveraging commodity WiFi for fine-grained finger gesture recognition," in *Proc. 17th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2016, pp. 201–210.

[31] S. Z. Kovalsky, N. Aigerman, R. Basri, and Y. Lipman, "Controlling singular values with semidefinite programming," *ACM Trans. Graph.*, vol. 33, no. 4, 2014, Art. no. 68.

[32] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, and C.-J. Hsieh, "ZOO: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models," in *Proc. 10th ACM Workshop Artif. Intell. Secur.*, 2017, pp. 15–26.

[33] K. Balasubramanian and S. Ghadimi, "Zeroth-order (non)-convex stochastic optimization via conditional gradient and gradient updates," in *Proc. 32nd Int. Conf. Neural Inf. Process. Syst.*, 2018, pp. 3459–3468.

[34] M. Schulz, D. Wegemer, and M. Hollick, "NexMon: The C-based firmware patching framework," 2017. [Online]. Available: https://nexmon.org

[35] T. N. Sainath, O. Vinyals, A. Senior, and H. Sak, "Convolutional, long short-term memory, fully connected deep neural networks," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, 2015, pp. 4580–4584.

[36] D. J. Berndt and J. Clifford, "Using dynamic time warping to find patterns in time series," in *Proc. 3rd Int. Conf. Knowl. Discov. Data Mining*, 1994, pp. 359–370.

[37] Y. Wang, K. Wu, and L. M. Ni, "WiFall: Device-free fall detection by wireless networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 2, pp. 581–594, Feb. 2017.

[38] P. Hillyard *et al.*, "Comparing respiratory monitoring performance of commercial wireless devices," 2018, *arXiv: 1807.06767*.

[39] C. Wang *et al.*, "Multi-touch in the air: Device-free finger tracking and gesture recognition via COTS RFID," in *Proc. IEEE Conf. Comput. Commun.*, 2018, pp. 1691–1699.

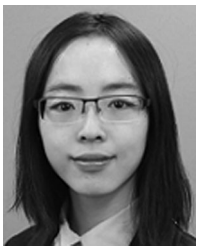
[40] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2005, pp. 46–57.

[41] Q. Sun, T. Shu, K.-B. Yu, and W. Yu, "A novel deceptive jamming method against two-channel SAR-GMTI based on two jammers," *IEEE Sensors J.*, vol. 19, no. 14, pp. 5600–5610, Jul. 2019.

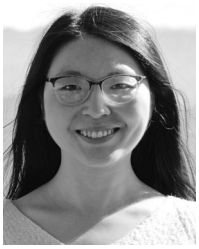
[42] Z. Chi *et al.*, "Countering cross-technology jamming attack," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2020, pp. 99–110.

[43] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "PhyCloak: Obfuscating sensing from communication signals," in *Proc. 13th USENIX Symp. Netw. Syst. Des. Implementation*, 2016, pp. 685–699.

[44] Y. Yao *et al.*, "Aegis: An interference-negligible RF sensing shield," in *Proc. IEEE Conf. Comput. Commun.*, 2018, pp. 1718–1726.

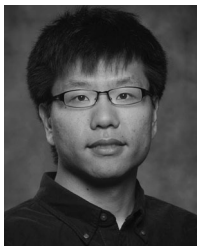


Pei Huang (Student Member, IEEE) received the BSc degree from Xidian University, Xi'an, China, in 2015, and the MSc degree from SUNY at Binghamton, Binghamton, New York, in 2017. She is currently working toward the doctorate degree in computer engineering at Clemson University, Clemson, South Carolina. Her research interests include security and privacy in eHealth/mHealth system, wireless networks, machine learning, and crowdsensing, with a focus on the security problems regarding physical layer properties in the Internet of Things (IoTs) recently.



Xiaonan Zhang (Member, IEEE) received the MS degree in electrical and computer engineering from Binghamton University, State University of New York, Vestal, New York, in 2017, and the PhD degree in computer engineering from Clemson University, Clemson, South Carolina, in 2020. She is currently an assistant professor with the Department of Computer Science, Florida State University, Tallahassee, Florida. Her research interests include wireless communication and networking, Internet of Things (IoT), and wireless security with an emphasis on interference mitigation, resource allocation, and physical-layer security in a heterogeneous wireless environment. She is a member of the ACM.

Sihan Yu (Student Member, IEEE) received the BE degree in computer science and technology from Liaoning University, Liaoning, China, in 2013, the ME degree in control engineering from the University of Chinese Academy of Sciences, Beijing, China, in 2016, and the MS degree in computer engineering from Virginia Tech, Blacksburg, Virginia, in 2018. He is currently working toward the PhD degree at Clemson University, Clemson, South Carolina. His research interests include cross-technology communication, physical layer security in wireless network, and the Internet of Things.



Linke Guo (Senior Member, IEEE) received the BE degree in electronic information science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2008, and the MS and PhD degrees in electrical and computer engineering from the University of Florida, Gainesville, Florida, in 2011 and 2014, respectively. From August 2014 to August 2019, he was an assistant professor with the Department of Electrical and Computer Engineering, Binghamton University, State University of New York. Starting from August 2019, he has been an assistant professor with the Department of Electrical and Computer Engineering, Clemson University. His research interests include wireless network, IoT, security, and privacy. He is currently serving as the editor of the *IEEE Transactions on Vehicular Technology*. He also serves as the poster/demo chair of IEEE INFOCOM 2020-2021. He was the publication chair of IEEE Conference on Communications and Network Security (CNS) 2016 and 2017. He was the symposium co-chair of Network Algorithms and Performance Evaluation Symposium, ICNC 2016. He has served as the Technical Program Committee (TPC) members for several conferences including IEEE INFOCOM, ICC, GLOBECOM, and WCNC. He is the co-recipient of Best Paper Award of Globecom 2015, Symposium on Communication and Information System Security. He is a member of the ACM.