# Wearable-User Authentication via Cross-Technology Interference in Heterogeneous Environments

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

***Abstract*—The increasing deployment of wireless sensors enables a broad spectrum of health-related wearable applications. Due to the sensitivity of collected personal health information, these wearables should be authenticated together with their users as "wearable-user pairs" to ensure that they are attached to legitimate users. However, various devices are equipped with dedicated sensing abilities and wireless protocols corresponding to data characteristics in practice. Traditional authentication methodologies may not work in this heterogeneous environment because of protocol incompatibility. For example, how to verify a new ZigBee-enabled monitor when the existing trusted device is Wi-Fi-enabled? Therefore, to achieve authentication across protocols, in this article, we leverage the unique cross-technology interference (CTI), triggered by heterogeneous wireless transmissions, along with human physiological activity measurements (e.g., respiration patterns) to design an authentication scheme between wearables and users. Specifically, the authentication from an unknown ZigBee wearable to a trusted Wi-Fi device is achieved by monitoring the channel state information (CSI) changes according to human respiration. Our approach not only successfully recognizes a legitimate wearable-user pair but also blocks illegal access from adversaries. Extensive experiments have been conducted to demonstrate both the security and feasibility of the proposed scheme. The designed mechanism can achieve over 92% authentication accuracy with human subjects.**

***Index Terms*—Biometrics, channel state information (CSI), device authentication, wireless coexistence.**

## I. Introduction

WEARABLE devices collect multidimensional data continuously, timely, and accurately to support a large variety of health-related applications, including fitness tracking and health monitoring. Recently, there are plenty of works to improve the efficiency and comfortableness in personal health monitoring by making wearable sensors smaller and more noninvasive with advanced technologies, e.g., nanomaterials. These wearables can be closely attached to the tissue surface to capture the thermal, electrical, mechanical, or chemical changes of objectives, including glucose concentration in sweat, the gas molecules in exhaled breath, and physiological signals that reflect heart function [1]. However, the privacy and security issue becomes the stumbling block. It is dangerous if the collected health data are leaked due to their sensitivity. Therefore, the identities of people accessing data should be verified to prevent unauthorized access. Moreover, in health monitoring, stronger authentication is expected, where the verification should not be limited to the user identity. The data sources also need authentication. If the health data are coming from malicious entities and mismatch with genuine user identities, applications may hazardously produce incorrect diagnosis results and healthcare recommendations. Consequently, to achieve these two goals simultaneously, a new wearable must first get authenticated to verify that it is possessed and accessed by legitimate users only, for which we denote as the "wearable-user authentication."

Unfortunately, current practices lack standardized regulations due to wearables' resource and ability constraints, as well as the various wireless protocols in use [2]. For example, a blood glucose monitor, whose data update frequency is low, may be a tiny device using the ZigBee protocol to achieve long battery life, whereas continuous electrocardiography (ECG) signals should be transmitted by Wi-Fi to meet their transmission bandwidth requirement. In this heterogeneous environment, where devices with different resource constraints use different wireless protocols to transmit various types of data, additional hubs/gateways are required for authentication in traditional authentication systems. However, ZigBee-enabled monitors can hardly fulfill security goals even with the help of a hub/gateway because ZigBee standard does not provide a strong security guarantee, and monitors have limited ability and resources for complicated protection. To overcome these constraints, we intend to find shared features of wearables despite using diverse wireless protocols and measuring different health parameters. The shared features we plan to utilize are the ubiquitous wireless signals transmitted from wearable devices, and we authenticate a new wearable-user pair with the help of a wearable that is already verified. For example, a new ZigBee-based wearable is to be verified that it is placed on the same legitimate user with a trusted Wi-Fi-based device, corresponding to the aforementioned examples of blood glucose monitor and ECG monitor. Existing authentication schemes may provide similar solutions, such as device-to-device (D2D) authentication. Specifically, most D2D authentication schemes in IoT either

Manuscript received April 26, 2021; revised July 13, 2021; accepted November 29, 2021. Date of publication December 13, 2021; date of current version July 7, 2022. The work of Linke Guo was supported in part by the National Science Foundation under Grant CNS-2008049 and Grant IIS-1949640. The work of Ming Li was supported in part by the National Science Foundation under Grant CNS-1943509. *(Corresponding author: Linke Guo.)*

This work involved human subjects or animals in its research. The authors confirm that all human/animal subject research procedures and protocols are exempt from review board approval.

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@clemson.edu; sihany@clemson.edu; 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).

Ming Li is with the CSE Department, The University of Texas at Arlington, Arlington, TX 76019 USA (e-mail: ming.li@uta.edu).

Digital Object Identifier 10.1109/JIOT.2021.3134667

use a preinstalled key [3] or generate a common key based on shared features, such as channel state information (CSI) and received signal strength indicator (RSSI) [4], and nonlinear distortion of speaker-microphone systems [5]. In practice, the major drawback of the above works is that they overlook wearable systems' heterogeneous abilities and wireless environments. They can only work for devices with similar embedded hardware or under the same wireless protocol and fail to authenticate the wearable-user pair. Meanwhile, extracting identical secret information from CSI requires a short distance between devices to (e.g., less than $0.4\lambda \approx 5$ cm for 2.4 GHz in [6], where $\lambda$ is the wavelength), which is too strict for general wearable systems.

To make sure that our scheme can support wearable authentication better, we explore the mutual influence between the coexisting heterogeneous wireless technologies, e.g., Wi-Fi and ZigBee transmissions in the 2.4-GHz band [7], which is named as cross-technology interference (CTI). Most previous studies focus on mitigating CTI to avoid packet corruption and thus, boost service quality [8]. However, the full potential of CTI is not reached. The on-body deployment of wearables in health monitoring provides an opportunity to trigger unique CTI sequences, which are reflected on CSI and affected by device distance, transmission power, and user-dependent physiological behavior, e.g., respiration and ECG [9]. In this work, instead of reducing CTI, we leverage its uniqueness to develop a novel authentication scheme among coarsely positioned devices of diverse capabilities. Our contributions are listed as follows.

1) Our work is the first to leverage CTI across Wi-Fi and ZigBee in heterogeneous environments for authentication.
2) By exploring the potential of CTI, we bypass the constraints of existing authentication approaches based on shared secrets and wireless signal physical layer properties. The achieved wearable-user pair authentication achieved more complex goals than regular authentication.
3) The authentication scheme is robust against illegitimate accesses. Our design does not need a centralized trusted third party, and thus, reduces deployment costs.

The remainder of this article is organized as follows. Section II gives preliminaries about wireless signals and how they are used in health monitoring, followed by our motivations in Section III. The theoretical reasoning is provided in Section IV. Section V gives the detailed design of our authentication scheme. Thorough evaluations are given in Section VI to prove the effectiveness. Section VII discusses related works. Finally, Section VIII concludes this article.

## II. Preliminaries

### A. Channel-State Information and Physiological Signal Sensing

*1) Channel-State Information:* The CSI is a metric to evaluate channel properties of transmission links that are multiple-input/multiple-output (MIMO) radio channel [10]. It is produced by estimating the time-varying channel frequency response for the orthogonal frequency-division multiplexing (OFDM) symbols. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, for example, scattering, fading, and power decay with distance.

Suppose a communication system has $N_{T_X}$ transmitter antennas, $N_{R_X}$ receiver antennas, and $N_s$ OFDM subcarriers in one channel. This channel exists $N_{T_X} \times N_{R_X} \times N_s$ subcarriers when transmitting signals. The CSI $\boldsymbol{H}(\boldsymbol{f}, \boldsymbol{t})$ measures channel frequency response in different subcarriers with frequency $f$ [11]. Let $\boldsymbol{X}(\boldsymbol{f}, \boldsymbol{t})$ and $\boldsymbol{Y}(\boldsymbol{f}, \boldsymbol{t})$ represent the transmitted and received signal with different subcarrier frequencies. $\boldsymbol{H}(\boldsymbol{f}, \boldsymbol{t})$ can be calculated at the receiver side using a known transmitted signal via $\boldsymbol{H}(\boldsymbol{f}, \boldsymbol{t}) = \boldsymbol{Y}(\boldsymbol{f}, \boldsymbol{t})/\boldsymbol{X}(\boldsymbol{f}, \boldsymbol{t})$

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

where $h_{mn}$ is the complex transmission coefficient from the transmitter antenna $m$ to the receiver antenna $n$. $h_{mn}$ reflects the condition of transmission link and is sensitive to the changes in the lengths of transmission paths. When a human subject is in the transmission environment of Wi-Fi signals, their movements change the path lengths of Wi-Fi signals and thus, perturb the CSI. From the variation of CSI, the human movements can be recognized.

*2) Physiological Signal Sensing by CSI:* The sensitive CSI is rich in information and can reflect not only vigorous human activities but also small-scale movements caused by physiological activities, such as breathing and heartbeats. A human respiration cycle includes inhalation and exhalation, during which air is taken in and pushed out by the forces from lung and surrounding muscles. An important muscle involved is the diaphragm, a dome-shaped muscle at the bottom of the lungs. It controls breathing and separates the chest cavity from the abdominal cavity. When a breath is taken, it flattens out and pulls forward, making more space for the lungs. During exhalation, the diaphragm expands and forces air out [12]. By monitoring the amplitudes and phases of CSI, the displacements of muscles that occur in respiration cycles can be detected [13]. When monitoring the respiration cycles, the muscle movements and the vibration of blood vessels in the chest area caused by heartbeats are also captured. Recently, there are works that track breathing and heartbeat simultaneously by filtering out the interference of breathing in CSI [14].

As indicated in [15], sensing physiological signals from CSI are not as accurate as from on-body sensors and faces practically constraints in a large-scale environment, but is still effective enough to identify individuals. The respiratory system, if elaborated as a mechanical behavior, is actually the pressure differences applied to the system, either by the respiratory muscles or by external devices, and the associated volume changes of the system [16]. Previous studies on the nature of respiration show that the properties of respiration are determined by physical factors, such as pulmonary structure, different respiration scenarios, mechanical properties of lung tissue (e.g., intraesophageal pressure, lung compliance, and lung resistance), the interaction with organs or body parts, etc., [17], [18]. The volume of breathing depends on the elastic forces within the respiratory system, while the breathing rate is decided by forces resulting from frictional resistance within the lung parenchyma and the surrounding tissues and forces relating to acceleration of mass. Most of these influence factors are determined by distinctive human demographic attributes and vary from person to person. This distinctiveness also applies to heartbeats. Inspired by these research findings, we leverage the existing Wi-Fi signals emitted from wearable devices and discover how the unique physiological information embedded in the CSI can help our goal of authentication.

### *B. Cross Technology Interference Between Heterogeneous Wireless Protocols*

In practice, the CSI is under the influence of the transmission of signals other than Wi-Fi signals. The 2.4-GHz ISM band is a license-free radio band that is shared by industrial wireless network standards based on IEEE 802.15.4 (ZigBee, WirelessHART, and ISA100), IEEE 802.11b/g/n, and other protocols. When these signals are propagating in the same frequency, they interfere with each other and the reliability of wireless communications could be deteriorated due to this CTI. The CTI among protocols will cause significant packet loss, where the degree of interference is determined by various types of factors, including transmission rate, energy, and distance. More specifically, 802.11b networks have a much larger impact than those of 802.11g due to its longer channel-time for 802.11 packets [7]. Under the presence of Wi-Fi traffic, the transmission latency will increase for traffic using 802.15.4 due to the use of the CSMA/CA protocol in the data link layer. When the 802.15.4 radio is far away from the smartphones or the channel RSSI is low, the Wi-Fi traffic is not corrupted. However, ZigBee packets are contaminated by Wi-Fi traffic, and thus, they will be discarded by the receiver. On the other hand, 802.11 packets will backoff during 802.15.4 transmissions when the distance is small.

Recent studies found out that when the power level of ongoing ZigBee traffic is not high enough to interrupt Wi-Fi transmission, the Wi-Fi packets will be successfully delivered, though the preambles of Wi-Fi packets are interfered and the amplitudes of CSI are changed [19]. In the heterogeneous environment of health monitoring, the CTI is inevitable. Instead of mitigating CTI, we plan to explore the uniqueness lying in the statistical features of CSI $h_{mn}$ triggered by CTI to supplement the distinctiveness of physiological information and thus, fulfill wearable-user authentication simultaneously.

## III. Motivation

### *A. Overview*

To address the diversity of commercial health-related wearables, we propose an authentication scheme that takes advantage of CTI-interfered CSI changes detected by on-body Wi-Fi-based wearables. Since wearables are attached to the human body surface, the CSI is jointly affected by the user's physiological activities, e.g., respiration and heartbeats, and CTI from other wearables belonging to this user together. Hence, not the device but the wearable-user pair is authenticated by the combined information, and illegitimate users, who fail to mimic the physiological activities and CTI, are prevented from using the device. Our scheme turns the "harmful" CTI from ZigBee wearables into a helpful hand.

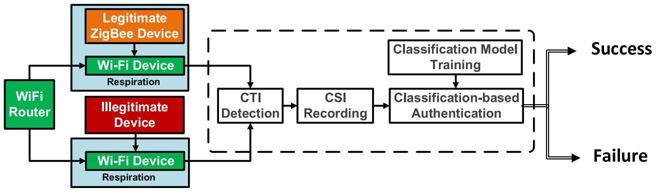


Fig. 1. System description.

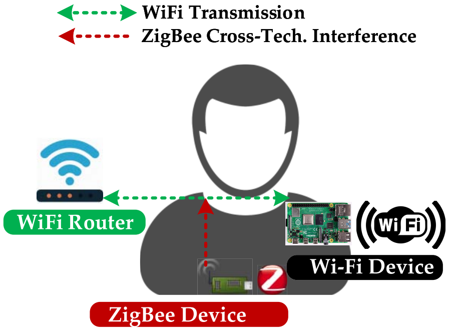


Fig. 2. System model.

Our proposed system is illustrated in Fig. 1. Assume that a Wi-Fi on-body device is trusted, and a wearable device using a different wireless protocol, e.g., ZigBee, is trying to authenticate itself to the Wi-Fi device before data collection. The ZigBee-based wearable sends ZigBee packets in the presence of a Wi-Fi transmission pair, i.e., a Wi-Fi router and the Wi-Fi device. After detecting the presence of CTI from CSI, the Wi-Fi device begins capturing CSI samples. The individual-dependent inhalation-exhalation process and heartbeats will result in wireless channel path changes and the distance from the ZigBee device to the Wi-Fi device, demonstrated as CSI characteristic changes in CTI-interfered Wi-Fi packets. Then, the Wi-Fi device is able to uncover unique features and decide if the new device is attached to the legitimate wearer's body by a trained classification model.

### *B. System Setting*

As shown in Fig. 2, we consider a healthcare scenario, where the user has several wearable devices attached to body for monitoring different physiological and daily activities.

1) *Wi-Fi Router:* It communicates with the Wi-Fi device using 802.11 protocol and works as an anchor for generating background Wi-Fi traffic.
2) *Wi-Fi-Based Wearable:* This device is considered as a trusted device, which is able to collect health-related data and send data to the cloud via a Wi-Fi router in 2.4-GHz band. It may be worn on wrist or attached to chest according to its functions. It detects and records

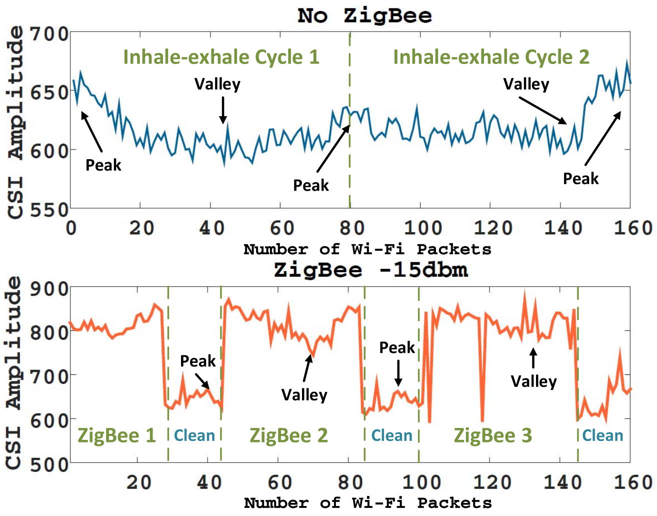


Fig. 3. Impact of ZigBee traffic on CSI.

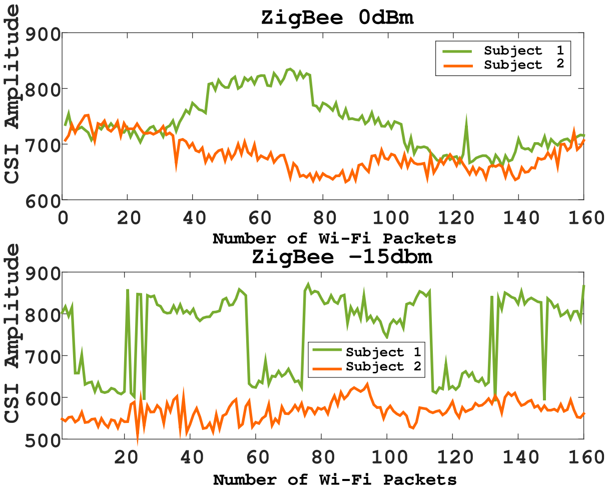


Fig. 4. ZigBee traffic on CSI-different Tx power.

CTI. It is also responsible for comparing the template with CTI-interfered CSI for authentication.

3) *ZigBee-Based Wearable:* The ZigBee-based device is capable of broadcasting ZigBee packets and generating CTIs with its transmission. It is attached to the user's upper body, where the majority of health monitoring devices are place, including chest, neck, and abdomen.

## C. From Human Respiration and CTI to CSI

To analyze the practicality of designing an authentication scheme using "interfered" CSI measurements, we demonstrate how CSI amplitudes change with physiological activities and CTI from ZigBee transmission. Specifically, as shown in Fig. 2, we use a Raspberry Pi 4 as the Wi-Fi wearable, which is installed with Nexmon [20], a C-based firmware patching framework for Broadcom/Cypress Wi-Fi chips enabling functions, including raw Wi-Fi signal transmission and CSI extraction, and a TI CC26x2R Wireless MCU LaunchPad to send ZigBee packets periodically on overlapping frequencies.

*1) CSI Changes With Physiological Activities and ZigBee Interference:* We attach the Wi-Fi device to a subject's chest, set up the transmission power of ZigBee device on abdomen, and measure the CSI values of Wi-Fi packets. Fig. 3 demonstrates CSI time series obtained with and without ZigBee interference in the tenth subcarrier of Wi-Fi Channel 1.

In the first round of data collection, there are no interfering signals in the transmission environment and the human subject is sitting still, so physiological activities, e.g., breathing, is the only factor that can greatly affect CSI. Despite random noises, the amplitudes of uncontaminated CSI show a clear cyclical up-and-down tendency, which matches the back-and-forth chest movements during respiration and indicates the existence of inhale–exhale cycles. Here, approximately two cycles are recorded.

Then, we add ZigBee interference to the previous settings by letting LaunchPad send a few packets at power −15 dBm. Each ZigBee packet is designed to cover approximately 40 Wi-Fi packets and the interval between ZigBee packets covers around 15 Wi-Fi packets. From Fig. 3, we can see that the CTI is captured by the increased CSI amplitudes while the peaks and valleys in respiration cycles can still be visually detected. From these findings, we tell that CTI can change CSI amplitudes while preserving some physiological features. We further speculate that given different patterns of ZigBee packet flow, the CSI pattern influenced by ZigBee packets may also vary.

*2) CSI Distinctiveness and Similarity Among Subjects:* Then, we place the two devices on two human subjects. The transmission power levels of the Wi-Fi device, the distance between the Wi-Fi device and router, and the distance between the Wi-Fi device and ZigBee device are set to be the same. The CSI amplitudes demonstrate apparent differences for two human subjects due to their distinct demographic attributes, as shown in Fig. 4. When the ZigBee device works at −15 dBm, the amplitudes from the two subjects almost have no coincidence point. The distinctiveness of CSI sequences between subject 1 and 2 is obvious. When the power of the ZigBee device is assigned with a larger value (0 dBm), the interfered amplitudes are much higher than those when the ZigBee power is −15 dBm, and two subjects' amplitudes move closer to each other. Nevertheless, they are still misaligned.

We use the Kendall rank correlation coefficient [21] to test whether two raw CSI sequences are statistically dependent. The sequences are aligned by the first peak. The correlation coefficients between Subject 1's and Subject 2's CSI sequences when the power of ZigBee is 0 and −15 dBm are 0.0666 and 0.0071 with a $p$-value of 0.1611 and 0.1879, respectively. It echoes the findings that CSI sequences are distinctive personwise and higher ZigBee noises may weaken the distinctiveness. The correlation coefficients between two Subject 2's CSI sequences when the power of ZigBee is 0 dBm is 0.8281 with a $p$-value of 0.0005, which verifies the similarity between the same subject's CSI sequences. The correlation coefficients between Subject 2's CSI sequences when the power of ZigBee is 0 and −15 dBm are 0.2844 with a $p$-value of 0.0001. It indicates that even being contaminated by different CTI, the CSI sequences coming from the same person are more

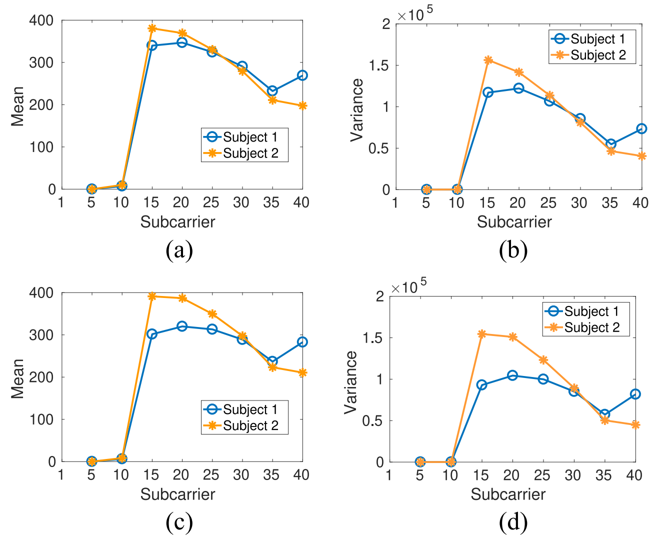


Fig. 5. Means and variances of CSI for different subjects. (a) Mean—two sub., −6 dBm. (b) Var.—two sub., −6 dBm. (c) Mean—two sub., −12 dBm. (d) Var.—two sub., −12 dBm.

closely correlated than those from different persons. Overall, the average same-person coefficient for ten subjects under the identical level of CTI is 0.88011, and the average different-person coefficient for ten subjects under the identical level of CTI is 0.08267.

In addition, we quantize this distinctiveness via dynamic time warping (DTW) distance. DTW is a technique used to measure the similarity between two arrays or time series with different lengths. We collect CSI series with the aforementioned settings from ten subjects. The DTW distances between series are calculated and normalized by the average amplitudes of clean CSI. The average DTW distances between CSI series of the same subject are 1.919, while the average DTW distances between different human subjects under 0 and −15 dBm ZigBee interference are 4.623 and 13.654. Obviously, CSI series obtained from the same user are similar but those obtained across subjects show distinctiveness.

*3) CSI Distinctiveness and Similarity on Wi-Fi Subcarriers:* To further investigate the distinctiveness of CSI sequences based on the aforementioned observations, we statistically explore the CSI amplitudes on different Wi-Fi subcarriers. An example of the means and variances of CSI amplitudes from thousands of Wi-Fi packets with different interference power levels on each subcarrier is calculated and demonstrated in Fig. 5. The differences are more significant at subcarriers 10-30, because these subcarriers react more acutely to CTI because of the higher sensitivity to chest displacement at their frequencies [22]. When the ZigBee transmission power is larger (−6 dBm), the gap between statistics is smaller. It echoes the findings in Section III-C2: the higher CTI hides more physiological features and brings CSI from different subjects closer, the lower CTI incurs less ZigBee-related information and may impede the authentication from device perspective. These differences are also visible on other pairs chosen from ten tested subjects.

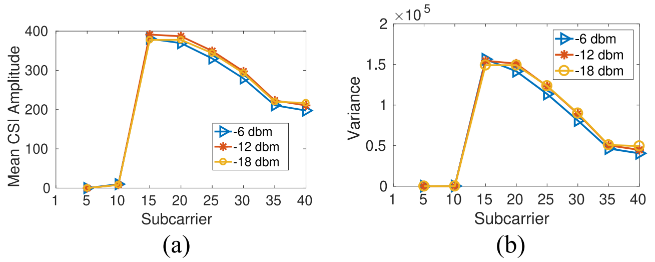


Fig. 6. Mean and variance of CSI for one subject. (a) Mean—subject 1. (b) Variance—subject 1.

TABLE I
DTW DISTANCES ON SUBCARRIERS

| Subcarrier | 15 | 20 | 25 | 30 |
|---|---|---|---|---|
| Same subject | 1.521 | 1.554 | 2.122 | 1.291 |
| Different subjects, -6 dBm | 6.344 | 4.758 | 1.397 | 2.006 |
| Different subjects, -12 dbm | 11.504 | 10.851 | 6.182 | 1.029 |

The feasibility of designing a wearable-user authentication scheme based on CSI sequences is demonstrated in Fig. 6 as supplementary to the statistical analysis in Section III-C2. Though the ZigBee power levels are different, the means and variances share a similar tendency and their values are quite similar for the identical human subject. This empirical observation shows that besides the fact that different human respiration and ZigBee transmission patterns uniquely impact CSI, the CSI sequences interfered by different levels of CTI for one subject nearly remain stable.

The average DTW distances between CSI series acquired from pairs of subjects are computed to show the similarity and distinctiveness, which are shown in Table I. The trends of DTW distances echo with the aforementioned analysis. Therefore, the feasibility of our proposed CTI-enabled authentication scheme is fully presented.

### *D. Adversarial Model*

We assume there is an active attacker, Eve, that can sense the wireless environment, inject new traffic, and replay packets to pretend itself as a legitimate one. The malicious device controlled by Eve is off-body and at least more than one wavelength away (12.5 cm for 2.4 GHz) from ZigBee devices in case being visually detected. The attacker may perform attacks whenever it detects the transmission from the legitimate device. Our work makes no exploration of protecting against passive attacks such as eavesdropping attacks and information leakage because the information exchanged during the authentication process reveals no value.

## IV. MEASURING DISTANCE VARIATIONS

In our scheme, we turn the traditional CSI-based device authentication problem into "how to verify the ZigBee device's physical proximities to the Wi-Fi device and the device is on the body." To formulate this problem, we define the term "relative distance," which is the dynamic distance between Wi-Fi device and ZigBee device during respiration. In the following, we theoretically demonstrate how the relative distance is touched by respiration and CTI and further prove

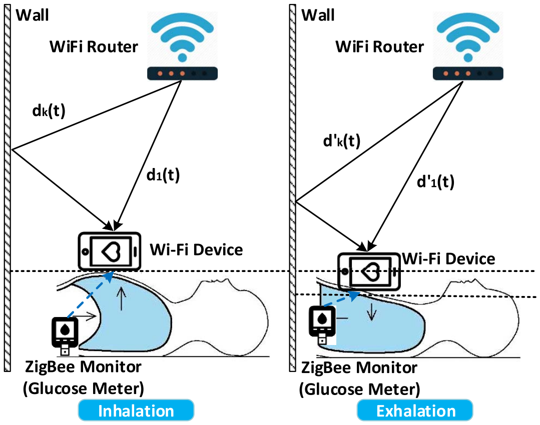


Fig. 7. Path changes due to respiration.

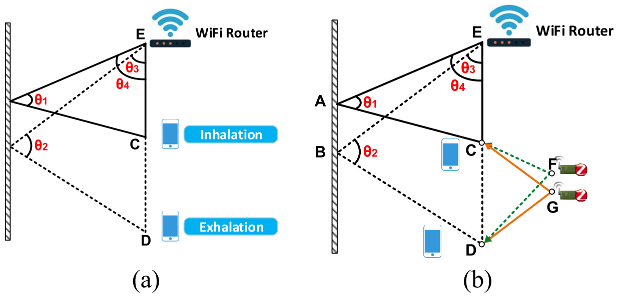


Fig. 8. CSI changes regarding distances. (a) Change of one single path. (b) Abdominal displacement.

the feasibility of leveraging unique CTI for authentication. In particular, the signal received by the Wi-Fi device at time $t$ is

$$r(f,t) = s(f,t)H(f,t) + \omega(f,t) \tag{2}$$

where $s(f,t)$ is the signal sent from the Wi-Fi router, $H$ is the CSI matrix, and $\omega$ is the noise. Note that we only consider the amplitudes of the CSI values in this work.

### A. Path Changes Due to Muscle Displacement

The displacement of muscles around the patient's chest largely depends on respiration rather than heartbeats. During regular respiration cycles, the human subject's chest and abdomen occur in a periodic way. This cyclic process alters the "relative distance" between the on-body Wi-Fi device and ZigBee device and impacts the path lengths of Wi-Fi connections. Fig. 7 illustrates that the regular respiration will cause path changes reflected by surroundings and the Line-of-Sight (LoS) path between the Wi-Fi device and the Wi-Fi router. To further investigate how respiration impacts the received CSI characteristics, we have the following formulation as in [11]:

$$\phi(t) = e^{-j2\pi d_k(t)/\lambda} \tag{3}$$

$$H(f,t) = e^{-j2\pi \Delta f t} \sum a_k(f,t)\phi(t) \tag{4}$$

where $a_k(f,t)$ is the attenuation (complex value) and initial phase offset of the $k$th path, $\phi(t)$ is the phase shift on the $k$th path caused by path length change, $\lambda$ is the wavelength, $d_k(t)$ is the change of path length on the $k$th path, $e^{-j2\pi \Delta f t}$ is the phase shift caused by the carrier frequency difference between the sender and receiver, and $t$ is the time variable. Hence, the power of CSI, $|H(f,t)|^2$, can be calculated as

$$|H(f,t)|^2 = \sum_k |a_k(f,t)|^2 + 2\sum_{k\neq m}\left| a_k(f,t)a_m(f,t)\cos\left(\frac{2\pi d_k(t) - 2\pi d_m(t)}{\lambda} + \phi_{km}\right)\right|$$

where $\phi_{km}$ is a constant value.

We take a step further to analyze how the path is changing during inhalation and exhalation. As shown in Fig. 8(a), $\Delta AEC$ represents the LoS path and $m$th path reflected by the wall when the user is inhaling, while $\Delta BED$ jointly draws the LoS path and $m$th path during exhaling. Since the drift of LoS path is far smaller than the distance from Wi-Fi device to router, $EC$ and $ED$ roughly coincide. The chest displacement of a normal adult is less than 6.25 cm (half of the wavelength for 2.4-GHz Wi-Fi) [23]. Therefore, to show CSI can be leveraged as a stable feature, we demonstrate that CSI changes can be mapped to the path changes during one inhale–exhale process.

*Theorem 1:* The CSI power in one respiration cycle is monotonically changing with time in correspondence to the inhale–exhale process.

*Proof:*

$$\frac{CD}{BD - AC} = \frac{\sin\theta_2 - \sin\theta_1}{\sin\theta_3 - \sin\theta_4} = \frac{\sin(\pi - 2\theta_3) - \sin(\pi - 2\theta_4)}{\sin\theta_3 - \sin\theta_4}$$
$$= \frac{2\sin\theta_3\cos\theta_3 - 2\sin\theta_4\cos\theta_4}{\sin\theta_3 - \sin\theta_4}.$$

Obviously, $0 < \sin\theta_3 < \sin\theta_4 < 1$ because $\theta_3 < \theta_4$. So

$$2\sin\theta_3\cos\theta_3 - \sin\theta_3 > 2\sin\theta_4\cos\theta_4 - \sin\theta_4.$$

Moreover

$$\frac{2\sin\theta_3\cos\theta_3 - 2\sin\theta_4\cos\theta_4}{\sin\theta_3 - \sin\theta_4}$$
$$= \frac{2(\sin\theta_3 - \cos\theta_3) - 2\left(\sin^3\theta_4 - \cos^3\theta_4\right)}{\sin\theta_3 - \cos\theta_4}$$
$$= 2 - 2\sin\theta_3\cos\theta_4 - 2\sin^2\theta_4 - 2\cos^2\theta_3 < 2.$$

Thus, $1 < [CD/(BD - AC)] < 2$, indicating that $0 < 2\pi d_k(t)/\lambda - 2\pi d_m(t)/\lambda < \pi/2$.

For two pairs of $(d_k(t_1), d_m(t_1))$ and $(d_k(t_2), d_m(t_2))$ satisfying the above inequality, the direction cosine of a direction vector $\boldsymbol{l}$ going through these pairs of point is

$$\cos\alpha = \frac{d_k(t_2) - d_k(t_1)}{\sqrt{[d_k(t_2) - d_k(t_1)]^2 + [d_m(t_2) - d_m(t_1)]^2}}$$
$$\cos\beta = \frac{d_m(t_2) - d_m(t_1)}{\sqrt{[d_k(t_2) - d_k(t_1)]^2 + [d_m(t_2) - d_m(t_1)]^2}}.$$

Then

$$a_{\boldsymbol{l}} = \frac{\partial\left(2 - 2\sin\theta_3\cos\theta_4 - 2\sin^2\theta_4 - 2\cos^2\theta_3\right)}{\partial \boldsymbol{l}}$$
$$= \cos\alpha(-2\sin\theta_3 - 4\sin\theta_4) + \cos\beta(-4\sin\theta_3 - 2\sin\theta_4)$$
$$= \sin\theta_3(-2\cos\alpha - 4\cos\beta) + \sin\theta_4(-4\cos\alpha - 2\cos\beta).$$

If $d_k(t_1) < d_k(t_2)$ (e.g., during exhaling), $d_m(t) < d_m(t_2)$

$$a_l < \sin\theta_4(-6\cos\alpha - 6\cos\beta) < 0.$$

The shift is monotonically decreasing during inhaling because

$$a_l > \sin\theta_3(-6\cos\alpha - 6\cos\beta) > 0.$$

The shift is monotonically increasing. ■

### *B. Relative Distances Changes During Respiration*

The CTI-interfered CSI can be estimated from the received symbols $r = (H+H^Z)s_k+w$ with known ground-truth symbols, which is usually transmitted on pilot subcarriers, as

$$\hat{H} = rs^* = \left(H + H^Z\right)|s| + ws^* \tag{5}$$

where $H^Z$ is the changes on CSI caused by CTI.

The ZigBee device is also experiencing periodic displacement caused by respiration no matter it is placed on the chest or abdomen. If it is placed on the chest, it experiences displacements similar in tendency but different in distances compared to chest displacement. If placed on the abdomen, the deviation produced by abdomen displacement on CSI measurement is comparably small due to the small abdominal wall displacement, which could be only 1/8 of the chest displacement [23]. The abdominal wall moves in the opposite direction to the direction of chest during breathing. As illustrated in Fig. 8(b), the relative distance drift between ZigBee device and Wi-Fi device during an inhale–exhale process is $|DF - CG|$, where $DF$ represents the extreme of exhaling and $FG$ is for the extreme of inhaling. Intuitively, if the line between the midpoint of $FG$ and the midpoint of $CD$ is perpendicular to $CD$, $|DF-CG| = 0$; if the midpoint of $FG$ is above the midpoint of $CD$, $DF-CG > 0$; otherwise, $DF-CG < 0$. If $DF-CG > 0$, the received CTI power of ZigBee packets decreases during exhaling because the Wi-Fi device moves farther away from the ZigBee device. $FG$'s midpoint is person-identifiable since it is determined by body figures and respiration situations. Therefore, the LoS path length in CSI power $|H(f,t)|^2$ and relative distance in CTI interference are both dynamically changing when the user is inhaling or exhaling, which makes the CSI sequence sole environmentwise and personwise, as well as unpredictable to attackers.

## V. CTI-Enabled Wearable Authentication

In the detailed design, the Wi-Fi device acquires a CSI template by training CSI sequences collected with CTI from an authorized ZigBee device. Then, to initiate the authentication protocol, a newly attached ZigBee device sends its authentication request packets and generate CTI. We expect that the received CSI changes will be close enough to the changes embedded in the template.

### *A. ZigBee Packet Design*

The ZigBee device has to send packets on ZigBee channels that are overlapped with Wi-Fi channels in the frequency domain, i.e., ZigBee Channel 11, ZigBee Channel 13, and Wi-Fi Channel 1, to raise CTI. As shown in Fig. 9, we assume the ZigBee device in our system is half-duplex, and it sends authentication request packets with length $T_p$ and time interval of $T_i$. Meanwhile, Wi-Fi packets in regular transmission have a length $T'_p$ and time interval $T'_i$. Generally, ZigBee packets last longer than Wi-Fi packets in the time domain, so $T_p > T'_p$. To let ZigBee packets cover the maximum number of Wi-Fi packets, their packet lengths and transmit intervals are designed as

$$T_p > n \times \left(2T'_p + T'_i\right), \quad T_i < 2n \times \left(T'_p + T'_i\right) - T_p$$

$$p \times \left(T_p + T_i\right) = q \times \left(T'_p + T'_i\right)$$

where $n, p,$ and $q$ are integers.

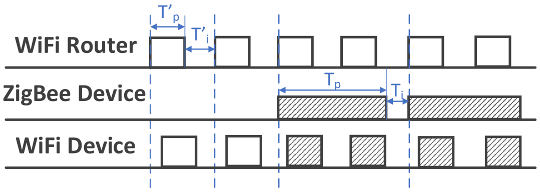


Fig. 9. Overlapped ZigBee packet design.

### *B. CTI Detection*

According to the experimental results in Section III-C, the statistics of CSI sequence changes after ZigBee packets get involved. After acquiring a sample of CSI at time $t$, the Wi-Fi device computes the variances $\boldsymbol{Var(t)} = \{\mathrm{Var}(t)_m, \ldots, \mathrm{Var}(t)_n\}$ on subcarriers $m$ to $n$ interfered by CTI for the latest $s$ samples. The dynamic thresholds for each subcarrier are assigned in line with the experimental setting in [24]

$$|\boldsymbol{H(t)}|^2 = \left\{\min|H(f_m,t)|^2, \ldots, \min|H(f_n,t)|^2\right\}$$

where $f_i$ is the center frequency of subcarrier $i$, $i \in [m,n]$ and $\min|H(f_i,t)|^2$ means the minimum CSI power in the latest $s$ samples at time $t$. If for more than half of the total subcarriers, $\mathrm{Var}(i) > \min|H(f_i,t)|^2$ while $\mathrm{Var}(t') < \min|H(f_i,t)|^2$ for $t' < t$, the Wi-Fi device believes that it confronts CTI and begins recording CSI sequences.

### *C. Authentication Mechanism Design*

We apply the long short-term memory (LSTM) recurrent neural networks (RNNs), which are capable of learning long-term dependencies and nonlinear dynamics when classifying time sequences in the authentication scheme. The authentication is successful only if the CTI-involved CSI sequences can be classified into the same class with the template.

*1) Template Acquisition and Training:* In practice, the types and locations of on-body wearables are limited, most of which are attached to the chest, abdomen, and wrist in corresponding to the locations of internal organs. If the device with a Wi-Fi module is worn on the wrist, i.e., smartwatches, the user places that hand on the chest and starts CSI recording. Otherwise, the Wi-Fi device is directly placed on the chest. The upper body area is divided by two lines separating the chest area with the abdomen and neck due to their different displacement distances during respiration so that CSI sequences collected in the same area share similar patterns. In both the chest and abdomen/neck sections, we choose three to seven locations, where the distances between these locations are 10 cm. By placing the ZigBee device on determined locations, a bunch of CSI sequences is collected. These CSI sequences are denoised with the principal component analysis [25] to extract dominant features and both "template 1" and "template 2" are labeled as class "legitimate."

If these devices are shared by multiple people, which means that there could be only one device but are multiple "wearable-user pairs" needed to be authenticated, the classification model treats the authentication as a multiclass classification task, where each class corresponds to the legitimate samples of each user. However, instead of directly output the predicted classes, we translate the results into "illegitimate" and "legitimate" for each user. For every user, the classes belonging to other users are equal to "illegitimate" classes from their point of view, which means that the authentication fails if their data are classified into any other users' "legitimate" class. If there is only one "wearable-user pair," the user collects some extra CSI sequences by placing the ZigBee device wherever away from their body and labels the CSI sequences as "illegitimate."

Finally, The LSTM RNNs are trained with these samples to learn their features.

*2) CSI Recording, Classification, and Authentication:* Suppose at timestamps $\{t_1, t_2, \ldots, t_n\}$, the Wi-Fi device measures a series of CSI powers from $\boldsymbol{P} = \{\boldsymbol{P}_{t_1}, \boldsymbol{P}_{t_2}, \ldots, \boldsymbol{P}_{t_n}\}$. We list the elements in $\boldsymbol{P}_{t_1}$ as an example

$$\boldsymbol{P}_{t_1} = \Big\{h_{11}^{1t_1}, \ldots, h_{1N_{\mathrm{Tx}}}^{1t_1}, \ldots, h_{N_{\mathrm{Rx}}1}^{1t_1}, \ldots, h_{N_{\mathrm{Tx}},N_{\mathrm{Tx}}}^{1t_1} \\ \cdots h_{11}^{N_{\mathrm{sh}}t_1}, \ldots, h_{1N_{\mathrm{Tx}}}^{N_{\mathrm{sh}}t_1}, \ldots, h_{N_{\mathrm{Rx}}1}^{N_{\mathrm{sh}}t_1}, \ldots, h_{N_{\mathrm{Tx}},N_{\mathrm{Tx}}}^{N_{\mathrm{sh}}t_1}\Big\}$$

where $N_{\mathrm{sh}}$ is the number of Wi-Fi subcarriers covered by the ZigBee channel. The CSI sequences, after truncated by a window and filled with forward filling and back filling, are passed to the LSTM layer. The LSTM layers use memory units with forget gates, combined with an input layer and an output layer. The forget gates control the oblivion of old CSI values and help updating the new cell state. The input layer picks the new CSI value for update and creates a new candidate cell state. Then, the cell state is weighted and calculated from the output of forget gates and candidate cell state. We use a log loss function and a sigmoid activation function in our model. The output layer is a fully connected one with a softmax activation function, and the outputs of each softmax function characterize the probability distribution over classes. The sequence will be classified into the one having the highest probability among classes "legitimate" and "illegitimate." The authentication is successful if $\boldsymbol{P}$ can be classified into "legitimate," which means that $\boldsymbol{P}$ is either this user's "template 1" or "template 2." Otherwise, the failure on authentication may be attributed to reasons like CTI is not detected, or the ZigBee device is not on the proper user, etc.

## VI. Scheme Evaluation

### A. Security Analysis

*1) Feasibility of CSI-Based Authentication:* In the proposed scenario, the channel is dynamic due to chest movement. Coherence time is a metric describing the dynamic features of a communication channel, which is defined as the time duration over which the channel impulse response is considered stable. An approximation of coherence time $T_c$ is given by $\widetilde{T_c} = 0.423/\widetilde{f_m}, \widetilde{f_m} = (\widetilde{v}/c)f_c$, where $f_c$ is the center frequency, $\widetilde{v}$ is the average approximation of subject, and $c$ is the speed of light. The human subject is sitting at a fix position, so the movement involved is slow and steady. The time duration of one ZigBee packet follows, $T_p < T_c$, which means that CSI values are not contaminated by Doppler shift, and the CSI-based authentication is feasible.

*2) Analysis of Device Authenticity:* We analyze how our scheme defends against two kinds of common active attacks to demonstrate device authenticity.

*Spoofing Attack:* Devices are verified based on the physiological activity and relative distance information. If the attacker Eve, who locates at a place one wavelength away, pretends to be a legitimate device and requests for authentication, she cannot generate the same CTI as the ZigBee device. So, she can succeed only if a sequence of CSI values guessed by Eve is close enough to the actual measurement, which has a very low probability. Even if she compromises Wi-Fi router and knows the respiration pattern due to channel reciprocity, Eve still cannot perform spoofing attack because of the unpredictable ZigBee interference with the Wi-Fi device.

*Injection and Replay Attacks:* An active attacker can inject a packet or record ZigBee packet and replay it to the Wi-Fi device for authentication. However, when recording CSI samples for authentication, the relative distances between the attacking device and Wi-Fi device are different from the relative distances between the legitimate device and Wi-Fi device. Therefore, the levels of CTI caused by the attacking device and the legitimate device are different. The Wi-Fi device can easily know that the CTI-interfered CSI samples do not share similar features. As a result, the attacking device will not be recognized as a legitimate one. These attacks are successfully defended.

### B. Experiment Setting

We detail our experimental settings consisting of devices, environment, and human subjects to evaluate the performance of our proposed wearable authentication scheme.

*1) Experiment Devices:* We use Texas Instrument SimpleLink Multistandard CC26x2R Wireless MCU LaunchPads (LAUNCHXL-CC26X2R1) and Raspberry Pi 4 in our experiment. To save the resource consumption on Raspberry Pi, the LSTM RNNs are first trained on a laptop. The Raspberry Pi is only responsible of testing after optimizing LSTM RNNs model into a TensorFlow Lite model or updating only a portion of layers in the model when new data are coming in. This step can greatly reduce the burden of Raspberry Pi.

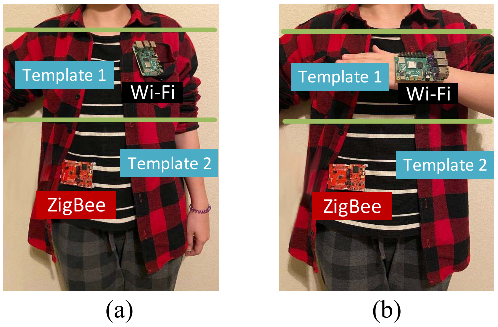


Fig. 10. Experiment settings. (a) Deployed setup 1. (b) Deployed setup 2.

*2) Wireless Environment:* We use Channel 1 (2401–2423 MHz with center frequency of 2412 MHz) among all 802.11n Wi-Fi channels. As for ZigBee, we choose Channel 11 (center frequency 2405 MHz) and Channel 13 (center frequency 2415 MHz) that overlap with Wi-Fi Channel 1. Twenty Wi-Fi packets are transmitted per second.

*3) Human Subject Setting:* Two setups as shown in Fig. 10. In the first setup, one Raspberry Pi is tied to the subject's chest and another Raspberry Pi is placed on the desk used as the Wi-Fi router. The launchpad is tied around abdomen. The Raspberry Pi is tied to wrist in the second setup, where users raise their arms and place it on the chest during authentication.

*4) Data Set Setting:* Our experiment is set up to verify that our scheme can work at a more strict scenario, where one device is shared by multiple people, or, in other words, there is only one device but are multiple "wearable-user pairs" needed to be authenticated. Ten female and ten male human subjects, whose ages are between 22 and 50 and heights are between 160 and 180 cm, are recruited. For each subject and each round, we record and label a CSI sequence lasting 20 s, which contains about 360 packets and covers four to seven respiration cycles. In total, we collect 30 rounds (10 min) for each individual, and 15 rounds for each ZigBee device. Before each round, the location of ZigBee devices is changed to be 10 cm away from the previous location by moving the elastic cord rings. The data set is split into training (80% in total, 40% for template 1 and 40% for template 2), validation (10%), and test (10%) sets. The trained models are validated on another 10% of data. The trained model is tested to Raspberry Pi on the remaining 10% data.

For each user, the classes belonging to the other 19 users equal to "illegitimate" classes from their point of view, which means that the authentication fails if their data are classified into any other users' "legitimate" class (either "template 1" or "template 2"). This data set setting is to mimic the situation that 20 people share one single device, while, in practice, the number of users should be much smaller.

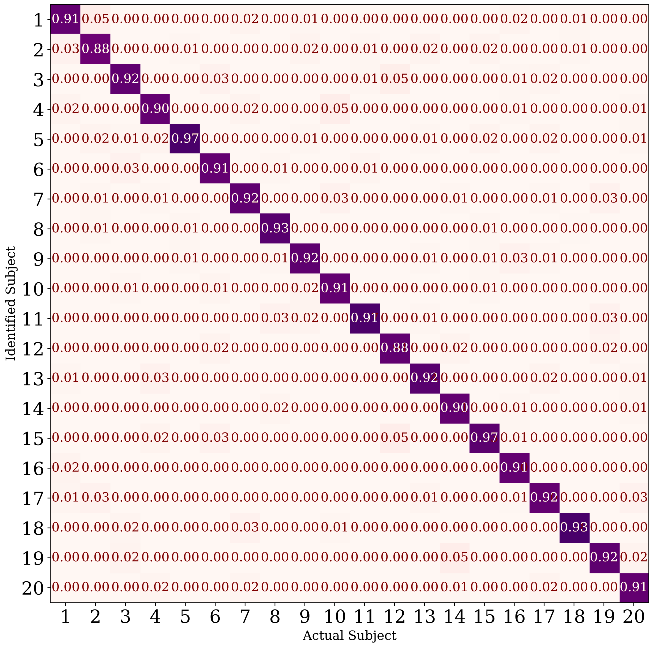


Fig. 11. Confusion matrix of accuracy.

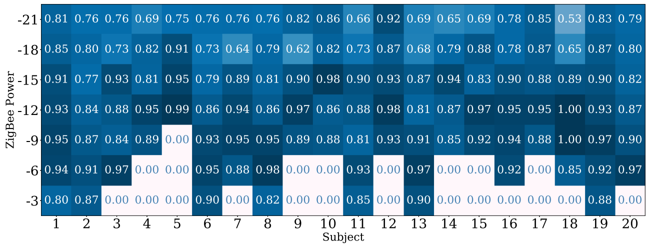


Fig. 12. Authen. accuracy—personwise.

## C. Device Authentication Performance

The number of received Wi-Fi packets is not constant for every round due to the changes in the environment, so the classification performance metrics for each subject is weighted averaged over the number of packets received. The average true positive rate (TPR) is reflected by the confusion matrix in Fig. 11. We observe that the achieved TPR is over 90% for 19 out of 20 subjects, where the highest among them is 97%. The average TPR is around 92.09% with a standard deviation of 2.39%. The false positive rates (FPRs), or false acceptance rate, have a mean of 7.95% and a standard deviation of 3.04%. The false negative rates (FNRs), or false rejection rates, have a mean of 7.96% and a standard deviation of 2.42%. The comparably high TPRs and low FPRs verify the effectiveness of our proposed authentication scheme. We then explore the detailed influence factors of performance.

*1) Optimal ZigBee Transmission Power:* Here, we use accuracy, which is the ratio of true positive and true negative to all results, to quantify performance. Due to the unique physical and physiological properties, the effect of CTI is different among individuals. Thus, the most beneficial (contributing to the highest TPR) ZigBee power is also different personwise. For example, the accuracy can be as high as 100% for subject 18 when the power is −12 dBm in Fig. 12, while the accuracy for subject 8 under the same setting is only 86%. Therefore, it would be better if the ZigBee power is a user-defined parameter. However, there are some common characteristics that lie within. For example, the accuracy is downgraded for the population when the power is below −15 dBm because the power level is too low to carry enough identifiable variations to CSI

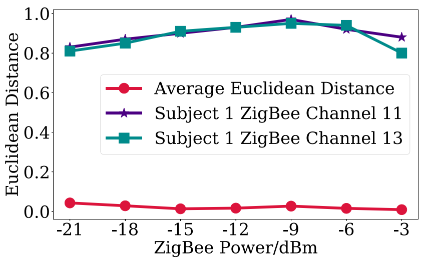


Fig. 13. Authen. accuracy—channelwise.

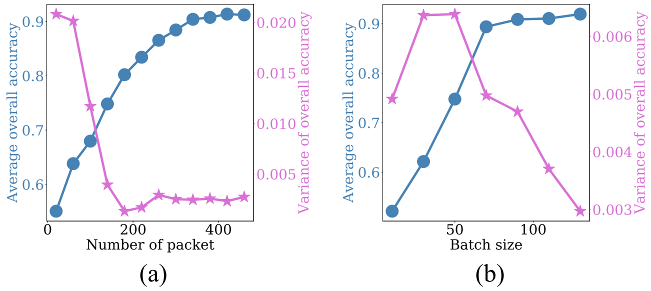


Fig. 14. Overall accuracy of authentication model. (a) Different packet length. (b) Different batch size.

values. Therefore, results under −15 dBm are discarded when considering the overall accuracy.

*2) ZigBee Channel Selection:* To identify whether choosing different ZigBee channels (frequencies) will affect the authentication performance, we compare the accuracy for ZigBee devices working on Channels 11, and 13, respectively. For each power level, we calculate the average Euclidean distances between the accuracy set with 20 subjects from Channel 11 and the set from Channel 13. The average Euclidean distances are drawn in Fig. 13. Only the accuracy from subject 1 is drawn for clarity. In all, the average Euclidean distance is always under 0.05 and is nearly 0 under some circumstances, indicating the small differences between the two sets. From the small Euclidean distances and proximity of two value sets from subject 1, we can tell that the authentication accuracy is stable in terms of frequency and will not be influenced by the selection of ZigBee channels.

*3) Choice of Training Parameters:* To study how the settings of LSTM RNN impact accuracy, we run training and testing under different training lengths (the numbers of input CSI samples) and batch sizes (the numbers of samples processed before the model update). Initially, we perform 50 rounds of training and testing under different training lengths with a batch size of 100. Then, the training length is set to 500 and we repeatedly test the model with varying sizes of batch. As shown in Fig. 14, the accuracy is increasing with more training data and larger batch size. When the training data contains more than 350 packets (transmitted in about 20 s) and the batch size is over 75, our system can achieve consistent accuracy of over 90%. The cost of building CSI profiles for accurate authentication is negligible.

### *D. Comparison Between Two Setups*

We further investigate if our scheme can achieve similar performance even if the Wi-Fi device is not closely attached to the chest. To compare the performance under two setups, Table II illustrates the statistics of TPR differences between the two sets of classification results. The overall average difference is as low as 2.469% and the STD is below 1%, from which we reason that the performance is not greatly impacted and remains stable even if the Wi-Fi device is tied on the wrist instead of chest. The displacements brought by chest are explicitly reflected in wrist movements when wrist is placed on the chest. The accuracy difference shows dissimilar patterns in terms of subjects due to their physical diversities. Generally, the differences are smaller when the ZigBee power is lower because less CTI is triggered. Despite of the differences, the performance remains high for both setups. Therefore, our scheme is generalized to common on-body devices placed on body.

TABLE II
ACCURACY COMPARISON FOR SETUP 1 AND SETUP 2

| Power<br>Metrics | -3 dbm | -6 dbm | -9 dbm | -12 dbm | -15 dbm |
|---|---|---|---|---|---|
| Average | 3.501% | 2.565% | 2.414% | 2.312% | 1.558% |
| STD | 0.572% | 0.817% | 0.833% | 1.124% | 0.798% |
| Median | 3.336% | 2.570% | 2.291% | 2.434% | 1.095% |

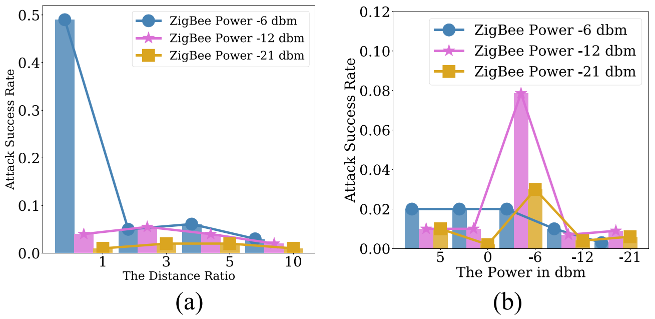


Fig. 15. Unintended successful authentication. (a) Distance versus Succ. rate. (b) Power versus succ. rate.

### *E. Performance Against Illegitimate Access*

Then, we test the performance against the adversarial device Eve. We define a metric as the attack success rate to quantify the defense results, which is the ratio of the number of CSI sequences from the active attackers that are falsely recognized as from the legitimate device to the total number of samples.

*1) Distance to the Wi-Fi Device:* The power of the illegitimate device is set to −6 dBm. The distance is expressed as a ratio of the distance from attacking device to the Wi-Fi device to the distance from the legitimate device to the Wi-Fi device. As shown in Fig. 15(a), it can pretend to be a legal device with a probability below 50% only if its distance to the Wi-Fi device is the same as that of an authenticated device, which is smaller than the overall authentication accuracy due to the unpredictable relative distance and environmental variations when the illegitimate device is placed off-body. However, any attacker in that small range will be visually detected. When the distance becomes larger, the probability plunges. The attacker cannot mimic CTI even by holding similar energy as a legal device from Wi-Fi device's view, so the probability is no greater than 8%, which does not exceed the misclassification rate in Fig. 11. Therefore, the attacker gains no advantage.

*2) Transmission Power:* Then, we set the distance ratio of the attacker to 3, and its attack ability is tested with different ZigBee transmission powers. The results are listed in Fig. 15(b). Obviously, the overall success rate is smaller than the misclassification rate of the original authentication scheme. Hence, the attacker is still powerless even he tries to altering its transmission power. Under such a low attack success rate, attackers can be blocked out with brief methods, i.e., put a restriction on the number of authentication attempts.

## VII. Related Work

### A. CSI-Based Respiration Measurement

In healthcare systems, CSI is acquired from deployed Wi-Fi-based devices to achieve contact-free respiration measurement, which is more convenient and nonintrusive than other methods [9], [22]. The chest movement caused by respiration is reflected in the amplitudes and phases of channel response. This method is first proposed in WiSleep [26] to detect human respiration rate for sleep monitoring based on CSI in commodity smartphones. Clear ripple-like patterns of CSI amplitudes, which correspond to the movement of chest, are detected. They also find out that not all the CSI sequences show the pattern of breathing. For example, subcarrier 30 does not contain as much information of breathing as other subcarriers. In their paper, sleeping position detection is also achieved. Further research works discover the possibility of detecting more detailed information, such as abnormal breathing patterns and heart rate [22], [27]. Liu *et al.* [28] further extracted biometrics from respiration interfered CSI to enable user authentication. Compared to these works, our work defines the "relative distance" and thus, captures more physiological information and achieves simultaneous device-user authentication.

### B. Device/User Authentication in Healthcare

Existing device or user authentication schemes designed for healthcare are based on physiological values, channel properties, etc., [29].

*1) Physiological-Based Schemes:* The physiological-based schemes can authenticate either user's or device's identity. They first extract features from some physiological signals, such as electrocardiogram (ECG) signals and electroencephalogram (EEG) signals, and then generate a common secret from the extracted features [30]–[32] for devices with similar features. Recently, smartwatches or wristbands are more and more used in authentication due to the plethora data they can collect. Vhaduri and Poellabauer [33] and Ekiz *et al.* [34] used multimodal biometrics to authenticate the wearable users with machine learning models. They are straightforward, but they cannot simultaneously verify device and user. They are not scalable because they require a powerful device to collect multiple dimensions of biometrics while in practice, some health monitoring devices may lack the required sensing module and do not have built-in mechanisms to authenticate themselves.

*2) Channel-Property-Based Authentication:* Channel property is a shared, symmetric metric, regardless of devices' sensing abilities. In [35], two devices are close to each other, so the channel reciprocity produces a common secret based on RSSI for two devices while preventing the eavesdropper from getting this secret. Shi *et al.* [36] analyzed the characteristics of on-body (both transceivers are located on the surface of or in close vicinity to body) and off-body (at least one transceiver is off-body) channels to block secret information from off-body attackers. The fundamental shortcoming is the RSSI values are integers and only changes within a narrow range when the person is breathing. Hence, they cannot capture physiological activities precisely [26].

Device authentication based on CSI is usually more accurate and achieves higher secret generation rate than RSSI-based ones. In [37], a CSI-based secret generation protocol is proposed using a validation recombination mechanism. However, it requires high signal-to-noise-ratio to reach an agreement as even a single bit mismatch will result in a failure. Despite of the advantages, CSI is very sensitive so it is easy to be contaminated or corrupted by CTI among monitoring traffics.

However, channel-property-based schemes are severely obstructed by the distance restriction and wireless coexistence in the healthcare scheme. The RSSI and CSI observed by two devices vary greatly if they are placed more than one wavelength away [6], [38]. Moreover, a healthcare system involves various wireless protocols due to the diversity in manufacturers and demands, while CSI is not supported in protocols other than Wi-Fi, and RSSI is not unified due to nonidentical transmission powers. Our work overcomes their limitations.

Yu *et al.* [39] used a hash function to generate a chain of authorization code and transmits the authorization code to achieve the authentication between ZigBee-based devices and Wi-Fi-based devices. In their settings, the devices using different protocols can understand each other's messages through cross technology communication techniques. It requires additional modification in device hardware and/or protocol design, which is not practical for regular health monitoring sensors. Compared to their work, our work achieves authentication with existing protocol designs and is easier to be used.

*3) Noncontact Respiration-Based Authentication:* Recently, researchers are investigating into leveraging channel properties that contain features brought by physiological activities for human identity authentication and people counting. To achieve authentication, existing works either extract human respiration rate from CSI [40] or directly using breathing patterns for classification [41]. These works are efficient in their evaluations regarding mitigating noises and trying to tackle the complex multiperson situation. However, these works merely focusing on mitigating interference, and primarily only natural environmental interference. For example, to combat noises, Wang *et al.* [40] combined CSI on different subcarriers to enhance the signal-to-noise ratio. This approach can select an optimal set of subcarriers under natural random noises but will probably enhance the CTI that spread over many subcarriers and worsen the noise contamination, especially if the CTI is intentionally injected into most Wi-Fi subcarriers.

In this case, intending to separate interferences from signals may detrimentally discard information for identification. On the contrary, our work bypasses these limitations by using CTI and achieving two goals, "wearable-user authentication" simultaneously.

## VIII. Conclusion

The growth of wearable devices brings significant security challenges. Most wearables cannot perform efficient authentication due to heterogeneous environments and constraints. This research work takes advantage of CTI resulted from wireless coexistence and embeds it with human physiological signals to achieve on-body wearable-user authentication. The changes of ZigBee-Wi-Fi relative distances and Wi-Fi path lengths during respiration are explored both empirically and theoretically. The proposed scheme breaks the boundary of protocol incompatibility and achieves simultaneous wearable-user authentication while preventing illegitimate access from unauthorized wearables. Through extensive experiments and analysis, we demonstrate the practicality, efficiency, and security of the authentication scheme.

## References

[1] B. Peng, F. Zhao, J. Ping, and Y. Ying, "Recent advances in nanomaterial-enabled wearable sensors: Material synthesis, sensor design, and personal health monitoring," *Small*, vol. 16, no. 44, 2020, Art. no. 2002681.

[2] J. Weber-Jahnke, L. Peyton, and T. Topaloglou, "eHealth system interoperability," *Inf. Syst. Front.*, vol. 14, no. 1, pp. 1–3, 2012.

[3] M. Shen *et al.*, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, May 2020.

[4] H. F. T. Ahmed, H. Ahmad, and C. Aravind, "Device free human gesture recognition using Wi-Fi CSI: A survey," *Eng. Appl. Artif. Intell.*, vol. 87, Jan. 2020, Art. no. 103281.

[5] X. Ji, X. Zhou, C. Yan, J. Deng, and W. Xu, "A nonlinearity-based secure face-to-face device authentication for mobile devices," *IEEE Trans. Mobile Comput.*, early access, Sep. 18, 2020, doi: 10.1109/TMC.2020.3025023.

[6] W. Xi *et al.*, "Instant and robust authentication and key agreement among mobile devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 616–627.

[7] 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.

[8] J. Huang *et al.*, "Towards anti-interference WiFi-based activity recognition system using interference-independent phase component," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM )*, 2020, pp. 576–585.

[9] 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.

[10] 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.

[11] 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.

[12] "Respiratory System: Facts, Function and Diseases." [Online]. Available: https://www.livescience.com/22616-respiratory-system.html (Accessed: Jul. 16, 2021).

[13] D. Zhang, Y. Hu, Y. Chen, and B. Zeng, "Breathtrack: Tracking indoor human breath status via commodity WiFi," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3899–3911, Apr. 2019.

[14] J. Liu, Y. Chen, Y. Wang, X. Chen, J. Cheng, and J. Yang, "Monitoring vital signs and postures during sleep using WiFi signals," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2071–2084, Jun. 2018.

[15] C. Wang, S. Chen, Y. Yang, F. Hu, F. Liu, and J. Wu, "Literature review on wireless sensing-Wi-Fi signal-based recognition of human activities," *Tsinghua Sci. Technol.*, vol. 23, no. 2, pp. 203–222, Apr. 2018.

[16] J. Mead and J. L. Whittenberger, "Physical properties of human lungs measured during spontaneous respiration," *J. Appl. Physiol.*, vol. 5, no. 12, pp. 779–796, 1953.

[17] B. Han, H. Hirahara, and S. Yoshizaki, "Streaming caused by oscillatory flow in peripheral airways of human lung," *Open J. Fluid Dyn.*, vol. 6, no. 3, pp. 242–261, 2016.

[18] P. J. Fadel, S. M. Barman, S. W. Phillips, and G. L. Gebber, "Fractal fluctuations in human respiration," *J. Appl. Physiol.*, vol. 97, no. 6, pp. 2056–2064, 2004.

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

[20] M. Schulz, J. Link, F. Gringoli, and M. Hollick, "Shadow Wi-Fi: Teaching smartphones to transmit raw signals and to extract channel state information to implement practical covert channels over Wi-Fi," in *Proc. 16th Annu. Int. Conf. Mobile Syst. Appl. Services*, 2018, pp. 256–268.

[21] A. I. McLeod, "Kendall rank correlation and mann-kendall trend test," *R Package Kendall*, Western University, London, ON, Canada, Dec. 2005. [Online]. Available: http://www.stats.uwo.ca/faculty/aim

[22] X. Liu, J. Cao, S. Tang, J. Wen, and P. Guo, "Contactless respiration monitoring via WiFi signals," *IEEE Trans. Mobile Comput.*, vol. 15, no. 10, pp. 2466–2479, Oct. 2016.

[23] R. Jagsi, J. M. Moran, M. L. Kessler, R. B. Marsh, J. M. Balter, and L. J. Pierce, "Respiratory motion of the heart and positional reproducibility under active breathing control," *Int. J. Rad. Oncol. Biol. Phys.*, vol. 68, no. 1, pp. 253–258, 2007.

[24] Z. Luo, W. Wang, J. Qu, T. Jiang, and Q. Zhang, "ShieldScatter: Improving IoT security with backscatter assistance," in *Proc. 16th ACM Conf. Embedded Netw. Sensor Syst.*, 2018, pp. 185–198.

[25] F. Viani, A. Polo, E. Giarola, M. Salucci, and A. Massa, "Principal component analysis of CSI for the robust wireless detection of passive targets," in *Proc. Int. Appl. Comput. Electromagn. Soc. Symp. Italy (ACES)*, 2017, pp. 1–2.

[26] X. Liu, J. Cao, S. Tang, and J. Wen, "Wi-sleep: Contactless sleep monitoring via WiFi signals," in *Proc. Real Time Syst. Symp. (RTSS)*, 2014, pp. 346–355.

[27] J. Liu, Y. Wang, Y. Chen, J. Yang, X. Chen, and J. Cheng, "Tracking vital signs during sleep leveraging off-the-shelf WiFi," in *Proc. 16th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2015, pp. 267–276.

[28] J. Liu, Y. Chen, Y. Dong, Y. Wang, T. Zhao, and Y.-D. Yao, "Continuous user verification via respiratory biometrics," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, 2020, pp. 1–10.

[29] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *J. Med. Syst.*, vol. 39, no. 10, p. 115, 2015.

[30] P. Huang, B. Li, L. Guo, Z. Jin, and Y. Chen, "A robust and reusable ECG-based authentication and data encryption scheme for ehealth systems," in *Proc. Global Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[31] A. R. Singandhupe, "Securing a UAV using features from an EEG signal," Ph.D. dissertation, Comput. Sci. Eng. Dept., Univ. Nevada, Reno, Nevada, 2017.

[32] N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "Highly reliable key generation from electrocardiogram (ECG)," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 6, pp. 1400–1411, Jun. 2017.

[33] S. Vhaduri and C. Poellabauer, "Multi-modal biometric-based implicit authentication of wearable device users," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3116–3125, Dec. 2019.

[34] D. Ekiz, Y. S. Can, Y. C. Dardağan, and C. Ersoy, "Is your smartband smart enough to know who you are: Towards continuous physiological authentication in the wild," 2019, *arXiv:1912.04760*.

[35] Y. Wu, Y. Sun, L. Zhan, and Y. Ji, "Low mismatch key agreement based on wavelet-transform trend and fuzzy vault in body area network," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 6, 2013, Art. no. 912873.

[36] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.

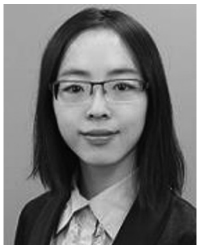
[37] W. Xi *et al.*, "Keep: Fast secret key extraction protocol for D2D communication," in *Proc. IEEE 22nd Int. Symp. Qual. Service (IWQoS)*, 2014, pp. 350–359.

[38] J. K. Flanagan and S. C. Cook, "Systems and methods for establishing secure communication using close proximity wireless communication," U.S. Patent 9 088 864, Jul. 21, 2015.

[39] S. Yu, X. Zhang, P. Huang, and L. Guo, "Secure authentication in cross-technology communication for heterogeneous IoT," in *Proc. IEEE Int. Symp. Dyn. Spectrum Access Netw. (DySPAN)*, 2019, pp. 1–2.

[40] F. Wang, F. Zhang, C. Wu, B. Wang, and K. J. R. Liu, "Respiration tracking for people counting and recognition," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5233–5245, Jun. 2020.

[41] S. M. M. Islam, O. Borić-Lubecke, Y. Zheng, and V. M. Lubecke, "Radar-based non-contact continuous identity authentication," *Remote Sens.*, vol. 12, no. 14, p. 2279, 2020.



**Pei Huang** (Student Member, IEEE) received the B.Sc. degree from Xidian University, Xi'an, China, in 2015, and the M.Sc. degree from the State University of New York, Binghamton, NY, USA, in 2017. She is currently pursuing the doctoral degree in computer engineering with Clemson University, Clemson, SC, USA.

Her research interests cover the 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 recently.

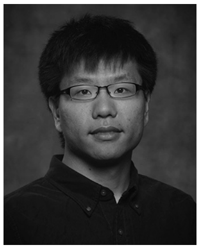
**Xiaonan Zhang** received the M.S. degree in electrical and computer engineering from Binghamton University, State University of New York, Vestal, NY, USA, in 2017, and the Ph.D. degree in computer engineering from Clemson University, Clemson, SC, USA, in 2020.

She is currently an Assistant Professor with the Department of Computer Sciencem, Florida State University, Tallahassee, FL, USA. Her research spans over general areas of wireless communication and networking, Internet of Things, and wireless security with an emphasis on interference mitigation, resource allocation, and physical-layer security in a heterogeneous wireless environment.

Dr. Zhang is a member of the ACM.

**Sihan Yu** (Student Member, IEEE) received the B.E. degree in computer science and technology from Liaoning University, Liaoning, China, in 2013, the M.E. degree in control engineering from the University of Chinese Academy of Sciences, Beijing, China, in 2016, and the M.S. degree in computer engineering from Virginia Tech, Blacksburg, VA, USA, in 2018. He is currently pursuing the Ph.D. degree with Clemson University, Clemson, SC, USA.

His research interests include cross-technology communication, physical layer security in wireless network, and Internet of Things.



**Linke Guo** (Senior Member, IEEE) received the B.E. degree in electronic information science and technology from Beijing University of Posts and Telecommunications, Beijing, China, in 2008, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Florida, Gainesville, FL, USA, 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, Binghamton, NY, USA. Since August 2019, he has been an Assistant Professor with the Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, USA. His research interests include wireless network, IoT, security, and privacy.

Dr. Guo is the co-recipient of Best Paper Award of Globecom 2015 and Symposium on Communication and Information System Security. He is currently serving as an Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He also serves as the Poster/Demo Chair of IEEE INFOCOM from 2020 to 2021. He was the publication chair of IEEE Conference on Communications and Network Security from 2016 to 2017. He was the symposium co-chair of Network Algorithms and Performance Evaluation Symposium, and ICNC 2016. He has served as the Technical Program Committee members for several conferences, including IEEE INFOCOM, ICC, GLOBECOM, and WCNC. He is a member of ACM.

**Ming Li** (Member, IEEE) received the B.E. degree in electrical engineering from Sun Yat-sen University, Guangzhou, China, in 2007, the M.E. degree in electrical engineering from Beijing University of Posts and Communications, Beijing, China, in 2010, and the Ph.D. degree in electrical and computer engineering from Mississippi State University, Starkville, MS, USA, in 2014.

She is currently an Associate Professor with the Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX, USA. Her research interests include mobile computing, Internet of Things, security, and privacy-preserving computing.

Dr. Li work won the Best Paper Awards in Globecom 2015 and DASC 2017. She has been serving as an Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. She received the NSF CAREER Award in 2020 and the ACM.