This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

PhyFinAtt: An Undetectable Attack Framework Against PHY Layer Fingerprint-based WiFi Authentication

Jinyang Huang, Bin Liu, Chenglin Miao, Xiang Zhang, Jiancun Liu, Lu Su, Zhi Liu, and Yu Gu

Abstract—WiFi connection has been suffering from MAC forgery attacks due to the loose authentication mechanism between access points (APs) and clients. To address this problem, the physical (PHY) layer information-based fingerprint has been adopted for safe WiFi authentication. Since such a fingerprint is constant and unique for each specific network interface card (NIC), it can effectively prevent MAC forgery attacks. However, the PHY layer information-based fingerprint is still vulnerable to malicious attacks as it is extracted from Channel State Information (CSI), and its stability can be affected by the wireless environment. In this paper, we propose a novel undetectable attack framework, called PhyFinAtt, base on which the attacker can undermine the stability of the PHY layer-based authentication fingerprints through human movement and further attack the WiFi authentication protocols. Specifically, we first demonstrate that human movement at a designated location can affect the PHY fingerprint. We then illustrate the impact of human movement on the PHY fingerprint and the relationship between the movement and the channel quality to ensure that the PHY fingerprint is destroyed by the movement in an undetected way without affecting normal communication. Extensive experiments in real-world scenarios show that our proposed attack can effectively disrupt the stability of the PHY fingerprints and significantly degrade the performance of the authentication protocols based on such fingerprints. To the best of our knowledge, this is the first study on effective attacks against the PHY information-based WiFi authentication protocols. Furthermore, we also present a practical defense mechanism without involving any additional equipment to mitigate attacks similar to PhyFinAtt.

Index Terms—WiFi connection, MAC forgery attack, authentication based on PHY information, fingerprint attack.

1 Introduction

1.1 Backgrounds and Motivations

As a pervasive communication medium, WiFi has been widely adopted to support various equipment connections in Wireless Local Area Networks (WLAN) and the Internet of Things (IoT). However, with the number of devices connected by WiFi reaching billion, many security issues have been discovered with WiFi connections [1], [2]. Among these issues, rogue access points (APs), rogue clients, and WiFi freeloading are the most prevalent ones, which have brought serious security threats. Taking the rogue AP attack as an example, the rogue AP copies the same service set identifier (SSID), IP address, and MAC address as that of the legitimate AP. Once user clients are fooled into connecting this rogue AP, the man-in-the-middle attack could be launched by the hacker, and all WLAN communication can be eavesdropped.

To address the above security issues, many WiFi authentication protocols have been developed. However, traditional authentication protocols, such as WPA, WPA2, and WEP, are vulnerable to MAC forgery attacks [3], [4] because their authentication information is on or above the MAC layer, and all this information can be forged. Recently, authentication using physical (PHY) layer information has drawn significant attention [5]–[11]. These algorithms propose to extract unique fingerprints from the PHY layer information, which relates to hardware to authenticate WiFi devices. Since the extracted unforgeable fingerprint is unique for every device, by establishing a legal device fingerprint library and using this hardware fingerprint for authentication, whether the connected device is a legal device can be correctly judged. Thus, these PHY information-based authentication protocols can reject illegal device access and resist MAC forgery attacks. The state-of-the-art PHY fingerprint-based protocols [5], [6] can achieve high detection ratios of more than 95% for MAC forgery attacks through fingerprint matching.

Although the PHY fingerprints used in existing works can help improve the security of WiFi connections, they are extracted from WiFi signals, and their stability is inevitably affected by the wireless environment. If an attacker deliberately attacks the wireless environment, the extracted fingerprint of a legal device may be changed, which is fatal to the PHY information-based WiFi authentication protocols.

- *Jinyang Huang, and Yu Gu are with the Anhui Province Key Laboratory of Affective Computing and Advanced Intelligence Machine and School of Computer and Information, Hefei University of Technology, Hefei, 230601, China.*
- *Jinyang Huang, Bin Liu, and Xiang Zhang, are with CAS Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei, 230026, China.*
- *Chenglin Miao, Department of Computer Science, Iowa State University, Iowa, 50011, America.*
- *Jianchun Liu, School of Computer Science and Technology, University of Science and Technology of China, Hefei, 230026, China.*
- *Lu Su, School of Electrical and Computer Engineering, Purdue University, Indiana, 47907, America.*
- *Zhi Liu, Department of Computer and Network Engineering, The University of Electro-Communications, Tokyo, 1828585, Japan.*
- *Corresponding author: Bin Liu (Email: flowice@ustc.edu.cn), and Xiang Zhang (Email: zhangxiang@ieee.org).*

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

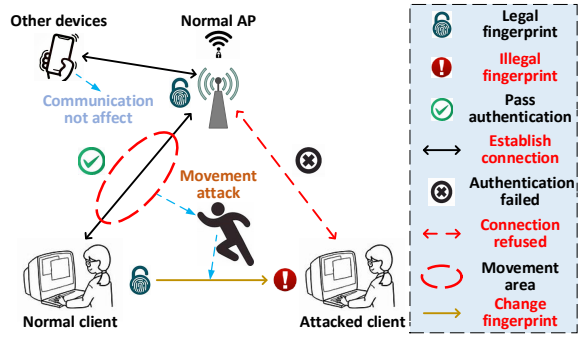


Fig. 1 An attack example based on the PhyFinAtt framework.

Despite the serious security threats, there is no existing work studying the attacks against the PHY information-based WiFi authentication protocols.

To fill the gap, in this paper, we propose a novel undetectable attack framework, called PhyFinAtt, base on which the attacker can effectively degrade the performance of the PHY information-based WiFi authentication protocols by interfering with the wireless environment using human movements. As shown in Fig. 1, before the attack, the normal client passes the fingerprint authentication of the AP and successfully accesses the WLAN. However, by using the designed human movements to affect the wireless environment and further affect the fingerprint extraction process, PhyFinAtt changes the extracted PHY fingerprint of the normal client and makes it unable to match that in the legal fingerprint library, which finally leads to the unsuccessful authentication. It is worth noting that the proposed attack is undetectable, and it does not require access to the client or the AP. Furthermore, the attack process is targeted, and it does not affect the normal communication of other devices.

1.2 Challenges and Contributions

To effectively attack the PHY information-based WiFi authentication protocols, the attacker should be able to destroy the extracted PHY fingerprint, which is usually stable for various environmental factors. Besides, the attack process should be unobtrusive and undetected, which means that normal communication should not be affected so that the authentication system cannot detect the attack behavior. In summary, we need to address two major challenges in order to perform effective attacks against the PHY information-based WiFi authentication protocols.

- **Stable PHY fingerprint:** Since the PHY fingerprint is determined by the hardware design, it is stable for various environmental factors, e.g., sampling time, temperature, and locations. Therefore, it is challenging to effectively attack and destroy the stability of the fingerprint during its extraction process.
- **Variable wireless environment:** Devices need good channel quality for regular communication, but the human movement in our proposed attack obviously downgrades the channel quality. Once the communication is affected, the attack can be easily detected. Thus, another challenge is to balance the tradeoff between the attack performance and the negative impact of attacks on the channel quality.

To address the above challenges, we first analyze the effect of human movement on PHY fingerprints and the relationship between the movements and channel quality. Then, a feedback mechanism is built to balance the effect of the movement attack on PHY fingerprints and the impact of movements on channel quality. Through human movements in the Fresnel Zone, the attacker can significantly change the PHY fingerprint of the attacked device without affecting communication much. Extensive experiments in real-world scenarios demonstrate the effectiveness of our proposed attack framework (i.e., PhyFinAtt). In addition, we also propose an effective defense mechanism to mitigate attacks similar to PhyFinAtt.

In summary, we make the following contributions:

- To the best of our knowledge, this is the first study on effective attacks against the PHY information-based WiFi authentication protocols.
- In our proposed attack framework, we establish a feedback mechanism to maximize the PHY fingerprint changes without affecting normal communication, which does not need additional hardware.
- To deal with fingerprint attacks similar to PhyFinAtt, we present an effective and practical defense mechanism based on the Channel State Information (CSI) fluctuation threshold without any additional equipment or system modifications.
- Extensive experiments with different types of devices are performed in various real-world scenarios. The experiment results show that under the PhyFinAtt attack, the stability of the PHY fingerprint is obviously undermined, and the authentication accuracy of the PHY information-based WiFi protocols drops significantly.

2 Related Work

The drawbacks of the existing authentication protocols in 802.11 WLAN have raised lots of security issues, e.g., rogue APs, rogue clients, and freeloading. For rogue APs and clients, by copying the SSID, IP address, and MAC address of legal devices, these rogue devices can easily access the WLAN and steal information from other devices connected to the same WLAN. The freeloading AP means that the attacking AP does not set a password, and all clients can access this AP without authentication. However, the information of the accessed clients could be risky and stolen. To fill such security loopholes, lots of pioneer PHY fingerprint-based methods [5]–[9], [12] have been proposed. Different from cryptographic solutions, fingerprint-based methods employ the hardware-related information derived from the PHY layer to generate a unique fingerprint for each device. This fingerprint is unique and constant for each device but distinct for different devices. Furthermore, this fingerprint is unforgeable due to its physical properties. Thus, this fingerprint can be used to distinguish different devices and determine whether the device trying to access the WLAN is legal equipment, which effectively prevents MAC forgery attacks.

Due to the advantages of preventing MAC forgery attacks, the PHY fingerprint-based authentication systems have received increasing attention from both academia and industry [5]–[9], [12], [13]. Some PHY fingerprints have already been applied in real-world systems [14]. G. Reus-Muns. et al. [15] proposed an additional physical layer authentication method that detects a specific emitter through RF fingerprinting. Moreover, the feasibility of this method is demonstrated based on stations over the large-scale over-the-air experimental POWDER platform in Salt Lake City, Utah. By analyzing a dataset of 400 GB signal data transmitted by 10000 radios, T. Jian. et al. [16] proposed a deep learning (DL)-based RF fingerprinting algorithm that can classify more than 1000 real devices. A DL-based RF fingerprinting system ORACLE was proposed in [17] to classify potential thousands of radios. By intentionally inserting and learning the effect of controlled impairments at the transmitter side, ORACLE can be effectively resilient to spoofing attacks in the real world.

According to the feature type used as the fingerprint, existing fingerprint-based WiFi authentication methods can be broadly classified into two categories: network traffic-based and hardware design-based.

Network Traffic-based: The work in [18] employed the data rate information derived from the header of the PHY frame as the fingerprint feature to classify the type of different network interface cards (NICs). Similarly, the inter-arrival time was used by the work [19] as the fingerprint to distinguish different AP types. As an improved method from the above two papers, the work in [20] used multiple wireless parameters, i.e., inter-arrival time, transmission rate, and frame size, to fingerprint target devices. However, since these features are all related to the network traffic, they may be changed due to the variation of the transmission content. Moreover, these network traffic-based methods need to collect a large amount of data, thus taking a long time and having high computation costs. Oppositely, since radiometric features are highly related to the device itself, it is a better way to use radiometric features as fingerprints.

Hardware Design-based: A set of radiometric features were extracted by PARADIS [21] as the device signatures, including phase error, I/Q imbalance, and carrier phase offset (CFO), to recognize different types of NICs. However, this work needs to attach multiple additional sensors co-located with the AP, which makes it inconvenient to deploy on existing equipment. Motivated by this work, the work in [5] inferred the device CFOs from WiFi CSI as their hardware fingerprints without any special hardware required to identify whether the device is legal equipment. However, this CFO-based fingerprint needs a long time to become stable, and multiple AP interference downgrades its performance. Recently, the most stable PHY fingerprint, which remains stable with respect to time, locations, and dynamic environments, was proposed in [6]. Specifically, the nonlinear phase errors (NLPEs) of different subcarriers were extracted by [6] as the device fingerprint after eliminating all linear phase errors (LPEs) since NLPEs are attributed to the oscillator drift and I/Q imbalance, which are the fundamental physical properties that cannot be manipulated and remain fairly consistent over time but vary significantly across devices.

Adversarial Attack and Jamming Attack: Some pioneer methods propose to destroy the fingerprint by adversarial samples or signal interferences [22], [23]. Specifically, Liu, Q. et al. [22] proposed a practical method to craft a white-box adversarial attack on the DL-based CSI feedback process. The attack object of this work is the DL-based CSI feedback process, and the structural information of the network must be known when the attack is launched due to the white-box. By injecting malicious packets, Sarita S. et al. [23] presented a game-theoretic study on the security problem of CFO-based continuous physical layer authentication in wireless networks and proposed adversarial attacks on CFO-based continuous physical layer authentication. Besides, by generating multiple kinds of adversarial examples by the vanilla model for training and leveraging the consistency loss for augmentation, Yang, J. et al. [24] proposed SecureSense to defend against adversarial attacks for secure device-free human activity recognition (HAR). Although these methods propose attacks or defenses against WiFi, these methods need to know the network structure in advance or have significant impacts on the normal communication of devices.

For all these authentication protocols, including network traffic-based methods and hardware design-based methods, their fingerprint features are all related to the distribution of electromagnetic fields since the electromagnetic field distribution information is used as an intermediate medium to extract these features. If the corresponding electromagnetic distribution is targeted to attack, the stability of the fingerprint will be affected. There is no existing work that has successfully attacked these WiFi authentication protocols based on PHY information without affecting the normal communication of other devices. Furthermore, there is no existing work studying the practical defense scheme against such attacks. Inspired by this requirement and to fill the research gap, we propose a novel undetectable device PHY fingerprint attack framework PhyFinAtt and present an effective defense mechanism accordingly to deal with the fingerprint attacks similar to PhyFinAtt without any additional equipment. The proposed defense mechanism is beneficial to the application of the PHY fingerprint-based authentication protocols for better maintaining the stability of the PHY fingerprints under malicious attacks.

3 Preliminaries And Observations

3.1 Overview of Channel State Information

Since CSI incorporates the hardware-related information and the channel characteristics encountered by the received signals (e.g., multipath effect, power decay, and scattering effect), most PHY information-based authentication protocols employ CSI as an intermediary to extract device-related fingerprints [5], [6], [21]. Using CSI, which can provide fine-grained PHY layer information and characterize the Channel Frequency Response (CFR) of the wireless channel, NICs can continuously capture fluctuations in channels [25].

In WiFi systems, the channel between each transmitter-receiver (Tx-Rx) antenna pair can be divided into multiple

subcarriers according to the *Orthogonal Frequency Division Multiplexing* (OFDM) technology [26]. Let $\boldsymbol{X}_i$ and $\boldsymbol{Y}_i$ be the frequency domain expressions of the transmitted and the received signals of the i^{th} Tx-Rx pair, respectively. Then, the relationship between these two signals can be represented using the following equation:

$$\boldsymbol{Y}_i = \boldsymbol{H}_i \boldsymbol{X}_i + \boldsymbol{N}_i, \tag{1}$$

where $\boldsymbol{H}_i$ is the complex-valued CFR of the i^{th} Tx-Rx pair, which can be measured by transmitting a known preamble of OFDM symbols between the transmitter and the receiver [26], and $\boldsymbol{N}_i$ denotes the additive white Gaussian noise.

According to the IEEE 802.11n standard [27], each channel in the 2.4GHz band has 56 subcarriers. Thus, the estimated value of $\boldsymbol{H}_i$ for the 56 subcarriers can be expressed as:

$$\boldsymbol{H}_i = [\boldsymbol{h}_i{}^{(1)}, \boldsymbol{h}_i{}^{(2)}, \cdots, \boldsymbol{h}_i{}^{(k)}, \cdots \boldsymbol{h}_i{}^{(56)}], \tag{2}$$

where $\boldsymbol{h}_i{}^{(k)}$ is complex-valued CFR of the k^{th} subcarrier in the i^{th} Tx-Rx pair. CSI measurements contain these CFR values, and $\boldsymbol{h}_i{}^{(k)}$ can be represented as:

$$\boldsymbol{h}_i{}^{(k)} = \left|\boldsymbol{h}_i{}^{(k)}\right| \cdot e^{-j \cdot \angle \boldsymbol{h}_i{}^{(k)}} = I_i{}^{(k)} + jQ_i{}^{(k)}, \quad k \in \boldsymbol{K} \tag{3}$$

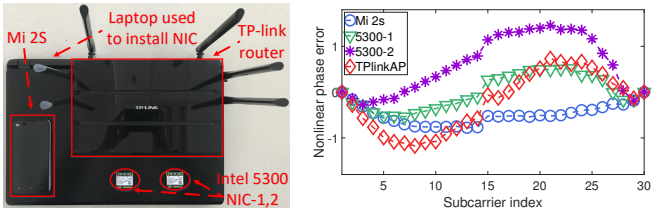
where $\left|\boldsymbol{h}_i{}^{(k)}\right|$ and $\angle \boldsymbol{h}_i{}^{(k)}$ denote the amplitude and the phase of the k^{th} subcarrier in the i^{th} Tx-Rx pair, respectively. Besides, the raw CFRs estimated in NICs can also be recorded as the I/Q signal. I and Q are the in-phase component and the quadrature component, respectively. $\boldsymbol{K}$ is the set of subcarrier indexes. The $\boldsymbol{\phi}$ is a vector and represents the measured phases of all subcarriers in one received packet, which can be calculated as:

$$\boldsymbol{\phi} = \arctan(\frac{Q}{I}). \tag{4}$$

3.2 Device-based Fingerprint

All fingerprint-based WiFi authentication protocols are related to electromagnetic field distribution. Network traffic-based methods transmit various kinds of content information from which fingerprints can be extracted, and the transmitted information is stored in the baseband signal. For hardware design-based methods, they use radiometric information to extract specific features, and the radiometric information is highly related to the carrier signal. Since the baseband signal and the carrier signal are modulated and then propagated by electromagnetic waves, these signals are inevitably affected by electromagnetic distribution. Owing to the fact that the attack target of PhyFinAtt is the electromagnetic distribution, PhyFinAtt is thus effective for all fingerprint-based WiFi authentication protocols.

In this paper, we first take the state-of-the-art NLPE feature-based authentication [6] as an example to illustrate our designed attacks since the NLPE feature is the most stable PHY fingerprint, which remains stable with respect to time, locations, and environments. Then, to evaluate the generalization ability of PhyFinAtt, we also test its performance on other PHY fingerprints used by the state-of-the-art authentication protocols in Sec. 6.3. Fig. 2 shows the NLPE features of four different devices, including two laptop NICs, an AP, and a cellphone. It is obvious that the NLPE features are different across devices and thus can be used as hardware fingerprints. The NLPE authentication



(a) Four different devices, including two NICs, an AP, and a cellphone.

(b) NLPE fingerprints of different devices.

Fig. 2 Four different devices and their NLPE fingerprints.

determines whether a device is legal or not by matching the collected fingerprint with the legal fingerprint library. If the similarity between the collected fingerprint and any fingerprint in the legal fingerprint library is greater than a threshold, the fingerprint owner is considered as a legal device, and the authentication succeeds. Otherwise, the authentication fails, and the device cannot access the WLAN.

Next, we discuss how to extract the NLPE PHY fingerprint. Owing to the imperfect hardware design and the variant signal transmission environment, the phases measured at the receiver are distinct from those at the transmitter. In particular, the phase difference between the transmitter and the receiver can be grouped into two categories, i.e., linear phase error (LPE) and NLPE [28]. LPE and NLPE represent that the phase errors change linearly or nonlinearly with respect to the subcarrier indexes, respectively.

According to [29], [30], for a particular pair signal of transmitter and receiver, the subcarrier phases $\boldsymbol{\phi}$ measured at the receiver can be formulated as:

$$\boldsymbol{\phi} = \boldsymbol{\varphi}_{re} + \boldsymbol{L}_{pbd} + \boldsymbol{L}_{sfo} + \boldsymbol{L}_{cfo} + \boldsymbol{L}_{tof} + \boldsymbol{N}_{to}, \tag{5}$$

where $\boldsymbol{\varphi}_{re}$ are the initial phases at the transmitter. $\boldsymbol{L}_{pbd}$, $\boldsymbol{L}_{sfo}$, $\boldsymbol{L}_{cfo}$, and $\boldsymbol{L}_{tof}$ express the phase offsets due to packet boundary detection (PBD), sampling frequency offset (SFO), CFO, and time of flight (ToF), respectively, and these phases are all LPEs [28]. According to [6], imperfect hardware design causes an NLPE, which means this NLPE is highly related to the hardware itself and is suitable to represent device information. Besides, by affecting multipath, human motion can also lead to an NLPE [28], [31]. Therefore, the last element $\boldsymbol{N}_{to}$ is the total NLPE and can be expressed as:

$$\boldsymbol{N}_{to} = \boldsymbol{N}_{ha} + \boldsymbol{N}_{mo}, \tag{6}$$

where $\boldsymbol{N}_{ha}$ and $\boldsymbol{N}_{mo}$ represent the NLPEs caused by imperfect hardware design and human motion, respectively. However, since it is difficult to eliminate the NLPE $\boldsymbol{N}_{mo}$ caused by human motion, the authentication protocol in [6] directly uses the total NLPE $\boldsymbol{N}_{to}$ as the fingerprint, which makes the authentication protocol vulnerable to malicious attacks. It is entirely possible for an attacker to use human motion to change a legitimate device's fingerprint (i.e., the NLPE $\boldsymbol{N}_{mo}$) and further attack the authentication process. In this paper, we study the possibility of performing such attacks.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

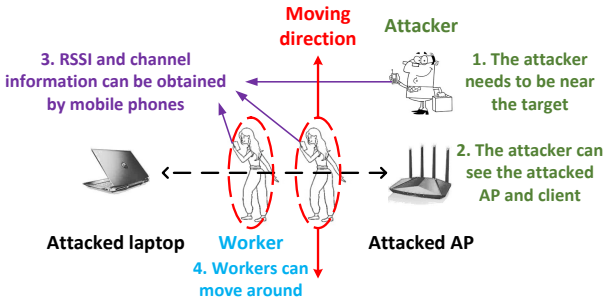


Fig. 3 Necessary capabilities for the attack and workers. The green, blue, and purple fonts represent the capabilities required for an attacker, workers, and both, respectively.

3.3 Effect of Motion on Fingerprint and Channel Quality

Effect of Motion on Fingerprint: Since $\boldsymbol{N}_{ha}$ is related to the imperfect hardware design of NIC and it is a constant for each specific NIC [6], the variation of NLPE fingerprint $\boldsymbol{N}_{to}$ equals that of $\boldsymbol{N}_{mo}$ caused by human motion. Specifically, by comparing $\boldsymbol{N}_{to}$ with $\boldsymbol{N}_{to}^{em}$ that is generated in a room without human motion, we can estimate the NLPE $\boldsymbol{N}_{mo}$ caused by human motion as:

$$\begin{aligned} \boldsymbol{N}_{to} - \boldsymbol{N}_{to}^{em} &= \boldsymbol{N}_{ha} + \boldsymbol{N}_{mo} - (\boldsymbol{N}_{ha} + \boldsymbol{N}_{mo}^{em}) \\ \boldsymbol{N}_{mo} &= \boldsymbol{N}_{to} - \boldsymbol{N}_{to}^{em}, \end{aligned} \tag{7}$$

where $\boldsymbol{N}_{to}^{em}$ and $\boldsymbol{N}_{mo}^{em}$ are the total variation of NLPE fingerprint and the NLPE generated by the motion when there is no human motion in the range, respectively. In particular, $\boldsymbol{N}_{mo}^{em}$ equals 0 [6]. Thus, $\boldsymbol{N}_{mo}$ can be estimated when the hardware design of NIC is fixed ($\boldsymbol{N}_{ha}$ is constant). Based on this fact, we can quantify the attack effect of the human motion on the NLPE fingerprint by determining the relationship between the motion intensity and the NLPE $\boldsymbol{N}_{mo}$.

By affecting the distribution of multipath and the length of each path, human movements ultimately affect the time-of-flight (ToF) of the signal. Moreover, the change of ToF can further affect the NLPE fingerprint. The reasons are described as follows. As shown in Eq. (5), the phase difference between the transmitter and the receiver is mainly caused by various phase errors. For all LPEs, only the phase error $\boldsymbol{L}_{tof}$ caused by the ToF changes significantly under the effect of human movements. However, the acquisition of the NLPE fingerprint needs to filter out the varying $\boldsymbol{L}_{tof}$. Thus, human movements can affect the NLPE fingerprint by changing the signal ToF.

Although static obstacles can change the multipath distribution, they cannot continuously change such distribution. Since the influence of constant multipath distribution changes is eliminated during the extraction of the NLPE fingerprint [6], the NLPE fingerprint cannot be changed by static obstacles. However, due to the constantly varying attitudes, human movements can continuously change the multipath distribution, which can further change the NLPE fingerprint. Thus, in this paper, instead of using static obstacles, we choose human movements as the attack medium.

Effect of Motion on Channel Quality: WiFi signals usually arrive at the receiver through multiple paths due to the effect of human bodies and other objects in the environment. If a wireless signal (the k^{th} subcarrier in the i^{th} Tx-Rx pair) arrives at the receiver through Υ different paths, the CFR $\boldsymbol{h}_i{}^{(k)}(\vartheta, t)$ can be calculated based on the following equation [29], [31]:

$$\boldsymbol{h}_i{}^{(k)}(\vartheta, t) = e^{-j\cdot 2\pi\Delta\vartheta t} \sum_{\wp=1}^{\Upsilon} \varpi_{\wp}(\vartheta, t) \cdot e^{-j\cdot 2\pi\vartheta\tau_{\wp}(t)}, \tag{8}$$

where j is the imaginary unit, ϑ represents the k^{th} subcarrier frequency, $\varpi_{\wp}(\vartheta, t)$ denotes the complex-valued representation of attenuation and initial phase offset of the $\wp^{th}$ path, and $e^{-j\cdot 2\pi\vartheta\tau_{\wp}(t)}$ denotes the phase shift on the $\wp^{th}$ path which has a propagation delay of $\tau_{\wp}(t)$. In addition, $e^{-j\cdot 2\pi\Delta\vartheta t}$ is the phase shift caused by the subcarrier frequency difference between the transmitter and the receiver.

Human posture can also affect channel quality. The changes in human posture during a movement can affect the size of the signal-blocking area and the length of the signal propagation paths, which can further lead to the variation of the attenuation coefficient $\varpi_{\wp}(\vartheta, t)$. According to Eq. (8), the variation of $\varpi_{\wp}(\vartheta, t)$ directly changes the absolute value of CFR $\boldsymbol{h}_i{}^{(k)}(\vartheta, t)$. Furthermore, since the absolute value of CFR has a positive relationship with the Received Signal Strength Indicator (RSSI) [26], the RSSI also fluctuates due to human motion. Therefore, the movement of human bodies obviously degrades the channel quality.

4 Attack Goal, Impact, and Threat Model

Attack Goal: The attack goal of PhyFinAtt is to make the attacked legal devices unable to access the WLAN. Through designed human movements at specific locations to affect the fingerprint extraction environment, PhyFinAtt destroys the PHY fingerprints of legal devices and further makes the attacked fingerprints unable to match the legal fingerprint library, which causes these legal devices to be unable to access the WLAN and finally results in the paralysis of the corresponding WLAN.

Attack Impact and Potential Implications: Apparently, in addition to affecting the PHY fingerprint, the movement of the human body at the specified location will also affect the communication quality in the environment. Therefore, the key impact of PhyFinAtt is to destroy the stability of PHY fingerprints and downgrade the communication quality in the environment. However, in order to ensure the stealth of the attack, the attack should be targeted and not be able to affect the normal communication of other devices. Therefore, how to set a reasonable attack intensity to balance the attack effect and the impact of the attack on the environment is a key research issue. Compared with the traditional jamming attacks [32], [33] that interfere with the communication of all devices, PhyFinAtt can make the attacked device unable to access the network without affecting the normal communication of other devices.

Threat Model: Fig. 3 shows the necessary capabilities for the attack and workers. The green, blue, and purple fonts represent the capabilities required for an attacker, workers, and both, respectively. To carry out the PhyFinAtt attack successfully, the attacker and workers need to have a total of four capabilities. We assume that the attacker can employ a few workers and let them walk around the

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

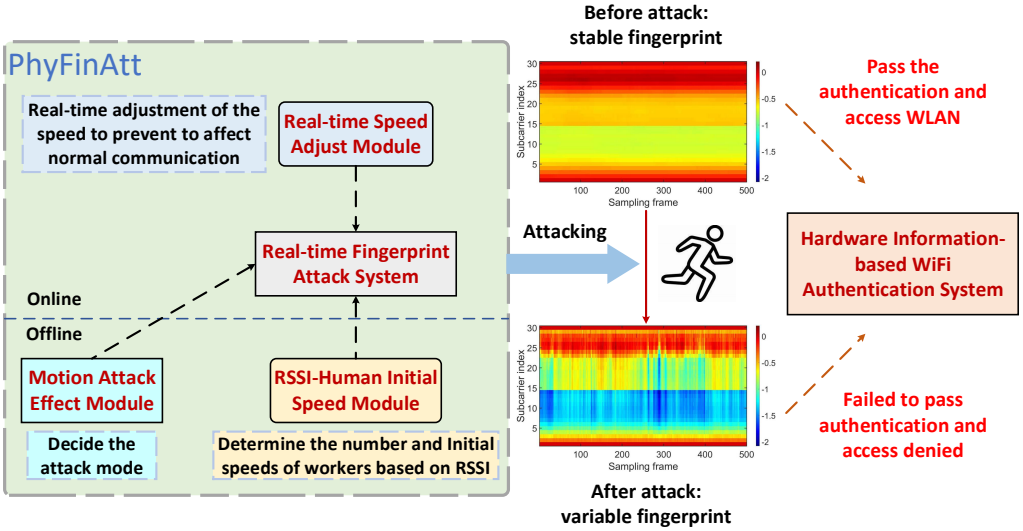


Fig. 4 PhyFinAtt framework.

room (**Capability 4**) where the attacked device is located. In addition, each worker has a smartphone that can be used to obtain real-time RSSIs and channel information about the attack targets (**Capability 3**). There are many smartphone Apps (e.g., *WiFi Analyzer*) that can help obtain such information in practice. Before the attack starts, to determine the initial attack intensity according to the real channel quality, the attacker needs to use a smartphone to measure the RSSI value within 50cm of the attacked device (**Capability 1, 3**). Then, during the attack, the employed workers walk back and forth in the area calculated by PhyFinAtt to influence the fingerprint extraction process. The determination of the attack area is based on the relative position of the transmitter and receiver, and the relative position can be roughly estimated by the attacker's visual inspection (**Capability 2**).

5 Attack Methodology

5.1 Overview

Fig. 4 shows our proposed PhyFinAtt framework, which contains four components, including two offline components (i.e., Motion Attack Effect Module and RSSI-Human Initial Speed Module) and two online components (i.e., Real-time Speed Adjust Module and Real-time Fingerprint Attack System). The Motion Attack Effect Module is used to determine the factors that can affect the NLPE fingerprint and decide the specific attack method. The purpose of the RSSI-Human Initial Speed Module is to determine an initial velocity for the workers' movement and the worker number according to the actual channel quality. The input of this module is the RSSI near the attacked AP ($< 50cm$), which is collected by the attacker's smartphone. The model output is the initial velocity and the number of workers. Then, to make the attack unobtrusive and keep RSSIs higher than the normal communication threshold during the attack process, the real-time worker speed adjustment is performed in the Real-time Speed Adjust Module. Finally, the Real-time Fingerprint Attack System is set to attack the extraction process of the PHY fingerprint and destroy the stability of this fingerprint. As shown in Fig. 4, after the attack, the original invariant NLPE fingerprint becomes unstable, which inevitably results in the failure of the WLAN access.

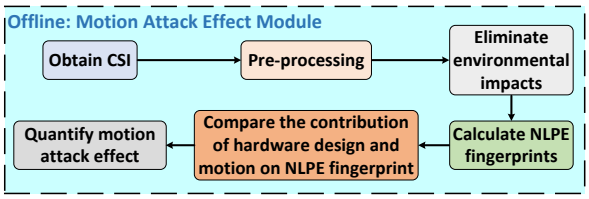


Fig. 5 Motion Attack Effect Module framework.

5.2 Motion Attack Effect Module

Fig. 5 shows the details of the Motion Attack Effect Module. In this module, we analyze the effect of human movement on the fingerprint and decide on the specific attack method. The attack effect measurement is also introduced in this part.

Obtain CSI and Pre-processing: The CSI phase is first extracted according to Eq. (4). Then, we unwrap the original phases to reconstruct the real phase relationship of all subcarriers. Finally, refer to [28], the frames with abnormal unwrapped phases are smoothed by the *moving average filtering* to obtain the stable NLPE fingerprint.

Eliminate Environmental Impacts: The phase errors of PBD ($\boldsymbol{L}_{pbd}$) and SFO ($\boldsymbol{L}_{sfo}$) in the same frame are all related to the subcarrier index set $\boldsymbol{K}$, which can be calculated as:

$$\boldsymbol{L}_{pbd} = 2\pi\alpha \cdot \boldsymbol{K}, \tag{9}$$

$$\boldsymbol{L}_{sfo} = 2\pi\beta \cdot \boldsymbol{K}, \tag{10}$$

where α and β are constants depending on PBD and SFO, respectively. Besides, the ToF offset $\boldsymbol{L}_{tof}$ is correlated to subcarrier frequencies:

$$\begin{aligned} \boldsymbol{L}_{tof} &= 2\pi t_f \boldsymbol{F} \\ &= 2\pi t_f (f_c \cdot \vec{\boldsymbol{q}} + f_b \boldsymbol{K}) \\ &= 2\pi t_f f_c \cdot \vec{\boldsymbol{q}} + 2\pi t_f f_b \boldsymbol{K} \\ &= \boldsymbol{Z} + 2\pi t_f f_b \boldsymbol{K}, \end{aligned} \tag{11}$$

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

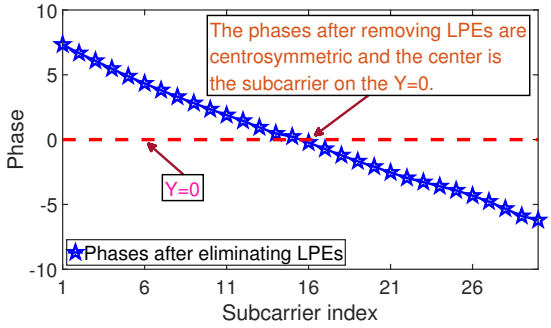


Fig. 6 The phases after eliminating environmental impacts.

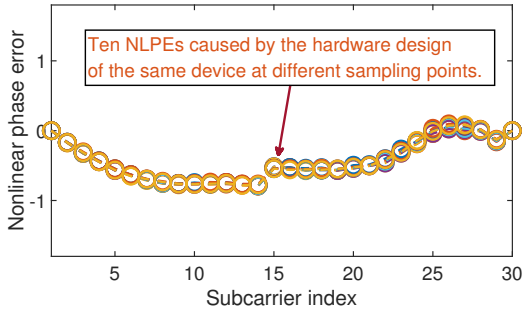


Fig. 7 The NLPEs caused by the hardware design for the same device at different sampling times.

where t_f is ToF, and it is affected by the device location. $\boldsymbol{F}$ is the subcarrier frequency set that is calculated based on the center subcarrier frequency f_c, the identity matrix $\vec{\boldsymbol{q}}$, the frequency difference between two adjacent subcarriers f_b (equals 312.5 kHz [27]), and the subcarrier index set $\boldsymbol{K}$, i.e., $\boldsymbol{F} = f_c \cdot \vec{\boldsymbol{q}} + f_b \boldsymbol{K}$. Since $2\pi t_f f_c \cdot \vec{\boldsymbol{q}}$ is independent of $\boldsymbol{K}$ and t_f is an invariant value in one received frame, we use $\boldsymbol{Z}$ to replace the first part.

Then, the phase estimated at the receiver is rewritten as:

$$\begin{aligned}\boldsymbol{\phi} &= \boldsymbol{\varphi}_{re} + \boldsymbol{L}_{pbd} + \boldsymbol{L}_{sfo} + \boldsymbol{L}_{cfo} + \boldsymbol{L}_{tof} + \boldsymbol{N}_{to} \\ &= \boldsymbol{\varphi}_{re} + 2\pi\alpha \cdot \boldsymbol{K} + 2\pi\beta \cdot \boldsymbol{K} + \boldsymbol{L}_{cfo} + \boldsymbol{Z} + 2\pi t_f f_b \boldsymbol{K} + \boldsymbol{N}_{to} \\ &= \boldsymbol{\varphi}_{re} + 2\pi(\alpha + \beta + t_f f_b)\boldsymbol{K} + \boldsymbol{L}_{cfo} + \boldsymbol{Z} + \boldsymbol{N}_{to} \\ &= \boldsymbol{\varphi}_{re} + 2\pi\lambda \cdot \boldsymbol{K} + \boldsymbol{L}_{cfo} + \boldsymbol{Z} + \boldsymbol{N}_{to} \\ &= 2\pi\lambda \cdot \boldsymbol{K} + (\boldsymbol{\varphi}_{re} + \boldsymbol{L}_{cfo} + \boldsymbol{Z}) + \boldsymbol{N}_{to} \\ &= 2\pi\lambda \cdot \boldsymbol{K} + \boldsymbol{C}^* + \boldsymbol{N}_{to},\end{aligned} \tag{12}$$

where λ is a constant for one specific frame, and it is the sum of α, β, and $t_f f_b$. Similarly, $\boldsymbol{L}_{cfo}$ and the real phase $\boldsymbol{\varphi}_{re}$ are also constants for each subcarrier in the same frame and can be measured by $\boldsymbol{\phi}$ [30]. Therefore, we use $\boldsymbol{C}^*$ to replace the sum of $\boldsymbol{\varphi}_{re}$, $\boldsymbol{L}_{cfo}$, and $\boldsymbol{Z}$.

Referring to [30], $\boldsymbol{C}^*$ can be estimated by the phases of a pair of mirror subcarriers measured at the receiver. Thus, we sum up the phases (ϕ_{-1} and ϕ_1) measured at the receiver of a pair of mirror subcarriers -1 and 1 as the following equation:

$$\begin{aligned}\phi_{-1} + \phi_1 &= 2\pi\lambda \cdot (-1 + 1) + 2 \cdot \boldsymbol{C}^* + N_{to,-1} + N_{to,1} \\ &= 2 \cdot \boldsymbol{C}^* + N_{to,-1} + N_{to,1},\end{aligned} \tag{13}$$

where $N_{to,-1}$ and $N_{to,1}$ represent the NLPEs of subcarrier -1 and subcarrier 1, respectively, and $N_{to,-1} + N_{to,1} \approx 0$ [6]. Accordingly, $\boldsymbol{C}^*$ can be calculated approximately as:

$$\boldsymbol{C}^* \approx \frac{\phi_{-1} + \phi_1}{2}. \tag{14}$$

Here, $\boldsymbol{C}^*$ is subtracted from the phases of all received frames for the elimination of environmental impacts. Fig. 6 shows the phases after eliminating the environmental impacts. We can observe that the processed phases across subcarriers are evenly distributed on both sides of $Y = 0$ and approximately centrosymmetric.

Calculate NLPE fingerprints: After removing LPEs, the total NLPE $\boldsymbol{N}_{to}$ (the NLPE fingerprint) caused by the imperfect hardware design and the human motion is expressed as:

$$\boldsymbol{N}_{to} \approx \boldsymbol{\phi}_E - 2\pi\lambda \cdot \boldsymbol{K}, \tag{15}$$

where $\boldsymbol{\phi}_E$ is the normalized phases after subtracting $\boldsymbol{C}^*$. Similar to [28], to obtain a relatively stable NLPE fingerprint $\boldsymbol{N}_{to}$ and to mitigate the location impact, we employ the deviation between the normalized phases $\boldsymbol{\phi}_E$ and the fitted line $\boldsymbol{L}$ to represent this steady NLPE fingerprint $\boldsymbol{N}_{to}^{st}$. Specifically, the fitted line $\boldsymbol{L}$ is generated by connecting two points, i.e., $(-28, \phi_{E,-28})$ and $(28, \phi_{E,28})$, which can be formulated as:

$$\boldsymbol{L} = \frac{\phi_{E,28} - \phi_{E,-28}}{56} \cdot \boldsymbol{K} + \frac{\phi_{E,-28} + \phi_{E,28}}{2}. \tag{16}$$

Therefore, the stable fingerprint $\boldsymbol{N}_{to}^{st}$ is obtained by:

$$\boldsymbol{N}_{to}^{st} = \boldsymbol{\phi}_E - \boldsymbol{L}. \tag{17}$$

Quantify Fingerprint Contribution and Attack Effect: Next, we compare the contribution of hardware design $\boldsymbol{N}_{ha}$ and human motion $\boldsymbol{N}_{mo}$ on the NLPE fingerprint to quantify the attack effect of human movement on the NLPE fingerprint. Since the NLPE caused by the imperfect hardware design $\boldsymbol{N}_{ha}$ is a constant for the specific network card [6], and $\boldsymbol{N}_{mo}^{em}$ equals 0 when there is no motion in the range [28], we thus calculate $\boldsymbol{N}_{ha}^{em}$ in an empty room without any human motion:

$$\begin{aligned}\boldsymbol{N}_{ha}^{em} + \boldsymbol{N}_{mo}^{em} &= \boldsymbol{\phi}_{E,em} - \boldsymbol{L}_{em}, \\ \boldsymbol{N}_{ha}^{em} &= \boldsymbol{\phi}_{E,em} - \boldsymbol{L}_{em},\end{aligned} \tag{18}$$

where $\boldsymbol{\phi}_{E,em}$ and $\boldsymbol{L}_{em}$ are the normalized phases and the fitted line in the empty room, respectively. Then, $\boldsymbol{N}_{ha}^{em}$ is obtained to represent the NLPE caused by the imperfect hardware design in all frames. Fig. 7 shows the NLPE $\boldsymbol{N}_{ha}^{em}$ of the same device at ten different sampling times. The multiple $\boldsymbol{N}_{ha}^{em}$ samples of the same device at different sampling times are basically coincident, which demonstrates that the NLPE caused by the hardware design is very stable.

Here, we subtract $\boldsymbol{N}_{ha}^{em}$ from the stable NLPE fingerprint $\boldsymbol{N}_{to}^{st}$ in each received frame to obtain the NLPE change caused by human motion. In this regard, the NLPE $\boldsymbol{N}_{mo}$ caused by human motion in each frame can be estimated as:

$$\begin{aligned}\boldsymbol{N}_{mo} &= \boldsymbol{N}_{to}^{st} - \boldsymbol{N}_{ha}^{em} \\ &= \boldsymbol{\phi}_E - \boldsymbol{L} - \boldsymbol{N}_{ha}^{em}.\end{aligned} \tag{19}$$

As shown in Eq. (19), since the greater NLPE $\boldsymbol{N}_{mo}$ caused by the motion, the bigger fingerprint difference after the motion attack, we estimate the attack effect by comparing the fingerprint difference before and after the attack. Specifically, the motion attack effect is quantified by calculating the correlation coefficient between the fingerprint after the attack $\boldsymbol{N}_{to}^{st}$ (obtained by Eq. (17)) and the original

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

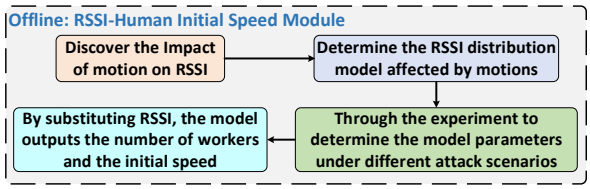


Fig. 8 RSSI-Human Initial Speed Module framework.

fingerprint $\boldsymbol{N}_{ha}^{em}$ (obtained by Eq. (18)) without human movement. PhyFinAtt employs *Pearson's method* to calculate fingerprint correlations. $P_{\boldsymbol{N}_{to}^{st},\boldsymbol{N}_{ha}^{em}}$ is used to denote the Pearson correlation coefficient between the attacked fingerprint $\boldsymbol{N}_{to}^{st}$ and the original fingerprint $\boldsymbol{N}_{ha}^{em}$, which can directly reflect the motion attack effect. In particular, the correlation coefficient $P_{\boldsymbol{N}_{to}^{st},\boldsymbol{N}_{ha}^{em}}$ is negatively related to the attack effect.

5.3 RSSI-Human Initial Speed Module

Fig. 8 shows the framework of the RSSI-Human Initial Speed Module. This module is used to choose the appropriate initial attack intensity (worker number and velocity) based on the channel quality so that the attack does not affect normal communication and cannot be detected.

Discover the Impact of Motion on RSSI: Generally, human movements can generate two impacts on RSSI, i.e., decreases in RSSI average values and fluctuations in time series. The occlusion of the human body makes RSSI attenuated, which finally results in a decrease in the average RSSI. Since the human body movement changes the number of indoor multipaths and the path length of signal propagation [30], RSSI is superimposed with the new path overlap relationship [28], which leads to fluctuations in RSSI.

Determine the RSSI Distribution Module: The impact of human body occlusion on RSSI can be expressed by the occlusion attenuation parameter ς [31]. In addition, FCC Frog eye [34] proves that the RSSI, under the influence of human motion, follows a normal distribution. Therefore, we model the fluctuation of RSSI affected by motions as:

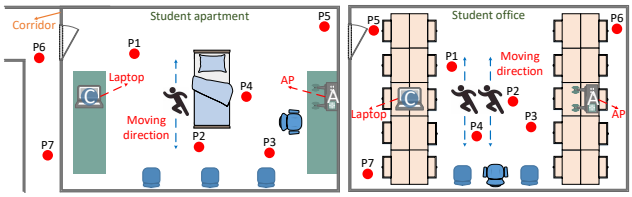
$$\ell = \varsigma \times \ell_{ini} + \boldsymbol{\mathcal{N}}\left(0, \nu^2\right), \tag{20}$$

$$R = \ell - B, \tag{21}$$

where ℓ_{ini} and ℓ denote the wave strength of a certain place without or with human movement, respectively. ς is an experimental-based parameter introduced to estimate the occlusion impact of the human body ($\varsigma \in [0, 1]$), and ν^2 represents the variance of the normal distribution $\mathcal{N}\left(0, \nu^2\right)$. B is the background noise determined by the environment and can be obtained by CSITOOL [26]. In particular, the range of B in most cases is around $90dBm$. Finally, the RSSI value R is obtained by subtracting the background noise B from ℓ.

The normal communication RSSI should be larger than $-77dBm$, which is the lowest value of the second grid signal strength of Android phones and is denoted as:

$$\begin{aligned} R &> -77, \\ \ell - B &> -77, \\ \varsigma \times \ell_{ini} + \boldsymbol{\mathcal{N}}\left(0, \nu^2\right) &> -77 + B. \end{aligned} \tag{22}$$



(a) Coefficient measurement in a student dormitory. **(b)** Coefficient measurement in a student office.

Fig. 9 Fluctuation coefficient measurement scenarios.

Since RSSI fluctuations follow a normal distribution, according to the *three-sigma rule*, the probability that RSSIs fluctuate from $\varsigma \times \ell_{ini} - B - 3 \times \nu$ to $\varsigma \times \ell_{ini} - B + 3 \times \nu$ is 0.9974. If the lowest RSSI in fluctuations meets the communication requirement, almost all RSSIs will meet this requirement. The fluctuation constraint can be rewritten as:

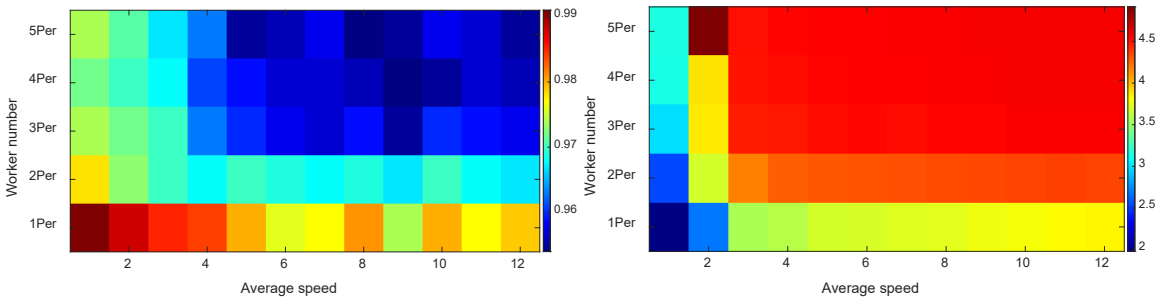
$$\begin{aligned} \varsigma \times \ell_{ini} - 3 \times \nu &> -77 + B, \\ 3 \times \nu &< \varsigma \times \ell_{ini} + 77 - B. \end{aligned} \tag{23}$$

Thus, the relationship between the fluctuation standard deviation ν and the initial wave strength ℓ_{ini} is obtained.

Determine the Model Parameters: As shown in Fig. 9, to calculate fluctuation parameters for constructing the relationship between movement speed and RSSI, we record the RSSI values before and after the human movement attack in two indoor scenarios, i.e., a student dormitory ($6.1 \times 4m^2$) and a student office ($16.3 \times 10.4m^2$). In the two scenarios, the locations P1-P4 are in line-of-sight (LOS) areas, and the locations P5-P7 are in non-line-of-sight (NLOS) areas. We record the RSSI values before and after the attack in locations P1-P7, respectively. The movement direction is perpendicular to the communication link. For each location, the occlusion attenuation parameter ς is calculated by the ratio of the average RSSI after the attack to the average RSSI before the attack. The standard deviation ν is obtained by calculating the standard deviation of the RSSI after the attack.

These attack scenarios contain different worker numbers and distinct movement speeds. To study the impact of various worker numbers and movement speeds on the attenuation coefficient ς and the fluctuation coefficient ν and to choose the appropriate attack intensity to perform attack, we set the number of workers from 1 to 5 (unobtrusive worker number range [35]), and the average movement speed is from 1 km/h to 12 km/h (normal movement speed range [36]) to calculate the corresponding coefficient values. Fig. 10 shows the heat map of the variation of the average attenuation coefficient ς and the fluctuation coefficient ν with different worker numbers and different movement speeds. Specifically, the abscissa represents different movement speeds, the ordinate represents the different worker numbers, and the depth of the color denotes the average coefficient value under the corresponding attack intensity. Fig. 10 (a) depicts the changes of the average attenuation coefficient ς with different worker numbers and different movement speeds in LOS areas. We can see that when the worker number is less than 3 and the average speed is less than 5, the occlusion effect is significantly enhanced with the increase of the worker number and the average speed.

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954



(a) Changes of the attenuation coefficient ς in LOS areas. **(b)** Changes of the fluctuation coefficient ν in NLOS areas.

Fig. 10 The impact of various worker numbers and movement speeds on the attenuation coefficient ς and the fluctuation coefficient ν.

TABLE 1 Model parameters in line-of-sight (LOS) areas. The first number and the second number are the number and speed of the workers, respectively, e.g., 3Per-3 means that there are 3 workers, and the speed of each worker is 3km/h.

Parameters	1Per-3	1Per-5	1Per-10	2Per-3	2Per-5	2Per-10	3Per-3	3Per-5	3Per-10
ς	0.97 to 1	0.96 to 1	0.96 to 1	0.95 to 0.99	0.94 to 1	0.95 to 0.99	0.95 to 0.99	0.93 to 0.99	0.93 to 0.99
ν	1.87 to 2.97	1.98 to 3.15	2.46 to 3.67	2.92 to 4.07	2.95 to 4.13	2.99 to 4.25	3.02 to 4.29	3.11 to 4.35	3.13 to 4.42

TABLE 2 Model parameters in non-line-of-sight (NLOS) areas.

Parameters	1Per-3	1Per-5	1Per-10	2Per-3	2Per-5	2Per-10	3Per-3	3Per-5	3Per-10
ς	0.89 to 0.97	0.89 to 0.96	0.88 to 0.96	0.86 to 0.95	0.86 to 0.94	0.87 to 0.95	0.85 to 0.95	0.85 to 0.93	0.84 to 0.93
ν	3.03 to 4.10	3.12 to 4.25	3.22 to 4.36	3.69 to 4.67	3.76 to 4.83	3.79 to 4.91	3.81 to 5.12	3.85 to 5.17	3.87 to 5.23

TABLE 3 The RSSI applicable scope of different initial attack intensities. The unit of RSSI is dBm.

Intensity	1Per-3	1Per-5	1Per-10	2Per-3	2Per-5	2Per-10	3Per-3	3Per-5	3Per-10
Scope	$[-61.57,\infty)$	$[-61.07,\infty)$	$[-60.36,\infty)$	$[-58.59,\infty)$	$[-58.13,\infty)$	$[-58.03,\infty)$	$[-56.64,\infty)$	$[-56.46,\infty)$	$[-55.85,\infty)$

However, the continued increase in the worker number and the average speed does not significantly affect the occlusion effect. This is reflected in the fact that when the work number increases to more than 3 and the average speed increases to more than 10 km/h, the attenuation effect does not increase significantly. A similar phenomenon can be found in the variation of the average fluctuation coefficient ν in NLOS areas shown in Fig. 10 (b). Therefore, we set the worker numbers to three grades from 1 to 3, and the moving speed to three grades of 3, 5, and 10km/h to perform an attack of appropriate intensity.

Since the RSSI attenuation coefficients ς in different scenarios are mostly between 0.8 and 1 [29], which are similar to the range of ς in the above two rooms, and the RSSI fluctuations ν caused by the same motion in different environments are also similar [31], the parameters calculated through these two rooms are representative and thus appropriate for other indoor environments.

Tab. 1 and Tab. 2 show the possible values of the occlusion attenuation coefficient ς and the fluctuation coefficient ν in LOS and NLOS areas, respectively. From these two tables, we observe that the larger worker number causes the smaller occlusion attenuation parameter ς, which means the occlusion effect becomes large as the worker number increases. Meanwhile, as the number of employed workers and their moving speed increase, the RSSI fluctuations become more intense, and their standard deviation ν increases accordingly. However, the growth rate of the standard deviation ν gradually decreases. Compared with LOS areas, the occlusion effect caused by the human body and the fluctuation differences of RSSI are more significant in NLOS areas.

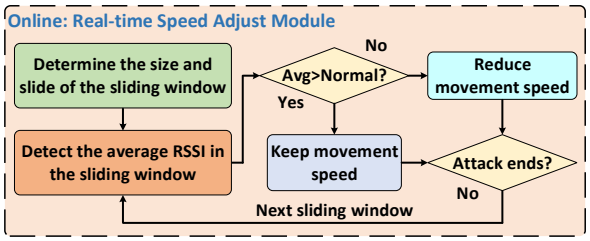


Fig. 11 Real-time Speed Adjust Module framework.

Therefore, in order not to affect the normal communication of all devices and make the attack undetected, we only need to ensure that the devices affected by motions in NLOS areas can meet the communication requirements. Such communication conditions are sufficient to meet the normal communication of all devices. Consequently, combining the parameter relationship in Eq. (23) and the possible parameter values under NLOS areas in Tab. 2, the applicable RSSI range for each attack intensity is given in Tab. 3. We observe that when each of the three workers moves at a speed of 10km/h, the attack intensity is the largest, and the RSSI (near the attacked AP, $< 50cm$) required by the environment is the highest, i.e., -55.85dBm.

Output the Initial Attack Intensity: By substituting the RSSI value of the Fresnel Zone near the attacked AP into Tab. 3, we can determine the initial attack intensity accordingly. Generally, the maximum allowed intensity is chosen as the initial attack intensity to perform the attack. In addition, since the human movement speed is approximately positively correlated with the RSSI fluctuation variance, the worker's speed is not limited to 3, 5, or 10km/h but can

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

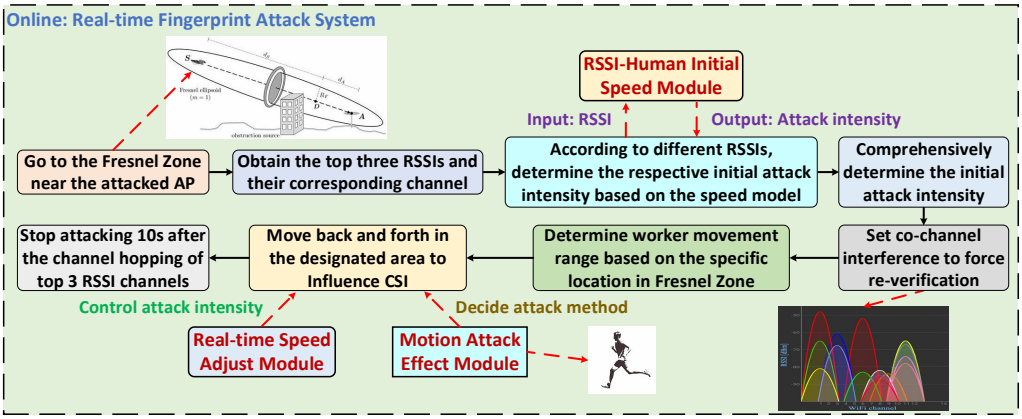


Fig. 12 Real-time Fingerprint Attack system framework.

be any value less than the maximum speed that meets the condition.

5.4 Real-time Speed Adjust Module

If the workers move too fast during the attack, normal communication may be affected. To address this issue, we design the Real-time Speed Adjust Module to timely monitor the channel quality and adjust the workers' movement speed. As shown in Fig. 11, an overlapped sliding window algorithm is first used in this module to detect the real-time RSSI in the environment. The size and step of the window are determined by the sampling rate S, the motion-related time factor t_{mov}, and the sliding constraint parameter ρ, which can be expressed as:

$$W_{si} = S \times t_{mov}, \tag{24}$$

$$W_{st} = \rho \times S \times t_{mov}, \tag{25}$$

where W_{si} and W_{st} denote the size and the step of the sliding window W, respectively. The sliding constraint parameter ρ is set to constrain the violent RSSI fluctuations caused by the instantaneous speed change to affect normal communication when the movement crosses two sliding windows. Based on empirical knowledge, t_{mov} is set to 0.5s, and ρ is set to 0.5. As shown in Fig. 11, in each sliding window during the attack, we calculate the average RSSI collected by the worker's smartphone. If the average RSSI in one window is greater than the normal threshold, the worker keeps the moving speed. Otherwise, the worker reduces the moving speed until the condition is met. Similar to the RSSI-Human Initial Speed Module setting, the normal communication threshold is set to $-77dBm$.

5.5 Real-time Fingerprint Attack System

Fig. 12 shows the attack system framework. Here, we introduce the movement range of the workers, the starting and ending conditions, and the specific execution process of the attack.

Go to Fresnel Zone and Obtain AP RSSI: The Fresnel Zone is the ellipsoidal area near LOS where the electromagnetic energy is most concentrated. Obstacles in the Fresnel Zone cause strong scattering of the transmitted electromagnetic waves. Therefore, the Fresnel Zone has the greatest influence on the signal, and we perform the movement attack in the Fresnel Zone. Specifically, we first go to the Fresnel Zone near the attacked AP ($< 50cm$) to measure its RSSI.

Then, we obtain the channel information of the attacked AP to determine the initial attack intensity. Since there are usually multiple APs in the same indoor environment, the RSSI value of the nearest AP (the attacked AP) is not necessarily the maximum value. Generally, the RSSI value of the nearest AP is in the top three among all indoor APs. Thus, to obtain the real attacked AP information, we collect the channel information corresponding to the top three RSSIs near the attacked AP ($< 50cm$ in the Fresnel Zone).

Comprehensively Determine Initial Attack Intensity: Since we do not know which of the top three RSSIs corresponds to the attacked AP RSSI, to ensure that the attack process does not affect normal communication, all channel constraints corresponding to the top three RSSIs should be met. According to the RSSI-Human Initial Speed Module, the lower RSSI in the model input corresponds to the weaker attack intensity in the model output. Therefore, we substitute the minimum of the three obtained RSSIs into this module, and the output attack intensity will be the lowest, and it will be used as the initial attack intensity.

It is worth noting that the average movement speed determined in the initial attack intensity is not constant, but employed workers need to roughly maintain this movement speed to perform the initial attack. Since all attacks end within one minute, workers can maintain an approximately constant movement speed by maintaining a relatively constant stride frequency and stride within one minute. Furthermore, the speed deviation between the set value and the actual value will not affect the attack result since the Real-time Speed Adjust Module timely calibrates the movement speeds of workers.

Set Co-channel Interference to Force Re-verification: The attack target of PhyFinAtt is the verification process of PHY information-based authentication protocols. As communication environment fluctuations cause channel hopping, which can further lead to devices entering the verification process, appropriate channel environment changes are necessary to cause the channel hopping of the attacked devices and re-verification. Since WiFi nodes automatically change the channel when their channel is severely inter-

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

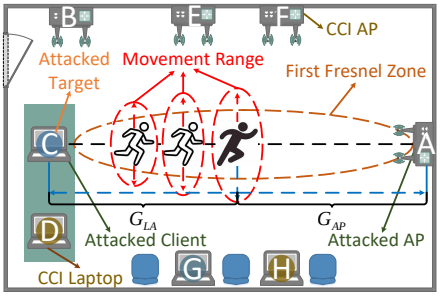


Fig. 13 The movement range of each worker.

fered with by co-channel interference (CCI) (CCI is caused by WiFi nodes with the overlapped frequency spectrum competing for channels [28]), and the channel hopping can cause reconnection and re-verification [37], we use CCI to force the attacked device to change channel and further enter verification process so that the attacks can be easily performed.

Specifically, we set the CCI according to the channel information of the obtained top three RSSIs. For each channel corresponding to the top three RSSIs, we use one interference AP with the overlapping channel and one interference client to generate CCI through large-scale data communication on the link formed by this interference AP and the client. To generate fast channel hopping for the attacked AP, the traffic rate of each interference link is set to 12MB/s based on practical experience.

Determine Attack Movement Range and Moving Method: Since moving in an area not exceeding 20% of the periphery of the first Fresnel Zone causes greater scattering of electromagnetic waves [38], to enhance the attack effect, the workers' movement range should be within this area. Specifically, as shown in Fig. 13, the first worker is at the center of the connection between the AP and the client. If environmental conditions permit, the second worker and the third worker are getting closer and closer to the attacked target in the Fresnel Zone. The movement range of each worker is related to its position in the Fresnel Zone, which can be expressed as:

$$U = \sqrt{\frac{\zeta G_{AP} G_{LA}}{G_{all}}}, \tag{26}$$

$$\mu = 2 \times 1.2 \times U, \tag{27}$$

where U is the radius of the first Fresnel Zone, and ζ represents the wavelength of the WiFi signal, which is about $13.4cm$ in the 2.4GHz band. G_{AP} and G_{LA} denote the distances between the moving subject and the attacked AP and the moving subject and the attacked client, respectively. G_{all} is the total distance between the AP and the client. μ expresses the length of the optimal worker movement range, which can exceed 20% of the first Fresnel radius. Fig. 13 shows that the workers' movements are perpendicular to the connection link between the AP and the client.

In particular, in the PhyFinAtt attack system, whether the attack method is a same path walk or a random path walk, as long as it satisfies the movement attack is performed near the first Fresnel Zone, it is valid. This is because different walk methods, i.e., a same path walk and a random path walk, have different path impacts, which may cause different electromagnetic interference on the PHY fingerprint. However, the key of the PhyFinAtt attack is not to change the PHY fingerprint into a fixed form but to make the stable PHY fingerprint unstable and reduce the similarity between the attacked fingerprint and the original fingerprint. Therefore, the fingerprint shape after being attacked is not the key point to attack. As long as the attacked fingerprint is not similar enough to the original fingerprint, the attack is considered successful.

Perform Attack and Stop Condition: The attack target of PhyFinAtt is the verification process of the PHY information-based authentication protocols rather than the normal communication process. Therefore, even if the first Fresnel Zones of different connection links overlap, the unrelated links of normal communication will not be affected by the PhyFinAtt attack. Only the target that is affected by the CCI and produces the channel hopping to enter the verification process will be attacked. Thus, observing the channel hopping of the attacked device is a sign of the attack's start.

After determining the workers' movement ranges, the attack is performed. During the attack process, the Real-time Speed Adjust Module monitors the workers' speeds from beginning to end to avoid affecting normal communication much. The adjustment of the movement speed is not determined by the state of the channel hopping but by the average RSSI in the environment. When the average RSSI in the environment is below the threshold, the movement speed will be reduced to mitigate the impact of motions on communication.

Each worker can observe the channel-hopping state of the attacked AP through the smartphone in his hand. Once the attacked device completes channel hopping, the re-verification process of the protocol will start, and different workers begin to perform the movement attack. Since the re-verification process usually completes within a few seconds and there is no reconnection chance when fingerprint re-verification fails, PhyFinAtt stops the fingerprint attack 10s after all channel re-verification processes start.

6 Experimental Evaluation

In this section, we evaluate the performance of the proposed PHY fingerprint attack framework (i.e., PhyFinAtt). Specifically, we first show the attack performance using two measures (*Pearson correlation coefficient* and *attack success ratio*). Then, we discuss the impacts of different factors on the attack effect.

6.1 Experimental Setting

Hardware Design: As shown in Fig. 14, in our experiments, we use a Thinkpad 420i laptop equipped with the Intel 5300 NIC and another Thinkpad 420i laptop equipped with the AX210 NIC as the fingerprint collectors to gather PHY information-based fingerprints of various testing devices, including APs, laptops, cellphones, and smartwatches.

Software Implementation: We modify the driver of the NICs in the fingerprint collectors and install two different CSI collection tools, i.e., CSITOOL [26] in the Ubuntu 14.04

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

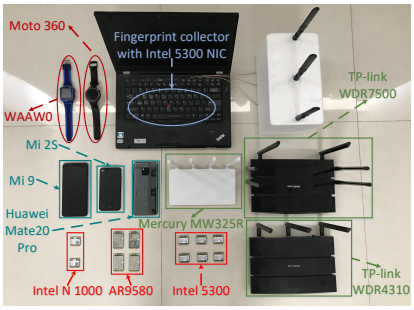


Fig. 14 Part of the tested WiFi devices.

TABLE 4 The device types of the collected fingerprints.

Device type	Quantity	Device type	Quantity
Laptop with Intel 5300	12	Xiaomi Mi-9	2
Laptop with AR9580	4	MEIZU 15	1
Laptop with N 1000	5	OnePlus 5	2
TP-link WDR7500	3	OnePlus 6	1
TP-link WDR4310	1	Samsung Galaxy S6	1
Mercury MW325R	1	Huawei Mate30Pro	2
Xiaomi Mi-2s	2	Moto 360 Watch	1
Huawei Mate20Pro	1	WAAWO Watch	1

operating system and PicoScenes [39] in the Ubuntu 20.04 LTS operating system to collect CSI for fingerprinting.

Fingerprint Acquisition Before and After Attack: It is worth noting that since there is currently no public data set about various PHY fingerprints of different devices [14], and there is no public fingerprint sample after a movement attack [40], we can only choose a self-built data set. To compare the fingerprints before and after the attacks, we use 40 WiFi devices, including 5 APs and 35 mobile clients, to collect the corresponding NLPE fingerprints. The mobile clients include various types of laptops, cellphones, and smartwatches. Tab. 4 shows the specific types and numbers of the adopted devices. In our experiments, we use the ICMP Ping method to collect raw CSIs, and the frame sampling rate is set to 100 frames per second. For each AP or client before and during the attack, we collect data for ten seconds every time, i.e., collecting 1000 CSI frames at one time.

6.2 Attack Performance

Performance Measures: We adopt two measures to evaluate the attack performance: the *Pearson correlation coefficient* (denoted by P) between the fingerprints of the same device before and after the attack to express the post-attack similarity and the *attack success ratio (ASR)*, which is the fraction of legal devices that cannot access WLAN after the attack to denote the attack accuracy. Here, we define the ASR as follows:

$$ASR = \frac{\xi_{de}}{\xi_{wh}} \times 100\%, \tag{28}$$

where ξ_{de} denotes the number of fingerprints that are denied in the authentication process, and ξ_{wh} denotes the total number of testing fingerprints.

Pearson Correlation Coefficient: In this experiment, we use 40 different WiFi devices to evaluate the attack performance, and these devices are described in Tab. 4. We perform our experiments in a dormitory shown in

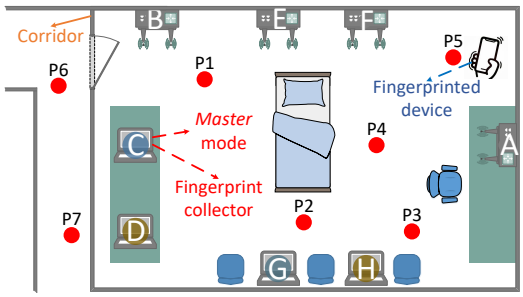


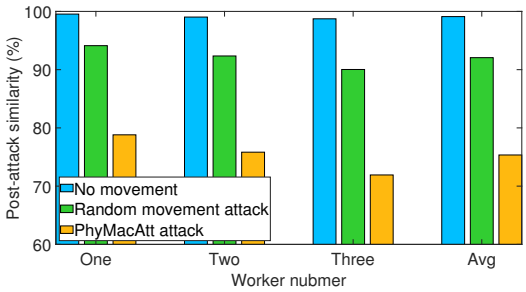
Fig. 15 One fingerprint collector and seven tested positions of the fingerprinted device in the dormitory ($6.1 \times 4m^2$).

Fig. 15, and the physical side of this dormitory is $6.1 \times 4m^2$. Here, we take the random attack as a baseline method, in which the workers randomly move in the dormitory and consider a reference scenario where there is no attack. For each device, we employ 6 volunteers to perform various movement attacks and collect the fingerprint sample data 50 times at different locations (P1 to P7 in Fig. 15) for each attack scenario. Totally, $3 \times 40 \times 50$ fingerprint samples are collected in our experiment. As described in Sec. 6.1, we collect ten seconds of CSI data for each fingerprint sample, and the sampling rate is 100 frames per second. Thus, each fingerprint sample contains 1000 CSI frames. To comprehensively measure the NLPE fingerprint changes, we use the average fingerprint of 1000 frames as the device fingerprint in one sampling.

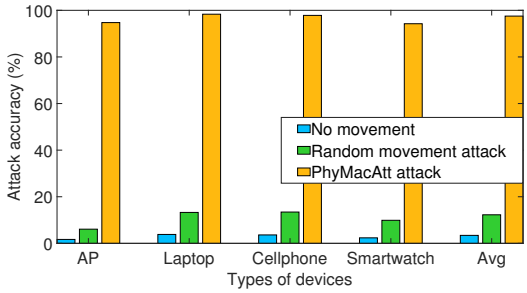
Fig. 16(a) shows the Pearson correlation coefficient (or the similarity) between the fingerprints of the same device before and after the attacks. Here, we vary the number of workers from 1 to 3 and report the average results over 40 devices. The reference fingerprints before attacks are collected from the same location in the empty room (the room in Fig. 15). We can observe that the proposed PhyFinAtt attack always achieves better performance (lower fingerprint similarity after the attack) compared with the random movement attack, and the average correlation coefficient after the PhyFinAtt attack can be lower than 76%. For the scenario where there is no attack, the NLPE fingerprint remains constant. Besides, the random attack cannot change the NLPE fingerprint significantly (the average correlation coefficient is 92.06%), which shows that the NLPE fingerprint is relatively stable and robust to normal indoor activities. In addition, Fig. 16(a) shows that the similarity between the same device fingerprints before and after the attack becomes lower as the number of workers increases. Furthermore, compared with the random movement attack, PhyFinAtt can improve the attack performance more significantly as the number of workers increases. This clearly demonstrates that the proposed PhyFinAtt framework is effective, and it can significantly change the NLPE fingerprint.

Attack Success Ratio (ASR): Next, we discuss the attack success ratio of the proposed attack framework. We first establish the legal fingerprint library for 40 WiFi devices. This library contains 50 fingerprint samples for each device, and these samples are collected in the unmanned student dormitory. For each attacked fingerprint sample, we cal-

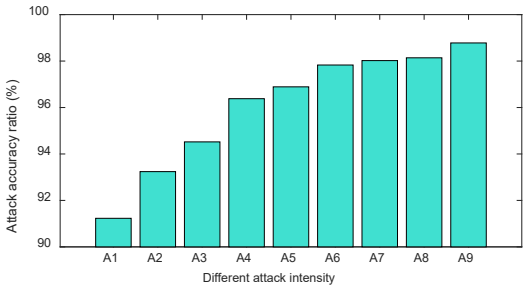
This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954



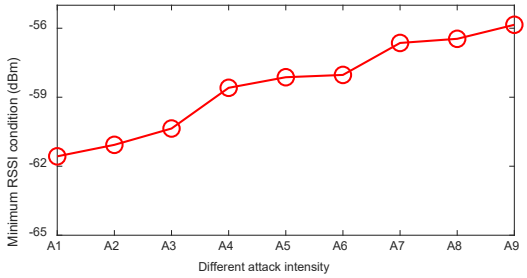
(a) Comparison of the post-attack similarities for different attack methods when the worker number is changing. (Avg: average)



(b) Comparison of the attack accuracy for different attack methods when the attacked device is different.



(c) Comparison of the attack accuracy under different attack intensities (A1-A9: different intensities).



(d) Comparison of the minimum RSSI condition for normal communication under different attack intensities.

Fig. 16 Comparison of the performance of different attack methods.

culate the average similarity coefficients P_{avg} between this sample and the 50 fingerprint samples of every device in the legal fingerprint library. If any P_{avg} exceeds 90%, we consider the device that generates this fingerprint sample to be legal, and it can access the WLAN (the attack is unsuccessful). Otherwise, the corresponding device is considered to be illegal, and the attack is successful. Then, for each device, we collect 50 fingerprint samples (i.e., $\xi_{wh} = 50$) under each attack method and calculate ASR based on Eq. (28). The results are shown in Fig. 16(b). For the scenario where there is no attack, the average ASR of all devices is 3.42%, and the ASRs of APs and smartwatches are lower than other devices whose fingerprints are more stable. Similarly, the average ASR of all devices is not high under the random attack. This demonstrates that the NLPE fingerprint is stable and robust to normal activities. However, under our proposed attack, the average ASR of all devices boosts to 97.53%. This clearly proves that the proposed PhyFinAtt framework can significantly destroy the stability of NLPE fingerprints and affect their normal verification, which finally leads to the result that legal devices cannot access the WLAN.

Attack Intensity Impact On Attack Accuracy and RSSI Requirement: To further understand the impacts of the attack intensity on the attack effect and the RSSI requirement for normal communication, we set different attack intensities and test the attack accuracy ratio (ASR) and the minimum RSSI value required by the environment in the corresponding intensity. Specifically, Fig. 16(c) shows the impact of different attack intensities on the attack accuracy. The X-axis represents different attack intensities, and A1-A9 denote the nine different attack intensities from 1Per-3 to 3Per-10 shown in Tab. 1. The Y-axis represents the average attack accuracy ratio. As the attack intensity increases, the ASR increases significantly, but the increase rate gradually decreases. Besides, Fig. 16(d) depicts the impact of different attack intensities on the minimum RSSI value required by the environment for normal communication. The constraint object of the minimum RSSI is the area near the attacked AP ($< 50cm$) in Fresnel Zone. From Fig. 16(d), we can observe that as the attack intensity increases, the minimum RSSI requirement for the normal communication of all devices also increases. Therefore, to perform an effective attack without affecting normal communication, PhyFinAtt chose the maximum attack intensity allowed by the environment to perform the fingerprint attack.

TABLE 5 Performance improvement of the proposed two different speed adjustment mechanisms.

Channel evaluation index	Without adjustment	**With adjustment**
Packet loss ratio	5.7%	**1.8%**
RSSI < -77dBm ratio	26.7%	**5.2%**

Channel Quality Protection: The RSSI-Human Initial Speed Module and the Real-time Speed Adjust Module in our proposed attack framework can help protect the channel quality. To verify this point, we remove the two modules from PhyFinAtt and then compare the corresponding channel quality with that when PhyFinAtt is performed. Specifically, for all NLOS devices in the student dormitory shown in Fig. 15, we use the ICMP Ping method and CSITOOL [26] to record the average packet loss ratio and the ratio of RSSI lower than -77dBm, respectively. The results are shown in Tab. 5. We can observe that these two attack intensity control modules can significantly reduce the negative impact of human motions on channel quality. Through initializing the worker number and speed and adjusting real-time speed, the average packet loss ratio of WiFi devices located in NLOS areas is obviously reduced. In addition, the RSSI in the corresponding location is also

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

TABLE 6 The performance of PhyFinAtt on different PHY information-based fingerprints.

Fingerprint type	ASR
CFO-based fingerprint	98.25%
CSI-based fingerprint	98.74%
CSITE framework-based fingerprint	98.61%
RSSI-based fingerprint	99.23%
Phase error range-based fingerprint	97.89%

significantly improved. The results demonstrate that the two attack intensity control modules ensure that the PhyFinAtt framework does not affect the normal communication of all devices while attacking the NLPE fingerprint.

6.3 Generalization

The proposed attack system PhyFinAtt is effective not only for the NLPE fingerprint but for all the PHY information-based fingerprints propagated through wireless channels.

In order to evaluate the generalization of the PhyFinAtt system, we report the ASRs of PhyFinAtt on five other PHY fingerprints adopted by state-of-the-art authentication protocols. Specifically, we extract the CFO-based fingerprint [5], the CSI-based fingerprint [7], the CSITE framework-based fingerprint [8], the RSSI-based fingerprint [12], and the phase error range-based fingerprint [9], respectively, as the attacked targets to evaluate the attack effectiveness of PhyFinAtt on different kinds of PHY fingerprints. The fingerprint collection before and after the attack and the ASR calculation method in this part are the same as that introduced in Sec. 6.2.

Tab. 6 shows the ASRs of PhyFinAtt for various PHY information-based fingerprints. We can observe that PhyFinAtt has good scalability for different attack targets, and it can achieve good performance on all types of fingerprints. The ASR for each fingerprint can reach more than 97.89%. The results also demonstrate that the attack on the electromagnetic field in Fresnel Zone effectively destroys the authentication fingerprints of different protocols and further affects their normal verification.

6.4 Deep Dive into PhyFinAtt

The main purpose of this section is to understand the impact of various factors on the attack effect of the PHY fingerprints. The performance evaluation indicators in this section are the correlation coefficient P and ASR introduced in Sec. 6.2. Furthermore, in this part, the employed worker number in different experiments is one.

6.4.1 Attack Effect of Different Motions

To explore which motions can effectively change the PHY fingerprint, we add three different types of activities, i.e., static activity, in-place activities, and moving activities, to test their attack effectiveness. Fig. 17 shows the sketch of different attack activities. The static activity (standing) is used as a reference state to observe the impact of the static human body on the PHY fingerprint. The in-place activities and the moving activities are used to observe the change of the PHY fingerprint when the position remains unchanged or changed.

Fig. 18 depicts the degree of impact of different activities on the PHY fingerprint (P) and the probability of a successful attack (ASR). From Fig. 18, we observe that the static

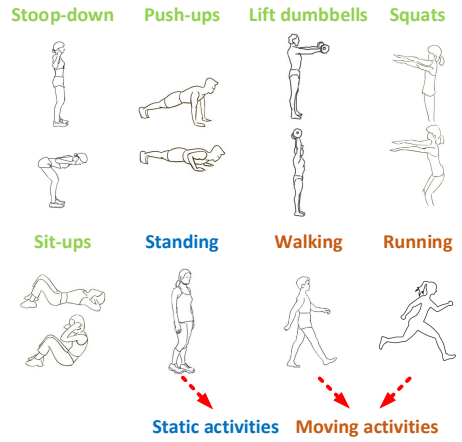


Fig. 17 Attack activity set: one reference static activity (standing), five in-place activities, and two moving activities.

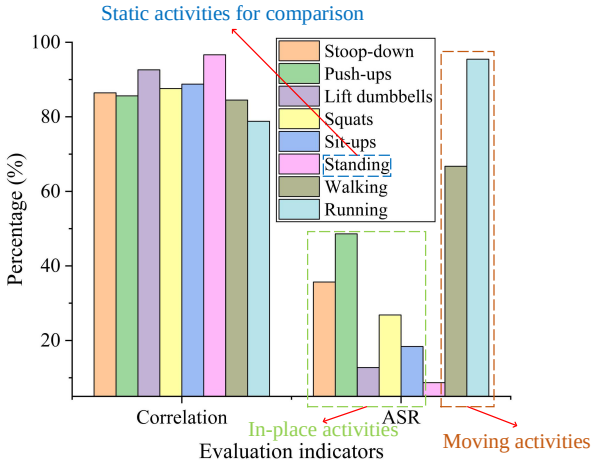


Fig. 18 The degree of impact of different activities on the PHY fingerprint and the probability of a successful attack.

human body basically does not change the PHY fingerprint, which shows that the change of the PHY fingerprint does not come from the occlusion of the human body. The impact of in-place activities on the PHY fingerprints is also not obvious. The similarity of fingerprints before and after the attack is mostly around 85%, so the success rate of the attack (ASR) is not high. This illustrates that the intensity of in-place activities without position change is not sufficient to change the PHY fingerprint. Compared with these two types of activities, the moving activity (running) can significantly change the PHY fingerprint and produce a higher ASR due to the rapid positional movement.

6.4.2 Attack Effect of Different Regions

To verify the impact of the moving range on the attack effect and to test the attack performance in a larger sensing range outside the first Fresnel Zone, we set five different moving ranges to observe the post-attack similarity and the ASR in the corresponding range. A single worker is located in the center of the first Fresnel Zone. Its running direction is perpendicular to the WiFi connection link, and the running range is different.

TABLE 7 The impact of different attack ranges on the attack effect of PhyFinAtt.

Metrics	Within Zone	**120%**	200%	280%	360%
Correlation	81.43%	**78.81%**	81.87%	83.54%	88.73%
ASR	91.37%	**95.47%**	89.75%	84.16%	64.24%

TABLE 8 The attack effect of various attack methods in different frequency bands.

Band	No	Random	**PhyFinAtt**
2.4 GHz	99.54%, 2.98%	94.12%, 10.98%	**78.81%, 95.47%**
5 GHz	99.63%, 3.07%	94.89%, 10.43%	**79.37%, 93.56%**

Tab. 7 shows the impacts of different attack ranges on the PHY fingerprint. Within Zone represents the range of running movement within the first Fresnel Zone, and different numbers mean different running ranges. For instance, 280% denotes the running range not exceeding 180% of the periphery of the first Fresnel Zone. From Tab. 7, we observe that as the attack range increases, the ASR first increases slowly and then decreases continuously. When the running range does not exceed 20% of the periphery of the first Fresnel Zone, the attack has the greatest impact on the PHY fingerprint, and the fingerprint similarity before and after the attack (the post-attack similarity) is only 78.81%. This is because when the running range is small, the displacement generated by the human body is also small and has less effect on the signal ToF and on the PHY fingerprint. On the other hand, since most of the electromagnetic energy is concentrated in the first Fresnel Zone [41], when the running range is too large and far away from the first Fresnel Zone, the impact of the movement on the distribution of electromagnetic energy will be reduced, and the corresponding effect on the PHY fingerprint will also be reduced accordingly.

Nevertheless, even if the moving range exceeds 2.8 times the diameter of the first Fresnel Zone, the attack accuracy can still reach 84.16%, which shows that a relatively satisfactory attack effect can still be achieved with a larger moving range. Furthermore, since the size of the first Fresnel Zone is positively related to the distance between the transmitting and receiving antennas, when the indoor environment is large, the effective attack range will also be larger.

The experimental results show that the PHY fingerprint is relatively stable. When the attack occurs at an NLOS area, the movement of the human body cannot significantly change the PHY fingerprint. Thus, in order to achieve the best attack effect when there is a complex multipath in the testing room, the PhyFinAtt system needs first to calculate the location of the first Fresnel Zone and perform the corresponding attack near this zone.

6.4.3 Attack Performance in 5GHz Band

To test the effectiveness of PhyFinAtt in different frequency bands, we next evaluate PhyFinAtt in the 5GHz frequency band. The experimental setting here is the same as that for the 2.4GHz.

Tab. 8 shows the performance of various attack methods in different WiFi bands. The two numbers in each cell denote the post-attack similarity and the attack success ratio, respectively. Although 5GHz and 2.4GHz have different subcarrier frequencies and wavelengths, the same attack method has similar attack performance in different frequency bands. The results also show that the proposed PhyFinAtt can always achieve the best performance.

TABLE 9 The impact of worker heights on the attack effect of PhyFinAtt.

Metrics	<160cm	160∼170cm	170∼180cm	**>180cm**
Correlation	80.13%	79.54%	78.13%	**75.53%**
ASR	91.62%	95.36%	96.13%	**96.79%**

TABLE 10 The frequency and probability that the RSSI value of the nearest AP is in the top three of the list.

Device	20mW	35mW	50mW	**Avg**
TP-link WDR7500	28/30	30/30	30/30	**97.78%**
TP-link WDR4310	29/30	30/30	30/30	**98.89%**
Mercury MW325R	27/30	29/30	30/30	**95.56%**

6.4.4 Attack Effect of Different Workers

To evaluate the effect of the workers' heights, we invite 10 volunteers with different heights to perform the PhyFinAtt attack. The ten volunteers include seven males and three females. The height distribution of these volunteers is two people below 160cm, three people from 160cm to 170cm, three people from 170cm to 180cm, and two people above 180cm.

Tab. 9 describes the effect of different worker heights on the attack performance. Apparently, Tab. 9 shows taller workers can produce better attack results. However, the effect of human heights on the attack is not significant. A worker with a height of less than 160cm can still effectively change the PHY fingerprint and achieve a high ASR when she is running.

6.4.5 RSSI Value of the Nearest AP

To verify that, in most cases, the RSSI value of the nearest AP ranks among the top three RSSI values of all indoor APs, we adjust the transmit power of various recognition APs and measure the RSSI value in the nearby area to rank its RSSI of all indoor APs. Since the transmit power of indoor APs usually does not exceed 50mW, the transmit power of various recognition APs is set to 20mW, 35mW, and 50mW, respectively.

Tab. 10 shows the frequency and probability that the RSSI value of the nearest AP (different type APs) is in the top three of the list. The numerator and denominator in each cell represent the top three times of RSSI intensity and the total number of measured times, respectively. For example, $28/30$ represents the RSSI value of the TP-link WDR7500 AP ranks in the top three among all indoor APs in 28 of the 30 measurements. This clearly shows that the RSSI of the nearest AP is able to rank among the top three RSSIs of all indoor APs even when the transmit power is set to a low level (20mW). This is because the maximum transmit power of indoor APs is usually set below 50mW, and the signal strength attenuates rapidly with increasing transmission distance.

6.4.6 Attack Performance under Different Distances

In this experiment, we evaluate the effect of the distance between the test position and the transmitter on the attack performance. Specifically, we vary the distance from 1m

This article has been accepted for publication in IEEE Transactions on Mobile Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TMC.2023.3338954

TABLE 11 The impact of different distances to the transmitter on the attack effect of PhyFinAtt.

Metrics	1m	2m	3m	4m	**5m**
Correlation	80.58%	78.49%	77.49%	76.54%	**94.33%**
ASR	92.56%	95.61%	96.12%	96.97%	**11.87%**

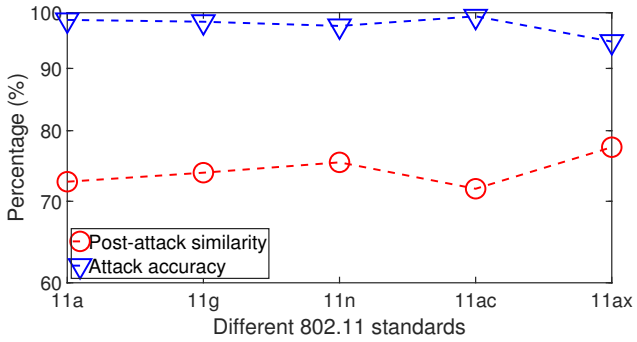


Fig. 19 Attack results of PhyFinAtt to different IEEE 802.11 standards and different operating systems.

to 5m and record the corresponding similarity P and the ASR. The results are shown in Tab. 11.

As shown in Fig. 13, the distance between transmitter A and receiver C is 4m. This means that when the worker is 5m away from transmitter A, he is 1 meter to the left of receiver C, which is outside the first Fresnel Zone. The results in Tab. 11 demonstrate that when the worker is in the Fresnel Zone, the distance changes between the worker and the transmitter have no significant effect on the attack performance, and once the worker performs the attack outside the Fresnel Zone, the attack performance will drop significantly.

6.4.7 Robustness to Different 802.11 Standards and Different Operating Systems

To further demonstrate the effectiveness of PhyFinAtt to different IEEE 802.11 standards and different operating systems, in addition to CSITOOL (working in Ubuntu 14.04), we also employ the PicoScenes [39] platform (working in Ubuntu 20.04 LTS) to collect the CSI data in different IEEE 802.11 standards, i.e., 802.11a/g/ac/ax and test the corresponding attack performance of PhyFinAtt to different IEEE 802.11 standards and different operating systems. The settings in the experiment, except for different IEEE 802.11 standards and different CSI collection tools, are the same as those presented in Sec. 6.2.

Fig. 19 shows the attack results of PhyFinAtt to different IEEE 802.11 standards, including the post-attack similarity and the attack accuracy ratio. We can observe that PhyFinAtt has similar and satisfactory attack effects on different IEEE 802.11 standards, which reflects similar post-attack similarities and attack success ratios. This clearly demonstrates that the PhyFinAtt system is not only valid for IEEE 802.11n standard but also robust to various IEEE 802.11 standards. Furthermore, since the used Picoscenes platform is installed on the Ubuntu 20.04 LTS operating system, these experiment results clearly show the strong compatibility of PhyFinAtt with the new version of the operating system.

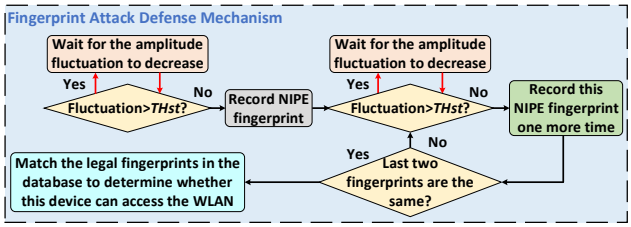


Fig. 20 The proposed defense mechanism.

TABLE 12 Performance of the defense mechanism.

Attack approach	No defense	**With defense**
Random attack	12.25%	**7.34%**
PhyFinAtt attack	97.53%	**13.25%**

7 Defense Mechanism

To deal with attacks similar to PhyFinAtt, we finally propose a practical defense mechanism, and its framework is shown in Fig. 20. Without any additional equipment or system modifications, this mechanism is only based on the CSI amplitude fluctuation threshold. Since the CSI amplitude fluctuation caused by human movements has an approximately positive correlation with the NLPE fingerprint changes caused by human movements, the degree of the NLPE change can be directly controlled by limiting the CSI amplitude fluctuation. As shown in Fig. 20, we continuously collect the device NLPE fingerprints (sampling rate $<$ 2Hz) many times when the CSI amplitude fluctuation is less than a threshold TH_{st}. If the collected NLPE fingerprints in the last two times are the same (similarity $P > 96\%$), we will output this fingerprint to match the legal fingerprint library. This mechanism effectively constrains that the output NLPE fingerprints are all in a stable state. According to experimental experience, this amplitude fluctuation threshold TH_{st} in our experiment is set to 4.

Tab. 12 shows the performance of the proposed defense mechanism. We can see that the defense mechanism significantly decreases the ASRs under various movement attacks. Specifically, under the PhyFinAtt attack, the ASR decreases from 97.53% to 13.25% when the proposed defense mechanism is applied. The results demonstrate that the proposed defense mechanism can significantly improve the robustness of the PHY fingerprint-based authentication protocols to human movement attacks.

8 Conclusion

In this paper, we propose a novel undetectable attack framework PhyFinAtt, based on which the attacker can effectively attack the PHY information-based WiFi authentication protocols. By undermining the unique authentication fingerprints derived from the PHY layer, PhyFinAtt makes legal devices unable to match the legal fingerprint library and unable to access the WLAN, which finally results in the paralyzing of the WLAN. Through the advanced setting of attack intensity and the real-time movement speed adjustment during the attack process, PhyFinAtt can effectively change the authentication fingerprint in an undetected way without affecting normal communication. We prototype and evaluate our proposed attack via extensive real-world

experiments. The results demonstrate the superiority of PhyFinAtt in terms of making changes in fingerprints and attack accuracy. Compared with random movement attacks, PhyFinAtt can increase the ratio of successful attacks by 85.28%. To mitigate attacks similar to PhyFinAtt, a practical defense mechanism based on the CSI fluctuation threshold is proposed without involving any additional equipment. With this mechanism, the ASR is reduced to 13.25%, and the robustness of the PHY fingerprint-based authentication protocols to human movement attacks is significantly improved.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (Grant No. 62302145), Anhui Province Science Foundation for Youths (Grant No. 2308085QF230), and Young teachers' scientific research innovation launches special A project (Grant No. JZ2023HGQA0100). We would like to thank the editors and anonymous reviewers for their insightful comments and constructive feedback.

REFERENCES

[1] Tian Xie, Guan-Hua Tu, Bangjie Yin, Chi-Yu Li, Chunyi Peng, Mi Zhang, Hui Liu, and Xiaoming Liu, "The untold secrets of wifi-calling services: Vulnerabilities, attacks, and countermeasures," *IEEE Transactions on Mobile Computing*, vol. 20, no. 11, pp. 3131–3147, 2020.

[2] Keyvan Ramezanpour, Jithin Jagannath, and Anu Jagannath, "Security and privacy vulnerabilities of 5g/6g and wifi 6: Survey and research directions from a coexistence perspective," *Computer Networks*, vol. 221, pp. 109515, 2023.

[3] Xuewei Feng, Qi Li, Kun Sun, Yuxiang Yang, and Ke Xu, "Man-in-the-middle attacks without rogue ap: when wpas meet icmp redirects," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 3162–3177.

[4] DM Ajay and E Umamaheswari, "Packet encryption for securing real-time mobile cloud applications," *Mobile Networks and Applications*, vol. 24, no. 4, pp. 1249–1254, 2019.

[5] Jingyu Hua, Hongyi Sun, Zhenyu Shen, Zhiyun Qian, and Sheng Zhong, "Accurate and efficient wireless device fingerprinting using channel state information," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1700–1708.

[6] Pengfei Liu, Panlong Yang, Wen-Zhan Song, Yubo Yan, and Xiang-Yang Li, "Real-time identification of rogue wifi connections using environment-independent physical features," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 190–198.

[7] Hongbo Liu, Yan Wang, Jian Liu, Jie Yang, and Yingying Chen, "Practical user authentication leveraging channel state information (csi)," in *Proceedings of the 9th ACM symposium on Information, computer and communications security*, 2014, pp. 389–400.

[8] Zhiping Jiang, Jizhong Zhao, Xiang-Yang Li, Jinsong Han, and Wei Xi, "Rejecting the attack: Source authentication for wi-fi management frames using csi information," in *2013 Proceedings IEEE INFOCOM*. IEEE, 2013, pp. 2544–2552.

[9] Jiahui Zhang, Qian Lu, Ruobing Jiang, and Haipeng Qu, "Pedr: A novel evil twin attack detection scheme based on phase error drift range," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2020, pp. 188–207.

[10] Ning Xie, Shengli Zhang, and Alex X Liu, "Physical-layer authentication in non-orthogonal multiple access systems," *IEEE/ACM Transactions on Networking*, vol. 28, no. 3, pp. 1144–1157, 2020.

[11] Haijun Tan, Ning Xie, and Alex X Liu, "An optimization framework for active physical-layer authentication," *IEEE Transactions on Mobile Computing*, 2022.

[12] Daniel B Faria and David R Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on Wireless security*, 2006, pp. 43–52.

[13] Hongyi Pu, Liang He, Chengcheng Zhao, David KY Yau, Peng Cheng, and Jiming Chen, "Fingerprinting movements of industrial robots for replay attack detection," *IEEE Transactions on Mobile Computing*, vol. 21, no. 10, pp. 3629–3643, 2021.

[14] Xinghao Guo, Zhen Zhang, and Jie Chang, "Survey of mobile device authentication methods based on rf fingerprint," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2019, pp. 1–6.

[15] Guillem Reus-Muns, Dheryta Jaisinghani, Kunal Sankhe, and Kaushik R Chowdhury, "Trust in 5g open rans through machine learning: Rf fingerprinting on the powder pawr platform," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[16] Tong Jian, Bruno Costa Rendon, Emmanuel Ojuba, Nasim Soltani, Zifeng Wang, Kunal Sankhe, Andrey Gritsenko, Jennifer Dy, Kaushik Chowdhury, and Stratis Ioannidis, "Deep learning for rf fingerprinting: A massive experimental study," *IEEE Internet of Things Magazine*, vol. 3, no. 1, pp. 50–57, 2020.

[17] Kunal Sankhe, Mauro Belgiovine, Fan Zhou, Luca Angioloni, Frank Restuccia, Salvatore D'Oro, Tommaso Melodia, Stratis Ioannidis, and Kaushik Chowdhury, "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 165–178, 2019.

[18] Cherita L Corbett, Raheem A Beyah, and John A Copeland, "Passive classification of wireless nics during active scanning," *International Journal of Information Security*, vol. 7, no. 5, pp. 335–348, 2008.

[19] Ke Gao, Cherita Corbett, and Raheem Beyah, "A passive approach to wireless device fingerprinting," in *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*. IEEE, 2010, pp. 383–392.

[20] Christoph Neumann, Olivier Heen, and Stéphane Onno, "An empirical study of passive 802.11 device fingerprinting," in *2012 32nd International Conference on Distributed Computing Systems Workshops*. IEEE, 2012, pp. 593–602.

[21] Vladimir Brik, Suman Banerjee, Marco Gruteser, and Sangho Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116–127.

[22] Qing Liu, Jiajia Guo, Chao-Kai Wen, and Shi Jin, "Adversarial attack on dl-based massive mimo csi feedback," *Journal of Communications and Networks*, vol. 22, no. 3, pp. 230–235, 2020.

[23] Serkan Sarıtaş, Henrik Forssell, Ragnar Thobaben, Henrik Sandberg, and György Dán, "Adversarial attacks on cfo-based continuous physical layer authentication: A game theoretic study," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[24] Jianfei Yang, Han Zou, and Lihua Xie, "Securesense: defending adversarial attack for secure device-free human activity recognition," *IEEE Transactions on Mobile Computing*, 2022.

[25] Ning Xie, Haijun Tan, Lei Huang, and Alex X Liu, "Physical-layer authentication in wirelessly powered communication networks," *IEEE/ACM Transactions on Networking*, 2021.

[26] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall, "Tool release: Gathering 802.11 n traces with channel state information," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 1, pp. 53–53, 2011.

[27] IEEE Committee, "Ieee standard for information technology," *IEEE Std 802.11n-2009*, pp. 1–565, Oct 2009.

[28] Jinyang Huang, Bin Liu, Pengfei Liu, Chao Chen, Ning Xiao, Yu Wu, Chi Zhang, and Nenghai Yu, "Towards anti-interference wifi-based activity recognition system using interference-independent phase component," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*. IEEE, 2020, pp. 576–585.

[29] Youwei Zeng, Dan Wu, Ruiyang Gao, Tao Gu, and Daqing Zhang, "Fullbreathe: Full human respiration detection exploiting complementarity of csi phase and amplitude of wifi signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 3, pp. 148, 2018.

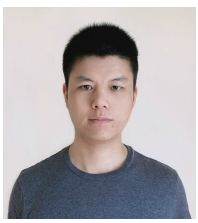
[30] Nan Yu, Wei Wang, Alex X Liu, and Lingtao Kong, "Qgesture: Quantifying gesture distance and direction with wifi signals," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 1, pp. 51, 2018.

[31] Wei Wang, Alex X Liu, Muhammad Shahzad, Kang Ling, and Sanglu Lu, "Device-free human activity recognition using com-

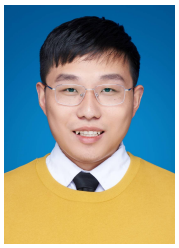
mercial wifi devices," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1118–1131, 2017.
[32] Jianwei Liu, Yinghui He, Chaowei Xiao, Jinsong Han, Le Cheng, and Kui Ren, "Physical-world attack towards wifi-based behavior recognition," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*. IEEE, 2022, pp. 400–409.
[33] Jianwei Liu, Yinghui He, Chaowei Xiao, Jinsong Han, and Kui Ren, "Time to think the security of wifi-based behavior recognition systems," *IEEE Transactions on Dependable and Secure Computing*, 2023.
[34] Wei Xi, Jizhong Zhao, Xiang-Yang Li, Kun Zhao, Shaojie Tang, Xue Liu, and Zhiping Jiang, "Electronic frog eye: Counting crowd using wifi," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 361–369.
[35] Andrea Zignoli, Antoine Godin, and Laurent Mourot, "Indoor running temporal variability for different running speeds, treadmill inclinations, and three different estimation strategies," *PloS one*, vol. 18, no. 7, pp. e0287978, 2023.
[36] Luke A Kelly, Andrew G Cresswell, and Dominic J Farris, "The energetic behaviour of the human foot across a range of running speeds," *Scientific reports*, vol. 8, no. 1, pp. 10576, 2018.
[37] Xiuzhen Guo, Yuan He, Xiaolong Zheng, Liangcheng Yu, and Omprakash Gnawali, "Zigfi: Harnessing channel state information for cross-technology communication," *IEEE/ACM Transactions on Networking*, vol. 28, no. 1, pp. 301–311, 2020.
[38] DE Bassey, Aniefiok O Akpan, and E Udoeno, "Uhf wave propagation losses beyond 40 percent fresnel zone radius in south-south, nigeria," *International Journal of Science and Research (IJSR)*, vol. 5, no. 2, pp. 470–475, 2016.
[39] Zhiping Jiang, Tom H Luan, Xincheng Ren, Dongtao Lv, Han Hao, Jing Wang, Kun Zhao, Wei Xi, Yueshen Xu, and Rui Li, "Eliminating the barriers: Demystifying wi-fi baseband design and introducing the picoscenes wi-fi sensing platform," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4476–4496, 2021.
[40] Junqing Zhang, Guanxiong Shen, Walid Saad, and Kaushik Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," *IEEE Communications Magazine*, 2023.
[41] Sol Kim, Hye-Won Jo, Jeong-Wook Kim, Ju-Ik Oh, Jong-Won Yu, and ByungKuon Ahn, "Curved-retrodirective beamforming system to improve microwave power transmission efficiency in the fresnel region," *IEEE Internet of Things Journal*, 2023.

Jinyang Huang received the Ph.D. degree in School of Cyberspace Security from the University of Science and Technology of China in 2022. He is currently a lecturer in the School of Computer and Information at Hefei University of Technology. His research interests include Wireless Security and Wireless Sensing. He is a TPC Member of IEEE ICME and Globecom. He is now an editorial board member of Applied Sciences.

Bin Liu received the B.S. and M.S. degrees, both in electrical engineering, from University of Science and Technology of China, Hefei, Anhui, China, in 1998 and 2001, respectively, and the Ph.D. degree from Syracuse University, Syracuse, NY, in 2006. Currently, he is an Associate Professor with the School of Information Science and Technology, University of Science and Technology of China. His research interests are Signal Processing and Computer Vision.

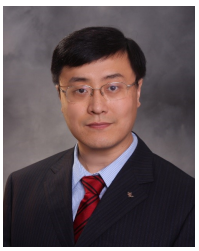


Chenglin Miao received the PhD degree in computer science and engineering from the State University of New York at Buffalo, in 2020. He is currently an assistant professor in the Department of Computer Science at the Iowa State University. His research interests include security and privacy, Internet of Things, and machine learning. He is a member of ACM and IEEE.



Xiang Zhang received the B.E. degree from Hefei University of Technology, China, in 2017, and his D.E. degree from the same university in 2023. Currently, he is a postdoc with the School of Cyber Science and Technology, University of Science and Technology of China. His research interests include wireless sensing and affective computing. He is a TPC Member of IEEE ICME and Globecom. He has served as a reviewer for IEEE TNNLS, TMM, and Pattern Recognition.

Jianchun Liu (Member, IEEE/ACM) received the Ph.D. degree in School of Data Science from the University of Science and Technology of China in 2022. He is currently an associate researcher in the School of Computer Science and Technology at University of Science and Technology of China. His main research interests are software defined networks, network function virtualization, edge computing and federated learning.



Lu Su is an associate professor in the School of Electrical and Computer Engineering at Purdue University. His research interests are in the general areas of Internet of Things and Cyber-Physical Systems, with a current focus on wireless, mobile, and crowd sensing systems. He received Ph.D. in Computer Science, and M.S. in Statistics, both from the University of Illinois at Urbana-Champaign, in 2013 and 2012, respectively. He has also worked at IBM T. J. Watson Research Center and National Center for Supercomputing Applications. He has published more than 100 papers in referred journals and conferences, and serves as an associate editor of ACM Transactions on Sensor Networks. He is the recipient of NSF CAREER Award, University at Buffalo Young Investigator Award, ICCPS'17 best paper award, and the ICDCS'17 best student paper award. He is a member of ACM and IEEE.

Zhi Liu (S'11-M'14-SM'19) received the Ph.D. degree in informatics in National Institute of Informatics. He is currently an Associate Professor at The University of Electro-Communications. His research interest includes video network transmission and mobile edge computing. He is now an editorial board member of Springer wireless networks and IEEE Open Journal of the Computer Society. He is a senior member of IEEE.

Yu Gu (M'10-SM'12) received his D.E. degree from the University of Science and Technology of China in 2010. Since 2012, he has been a Professor and Dean Assistant at the School of Computer and Information, Hefei University of Technology. Now he is a Professor of the University of Electronic Science and Technology of China since 2023. His current research interests include pervasive computing and affective computing. He is a member of ACM and a senior member of IEEE.