Jian *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2020) 9:5
https://doi.org/10.1186/s13677-020-0154-7

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

PHYAlert: identity spoofing attack detection and prevention for a wireless edge network

Zhiping Jiang[1], Kun Zhao[2], Rui Li[1*], Jizhong Zhao[2] and Junzhao Du[1]

Abstract

Delivering service intelligence to billions of connected devices is the next step in edge computing. Wi-Fi, as the *de facto* standard for high-throughput wireless connectivity, is highly vulnerable to packet-injection-based identity spoofing attacks (PI-ISAs). An attacker can spoof as the legitimate edge coordinator and perform denial of service (DoS) or even man-in-the-middle (MITM) attacks with merely a laptop. Such vulnerability leads to serious systematic risks, especially for the core edge/cloud backbone network.

In this paper, we propose PHYAlert, an identity spoofing attack alert system designed to protect a Wi-Fi-based edge network. PHYAlert profiles the wireless link with the rich dimensional Wi-Fi PHY layer information and enables real-time authentication for Wi-Fi frames. We prototype PHYAlert with commercial off-the-shelf (COTS) devices and perform extensive experiments in different scenarios. The experiments verify the feasibility of spoofing detection based on PHY layer information and show that PHYAlert can achieve an 8x improvement in the false positive rate over the conventional signal-strength-based solution.

Keywords: Identity spoofing attack, Channel state information, Wireless intrusion detection, Wi-Fi

Introduction

Edge computing is envisioned as a promising technology for enabling intelligence for billions of devices in the future, ranging from a Wi-Fi-connected thermometer and smartwatch to an edge-computing server. In addition to the connection, networked intelligence is also important. On top of the physical devices and network, edge computing performs the mission of orchestrating massively connected devices into single and unified service intelligence.

A reliable network is a prerequisite for the edge system to deliver QoS-enabled complex service intelligence [1, 2]. However, various challenges exist in the depth. An IoT system comprises a connected heterogeneous network, such as Wi-Fi, Bluetooth, ZigBee, RFID or a wired connection [3, 4]. Except for the wired connection, the above connectivities are significantly vulnerable to a packet-injection-based identity spoofing attack (PI-ISA) because of their in-air broadcast transmission nature. An attacker can perform denial of service (DoS) or even man-in-the-middle (MITM) attacks indiscriminately on the IoT network using COTS devices. A PI-ISA casts a serious threat to a network, and the difficulties of detection and elimination have drawn tremendous academic attention in ISA detection and prevention for various physical networks. Some previous works identify the ISA vulnerability for BT [5], ZigBee [6], and RFID [7]. From the viewpoint of the edge network, a PI-ISA targeted to a BT, ZigBee, or RFID network has a relatively small and limited threat to the whole edge system integrity, because these types of networks are usually adopted for the edge nodes and their failure is noncontagious. However, the scenario changes remarkably for a Wi-Fi targeted attack. As the *de facto* backbone network for billions of IoT devices [8], the Wi-Fi network is unprecedentedly vulnerable to a PI-ISA [9]. From the attacker's perspective, launching an attack has never been as easy as it is today. The network surrounding or behind a wall can be instantly paralyzed using merely a laptop or even a smartphone in the attacker's pocket [10]. In contrast, it is extremely difficult to identify and localize the attacker [11].

*Correspondence: rli@xidian.edu.cn
[1] School of Computer Science and Technology, Xidian University, Xi'an, China
Full list of author information is available at the end of the article

All these threats exploit a main vulnerability in the Wi-Fi design whereby management frames (MFs) of the 802.11 standard, which maintain the network operation, are transmitted in clear text [12]. An attacker can spoof the identity by forging MFs and use a spoofed identity as a springboard to initiate various attacks [13], e.g. DoS attacks, Wi-Fi *phishing*, password cracking, or even an MITM attack.

Unfortunately, traditional Wi-Fi anti-spoofing designs have very limited efficacy. Amendment 802.11w tries to encrypt several important MFs, However, a new flaw has been identified [14]. There is growing interest in exploiting physical layer information for wireless security; however, the received signal strength (RSS) is the only accessible physical layer information provided by most commercial hardware. The wireless intrusion detection system (WIDS) [15] based on RSS anomaly detection can detect most MF spoofing attacks. The WIDS comprises many predeployed Wi-Fi sniffers, which monitor Wi-Fi traffic and detect the anomaly signal strength variance. Due to privacy issues and the high deployment costs, most WIDS systems are only deployed in an office environment. An RSS-based WIDS can be near-perfectly spoofed by a smart antenna system using the beamforming technique [16].

To protect the Wi-Fi-based backbone network, we shall devise a single-station-based management frame authentication mechanism. We find that channel state information (CSI), 802.11n PHY layer information, is now available in commercial wireless NICs [17, 18]. Originally designed to achieve explicit beamforming feedback, the CSI reflects the channel frequency response (CFR) for the subcarriers of the underlying 802.11a/g/n OFDM transmission. Some initial investigations showed that CSI has some unique advantages over the RSS. First, the CSI captures the multipath profile for the wireless transmission rather than the coarse signal strength; therefore, it is insensitive to the transmit power (Tx-power). An attacker cannot fool CSI-based detection by optimizing the Tx-power. Second, since the multipath effect can be generally modeled as a typical Rayleigh distribution, CSI has rapid spatial decorrelation characteristics, which makes it quite difficult to predict the CSI for a given position. Third, CSI is a high-dimensional fingerprint; it records 30 complex values for each spatial stream. For a typical SIMO 1 × 3 connection, the CSI is 90-dimensional and becomes 270-dimensional for a 3 × 3 MIMO connection. It is extremely difficult for an attacker with a rational attack ability to penetrate a CSI-based authentication system. Figure 1 shows an experimental comparison between CSI- and RSS-based authentication systems. Real-world proof-of-concept experiments make us believe that a CSI-based fingerprint is a promising solution for identity spoofing detection.

Leveraging the above advantages, we propose and prototype PHYAlert, a CSI-based MF authentication system with COTS hardware. The main idea is intuitive yet effective: both data frames or management frames are transmitted in identical wireless channels. Thus, their CSI should be highly similar. However, for a forged frame injected by an attacker, the CSI similarity will breakdown, because the forged frame is transmitted from somewhere else. Therefore, we can label this frame as suspicious. To learn the CSI pattern of the legitimate frames, PHYAlert is based on a security assumption that the encrypted data frames are difficult to compromise in a short time [19]. Based on this key assumption, we believe that an attacker with a rational attack ability cannot fabricate legitimate data frames. Therefore, the CSI of the correctly decrypted data frames can be regarded as the fingerprint of the legitimate stations. To implement this idea, there are three main challenges.

First, the spoofing detection problem can be formalized into a hypothesis test, where $\mathcal{H}_0$ represents accepting

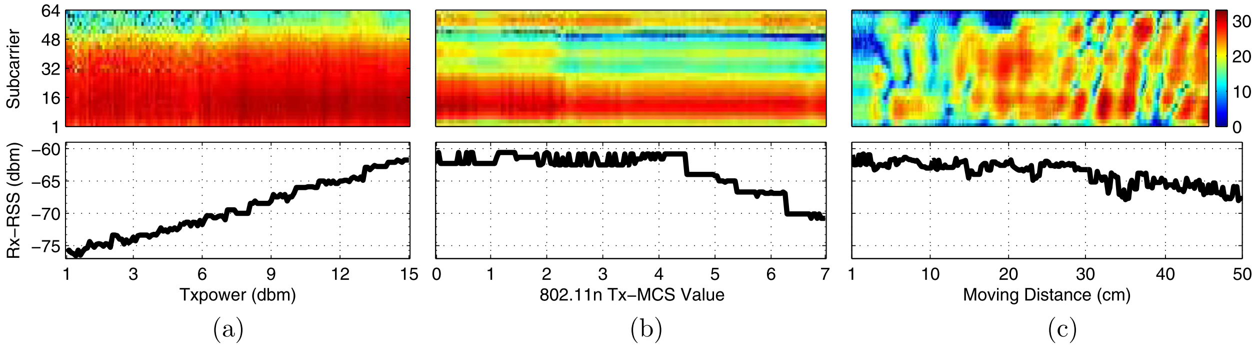


Fig. 1 **a** The CSI amplitude remains unchanged when the Tx-power increases, while the Rx-RSS increases by 13 dBm. **b** When the MCS value [1] increases, the CSI remains unchanged, but the Rx-RSS decreases by 10 dBm. **c** When the client is moving, the CSI shows rapid spatial de-correlation, while the RSS changes slowly along the distance

the newly arrived frames and $\mathcal{H}_1$ represents rejecting them. However, due to client mobility or a channel disturbance, the *probability density functions* (PDFs) for both distributions, denoted by $f_{\mathcal{H}_0}$ and $f_{\mathcal{H}_1}$, change frequently. To address this problem, we have to design a universal detection mechanism that can work without any prior knowledge about $f_{\mathcal{H}_0}$ and $f_{\mathcal{H}_1}$ except that $f_{\mathcal{H}_0} \neq f_{\mathcal{H}_1}$.

Second, it is difficult to determine the threshold γ for detection without any prior knowledge about $f_{\mathcal{H}_0}$ and $f_{\mathcal{H}_1}$. Moreover, γ should be adaptively adjusted for different scenarios, i.e. a dynamic threshold scaling (DTS) mechanism must be carefully designed.

Third, in mobile scenarios, the frames sent even from legitimate stations may be rejected due to the large CSI difference, i.e., a false positive (FP). Effectively transmitting management frames is a problem for even legitimate stations.

The main contributions of this paper are as follows. We propose and prototype PHYAlert, a CSI-based management frame authentication and spoof detection system. Solely based on on-site CSI data, PHYAlert achieves single-station-based authentication in both stationary and mobile environments. We prototype PHYAlert with COTS hardware, and extensive experiments demonstrate that PHYAlert has remarkable performance in terms of accuracy and robustness. In one mobile scenario, the RSS-based method has a 18% false positive rate, while PHYAlert has a false positive rate of only 2%. In another mobile scenario, PHYAlert achieves an 8x improvement in the false positive rate.over traditional methods.

Background and related work

The vulnerability of a Wi-Fi network

The first major security flaw of 802.11 concerns wired equivalent privacy (WEP) [20]. An attacker can recover the passphrase almost immediately after catching the four-way handshake. The 802.11i amendment, or implemented as WPA2, fixed this flaw. WPA2 is quite difficult to compromise by brute force and has to this day successfully protected Wi-Fi communication [19].

The denial of service (DoS) attack has become the next major attack technique [21]. Since management frames (MFs) are transmitted in clear text without integrity protection, an attacker can easily forge certain MFs, such as a de-authentication frame, to cut even all wireless connections [22]. The amendment 802.11w aims to fix the flaw by encrypting these key MFs. However, an attacker can bring a victim to an authentication deadlock by carefully injecting an unexpected de-authentication during handshakes [14]. On the other hand, 802.11w does not protect all MFs; it cannot prevent a *quiet attack* and a *channel switch attack* [23].

A very serious security flaw has been revealed recently in the Wi-Fi protected setup (WPS) [24], which is activated by default in most WPS-supported devices. The flaw allows an attacker to brute-force attack the WPS PIN code in a few hours. With the WPS PIN code, an attacker can recover the WPA2 preshared key and become an inside attacker. Once receiving the integrity group temporal key (IGTK) shared by all legitimate clients, the 802.11w and 802.11i protections are entirely compromised.

Approaches for Wi-Fi protection

MAC Layer

In addition to the amendments proposed by the 802.11 task group, in the MAC layer, the sequence number (SN) is the main element for frame integrity validation. By detecting the sudden shift in the SN caused by injected spoofing frames, a spoofing attack may be detected [25]. This protection can be easily compromised when carefully following the original SN. An advanced approach is to pseudorandomize the SN, such that an attacker cannot correctly follow the underlying pattern [26]. However, a major problem is that these approaches require a modification of both the AP and client, which makes it difficult to implement these approaches in real applications.

PHY Layer

Various PHY layer approaches can be categorized into transmitter identification-based and location distinction-based approaches.

Transmitter Identification: In this category, the main challenge is to discover the intrinsic transmitter characteristics [27], such as the temporal transient signature [28], DAC nonlinearity, frequency offset, phase offset [29], or slight offset among the spatial streams in the MIMO configuration [30]. The main advantage of these approaches is that they can model a transmitter precisely and consistently and provide robust source authentication service. However, these approaches usually require raw passband or baseband information, which requires expensive hardware, e.g. USRP or a vector network analyzer (VNA), to capture this low-level information, and also requires a large amount of computation resources to process these low-level signals. In addition, the high deployment cost hinders the practical use of these approaches.

Location Distinction: Recalling the spatial position diversity, location distinctiveness could be considered as the location fingerprint for a client [31].

The RSS-based system was vastly researched in early works. The wireless intrusion detection system (WIDS) is the initial exploration in this field[15]. The WIDS usually consists of many wire-connected Wi-Fi sniffers. An attacker is collaboratively identified by detecting the anomaly RSS variance for the same MAC address. Combined with an indoor localization system, [32] could find the attacker for the first time. The WIDS can hardly be seen in the public environment due to the high deployment cost, and recent theoretical work [16] also proved that an RSS-based anti-spoofing system can be fully compromised by beamforming antenna systems.

With the popularity of new COTS hardware and software-defined radio (SDR) systems, fine-grained physical layer information is now easy to obtain. SpotFi [33] provides sub-meter-level spot localization based on CSI. HuFu [7] exploits the tag imperfection profile to implement tag authentication in an RFID system. With multiple linear antenna arrays deployed in an indoor environment, angle of arrival (AoA)-based approaches [34] can provide fine-grained indoor localization. Based on the same hardware, SecureArray [35] was proposed, which is very similar to our system. In this work, the AoA profile is used to identify different clients and provide intrusion detection service. Compared to PHYAlert, SecureArray depends highly on the number of antennas N_l. The number of clients that SecureArray can identify simultaneously is $N_l - 1$, which limits the application in crowd and noise environments. Moreover, when the distance between an attack and the victim is less than half the wavelength, the false positive (FP) rate soon increases rapidly. However, SecureArray and PHYAlert can have deep cooperation. With a linear phased array, PHYAlert can reduce the false negative (FN) rate caused by user mobility, while SecureArray can improve the resolution within the coherent distance by using the PHYAlert approach.

CSI, OFDM, and Wi-Fi

CSI usually refers to the channel frequency response (CFR) $\mathbf{h}$ in the model: $\mathbf{y} = \mathbf{hx} + \mathbf{n}$, where $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{n}$ are the transmitted, received and noise signals in the frequency domain, respectively. CSI is a description of the wireless link path rather than the RSS; mathematically,

$$\mathbf{h} = |\mathbf{h}|\, e^{j\angle \mathbf{h}}$$

where $|\mathbf{h}|$ and $\angle \mathbf{h}$ denote the channel response in the amplitude and phase, respectively. In a Wi-Fi network, the dimension of the CSI increases rapidly along with the introduction of orthogonal frequency division multiplexing (OFDM) and MIMO-based spatial multiplexing (SM) technologies [12]. For a typical 3 × 3 MIMO connection, there are 9 individual Tx-Rx pairs. For each pair, OFDM modulation splits the 20 MHz channel into 64 equal-width narrowband subcarriers. Eventually, the dimension of the CSI increases to 576. The CSI is measured in the preamble stage for each frame. The long training field (LTF) [12] in the preamble contains a known pilot signal, and the 802.11 protocol uses this known pilot to estimate the CSI [36].

Security analysis for a CSI-based physical layer fingerprint

As mentioned in the previous section, Wi-Fi OFDM and MIMO technologies enable one to authenticate the frames based on the location distinctiveness. In this section, we investigate the degree of distinctiveness under the 802.11n specification, and provide the theoretical basis for PHYAlert.

Fading phenomena in a wireless channel can be categorized into three types: path loss, shadowing, and multipath fading for large, middle, and small scales, respectively [37]. Multipath fading contributes most of the location distinctiveness. In a rich scattering space, e.g. an urban environment, a sufficiently wide bandwidth and multiple varying antennas could produce significant frequency selective and spatial selective fading. Fading has rapid decorrelation characteristics and i.e. strong location distinctiveness. Here, we analyze the location distinctiveness provided by multipath fading.

Assuming *a wide-sense stationary uncorrelated scattering* (WSSUS) channel model, the channel frequency response (CFR) for a flat-frequency narrow-band channel can be modeled as a sum of m_p independent paths [37]:

$$H(f) = \mathcal{F}\left\{\sum_{n=1}^{m_p} H_n \delta(\tau - \tau_n)\right\} = \sum_{n=1}^{m_p} H_n \exp(-j2\pi f \tau_n) \quad (1)$$

where $\delta(\cdot)$ is the Dirac delta function and τ_n and H_n represent the path delay and channel coefficient for the n-th multipath, respectively. Then, we evaluate the frequency domain correlation function:

$$R_H(\Delta_f) = E\left[H(f)H(f - \Delta_f)\right] \quad (2)$$

Assuming the multipath gain is independent and has zero mean, Eq. 2 can be simplified as

$$R_H(\Delta_{f_c}) = E\left[\sum_{n=1}^{m_p} |H_n|^2 \exp\left(-j2\pi\,\Delta_f \tau_n\right)\right] \quad (3)$$

This expectation can be further approximated as

$$R_H(\Delta_{f_c}) = \int_0^{\infty} S_H(\tau) \exp\left(-j2\pi\,\Delta_f \tau\right) d\tau \quad (4)$$

where $S_H(\tau)$ is the *power delay profile*. Equation 4 indicates that in a certain multipath environment with delay profile $S_H(\tau)$, the channel correlation varies according to Δ_f.

In an urban environment, the **coherent bandwidth** is empirically 2 MHz [38] and usually corresponds to approximately 6 independent channel frequency responses in a typical 802.11 20-MHz bandwidth. However, we should note that the channel bonding feature in 802.11ac can provide as much as 160 MHz of bandwidth, which in turn provides much richer channel estimation.

In the spatial domain, the displacement of a receiver's antenna will change Eq. 1 to:

$$H(\Delta) = \sum_{n=1}^{m_p} H_n \exp\left[-j2\pi \cos\alpha_n \frac{\Delta}{\lambda_c}\right] \quad (5)$$

where Δ is the relative displacement and α_n is the angle of arrival of the n-th path. We still use a correlation function to investigate the spatial correlation property.

$$R_H(\Delta) = E\left[H(f)H(f-\Delta_{f_c})\ \right] \tag{6}$$

Assuming that the multipath gain is independent and has zero mean and that the multipath gains are constant as a function of the angle of arrival, Eq. 6 can be simplified as

$$R_H(\Delta) = E\left[\frac{2\sigma_H^2}{m_p}\exp\left[\frac{j2\pi\Delta\cos\left(\beta-\frac{2\pi(n-1)}{m_p}\right)}{\lambda_c}\right]\right] \tag{7}$$

When m_p is large, this correlation function will converge to

$$R_H(\Delta)=\frac{2\sigma_H^2}{2\pi}\int_{-\pi}^{\pi}\exp\left[\frac{j2\pi\Delta\cos(\theta)}{\lambda_c}\right]d\theta=2\sigma_H^2 J_0\left(\frac{2\pi\Delta}{\lambda_c}\right) \tag{8}$$

where $J_0(x)$ is the zeroth-order Bessel function of the first kind. Note that elementary functions cannot represent the general solution of the Bessel function. We use two adjacent asymptotic forms [39] to approximate the Bessel function $J_0(x)$, as shown below.

$$J_0(x) = \begin{cases} \mathbf{a}X^T & 0 < x < \pi \\ \sqrt{\frac{2}{\pi x}}\cos\left(x-\frac{\pi}{4}\right) & x \geq \pi \end{cases} \tag{9}$$

Considering the situation in which an eavesdropper is more than half a wavelength away from the legitimate AP, $\Delta \geq \frac{\lambda_c}{2}$ (i.e., $\frac{2\pi\Delta}{\lambda_c} \geq \pi$), we have

$$\begin{aligned} R_H(\Delta) &= 2\sigma_H^2 J_0\left(\frac{2\pi\Delta}{\lambda_c}\right) \\ &= 2\sigma_H^2\frac{1}{\pi}\sqrt{\frac{\lambda_c}{\Delta}}\cos\left(\frac{2\pi\Delta}{\lambda_c}-\frac{\pi}{4}\right) \\ &\leq 2\sigma_H^2\frac{1}{\pi}\sqrt{\frac{\lambda_c}{\Delta}} \end{aligned} \tag{10}$$

Equation (10) clarifies that the channel estimation of two antennas will rapidly decorrelate in a rich scattering environment once they are spaced more than half a wavelength; i.e., it will be very difficult for an attacker to forge the victims' CSI, which is even more difficult in MIMO situations. For a 3×3 MIMO connection, there are 9 independent Tx-Rx spatial streams. In such a configuration, it is extremely difficult to perform physical layer spoofing. In this way, we theoretically prove the physical layer anti-clone property of CSI.

PHYAlert design

In this section, some observations on the characteristics of CSI are presented first. Then, we present the design of PHYAlert.

CSI as a fingerprint for packet authentication

CSI, as a fine-grain description for a wireless channel, has the unique property of spatial decorrelation. This property means that the CSI vectors measured from very close positions are highly similar; i.e. their correlation efficiency is $\rho \approx 1$. However, ρ will soon decrease to 0 once separated by only half a wavelength. In addition, the CSI captures the channel response for each of the 802.11 subcarriers; thus, it is rich in dimension and can withstand a transmission power scanning attack, which can fool traditional RSS-based approaches. The CSI dimensionality is very rich. In 3x3 MIMO transmission, the dimensionality can reach 270 by Intel 5300 NIC or even 1026 by Atheros 9300 NIC. Apparently, an attacker with high cooperation cannot estimate the victim's CSI or fool CSI-based detection.

We carry out a proof of concept (PoC) experiment to assess CSI-based spoofing detection. An edge backbone coordinator, as the victim machine, receives 3000 frames. The second half of the received frames include the attacking ones, which are injected by a laptop only 20 cm away. Figure 2a shows the per-packet CSI amplitude. It is apparent that the CSI amplitude of the injected frames is so distinct from the rest that we can visually identify them at a glance. Figure 2b and c show the CSI distribution of the 20th subcarrier of the first half and second half of the received frames, respectively. We see that, due to the carrier frequency offset (CFO) and sampling frequency offset (SFO), the phase distribution is roughly uniform [18],i.e. providing no discrimination. However, the CSI amplitude is stable and sensitive to the wireless channel. Based on the above observations, we decide to use the amplitude values to perform CSI-based spoofing detection.

PHYAlert architecture

Our system comprises two parts: the *PHYAlert detector* and *PHYAlert transmission improvement*. The PHYAlert detector incorporates both the CSI amplitude and time to characterize the distance between receiver frames. The detector then attempts to identify the suspicious management frames via a CSI distance-based hypothesis test. However, the rigorous test may lead to a certain false negative rate, which harms the network performance. The PHYAlert transmission improvement (PTI) is employed to remedy these issues. A linear time-varying (LTV) channel, i.e. a wireless channel under mobility, can be seen as a quasi-linear time-invariant (quasi-LTI) channel within the period of the channel coherent time. Leveraging this property, the PTI transmits management frames immedi-

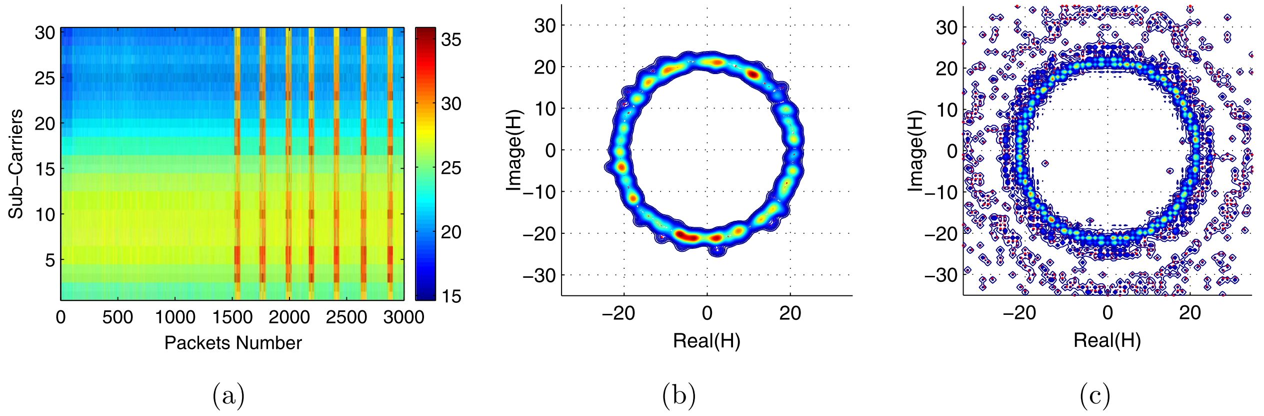


Fig. 2 **a** CSI amplitude graph of 3000 received frames including frames injected by an attack. **b** and **c** CSI distribution I/Q view for the 20th subcarrier of the first and second half of the frames, respectively

ately after a train of empty data frames. In this way, the management frames can pass the PHYAlert detector.

PHYAlert detector

The PHYAlert detector implements the CSI-based hypothesis test. Given a train of recently received (and correctly decrypted) data frames S_d, the PHYAlert detector extracts the CSI fingerprint from the frame train. Then, for the latest received management frame M, the PHYAlert detector calculates how closely M's CSI follows the CSI fingerprint learned from S_d. If the *distance* is below τ, an adaptively adjusted threshold, M is labeled as *legitimate*; otherwise, M is labeled as *suspicious* if the distance is above the threshold. In addition to the general goal, two technical preferences must also be satisfied: a low computational overhead and biased receiver operating characteristic (ROC). First, the network performance and energy consumption are critical for the edge backbone network; thus, an unoptimized computation for the per-packet CSI vector is unacceptable. Second, for the PHYAlert detector, a low false positive error (FPE) rate is much more preferred than a low false negative error (FNE) rate, because the FPE, i.e. the chance to accept the attacking frames, is the primary threat to the edge backbone network. However, the FNE, i.e. the chance to reject a frame, is acceptable with some degradation in exchange for network security.

Deep-learning-based classifiers are ideal solutions [40, 41]. However, regarding the performance preference, we formalize the hypothesis test into an online anomaly detection problem [42]. More specifically, we adopt the K-nearest-neighbor algorithm [43] to solve this problem. To further reduce the computational overhead, we reduce the CSI vector dimension. First, we remove the phase value for the complex-numbered CSI vector leaving only the amplitude vector, because the phase with a near-uniform distribution provides no discrimination. Second, in typical open-space urban or indoor office environments, the coherent channel bandwidth is approximately 1 MHz; i.e., the adjacent subcarriers are highly correlated, also providing no discrimination . Therefore, we reduce the dimension of the amplitude vector by merging the adjacent 2 or 3 values.

Now, we present the detailed design of the PHYAlert detector. To support the recent CSI fingerprint, each receiver maintains a fixed length FIFO amplitude vector buffer B_{am} with length L_W, which buffers the latest received CSI. Given a latest received management frame, we use a metric called the trend following factor (TFF) to reflect its trend-following characteristic.

The TFF is based on a joint distance metric: the amplitude-time distance (ATD). We first present the TGD design and then the TFF calculation. We define the amplitude space distance between two amplitude vectors as their $\mathbf{L}_2$ norm, i.e. $d_{am}(A,B) = \|A - B\|_2$. Then, to characterize the time gap between two frames, we define the *time distance* as $d_t(A,B) = e^{\lambda(|t_A - t_B|)}$. By jointing these two distances, we have the ATD as

$$d_{atd} = d_{am} \cdot d_t$$

Let $N_k^{atd}(F) = \{A_1, A_2, A_3\}$ be the top k-nearest neighbor of frame F in the amplitude buffer B_{am} under the ATD. Then, we define the TFF of F as

$$TFF(F) = \sum_{i=1}^{k} d_{atd}(F, A_i), P_i \in N_k^{atd}(M)$$

With the above definitions, the PHYAlert detector uses the threshold τ to perform the hypothesis test as

$$\text{Determination for F is} \begin{cases} legitimate, & TFF(F) \leq \tau \\ suspicious, & TFF(F) < \tau \end{cases} \quad (11)$$

Adaptive Threshold Adjustment (ATA) Recalling the biased ROC preference of PHYAlert, we focus on how τ

should adapt to the channel dynamics, or more specifically, how to adjust τ based on the TFF values of the previously accepted frames. When the channel dynamics are relatively low, i.e. in a relatively stationary environment, the TFF values of the previous frames have a relatively small variance. In contrast, the TFF value for a spoofing frame should be quite distant. In a mobile environment, since the TFF values of the previous frames have large variance, the TFF value for a spoofing frame appears not to be that distant. In this case, the risk of FPE increases. Based on the above analysis, we conclude that τ should be negatively related to the TFF values of previous frames.

As shown in the following equation, we correlate τ with the percentile i of the latest TFF values.

$$\tau = p_i(\{TTF_b(B_{am})\}), 1 \leq b \leq L_w$$

, where $p_i(\cdot)$ is the i-th percentile function. To reflect the negative correlation, we further adapt i with respect to a metric of the channel dynamics, σ_W, which is defined as

$$\sigma_W = \overline{(std_n(|P_j - P_{j+1}|))}, j \in [1, L_w - 1]$$

Then, we define an effective negative correlation between i and σ_W, $i = \frac{i_0}{\sigma_W/\sigma_W^r}$, where $i = 75$ is the default value and σ_W^r is the initial value measured at the startup.

PHYAlert transmission improvement

Due to the bias ROC preference, PHYAlert has a higher chance to label a legitimate frame under weak confidence as *suspicious*, especially in mobile scenarios. To guarantee that the network operation and performance are not severely affected by the PHYAlert detector, a specific design is required to guarantee transmission from a legitimate sender.

As previously discussed, a mobile wireless channel, i.e. an LTV-type channel, can be seen as a quasi-LTI-type channel if the transmissions are within the channel coherent time. In other words, the shorter the inter-frame interval, the more invariance the CSI exhibits. A PoC experiment is shown in Fig. 3 to validate this phenomenon. In the experiment, file transmission with a high frame rate is performed between a pair of fast moving stations. Figure 3a shows the amplitude graph during 3 s of transmission, which exhibits strong and frequent multipath fading. However, if we gradually focus on the shorter period each time, the invariance emerges in the amplitude graph, showing the quasi-LTI characteristics.

Based on quasi-LTI theory, we propose the PHYAlert transmission improvement (PTI) method to ensure the delivery of management frames. The idea is intuitive: the management frame is not transmitted directly but immediately after a fast train of short data frames or precursor frames. The fast frame stream will create a temporary quasi-LTI moment. Thus, the highly similar amplitudes of the data frames will create stable channel dynamics, which help the following management frame pass the PHYAlert detector.

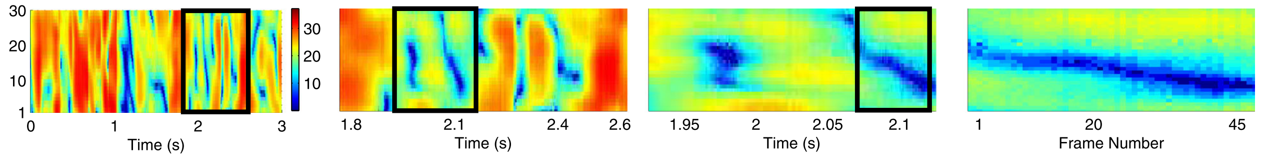
Despite the intuitive solution, there are two problems that we should consider. The first problem is whether the frequency of the "precursor" data frames is high enough and whether there are sufficient "precursor" data frames. For each management frame F, we create a frame stream $S_d = \{D_0, D_1, ..., D_{l_j}, F\}$, where D_i is the short data frame stream. We need to determine the transmission frequency f_p and length l_j for S_d.

Suppose that the radial moving velocity of the legitimate station is v_o. Then, the displacement per frame Δ will be $\frac{v_o}{f_p}$. According to Eq. 8, $R_H(\Delta) = 2\sigma_H^2 J_0\left(\frac{2\pi v_o}{\lambda_c f_p}\right)$. Since the displacement is very small, the Bessel function can be approximated as $J_0(x) = \mathbf{a}X^T, 0 < x < \pi$ according to Eq. 9. This asymptotic form provides a sufficient accurate solution in this case. To satisfy $J_0(x) < \eta$, where η is the channel correlation threshold, we have to solve the function $\alpha X^T \geq \eta$. Typically, we set $v_o = 1.5\,m/s$, $\lambda_c = 0.12\,m$, and $\eta = 0.8$, and we can obtain $f_p > 30$. Empirically, we use $f_p = 60$, which is a relatively low value and will satisfy most moving scenarios and avoid jamming the channel.

For the second problem, i.e. whether the stream is long enough, we design a simple strategy for l_j:

$$l_j = 2^j \times \left(\delta\left(L_W\left(1 - \frac{i}{75}\right)\right) + 1\right), j \in (2, 3..., N), l_j \leq L_W \quad (12)$$

where $\delta(\cdot)$ is the integer rounding function.



(a) (b) (c) (d)

Fig. 3 A highly dynamic LTV channel can become a quasi-LTI channel with a higher sampling rate. **a** 1x zoomed, **b** 3.75x zoomed, **c** 15x zoomed, **d** 60x zoomed

Parameters settings

As shown in the above text, PHYAlert embraces several parameters, λ, k, and the percentile i. Ideally, these parameters could be globally optimized; however, the real-world network-wide configurations and constraints are tightly coupled with the parameters, which makes it very difficult to even model their interactions. In the current version of PHYAlert, according to our extensive evaluations, which are detailed in "Prototype and evaluation" section, we employ empirically optimized settings of $k = 5$, $\lambda = 1$, $L_w = 40$ and $i = 75$. Definitely, part of our future work will aim to further reduce the number of parameters and adaptively optimize the more essential parameters.

Prototype and evaluation

In this section, we briefly describe the system prototyping and detail the threat detection evaluation from "Threat settings" section to "PHYAlert transmission improvement" section and the performance evaluation in "Performance evaluation" section.

System prototyping

We prototype the PHYAlert alert system using *off-the-shelf* hardware. A mini-PC equipped with an Intel 5300 Wi-Fi card is used as an AP. We also use the modified 5300 driver [17] to collect the CSI data. In the software settings, we temporarily disable the threshold scaling function and retain the other parameters by default to identify the impacts of various parameters.

Threat settings

To evaluate the threat detection accuracy of PHYAlert, seven attack scenarios are designed as described in Table 1. In each test case, three laptops, Alice, Bob, and Eve, represent the legitimate AP, victim client, and attacker, respectively. Briefly speaking, Alice, the legitimate AP, is not moving in all scenarios; in scenarios A to C, the victim client Bob is not moving; and in scenarios D to F, Bob walks with different speeds. In scenario G, both Bob and Eve move quickly.

For each scenario, we run a 5 min test. In the test, Alice and Bob continuously transmit to each other an ICMP *echo request* using the *ping* command, which forms the encrypted data frame stream S_{en}. In addition to the data frame stream, Bob periodically injects 20 probe request (a management frame) frames to Alice and replies immediately by 20 probe responses (also a management frame). These probe request/response frames form the unencrypted stream S_u. Eve initiates the DoS attack and wishes to disconnect Bob from Alice. He continuously injects a forged *deauthentication* frame to Bob with Alice's MAC address wishing to impersonate Alice. To increase the attacking success rate, Eve scans the Tx-power from 1 to 15 dBm.

Table 1 Description of the Attack Scenarios

A	Alice, Bob, and Eve are motionless in a silent environment.
B	Same as A, but with some crowd flow.
C	Same as A, but Eve moves slowly.
D	Same as A, but Bob walks with a normal speed.
E	Slower version of D
F	Faster version of D
G	Both Bob and Eve walk with a normal speed.

We mainly focus on two error rates measured on Bob's side: the FP error (FPE) rate and the FN error (FNE) rate. Specifically, the FPE rate is the number of forge deauthentication frames that are wrongfully accepted by Bob over the total number of received deauthentication frames. Similarly, the FNE rate is the number of wrongfully rejected frames over the total number of frames received by Bob.

Comparison with traditional solutions

For each scenario, we compare PHYAlert and RSS-based spoofing detection. Figure 4 shows a comparison of the CSI and RSS views for the same group of received frames in scenario A, i.e. motionless in a quiet environment. In Fig. 4a, the periodically anomalous red lines appearing on the relatively stable background are obviously the CSI for Eve. As described in "Security analysis for a CSI-based physical layer fingerprint" section, the rapid spatial decorrelation characteristic highlights Eve's signal in the spectrum view. Moreover, the insensitivity of CSI to Tx-power makes it tolerable to Tx-power scanning spoofing. On the other hand, the RSS view in Fig. 4b unfortunately fails to recognize the attacking frames when Eve's signal is indistinguishable from the background level around the 800th frame.

Figure 5 shows the error rates of the CSI-based and RSS-based approaches. First, a significant error reduction is achieved by PHYAlert in relatively quiet scenarios. In the stationary scenarios, PHYAlert achieves a 0% FPE, while the RSS-based approach has a 6% FPE. In the moving scenarios, these numbers are 2% and 17%, respectively. PHYAlert achieves an error reduction of more than 8x compared to RSS-based detection.

Impacts of parameter tuning

CSI update frequency f_s

During the test, we scale the CSI sampling rate f_s from 1 to 400 Hz. Figure 6 shows the corresponding FPE and FNE in all test scenarios. In the stationary scenarios, both the FPE and FNE are near 0 when $f_s > 10$ Hz. In the moving scenario, a higher f_s is required to suppress the FPE and FNE. Specifically, the FPE is below 5% if $f_s \geq 100$ Hz in all scenarios and lower than 3% in the highly mobile scenario G if

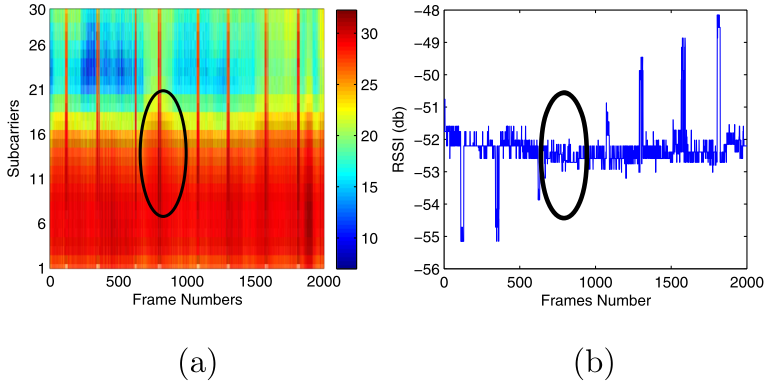


Fig. 4 The CSI amplitude (**a**) and RSS (**b**) for the received frames. The attacker injects the attacking frames every 300 frames with gradually increasing Tx-power

$f_s \geq 400$ Hz. However, we should recall that the DTT function is temporarily disabled during the parameter tuning tests.

KNN number k

In this test, we scale k and f_s individually, and Fig. 7 shows the joint error rate. According to the PHYAlert detector algorithm, k and f_s determine the number of accepted frames used for detection. In the stationary scenarios, as shown in Fig. 7a and b, both the FPE and FNE decrease to a lower level when $k > 7$ In the moving senario, however, a lower k is preferred. The reason is that a higher k includes more relatively old samples in the computation, which deviate more from the recently received ones. Based on the evaluation, in a real application, k is set to 5 to cover both the stationary and moving cases.

Impacts of adaptive threshold tuning

In this test, we scale the CSI update frequency f_s and inspect the changes in the channel stability metric $\overline{\sigma_W}$ and percentile value i. The results are shown in Fig. 8. In Fig. 8a, we see a significant channel stability improvement when $f_s > 100$. Meanwhile, the percentile value i increases adaptively according to $\overline{\sigma_W}$, as shown in Fig. 8b. Figure 8c and d show the FPE and FNE with adaptive threshold tuning. We see that, in scenario A, the FPE decreases to 0 when f_s is merely 5 Hz, and when $f_s > 100$ Hz, the FPE is 0 for all scenarios. On the other hand, it requires a higher f_s to suppress the FNE.

PHYAlert transmission improvement

We evaluate the PTI performance for different update frequencies and numbers of precursor frames. Figure 9a and b show the PTI performance in most stationary and moving scenarios. We can see that a low update frequency f_s leads to a large number of transmission failures even in most stationary scenarios. The precursor frames significantly improve the transmission. In the 5 Hz case, 90% and 78.5% transmission success rates can be achieved with L_w precursor frames in scenarios A and G, respectively. When $f_s = 40Hz$, the PTI improves the success rate to 97.3% and 90.1%, respectively.

Performance evaluation

We deploy PHYAlert in two typical network structures to evaluate the computational cost in a simulated edge

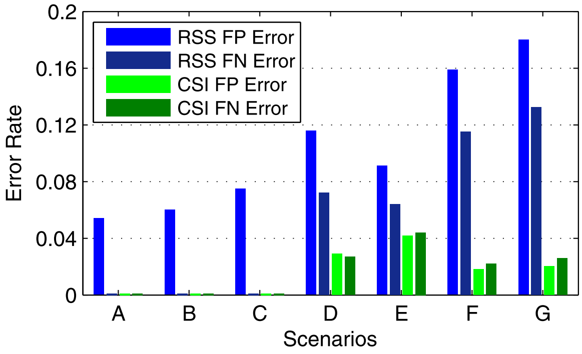
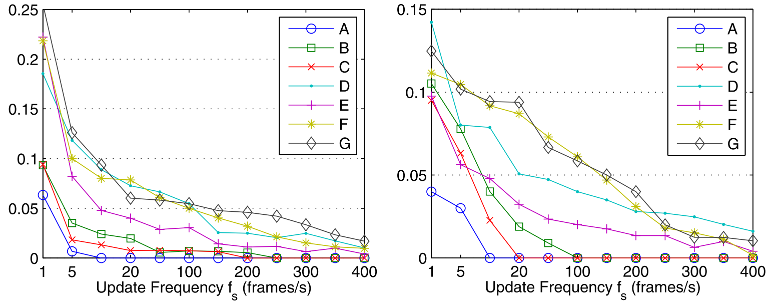


Fig. 5 PHYAlert has better performance than the RSS-based approach in terms of both FPE and FNE



(a) (b)

Fig. 6 Both the FPE (**a**) and FNE (**b**) decrease when f_s increases

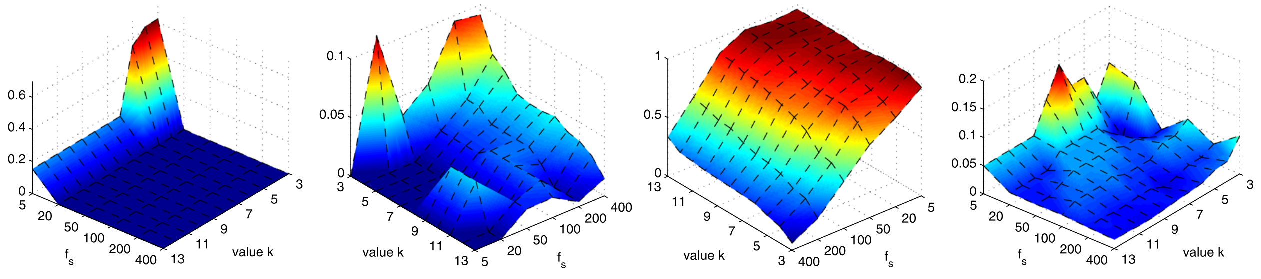
network. In the first structure, we assume a centralized detection system. In this case, the CSI data collected at the AP are all forwarded to a dedicate threat detection server. In the second structure, we employ a distributed structure, in which we push forward the threat detection computation to the local AP. We use a mini-PC with a 1.6-GHz single-core CPU and 4 GB of memory to host the AP functionality. We use an Intel 5300 Wi-Fi card with a modified driver [17] to collect the CSI. For the dedicated server, we run the threat detection algorithm on a 16-core server with 64 GB of memory. In both evaluations, more than 50 real mobile devices generate various Wi-Fi traffic to cover a wide range of common uses. In addition to the routine functionality, the AP forwards the CSI measurement to the server or performs the computation locally.

According to the test, each CSI measurement is 163 bytes on average, and the CSI measurement data rate is 14.3 Mbps per 1000 Mbps of data traffic. In other words, the CSI measurement forwarding increases approximately 1/7 of the total Wi-Fi traffic.

For the centralized setup, we duplicate the total traffic 100 times to simulate a threat detection range covering 50 APs or 2500 client users. Figure 10a shows the system response graph. We can see that the response time remains under 20 ms when there are more than 1500 clients. The factor k shows a strong influence on the computational cost; when $k = 9$, the response time is nearly twice that of $k = 5$. On the AP end, the response time graph shown in Fig. 10b is very impressive. Performing the threat computation while maintaining high-throughput network traffic, the response time is smaller than 20 ms when $k = 7$. In addition, the response is so linear that the response time is highly predictable.

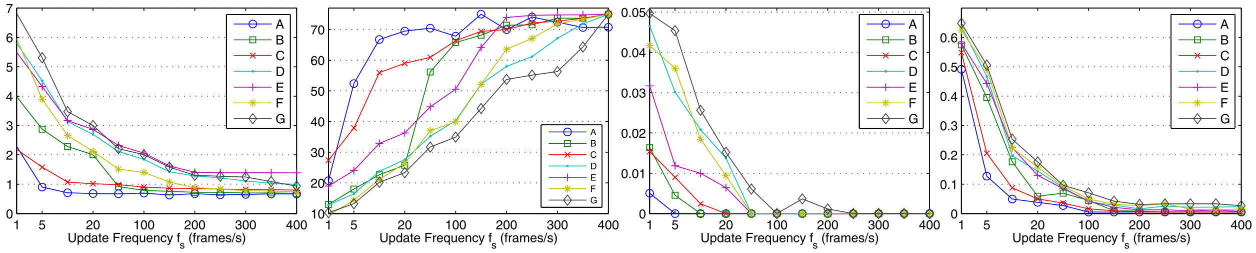
Security analysis

Detection of a Man-In-The-Middle Attack: The spoofing detection of PHYAlert is based on the authenticity of the 802.11 data frame. If the data frames are replayed, a man-in-the-middle (MITM) attack may succeed. However, there are few possibilities to perform such attacks. For an attacker with a reasonable attacking ability, it is quite difficult to forge any encrypted data frames that could successfully pass the layer-by-layer format check at the victim. Therefore, the only effective attack strategy is to replay any unmodified data frames. This limitation makes the attack easy to recognize. The intuitive protection is to compute the *message signature* for the data frames and check if this signature has appeared once during the same Wi-Fi session. A slight modification to the Wi-Fi driver could achieve this goal.



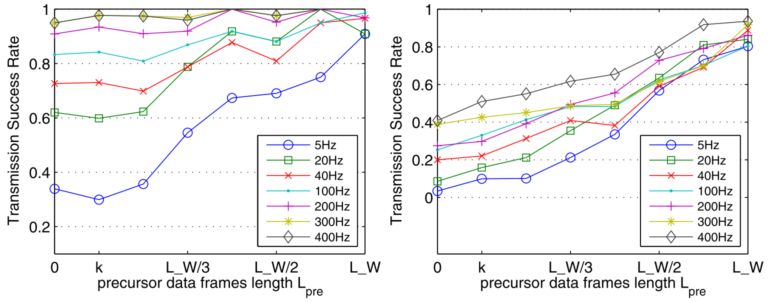
(a) (b) (c) (d)

Fig. 7 The joint impact of k and the sampling rate f_s in scenarios A and G. **a** FPE in A, **b** FNE in A, **c** FPE in G, **d** FNE in G



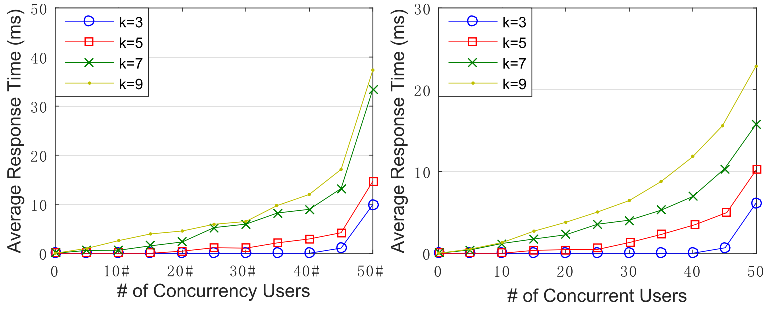
(a) $\overline{\sigma_W}$ (b) Percentile i (c) FPE (d) FNE

Fig. 8 a shows the average window stability σ_W of 7 scenarios for different f_s. **b** shows the percentile i according to $\overline{\sigma_W}$. **c** and **d** present the corresponding FP and FN error rates using the percentile i shown in **b**



(a) (b)

Fig. 9 The success rate with a different number of precursor frames in scenarios A and G



(a) (b)

Fig. 10 The average response time of threat detection deployed on a dedicated server (**a**) and an AP frontend (**b**)

Limitations

Vulnerability Under a Wireless Protection Setup (WPS) Attack: As briefly reviewed in "Background and related work" section, *brute-force WPS*s are currently the most threatening attack to a Wi-Fi network. An attacker can recover the WPA/AES plain text passphrase in a few hours. Once Eve cracks the passphrase, Eve could initiate various MAC layer attacks. Obviously, the defense against this attack is not a part of the PHYAlert design.

However, PHYAlert could still protect clients who have already connected to the AP before Eve breaks in. For each device, WPA2 uses the EAPOL protocol to generate a unique transmission password based on the pre-shared key. For the clients that have already connected, Eve cannot catch the complete 4-way handshake. Therefore, Eve cannot decrypt and forge data frames.

Inability to detect rogue APs: The protection scope of PHYAlert starts from a successful association to a WPA2/AES protected AP and ends with a legitimate disconnection. In PHYAlert, the ability to detect spoofing MFs lies in the a priori physical layer knowledge of the legitimate AP. Without the training phrase, PHYAlert cannot work; i.e. it is unable to detect rogue APs.

Conclusion

The identity spoofing attack in a Wi-Fi network presents severe threats to the edge network. In this work, we propose PHYAlert, a distributed identity spoofing attack alert system. PHYAlert profiles client users with a physical layer fingerprint and uses the fingerprint to authenticate the Wi-Fi management frames that are transmitted in clear text. Regarding the large network traffic variation, the detection algorithm is shaped with a linear yet efficient core and can even harness traffic burstiness to enhance the detection accuracy in a mobile scenario. Since client profiling and threat detection do not require multiparty collaboration, PHYAlert can be deployed at the IoT AP frontend, which is usually the edge coordinator. We prototype PHYAlert, and extensive evaluations show that our design significantly outperforms traditional solutions.

Acknowledgements
The authors would like to thank the School of Computer Science and Technology of Xidian University and School of Computer Science of Xi'an Jiaotong University for supporting this work.

Authors' contributions
ZJ was the main researcher and writer of the manuscript. RL conceived the study and conducted a large part of the evaluations. KZ and JZ contributed the theoretical proof. JD contributed part of the writing and the evaluations. All authors read and approved the final manuscript.

Authors' Information
Zhiping Jiang is an Assistant Professor in the School of Computer Science and Technology of Xidian University, Xi'an, China. His research interests are pervasive computing, wireless sensing, network security and acoustic/wireless Communication.
Kun Zhao is an Assistant Professor in the School of Computer Science of Xi'an Jiaotong University, Xi'an, China. His research interests are network security, privacy preservation in AI and pervasive computing.
Rui Li is an Associate Professor in the School of Computer Science and Technology of Xidian University, Xi'an, China. His research interests are mm-wave radar, wireless sensing, sensor networks, and natural language processing.
Jizhong Zhao is a Professor in the School of Computer Science of Xi'an Jiaotong University, Xi'an, China. His research interests are AI, network security, and multi-modal sensing.
Junzhao Du is a Professor in the School of Computer Science and Technology of Xidian University, Xi'an, China. His research interests are mobile AI, cloud computing, radar sensing and mobile computation.

Funding
This work is supported by the National Key R&D Program of China No. 2017YFB1003000, Natural Science Foundation of China (NSFC) No. 61802291 and No.61502374, National Postdoctoral Program for Innovative Talent No. BX20180235, Fundamental Research Funds for the Central Universities No. JB190304, Shaanxi Fund No. 2018JM6125, No. B018230008, and No. BD34017020001, Open Fund of State Key Laboratory of Computer Architecture No. CARCH201704, and the Youth Innovation Team of Shaanxi Universities.

Availability of data and materials
Not Applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]School of Computer Science and Technology, Xidian University, Xi'an, China.
[2]School of Computer Science, Xi'an Jiaotong University, Xi'an, China.

Received: 10 September 2019 Accepted: 13 January 2020
Published online: 28 January 2020

References

1. Yin Y, Chen L, Xu Y, Wan J, Zhang H, Mai Z (2019) Qos prediction for service recommendation with deep feature learning in edge computing environment. Mob Networks Appl:1–11. https://doi.org/10.1007/s11036-019-01241-7
2. Gao H, Xu Y, Yin Y, Zhang W, Li R, Wang X (2019) Context-aware qos prediction with neural collaborative filtering for internet-of-things services. IEEE Internet Things J:1–1. https://doi.org/10.1109/JIOT.2019.2956827
3. Gao H, Duan Y, Shao L, Sun X (2019) Transformation-based processing of typed resources for multimedia sources in the iot environment. Wirel Netw. https://doi.org/10.1007/s11276-019-02200-6
4. Chen Y, Deng S, Ma H, Yin J (2019) Deploying data-intensive applications with multiple services components on edge. Mobile Netw Appl. https://doi.org/10.1007/s11036-019-01245-3
5. Huang J, Albazrqaoe W, Xing G (2014) Blueid: A practical system for bluetooth device identification. In: IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. IEEE. https://doi.org/10.1109/infocom.2014.6848235
6. Nguyen NT, Zheng G, Zhu H, Rong Z (2011) Device fingerprinting to enhance wireless security using nonparametric bayesian method. Proceedings - IEEE INFOCOM 34(17):1404–1412
7. Wang G, Qian C, Cai H, Han J, Ding H, Zhao J (2018) Towards replay-resilient rfid authentication. In: Proceedings of the 24th Annual International Conference on Mobile Computing and Networking - MobiCom '18. ACM Press. https://doi.org/10.1145/3241539.3241541
8. Polianytsia A, Starkova O, Herasymenko K (2016) Survey of hardware iot platforms. In: Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T. IEEE. pp 152–153
9. Jiang Z, Zhao J, Li XY, Han J (2013) Rejecting the attack: Source authentication for wi-fi management frames using csi information. In: 2013 Proceedings IEEE INFOCOM. IEEE. https://doi.org/10.1109/infcom.2013.6567061
10. Vanhoef M, Piessens F (2014) Advanced wi-fi attacks using commodity hardware. In: Proceedings of the 30th Annual Computer Security

Applications Conference on - ACSAC '14. https://doi.org/10.1145/2664243.2664260

11. Zhou T, Cai Z, Xiao B, Chen Y, Ming X (2017) Detecting rogue ap with the crowd wisdom. In: 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). https://doi.org/10.1109/icdcs.2017.31
12. IEEE Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 11: Wireless lan medium access control (mac)and physical layer (phy) specifications amendment 5: Enhancements for higher throughput. IEEE. https://doi.org/10.1109/ieeestd.2009.5307322
13. Xin L, Starobinski D, Noubir G (2016) Cascading denial of service attacks on Wi-Fi networks. In: IEEE Conference on Communications and Network Security (CNS), IEEE. pp 91–99
14. Eian M, Mjolsnes SF A formal analysis of ieee 802.11w deadlock vulnerabilities. IEEE. https://doi.org/10.1109/infcom.2012.6195841
15. Sheng Y, Tan K, Chen G, Kotz D, Campbell A Detecting 802.11 mac layer spoofing using received signal strength. IEEE. https://doi.org/10.1109/infocom.2008.239
16. Wang T, Yang Y Analysis on perfect location spoofing attacks using beamforming. IEEE. https://doi.org/10.1109/infcom.2013.6567087
17. Halperin D, Hu W, Sheth A, Wetherall D (2011) Tool release: Gathering 802.11n traces with channel state information. ACM SIGCOMM CCR
18. Xie Y (2015) Precise power delay profiling with commodity wifi. IEEE Trans Mobile Comput PP(99):1–1
19. Shojaie B, Saberi I, Salleh M (2017) Enhancing eap-tls authentication protocol for ieee 802.11i. Wirel Netw 23(5):1491–1508
20. Borisov N, Goldberg I, Wagner D (2001) Intercepting mobile communications: the insecurity of 802.11
21. Kaur J (2016) Mac layer management frame denial of service attacks. In: International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE). IEEE. pp 155–160
22. Bellardo J, Savage S 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions
23. Konings B, Schaub F, Kargl F, Dietzel S Channel switch and quiet attack: New dos attacks exploiting the 802.11 standard. IEEE. https://doi.org/10.1109/lcn.2009.5355149
24. Han J, Park T (2017) Security-enhanced push button configuration for home smart control. Sensors 17(6):1334
25. Guo F, Chiueh T-c Sequence number-based mac address spoof detection. In: Lecture Notes in Computer Science. Springer Berlin Heidelberg. pp 309–329. https://doi.org/10.1007/11663812_16
26. Aslam B, Islam MH, Khan SA Pseudo randomized sequence number based solution to 802.11 disassociation denial of service attack. IEEE. https://doi.org/10.1109/mcwc.2006.4375224
27. Shahzad M, Singh MP (2017) Continuous authentication and authorization for the internet of things. IEEE Internet Comput 21(2):86–90
28. Liu M, Mukherjee A, Zhang Z, Liu X (2016) Tbas: Enhancing wi-fi authentication by actively eliciting channel state information. In: 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). IEEE. https://doi.org/10.1109/sahcn.2016.7733021
29. Polak AC, Dolatshahi S, Goeckel DL (2011) Identifying wireless users via transmitter imperfections. IEEE J Sel Areas Commun 29:1469–1479. https://doi.org/10.1109/jsac.2011.110812
30. Shi Y, Jensen MA (2011) Improved radiometric identification of wireless devices using mimo transmission. IEEE Trans Inf Forensic Secur 6(4):1346–1354
31. Mathur S, Reznik A, Ye C, Mukherjee R, Rahman A, Shah Y, Trappe W, Mandayam N (2010) Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]. IEEE Trans Wirel Commun 17(5):63–70. https://doi.org/10.1109/mwc.2010.5601960
32. Hao C, Zhang Y, Wei L, Ping Z (2017) Non-cooperative wi-fi localization via monitoring probe request frames. In: Vehicular Technology Conference
33. Kotaru M, Joshi K, Bharadia D, Katti S (2015) Spotfi:decimeter level localization using wifi. Acm Sigcomm Comput Commun Rev 45(4):269–282
34. Gjengset J, Xiong J, Mcphillips G, Jamieson K (2014) Phaser: enabling phased array signal processing on commodity wifi access points. In: International Conference on Mobile Computing & Networking
35. Xiong J, Jamieson K Securearray: improving wifi security with fine-grained physical-layer information. In: ACM MobiCom'13
36. Xu M, Fang Y, Liu S, Jian S, Zhu H (2018) Sparse channel estimation for mimo-ofdm systems in high-mobility situations. IEEE Trans Veh Technol PP(99):1–1
37. Rappaport T (1996) Wireless communications: principles and practice 2. prentice hall PTR New Jersey
38. Janssen GJ, Stigter PA, Prasad R (1996) Wideband indoor channel measurements and ber analysis of frequency selective multipath channels at 2.4, 4.75, and 11.5 ghz. IEEE Trans Commun 44(10):1272–1288. https://doi.org/10.1109/26.539768
39. Abramowitz M, Stegun IA, et al. (1972) Handbook of Mathematical Functions, Vol. 1. Dover, New York
40. Yu J, Li J, Yu Z, Huang Q (2019) Multimodal transformer with multi-view visual representation for image captioning. arXiv preprint arXiv:1905.07841
41. Kuang L, Yan X, Tan X, Li S, Yang X (2019) Predicting taxi demand based on 3d convolutional neural network and multi-task learning. Remote Sens 11(11):1265
42. Salehi M, Leckie C, Bezdek JC, Vaithianathan T, Zhang X (2017) Fast memory efficient local outlier detection in data streams (extended abstract). In: 2017 IEEE 33rd International Conference on Data Engineering (ICDE). IEEE. https://doi.org/10.1109/icde.2017.32
43. Ying G, Ganesan RK, Bischke B, Bernardi A, Maier A, Warkentin H, Steckel T, Dengel A (2017) Grid-based outlier detection in large data sets for combine harvesters. In: 2017 IEEE 15th International Conference on Industrial Informatics (INDIN). IEEE. https://doi.org/10.1109/indin.2017.8104877

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.