PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks

Dan Shan, Kai Zeng, Weidong Xiang, Paul Richardson, and Yan Dong

***Abstract*—Exploiting the unique properties of the physical layer to enhance or complement authentication strength in wireless networks has attracted a lot of research attention recently. In this paper, we propose a novel PHYsical layer Challenge-Response Authentication Mechanism (PHY-CRAM) for wireless networks. PHY-CRAM is suitable for both one-way and mutual authentication. It fully utilizes the randomness, reciprocal, and location decorrelation features of the wireless fading channel, and is immune to various passive and active attacks. In the authentication procedure, challenge-response signals are exchanged at the physical layer, which allow two devices to verify their shared secrets while not revealing these secrets to attackers. PHY-CRAM adopts orthogonal frequency-division multiplexing (OFDM) technique which separately modulates the higher layer information and shared keys on subcarriers' phases and amplitudes respectively, in order to prevent channel probing from traffic-related information. We conduct extensive simulation study and develop a prototype using field-programmable gate array (FPGA) and discrete radio frequency (RF) components to evaluate PHY-CRAM in real-world environments. It shows that PHY-CRAM achieves both high successful authentication rate and low false acceptance rate in various channel conditions and under various attacks.**

***Index Terms*—Physical-layer security, challenge-response authentication, wireless channel, OFDM, FPGA.**

I. Introduction

With the rapid advancement of wireless communication technology and ever-increasing mobile applications, securing wireless communication becomes more and more important and challenging. Compared to a wired network, ensuring security in a wireless network faces greater challenges mainly due to its "open air" nature since an attacker can easily eavesdrop or intercept the wireless communication channel. On the flip side, the inherent and unique properties of the wireless physical layer can be exploited to enhance the wireless network security. There has been an increasing interest in complementing or enhancing authentication in wireless networks by exploiting physical layer characteristics [1]–[10]. Physical layer authentication/identification benefits a number of wireless applications such as forensics [11], identity-based attack detection [12], access control [13], malfunctioning detection [14], and tracking [15] etc.

Manuscript received November 11, 2012, revised March 10, 2013 and April 30, 2013. This material is based upon work partially supported by the US National Science Foundation CAREER award under Grant Number (CNS-1149500), and NSFC-MSRA joint fund (60933012).

D. Shan, K. Zeng, W. Xiang, and P. Richardson are with the ECE and CIS Departments, University of Michigan — Dearborn, Dearborn, MI, 48128 USA (e-mail: {danshan, kzeng, xwd, richarpc}@umd.umich.edu).

Y. Dong is with Department of Electronics and Information Engineering Huazhong University of Science and Technology, Wuhan 430074, China (e-mail: dongyan@mail.hust.edu.cn).

Digital Object Identifier 10.1109/JSAC.2013.130914.

In this paper, we propose a novel physical layer challenge-response authentication mechanism (PHY-CRAM) for wireless and mobile applications. Being different from encryption based challenge-response authentication techniques, PHY-CRAM exchanges unencrypted shared secrets among participants. These shared secrets are masked by a random number and the channel fading, while the verifier is able to verify the secrets without knowing the channel state information (CSI) owing to a reverse operation in the response signal and channel reciprocity. An attacker, on the other hand, cannot experience exactly the same channel fading as any legitimate user experiences due to location distinction, and can hardly learn the shared secrets. Since PHY-CRAM does not need to estimate CSI, the training and synchronization sequences in the header are eliminated; this feature prevents the attackers from probing the channel and increases security strength.

The security strength of PHY-CRAM depends on the randomness of the fading channel and the relative geographic location between the attacker and legitimate users, but not depends on the computation complexity. That is, even when the attacker's computational power is increased, PHY-CRAM does not need to increase its key length in order to maintain the same security strength, as long as the channel randomness is remained. However, conventional authentication schemes (such as CRAM-MD5 [16] and CHAP [17]), usually require longer keys to maintain a desirable computational security strength if the attacker's computing power improves. Longer keys usually imply higher computation overhead, communication overhead, energy consumption, and storage overhead, which are not desirable in resource constrained networks, such as sensor and mobile networks. PHY-CRAM does not intend to replace the existing conventional challenge-response authentication protocol, but serves as an alternative that does not depend on computational security.

PHY-CRAM features another unique characteristic that, it eliminates channel coding, channel estimation and frequency offset compensation for most messages during the challenge-response authentication. This feature does not only simplifies the baseband design, but also prevents the attackers from probing the channel and provides better security strength.

PHY-CRAM is also unique compared to other existing physical layer authentication mechanisms. Different from the existing RF fingerprinting schemes [6]–[8], [18], PHY-CRAM is immune to impersonation attacks, it does not require a high end signal analyzer, and it favors dynamic environments. Compared to wireless channel based authentication [1]–[5], it does not require the legitimate user to be at a specific location and does not need channel estimation or training. PHY-CRAM is also different from signal watermarking [9], [10], which conveys a cryptographically secure digital signature along with

the primary transmission by superposition or superimposing. In short, PHY-CRAM is simple, secure, robust, and flexible, and can be applied in any wireless networks for authenticating nodes that share a secret without requirement of any auxiliary instruments, channel estimation or being at a specific location.

We summarize our major contributions as follows:

- In section IV, we propose a novel physical layer challenge-response authentication mechanism in wireless networks, PHY-CRAM, which is suitable for both one-way and mutual authentication.
- We conduct extensive simulation to evaluate the performance of PHY-CRAM under different channel conditions and signal to noise ratios (SNRs), as reported in subsection VI-A.
- We develop a prototype using FPGA and discrete RF components and conduct real-world experiments to evaluate PHY-CRAM in various indoor and outdoor environments and under various channel conditions, as reported in subsections VI-B and VI-C.
- The security strength of PHY-CRAM is analyzed and evaluated under various attacks in section V.
- Comparison to traditional challenge-response mechanism is discussed in section II.

Throughout the paper, $()^T$, $()^H$ and $\odot$ denote transpose, conjugate transpose, and element-wise multiplication, respectively.

II. Related Works

A. RF Fingerprinting for Device Identification

RF fingerprinting exploits the transceiver hardware impairments to identify different wireless devices. Two main approaches of RF fingerprinting are introduced in the literature: transient-based methods [6] and modulation-based methods [7]. The former one identifies devices according to the transient behaviour of the device's amplifier when switching from the idle state to transmission state, while the latter one applies the imperfection of the modulated signal.

It was recently found that RF fingerprinting is vulnerable to impersonation attack [8], while PHY-CRAM is immune to such attack.

B. Wireless Channel Based Authentication

Wireless channel based authentication is based on the fact that the CSI is location-specific due to path loss and channel fading [2], [3]. This type of authentication requires a legitimate user to be authenticated at a specific location. It might not work well in a highly dynamic environment where the channel state changes drastically over time due to fading or mobility. The authentication algorithm may need a large number of samples to ensure a desirable performance. It is also subject to mimicry attacks [19] where an attacker can gain the legitimate channel information when it is close to the legitimate devices. A recent remedy is proposed to prevent mimicry attacks, but it requires time synchronization among legitimate parties [5].

Time correlation property of the wireless channel is also exploited to support message authentication in time-varying channels [1], [4]. This kind of authentication checks the message authenticity during a communication session, while it assumes that the very first messages (frames) are already authenticated.

PHY-CRAM does not require the legitimate user be at a specific location, and eliminates channel profile training/probing. Moreover, PHY-CRAM utilizes the randomness of the fading channel to hide the shared secret used for authentication, while channel based authentication decides if the frames are sent from the same channel or not.

C. Physical Layer Signal Watermarking

Physical layer signal watermarking or fingerprinting is a mechanism to convey a cryptographically secure authentication code or tag along with the primary transmission or message [9], [10]. General signal watermarking through low-power perturbations of the signal constellation is proposed in [9].

From methodology point of view, PHY-CRAM is different from signal watermarking since it does not add any authentication code or tag into the signal. From applicability point of view, PHY-CRAM initializes a secure communication, while signal watermarking applies to message authentication during communication.

D. Key Generation from Wireless Channel

PHY-CRAM is different from physical layer key generation [20]–[23] although they are based on common physical layer foundations (i.e., channel reciprocity, randomness, and location decorrelation). First, they serve for different purposes. The former is for authentication and the latter is for shared key generation. Second, PHY-CRAM exploits the reciprocity to "decrypt" the shared secret used for authentication, while wireless channel key generation relies on the reciprocity to ensure highly similar channel states observed by the two key generation parties. Furthermore, PHY-CRAM does not need to sound the channel explicitly or to reconcile the key disagreement.

III. System Setup

A. Application Model

We consider a wireless network with I legitimate users B_i, $i = 0, ..., I-1$. Node pairs that need to authenticate each other share a set of secrets. For example, in a wireless local area network (WLAN), the access point shares different secret keys with each client. Specifically, the shared keys (bit strings) between B_j and B_k are denoted as $\{\mathbf{X}_j^{(j,k)}, \mathbf{X}_k^{(j,k)}\}$, where $\mathbf{X}_j^{(j,k)} := [X_{0,j}^{(j,k)}, ..., X_{M-1,j}^{(j,k)}]^T$, $X_{m,j}^{(j,k)} \in \{0,1\}$ $(m = 0, ..., M-1)$ is the $(m+1)$th bit, and M is the key length. $\mathbf{X}_k^{(j,k)}$ follows the same definition. For one-way authentication, only one key is necessary, while for mutual authentication, two keys are used. For simplicity, we drop the index $^{(j,k)}$ whenever there is no misunderstanding.

Security of the system relies on the secrecy of $\{\mathbf{X}_j, \mathbf{X}_k\}$. If an attacker knowns $\{\mathbf{X}_j, \mathbf{X}_k\}$, it has the ability to impersonate either B_j or B_k.

B. Communication Model

A frequency band with bandwidth W is occupied by the wireless network, where the users who want to authenticate

each other are within their communication ranges. Orthogonal frequency-division multiplexing (OFDM) is adopted as the physical layer technique, since it enjoys high spectrum efficiency and good immunity to multipath, and can utilize the reciprocal feature of wireless channels easily. Each channel associates with a channel coherence time T_C, below which the channel is considered as temporally correlated. Define N and L as the number of subcarriers and length of cyclic prefix (CP) in OFDM modulation, respectively. Then the subcarrier spacing equals to W/N. A proper design on the system guarantees that N and L are large enough to overcome frequency-selective fading, while N is also small enough to overcome the Doppler shifts in mobile environments [24].

C. Attacker Model

We assume a very powerful attacker E, who knows all the communication protocols and authentication schemes adopted in the network. Besides, E is able to monitor and replay any messages and signals sent in the network. E may be very close to a legitimate user, say just one or few wavelengths away from legitimate users. However, E does not know $\{\mathbf{X}_j, \mathbf{X}_k\}$. E's goal is to pass the authentication with legitimate user(s).

IV. The Physical Layer Mutual Authentication Mechanism: PHY-CRAM

A. The Basics

PHY-CRAM is realized by transmission and reception of a few frames between two participants. All these frames have (K_1+K_2) OFDM symbols. The first K_1 symbol is modulated with differential phase shift keying (DPSK) scheme, and contains binary data regarding the traffic information and user information, like frame type, media access control (MAC) address, and time stamp etc (referred to as traffic information). Due to the importance of traffic information, data interleaving, convolutional encoding and cyclic redundancy check (CRC) are adopted. We randomize the amplitude of each subcarrier since equal power level reveals CSI to the attacker, while CSI is not required to demodulate DPSK signal.

The last K_2 symbols in each frame carry PHY-CRAM information, which contains the shared keys $\mathbf{X}_j$ and $\mathbf{X}_k$, as well as a set of random values D_n. PHY-CRAM information may be repeated for several times to resist noise. For simplicity, we assume that both traffic information and PHY-CRAM information can be accommodated in a single OFDM symbol (however, PHY-CRAM is not confined to this condition). As a result, $K_1 = 1$ and K_2 equals to the number of repetitions for PHY-CRAM information, and the corresponding frame structure is shown in figure 1.

Note that the DPSK modulation for traffic information does not require at least two OFDM symbols or an "initial" OFDM symbol with pre-known phase information, since the differential encoding can be conducted subcarrier-by-subcarrier [25]. Taking DBPSK as an example, the phase difference between subcarrier 10 and subcarrier 11 carries one bit, while the phase difference between subcarrier 12 and subcarrier 13 carries another bit (all these subcarriers are within one OFDM symbol). Since the subcarrier spacing is designed to be much smaller than the coherence bandwidth, the channel responses

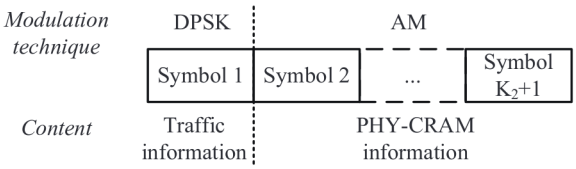


Fig. 1. Frame structure of PHY-CRAM messages

on two adjacent subcarriers are highly correlated. The phases at subcarriers 10 and 12 may be randomized to further increase the security strength.

Based on the communication model given in subsection III-B, Doppler spread caused by relative speed between two participants are neglected, and there is no inter-carrier interference (ICI) in the system. As a result, the OFDM system can be considered as the superposition of N independent narrow band subsystems that experience flat-fading channels, and each subsystem is modelled simply by

$$Y_n = H_n X_n + W_n, n = 0, ..., N-1 \tag{1}$$

where Y_n and X_n denote the frequency-domain symbol at receiver (Rx) and transmitter (Tx), respectively, W_n the additive white Gaussian noise (AWGN), and H_n the frequency-domain channel response, all at subcarrier n. Due to its simplicity, frequency-domain representation is used throughout the paper.

Without loss of generality, we map the M-length shared key $\mathbf{X}_j$ or $\mathbf{X}_k$ onto the subset of subcarriers with M smallest indices; for example, $X_{0,j}$ is mapped onto subcarrier 0, and $X_{M-1,j}$ onto subcarrier $M-1$ etc. Then the index n in $X_{n,j}$ or $X_{n,k}$ denotes both the subcarrier index and bit location.

B. The Authentication Procedure

We use subcarrier n to show the basic principle of PHY-CRAM, with two participants B_j and B_k. Without loss of generality, assume that B_k wants to start a conversation with B_j. The mutual authentication between them contains three stages as shown in figure 2.

In stage 0, B_k sends an "authentication request" frame to B_j. The frame contains only traffic information, so only symbol 1 is used. All the information in this frame is not encrypted. This frame does not reveal CSI information to the attackers, since there is no pilot or synchronization header and the amplitudes of all subcarriers are randomized.

After receiving the authentication request, B_j authenticates B_k in stage 1. If B_k passes the authentication, B_j will also be authenticated by B_k (actually B_k does not need to know the result in stage 1, but can always send challenge to start the authentication; however, B_j responds to this challenge only if B_k passes the authentication in stage 1). The mutual authentication succeeds if and only if both stage 1 and stage 2 show positive results. One-way authentication can be realized by only applying stage 0 and stage 1.

During stages 1 and 2, a typical challenge-response procedure is defined. Detailed steps of stage 1 are shown in figure 3, while those of stage 2 can be derived by switching two participants. These steps include:

Step (1) At time t_1, B_j uses a random number D_n within the range $[K_3, K_4]$ to modulate amplitudes of subcarriers in

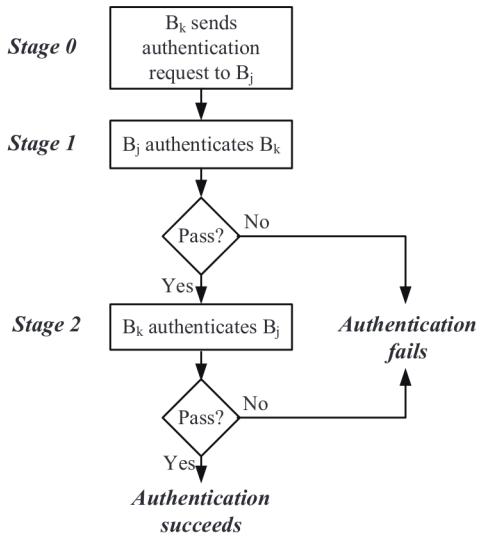


Fig. 2. Basic procedure of PHY-CRAM

the last K_2 OFDM symbols, where $0 < K_3 < 1 < K_4$, and transmits the resulting frame to B_k. Here D_n is a random number with the purpose to prevent the attacker from probing the channel. This frame is actually a challenge for authentication.

Step (2) B_k receives $D_n H_{jk,n} + W_n^{(1)}$, where $H_{jk,n}$ denotes the wireless channel between B_j and B_k at the n^{th} subcarrier, and $W_n^{(1)}$ the AWGN. As a response to the challenge, $\mathcal{M}(X_{n,k})/(D_n H_{jk,n} + W_n^{(1)})$ is transmitted by B_k at time t_2, where $X_{n,k}$ is the n^{th} element in $\mathbf{X}_k$ and $\mathcal{M}(\cdot)$ denotes a constellation mapping scheme. The shared key $\mathbf{X}_k$ is masked by the wireless channel $H_{jk,n}$. At time t_3, this frame arrives at B_j , who authenticates B_k according to its received signal. Both B_j and B_k should do these processing fast enough to ensure that $t_3 - t_1 \ll T_C$.

The signals defined in these two steps as shown in figure 3 are classified as PHY-CRAM information, and are modulated on the last K_2 OFDM symbols. Similar to the "authentication request" frame, traffic information in stage 1 and stage 2 is carried in the first OFDM symbol.

The constellation mapping scheme $\mathcal{M}(\cdot)$ is defined as

$$\mathcal{M}(x) = \begin{cases} K_3, x = 0 \\ K_4, x = 1 \end{cases} \tag{2}$$

which maps the binary values to positive real values K_3 or K_4. In other words, we adopt amplitude modulation (AM) for PHY-CRAM information, while K_3 and K_4 determine both the randomness of D_n and the euclidean distance of the constellation. The ratio K_4/K_3 should be large enough to hide the CSI, while too large value of K_4/K_3 leads to high transmission power at some subcarriers. In practice, $[K_3, K_4]$ should have the similar range as the channel fading (the normalized value of $H_{jk,n}$) has. For example, if the largest channel gain is 10 dB larger than the smallest channel gain on all subcarriers, it is appropriate to set $K_3 = 0.5$ and $K_4 = 1.5$.

The key feature of this authentication mechanism is that, the shared key $X_{n,k}$ is secured by the wireless channel which is cancelled out at the verifier, and only the verifier can derive $X_{n,k}$ in multipath environments.

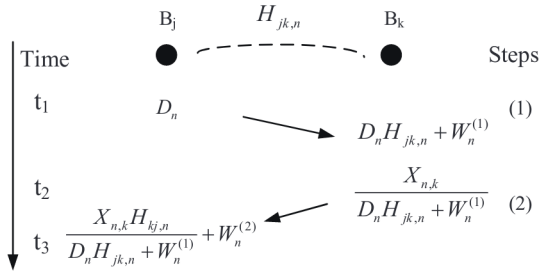


Fig. 3. Detailed steps in stage 1 of PHY-CRAM

We denote the symbols at subcarrier n in step u before and after transmission as $T_n^{(u)}$ and $R_n^{(u)}$, respectively. For example,

$$R_n^{(2)} = \frac{X_{n,k} H_{kj,n}}{D_n H_{jk,n} + W_n^{(1)}} + W_n^{(2)}. \tag{3}$$

In real systems, all the signals modulated on subcarriers are complex values, with real and imaginary parts represented by I-branch and Q-branch respectively. However, phases of all signals defined in steps (1) and (2) are useless, since they adopt AM modulation. Therefore, all the notations defined in this section represent their absolute values.

All frames in the authentication procedure do not contain any pre-known synchronization header, pilots or reference signals. Timing and frequency synchronization to these frames at the receiver are realized simply through autocorrelation on CP [26]. Throughout the procedure of PHY-CRAM, channel estimation is never needed.

C. The Verification Scheme

In step (2) of stage 1, B_j needs to verify that whether the counterpart is legal or not through the response received, while B_k meets exactly the same problem in stage 2. So we only take B_j as an example.

To enhance the signal quality, B_j combines the received signals on all subcarriers, and get

$$\mathbf{R}^{(2)} := [R_0^{(2)}, ..., R_{M-1}^{(2)}]^T. \tag{4}$$

Moreover, B_j knowns $\mathbf{X}_k$ since it is the shared key. Then B_j wants to verity the identity of B_k through comparison between $\mathbf{R}^{(2)}$ and $\mathbf{X}_k$. To be precise, we define this problem as follows:

$Problem\ 1$: Given $\mathbf{R}^{(2)}$ and $\mathbf{X}_k$, make a decision on whether frame (2) is sent from B_k or not.

To solve this problem, we first ignore the noise, and make an approximation that $H_{kj,n} = H_{jk,n}$. Then (3) becomes

$$R_n^{(2)} = \frac{X_{n,k}}{D_n} \tag{5}$$

where $n \leq M - 1$, and (4) becomes

$$\mathbf{R}^{(2)} = \left[\frac{X_{0,k}}{D_0}, ..., \frac{X_{M-1,k}}{D_{M-1}} \right]^T. \tag{6}$$

Then we get the following relationship

$$\mathbf{R}^{(2)} \odot \mathbf{D} = [X_{0,k}, ..., X_{M-1,k}]^T = \mathbf{X}_k \tag{7}$$

where $\mathbf{D} := [D_0, ..., D_{M-1}]^T$ is known by B_j (since $\mathbf{D}$ is generated by B_j), while the unknown channel responses $H_{kj,n}$ and $H_{jk,n}$ cancel each other.

With existence of low noises and slight difference between $H_{kj,n}$ and $H_{jk,n}$, $\mathbf{R}^{(2)} \odot \mathbf{D}$ and $\mathbf{X}_k$ are not exactly the same, but should be similar. Therefore, a straightforward solution to $Problem\ 1$ is to check the Euclidean distance between $\mathbf{X}_k$ and $\mathbf{R}^{(2)} \odot \mathbf{D}$:

$Solution\ 1$: Frame (2) is sent from B_k if and only if $||\mathbf{R}^{(2)} \odot \mathbf{D} - \mathbf{X}_k|| < C_0$, where C_0 is a constant real number. □

However, it is hard to determine C_0, since bounding Euclidean distance is hard. On the other hand, the value of cross-correlation is tightly bounded between [0,1]. Then we define $\bar{\mathbf{R}}_\mathbf{D}$ and $\bar{\mathbf{X}}_k$ as mean values of $\mathbf{R}^{(2)} \odot \mathbf{D}$ and $\mathbf{X}_k$ respectively, and give another solution:

$Solution\ 2$: Frame (2) is sent from B_k if and only if

$$\frac{(\mathbf{R}^{(2)} \odot \mathbf{D} - \bar{\mathbf{R}}_\mathbf{D})^H \cdot (\mathbf{X}_k - \bar{\mathbf{X}}_k)}{||\mathbf{R}^{(2)} \odot \mathbf{D} - \bar{\mathbf{R}}_\mathbf{D}|| \cdot ||\mathbf{X}_k - \bar{\mathbf{X}}_k||} < C_1 \tag{8}$$

where C_1 is a constant real number. □

The value of parameter C_1 in $Solution\ 2$ must be selected properly in order to get a balance between the successful authentication rate β (the rate that a legitimate user passes the authentication) and false acceptance rate α (the rate that an attacker passes the authentication). We will use receiver operating characteristic (ROC) to evaluate PHY-CRAM's performance.

D. Peak Reduction

Let's focus on the response $T_n^{(2)} := \mathcal{M}(X_{n,k})/(D_n H_{jk,n} + W_n^{(1)})$ sent by B_k in step (2) of stage 1. The absolute value of $T_n^{(2)}$ may be extremely large if (1) $\mathcal{M}(X_{n,k}) = K_4$, (2) $D_n = K_3$ and (3) $H_{jk,n}$ experiences deep fading ($|H_{jk,n}| \ll 1$). The probability that these three conditions occur simultaneously is low; as a result, the number of high peaks is small compared to the number of subcarrier N. However, a few high peaks at frequency-domain may not be preferred by some communication systems.

We solve the high-peak issue by adding a peak reduction operation defined as follows:

$$\widetilde{T}_n^{(2)} = \begin{cases} T_n^{(2)}, & if\ |T_n^{(2)}| \le A_{\max} \\ A_{\max} T_n^{(2)}/|T_n^{(2)}|, & otherwise \end{cases} \tag{9}$$

where $\widetilde{T}_n^{(2)}$ denotes the signal after peak reduction, and $A_{\max}$ denotes the maximum allowable amplitude of the signal at any subcarrier.

In (9), all the high peaks are cut off, and channel effects at corresponding subcarriers (named bad subcarriers) may not be cancelled out. In this case we consider that the information carried by bad subcarriers are random values rather than (part of) the shared key. Since all subcarriers are independent, good subcarriers which do not have high peaks still contribute to the verification scheme, while happening of high peaks only reduces the effective length of shared key.

E. Effect of timing offset

When CP is used for timing synchronization, timing offset is more serious, since the peak of CP-correlator is smooth. Performance of traditional OFDM systems is not affected as long as the timing offset plus channel delay spread (in number of samples) does not exceeds L (we call this kind of timing offset as "tolerated timing offset"), since the effect of timing offset is absorbed by channel estimation [27]. Now we analyse the effect of tolerated timing offset to PHY-CRAM where channel estimation is absent.

Assume that the timing offset at B_k in step (1) and at B_j in step (2) are δ_k and δ_j respectively. Then according to [28], the equivalent channel response from B_j to B_k, and from B_k to B_j, are $H'_{jk,n} = H_{jk,n} e^{j2\pi\delta_k/N}$ and $H'_{kj,n} = H_{kj,n} e^{j2\pi\delta_j/N}$ respectively. Then in the ideal case of static channel with no noise, (6) changes to

$$\mathbf{R}^{(2)'} = [\frac{X_{0,k}}{D_0} e^{j2\pi(\delta_j-\delta_k)0/N}, ..., \frac{X_{M-1,k}}{D_{M-1}} e^{j2\pi(\delta_j-\delta_k)(N-1)/N}]^T \tag{10}$$

which has the same amplitude but different phase compared with (6). As only the amplitude of PHY-CRAM information is used for further processing, performance of the verification scheme (either $Solution\ 1$ or $Solution\ 2$) with tolerated timing offsets at either B_j or B_k is not affected.

Tolerated timing offset degrades the performances of higher-order DPSK modulations, like differential quadrature phase shift keying (DQPSK) or differentially encoded 8-phase shift keying (D8PSK). As a result, DBPSK is recommended if differential encoding is conducted at frequency-domain. On the flip side, if differential encoding is conducted at time-domain [29], higher-order DPSK modulations may be adopted, with the restriction that $K_1 \ge 2$.

Once time offset δ_k or δ_j exceeds L (named large timing offset), signal quality is reduced dramatically, and CRC in symbol 1 may be wrong; we classify this situation as frame drop/error, rather than timing offset. The work in [26] shows that such large timing offset seldom happens when SNR is higher than 3 dB, while PHY-CRAM and most other authentication schemes running in wireless environments require that SNR is no less than 10 dB according to our experiments. Therefore, the effect of large timing offsets is negligible.

F. Effect of frequency offset

Frequency offset comes from two sources: LO drift between Tx and Rx, and Doppler effect. It imposes two impairments to OFDM systems: ICI and phase shifts [30]. Most short range OFDM systems have large subcarrier spacing, which is much bigger than frequency offset caused by LO drift and Doppler shift. For example, the WiFi system features subcarrier spacing of 312.5 KHz, while the frequency offset mentioned above is at the level of 3 KHz. As a result, ICI can been ignored in such system. Due to the same reason analysed in subsection IV-E, phase shifts caused by either timing offset or frequency offset do not affect PHY-CRAM. Therefore, frequency offset estimation and compensation are unnecessary in PHY-CRAM. The real-world testing we conduct show good results without frequency offset compensation.

V. Analyses on the Attacks

To evaluate the security strength of PHY-CRAM, we analyse various types of attackers in this section. Without loss of generality, we only take subcarrier n for example.

A. Passive attackers

A passive attacker E_P only monitors all frames inside the network during authentication, and tries to learn $\{\mathbf{X}_j, \mathbf{X}_k\}$ from whatever it gets. If E_P learns something in $\{\mathbf{X}_j, \mathbf{X}_k\}$, it may initiate an authentication procedure with some users; however, as long as E_P is silent during legitimate users' authentication procedure, it is still considered as passive.

Stage 0 does not need to be secured, since it does not reveal the shared key or CSI.

As shown in figure 3, stages 1 and 2 are symmetrical with each other and undergo the same passive attacks. Therefore, we only analyse stage 1.

We first assume that E_P is not too close to B_j and B_k, so that h_{jk}, h_{jE} and h_{kE} are all uncorrelated (case 1). The noises at E_P's receiver are ignored. Then all the frames received by E_P, except "link set up request" which contains no information about the shared keys, are

$$R_{E,n}^{(1)} = D_n H_{jE,n} \tag{11}$$

and

$$R_{E,n}^{(2)} = \frac{X_{n,k} H_{kE,n}}{D_n H_{jk,n} + W_n^{(1)}} \tag{12}$$

where $H_{jE,n}$ and $H_{kE,n}$ denote the wireless channels between B_j and E_P, and between B_k and E_P, respectively. In (11) and (12), five unknown factors exist in two equations, despite of the noise. Therefore, there is no way for E_P to derive $\mathbf{X}_k$.

Then we consider two more aggressive cases that, E_P is very close to B_j (case 2) or B_k (case 3), respectively. Then besides (11) and (12), E_P gets more information. For case 2, it gets

$$H_{jE,n} \approx 1 \tag{13}$$

because the direct path between E_P and B_j is much stronger than any multipath if they are very close to each other, and

$$H_{jk,n} \approx H_{kE,n} \tag{14}$$

which is obvious.

Combing (9) to (12) and ignoring the noise, we have

$$X_{n,k} \approx R_{E,n}^{(1)} R_{E,n}^{(2)} \tag{15}$$

and interestingly, for case 3, we get the same result as in (15).

As a result, E_P is able to get a rough estimate on $\mathbf{X}_k$ through what it hears in both case 2 and case 3. It seems dangerous to PHY-CRAM. However, E_P cannot be too close to B_j or B_k, since each radio occupies a certain area of space. Furthermore, $\mathbf{X}_k$ estimated by E_P is very noisy due to the approximation in (13) and (14), while B_k has perfect information about $\mathbf{X}_k$. Therefore, the attacker E_P is still identifiable.

A passive attacker is able to derive part of the information in $\mathbf{X}_k$ from channel correlation among adjacent subcarriers. We consider this as a truncation to the shared key. Actually if we modulate shared keys on a selected set of subcarriers with a spacing bigger than the coherence bandwidth, a passive attacker will learn nothing about $\mathbf{X}_k$ through channel correlation.

Note that the traffic-related information, like MAC addresses and package type etc, is DPSK modulated (with randomized amplitudes), while the PHY-CRAM information containing shared keys is AM-modulated. Therefore, the traffic information, which is easy to be captured by passive attackers, reveals only (part of) the wireless channel's phase information, which cannot be used to estimate shared keys.

B. Active attackers

A passive attacker E_A may transmit messages during legitimate users' authentication procedure to facilitate his attacks.

If an attacker initiates stage 0 (sends authentication request to B_j), it will be authenticated by B_j in stage 1, and it can hardly succeed since it does not have the shared key. On the other hand, stage 1 is more vulnerable than the other two stages, since during stage 0 B_k does not know the legality of its counterpart. After procedure 1 is finished successfully, B_j will know that whether B_k is legal or not, and any further response to B_k is safe. Therefore, a threat to PHY-CRAM comes from step (2) in procedure 1, since B_k needs to identify whether the challenge is sent from B_j or not.

We first assume that all users are active and will respond to all requests timely. Therefore, in step (1) B_j will definitely send a challenge. Moreover, since the channel is symmetrical in two directions, B_j is able to adjust its transmission power properly to guarantee a nearly constant SNR at B_k, with the help from its received signal's SNR at stage 0. The underlying assumption here is that, in stage 0 the transmission power of B_k must be constant (transmission power on each subcarrier is random, but the overall transmission power is constant). In this way, any active attacks during step (1) or (2) can be easily detected. For example, if E_A tries to overcast B_j's signal by using high transmission power, B_k detects the attack directly; on the other hand, if E_A maintains the signal at the same power level, it cannot effectively modify the challenge information as it wants. Note that due to the absence of any pre-known signal contained in all OFDM symbols, there is no way for E_A to estimate the channel between itself and B_k so as to modify the challenge signal precisely; the only way E_A can modify the challenge is to overcast it by high transmission power. As a result, PHY-CRAM is still safe facing active attackers.

In case that B_j does not send respond to B_k timely, E_A may take the role of B_j successfully, and steal $\mathbf{X}_k$ from the response of B_k. We solve this problem by sharing two distinguished keys, $\mathbf{X}_j$ and $\mathbf{X}_k$, between B_j and B_j. After B_k has been authenticated by B_j, B_k also authenticates B_j; if B_j cannot provide a valid response, B_k would consider that its shared key has been compromised and revoke it. Moreover, E_A cannot actively steal the shared key since it impersonates B_j; it can only wait for other users to initiate the conversation, as shown in figure 2.

The active attack introduced in [31] requires that both participants in the authentication procedure send pre-known sounding signals. However, in PHY-CRAM, the sounding signals D_n are random signals, so neither two participants nor attackers can derive CSI.

C. Impersonation attacks

Although impersonation attacks [8] belong to active attacks, it is emphasized here due to its significant threat to other

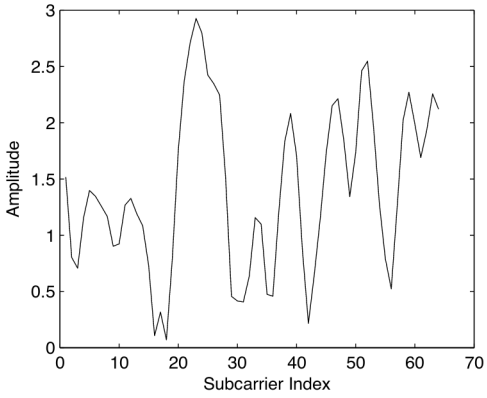


Fig. 4. Amplitude of the frequency-domain channel response $|H_{jk,n}|$ in urban channel over subcarrier index

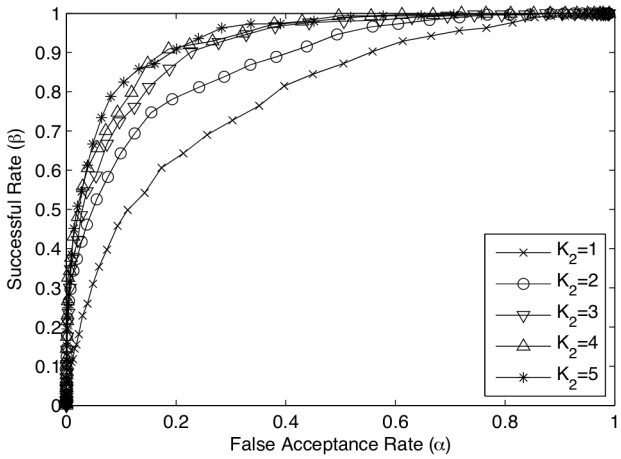


Fig. 5. ROC curves of PHY-CRAM for one-way authentication in rural channel derived by simulation, with various settings for K_2

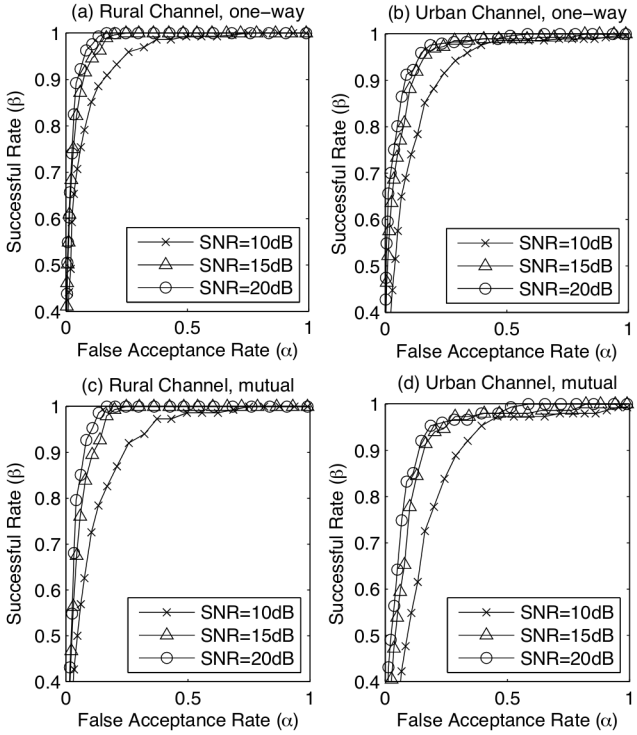


Fig. 6. ROC curves of PHY-CRAM for one-way (a)(b) and mutual (c)(d) authentication under rural channel (a)(c) and urban channel (b)(d) derived by simulation, with key length M = 40

physical-layer security schemes [6], [7], [13], [18]. Two kinds of impersonation attacks, signal replay attack and feature replay attack, are analysed here.

In a signal replay attack, the attacker E stores the waveforms shown in (11) and (12), and use (10) to impersonate B_k. However, E cannot succeed because the challenge sent from B_j contains a random number D_n.

Feature replay attack is also similar to "mimicry attack" as introduced in [5]. This attack cannot succeed due to the same reason that no training or synchronization sequences exist in PHY-CRAM.

VI. Performance Evaluation

SNR determines the signal quality of PHY-CRAM information, while channel fading characteristics affect the number of high peaks and the effective length of shared key. We evaluate how these two factors affect PHY-CRAM's performance by computer based simulations.

Randomness of the channel over space determines the performance of PHY-CRAM under passive attacks and feature replay attacks, while processing delay determines reciprocal property of the wireless channel. These factors are closely related with channel's spatial and temporal correlation characteristics, as well as implementation issues. As a result, we design a prototype for PHY-CRAM and conduct extensive real-world testing in various channel environments to evaluate these factors.

A. Simulation Results

We conduct Monte Carlo simulation to get an initial estimate on the performance of PHY-CRAM with respect to noises, multipaths, the number of repetitions K_2, and key length M, while W, N and L are fixed at 10 MHz, 64 and 16, respectively. There are 100 pairs of legitimate users. The rural/urban channels defined in [32] are selected as channel models, with 10/20 multipaths, fixed amplitudes and random phase shifts. Maximum delay spread of two channels equal to 0.528 μs and 2.14 μs, respectively, the latter of which exceeds the length of CP adopted in the simulation. In other words, we select a very bad urban channel in order to evaluate the effect of deep fading to PHY-CRAM's performance.

Figure 4 plots a snapshot of the frequency-domain channel response's amplitudes ($|H_{jk,n}|$) in urban channel, where most amplitudes fall in the range of $[0.5, 2.5]$. The fading condition in rural channel is much better. As a result, we set $K_3 = 0.5$, $K_4 = 2.5$ and $A_{max} = 5$ in the simulations.

Performance of PHY-CRAM is represented by ROC, which reflects successful authentication rate β versus false acceptance rate α. The performance of both one-way authentication (stages 0 and 1) and mutual authentication (stages 0, 1 and 2) are evaluated. For both cases, legitimate users use shared keys for authentication, while a naive attacker generates length-M random vectors for authentication.

The performance of PHY-CRAM with respect to K_2 is shown in figure 5, where all ROC curves are derived in the rural channel with SNR=10 dB and $M = 30$. It is shown that, the performance enhancement is not obvious when $K_2 > 3$.

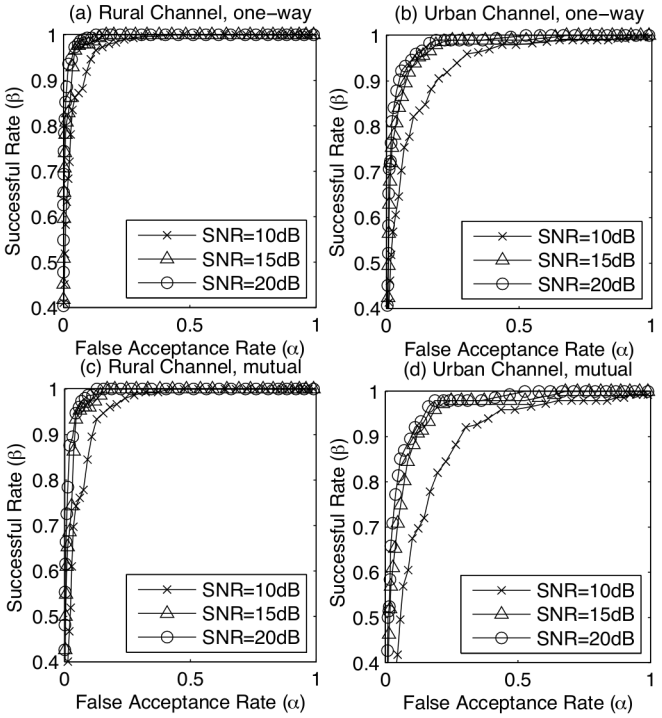


Fig. 7. ROC curves of PHY-CRAM for one-way (a)(b) and mutual (c)(d) authentication under rural channel (a)(c) and urban channel (b)(d) derived by simulation, with key length M = 60

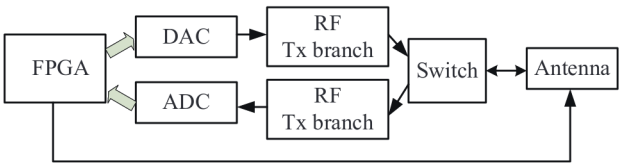


Fig. 8. Block diagram of the prototype

Since larger K_2 leads to larger energy consumption, we set $K_2 = 3$ in the following simulations.

Figures 6 and 7 plot the ROC curves for one-way and mutual authentication under rural and urban channels with key length M = 40 and 60, respectively. As expected, larger M and higher SNR lead to better results. In both channels, the performance is very good when $M = 60$ and SNR ≥ 15 dB.

B. Design of the Prototype

The prototype contains MAC, baseband and radio frequency (RF) designs. Baseband signal processing algorithms and MAC protocol are realized on a field-programmable gate array (FPGA) platform to ensure low latency. Block diagram of the prototype is given in figure 8. The FPGA features 120K logic elements, 4M memory, 288 multipliers and 531 I/O pins, and is mounted on a Terasic Cyclone III development board which is connected to a daughter board containing ADC and DAC. Analogue inputs/outputs of the daughter board are connected to Rx/Tx branch of RF circuits, which are designed using discrete RF components. These two branches are connected to a switch to realize a half duplex transceiver. On/off state of the switch is controlled by FPGA through I/O pins.

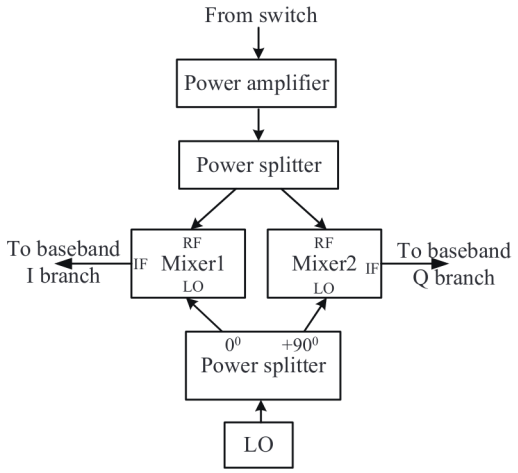


Fig. 9. Receiver branch of RF circuits designed by discrete RF components

Principle of the Rx branch in the RF circuits is shown in figure 9. The RF signal from switch is amplified by one or two low-noise amplifiers (LNAs), split into two identical streams, and sent to the 'RF' ports of two mixers, respectively. Meanwhile, the carrier signal from signal generator (the LO) is sent to another power splitter with 90° phase shift between two outputs, in order to get in-phase and quadrature carriers for mixers. Then baseband signals with real part (I-branch) and imaginary part (Q-branch) can be derived from the 'IF' ports of two mixers. The Tx branch has the same structure as that of the Rx branch with different signal directions. The system operates on 2412 MHz. Transmission power for all frames is between -5 dBm to 5 dBm according to the distance between Tx and Rx.

C. The Real-world Testing

We conduct extensive real-world testing using the prototype to further evaluate PHY-CRAM's performance. Four channel types are considered: line-of-sight (LOS) with 3-meter distance between Tx and Rx (LOS-3m), LOS-6m, non-line-of-sight (NLOS) with 6-meter distance (NLOS-6m), and LOS-28m. The first three channels are inside of a garage with a truck and metal roof, while the last one locates at a courtyard with concrete ground and is surrounded by walls. Radios of legitimate users use CP for timing synchronization, while do not conduct frequency offset estimation or compensation. Two sets of prototype act as B_j and B_k respectively, while other two sets of prototype act as two attackers, who mount their antennae 10 m and 0.1 m away from B_j respectively. B_k starts the conversation and is identified by B_j, as introduced in subsection IV-B. During the authentication procedure, attackers record all the frames and try to figure out $\mathbf{X}_k$. The nearby attacker estimates $\mathbf{X}_k$ according to (15) (we call it smart attacker), while the far away attacker generates values for $\mathbf{X}_k$ randomly (we call it naive attacker).

We test 99 different legitimate users with one pair of radios by changing the software running on FPGA, while each user's authentication procedure is repeated for 5 times. The successful authentication rates for all users in all runs in a certain channel are averaged, while results belonging to

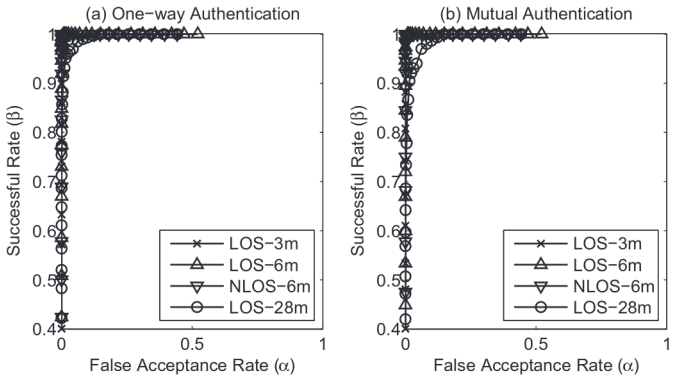


Fig. 10. ROC curves of PHY-CRAM for one-way (a) and mutual (b) authentication derived from real-world testing under four channels, with existence of a naive attacker

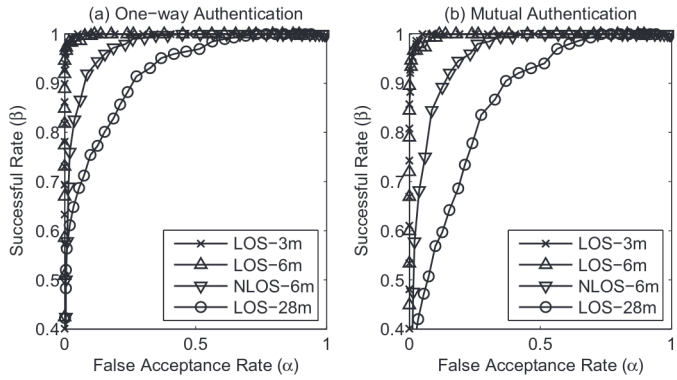


Fig. 11. ROC curves of PHY-CRAM for one-way (a) and mutual (b) authentication derived from real-world testing under four channels, with existence of a smart attacker

different channels are separated. SNRs at Rx for all frames are maintained at 15 dB to 20 dB, by adjusting the transmission power and the gain of Rx's LNA. We set $K_1 = 0.5$ and $K_2 = 1.5$ since the frequency-domain channel response on all subcarriers fall in the range of $[0.5, 1.5]$ in most cases in all channel conditions, and $K_2 = 3$. A_{max} is set to 8 due to hardware limitations (mainly due to the maximum range of integers that can be presented by FPGA in our design). All other design parameters adopt the same values as used in the simulations.

We first measure $t_3 - t_1$ (the round-trip latency of one-way authentication defined in figure 3) by examining the signal received by passive attackers. We find that $t_3 - t_1$ is as low as 36 μs, and is very stable.

The ROC curves with existence of the naive attacker under four channel types are plotted in figure 10, which shows very good performance under all channel types. Successful authentication rate and false acceptance rate follow the same definitions as those in subsection VI-A. Performance of PHY-CRAM in short-distance channels is even better than those obtained by simulation, because the delay spreads in these channels are much lower than those assumed in the simulations, and the low-SNR case (SNR=10 dB) is avoided. Figure 10 also validates the reciprocal property of the wireless channel, and shows near-perfect performance in good channel conditions.

The ROC curves with existence of a smart attacker under four channel types are plotted in figure 11. Performance differs dramatically in different channels. Short-distance LOS channels show the best performance, followed by short-distance NLOS case. Long distance LOS channel is the worst case, since 0.1 m is too short compared with 28 m, and the approximation in (14) becomes more precise. However, the attacker does not always have chance to stay so close to the legitimate user.

D. Security Analysis

Shared keys are encrypted by the wireless channel in PHY-CRAM, so the security strength of PHY-CRAM is determined by the entropy of wireless channel. The real-world experiments in [33] show that, each independent channel provides 4.38 bits of entropy with 0.5 dB quantization accuracy, and 3.5 bits of entropy with 1 dB quantization accuracy, while the quantization accuracy is mainly determined by SNR. In PHY-CRAM, there is no quantization step. However, higher SNR leads to a larger value of C_1 in (8), and more efforts for attackers to forge a shared key that satisfies (8); this is equivalent to a larger entropy of the encryption keys.

Given the works in [33], we make a moderate assumption that each independent channel provides 4 bits of entropy. Then overall entropy of the wireless channel is determined by the number of independent channels over the frequency band occupied by the wireless network, which equals to W/B_C, where B_C denotes the coherence bandwidth. According to [34], $B_C = 1/(5\sigma_\tau)$, where σ_τ denotes the root mean square (RMS) delay of the wireless channel. For a WiFi system running at 20 MHz bandwidth with $\sigma_\tau = 0.2$ μs, the overall entropy is 80 bits.

Note that the system provided in this paper is only a baseline of PHY-CRAM. Additional entropy can be obtained by utilizing the time-varying characteristic of the wireless channel, i.e., to partition the shared keys into multiple pieces and conduct authentication for all of them in multiple runs of the baseline PHY-CRAM procedure.

E. Comparison with Conventional Authentication Algorithms

Compared with conventional challenge-response authentication schemes, PHY-CRAM consumes less power at transceivers' baseband, due to the missing of channel estimation and frequency offset estimation for all OFDM symbols, and the missing of channel coding and decoding for PHY-CRAM information.

On the flip side, PHY-CRAM requires higher transmission power compared with conventional schemes. For performance comparison, we assume that the length of (encrypted) shared key is 60 bits, $K_2 = 2$, while conventional schemes adopt rate 1/2 convolutional encoder, Viterbi decoder and LMMSE estimator [35]. Conventional schemes need to maintain a BER of 8E-4 to keep β in one-way authentication above 95%, and the corresponding SNR under the rural channels simulated in subsection (VI-A) is about 10 dB, while PHY-CRAM requires 13-15 dB SNR under the same conditions.

Figure 12 gives rough estimation on the dynamic power consumptions of both schemes with respect to the distance be-

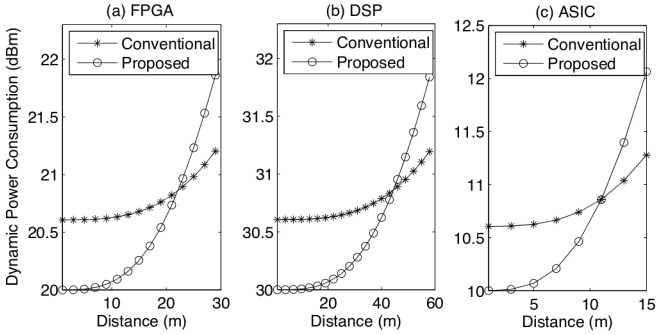


Fig. 12. Rough estimation on the power consumptions of conventional wireless transceiver and the transceiver of PHY-CRAM during authentication

tween Tx and Rx, if the baseband of transceiver is designed by FPGA, DSP and application-specific integrated circuit (ASIC), respectively. We consider that dynamic power consumption equals P^{BS} (dynamic power consumed at baseband) plus P^{RF} (dynamic power consumed at RF). In our FPGA design, $P^{BS} \approx 100$ mW, which is about 15 mW less than the power consumption of conventional baseband; this is mainly due to the elimination of Viterbi decoder IP core, which consumes 12 mW dynamic power [36]. DSP design and ASIC design for the same function are believed to consume about 10 times [37] and 10% [38] of the power consumed by FPGA, respectively. We ignore the power consumed at the Rx's RF circuitry and assume that $P^{RF} = \eta P_T$, where η and P_T denote the power efficiency and power level of the RF amplifier at Tx, respectively. Moreover, the signal power at Rx with distance d is modelled by $P_T/(L_0 d^{\gamma})$, which must satisfy the SNR requirements (15 dB for PHY-CRAM and 10 dB for conventional system), with L_0 and γ denoting pathloss at $d = 1$m and pathloss exponent, respectively. We assume that $W = 10$ MHz, noise floor equals to -114 dBm/MHz, $\eta = 0.25$, $L_0 = 10^4$, and $\gamma = 3.3$ [39]. Based on these conditions, PHY-CRAM consumes less power than the cryptographic system when communication range is shorter than 20 m, 40 m and 10 m, if FPGA, DSP and ASIC are adopted, respectively.

VII. Conclusions

We proposed a novel mutual challenge-response authentication mechanism named PHY-CRAM, which is simple, low-complexity, robust, and flexible. By eliminating any training and synchronization sequences, the CSI is kept secret to attackers, while the transmission of shared keys are secured by CSI. With a naive attacker, PHY-CRAM achieves almost perfect performance in dense multipath environments. When there exists a smart attacker, PHY-CRAM still works well under most channel conditions.

Moreover, PHY-CRAM is prototyped by FPGA and discrete RF components. Based on this prototype, we conduct real-world tests to validate PHY-CRAM's performance, and eliminated channel modelling error. These testing results show that the reciprocal property of wireless channel is well maintained when processing delays of the challenge-response signals are less than 40 μs, and that PHY-CRAM is robust under various channel environments.

Security strength of PHY-CRAM increases proportionally to RMS delay and bandwidth of the wireless channel. Energy consumption of PHY-CRAM can be comparable to or even lower than that of cryptographic authentication schemes in short range applications. As a result, PHY-CRAM can be a good alternative to traditional authentication schemes for short-range applications in dense-multipath environments.

References

[1] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, July 2008.

[2] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. 13th annual ACM international conference on Mobile computing and networking*, ser. MobiCom '07. New York, NY, USA: ACM, 2007, pp. 111–122. [Online]. Available: http://doi.acm.org/10.1145/1287853.1287867

[3] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proc. 14th ACM international conference on Mobile computing and networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 26–37. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409949

[4] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010. [Online]. Available: http://dl.acm.org/citation.cfm?id=1921927.1921939

[5] Y. Liu and P. Ning, "Enhanced wireless channel authentication using time-synched link signature," in *IEEE International Conference on Computer Communications (INFOCOM'12), Mini-Conference,*, 2012.

[6] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27–33, 2007.

[7] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *In Proc. ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2008.

[8] B. Danev, H. Luecken, S. Čapkun, and K. Defrawy, "Attacks on physical-layer identification," in *WiSec '10: Proc. 3th ACM Conference on Wireless Network Security*. ACM, 2010, pp. 89–98.

[9] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forens. Security*, vol. 3, no. 1, pp. 38 –51, march 2008.

[10] N. Goergen, W. Lin, K. Liu, and T. Clancy, "Extrinsic channel-like fingerprint embedding for authenticating mimo systems," *IEEE Trans. Wireless Commun.*, vol. 10, no. 12, pp. 4270 –4281, december 2011.

[11] A. Mikkilineni, "Forensic characterization of rf devices," in *Information Forensics and Security, 2009. WIFS 2009. First IEEE International Workshop on*, Dec 2009, pp. 26–30.

[12] K. Zeng, K. Govindan, D. Wu, and P. Mohapatra, "Identity-based attack detection in mobile wireless networks," in *INFOCOM, 2011 Proc. IEEE*, april 2011, pp. 1880 –1888.

[13] J. Hall, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *In Proc. 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT*. Kranakis, 2004, pp. 201–206.

[14] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improving intra-cellular security using air monitoring with rf fingerprints," in *Wireless Communications and Networking Conference (WCNC)*, 2010, pp. 1–6.

[15] S.-P. Kuo and Y.-C. Tseng, "Discriminant minimization search for large-scale rf-based localization systems," *IEEE Trans. Mobile Computing*, vol. 10, no. 2, pp. 291–304, Feb 2011.

[16] J. C. Klensin, R. Catoe, and P. Krumviede, "Imap/pop authorize extension for simple challenge/response," *RFC 2195*, September 1997.

[17] K. Fox and W. A. Simpson, "Ppp challenge handshake authentication protocol (chap)," *RFC 1994*, August 1996.

[18] B. Danev and S. Čapkun, "Transient-based identification of wireless sensor nodes," in *IPSN '09: Proc. 8th IEEE/ACM Information Processing in Sensor Networks*. IEEE/ACM, 2009, pp. 25–36.

[19] Y. Liu and P. Ning, "Poster: Mimicry attacks against wireless link signature," in *16th ACM Conference on Computer and Communications Security (CCS'11)*, 2011.

[20] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *CCS '07: Proc. 14th ACM conference on Computer and communications security*. ACM, 2007, pp. 401–410.

[21] Suhas Mathur and Wade Trappe and Narayan Mandayam and Chunxuan Ye and Alex Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM international conference on Mobile computing and networking MobiCom 2008*, 2008, pp. 128–139.

[22] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th annual international conference on Mobile computing and networking MobiCom '09*, 2009, pp. 321–332.

[23] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *IEEE Infocom 2010*, March 2010.

[24] T. Wang, J. Proakis, E. Masry, and J. Zeidler, "Performance degradation of ofdm systems due to doppler spreading," *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1422–1432, June 2006.

[25] P. Tan and N. C. Beaulieu, "Precise ber analysis of /4-dqpsk ofdm with carrier frequency offset over frequency selective fast fading channels," *IEEE Trans. Wireless Commun.*, Oct 2007.

[26] D. Lee and K. Cheun, "A new symbol timing recovery algorithm for ofdm systems," *IEEE Trans. Consum. Electron.*, vol. 43, no. 3, pp. 767–775, Aug 1997.

[27] M. Morelli and U. Mengali, "A comparison of pilot-aided channel estimation methods for ofdm systems," *IEEE Trans. Signal Process.*, vol. 49, no. 12, pp. 3065–3073, Dec 2001.

[28] B. Yang, K. Letaief, R. Cheng, and Z. Cao, "Timing recovery for ofdm transmission," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 11, pp. 2278–2291, Nov 2000.

[29] J. A. Hurst and I. Wassell, "Double differentially demodulated scheme for short burst ofdm systems operating in frequency selective environments," *Electronics Letters*, vol. 36, no. 18, pp. 1559–1560, Aug 2000.

[30] Y. Mostofi and D. C. Cox, "A robust timing synchronization design in ofdm systemspart i: Low-mobility cases," *IEEE Trans. Wireless Commun.*, Dec 2007.

[31] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in *The 17th European Symposium on Research in Computer Security (ESORICS)*, sep 2012.

[32] 3GPP, "Tr 25.943: Technical specification group radio access networks - deployment aspects," 3GPP, Tech. Rep., 2009.

[33] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secret keys from entangled sensor motes: Implementation and analysis," in *Proc. Third ACM Conference on Wireless Network Security (WiSec '10)*. ACM, mar 2010, pp. 139–144.

[34] *Mobile Cellular Telecommunications Systems*. Mcgraw Hill, 1989.

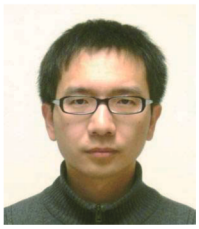
[35] M.-H. Hsieh and C.-H. Wei, "Channel estimation for ofdm systems based on comb-type pilot arrangement in frequency selective fading channels," in *IEEE Trans. Consum. Electron.*, vol. 44, Feb. 1998, pp. 217–225.

[36] S. Shaker, S. Elramly, and K. Sheriata, "Fpga implementation of a reconfigurable viterbi decoder for wimax receiver," in *Microelectronics (ICM), 2009 International Conference on*, 2009, pp. 264–267.

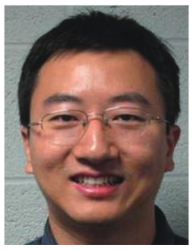
[37] H. K. Boyapati and R. V. R. Kumar, "A comparison of dsp, asic, and risc dsp based implementations of multiple access in lte," in *Communications, Control and Signal Processing (ISCCSP), 2010 4th International Symposium on*, 2010, pp. 1–5.

[38] I. Kuon, I. Kuon, and J. Rose, "Measuring the gap between fpgas and asics," in *FPGA '06 Proc. 2006 ACM/SIGDA 14th international symposium on Field programmable gate arrays*, 2006, pp. 21–30.

[39] H. Hashemi, "The indoor radio propagation channel," *Proc. IEEE*, vol. 81, no. 7, pp. 943–968, July 1993.



Dan Shan (S'10) received his B.S. and M.S. degrees in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China in 2004 and 2007, respectively. Since 2007, he has been a research assistant with the University of Michigan Dearborn, where he is currently a Ph.D. candidate. His research interests include channel modelling and signal processing for wireless communications, vehicular networks, cognitive radio, physical-layer security, ultra-wideband (UWB) and software-defined radio.



Kai Zeng received his Ph.D. degree in Electrical and Computer Engineering at Worcester Polytechnic Institute (WPI) in 2008. He obtained MS in Communication and Information Systems and BS in Communication Engineering both from Huazhong University of Science and Technology, China in 2004 and 2001, respectively. He was a postdoctoral scholar in the Department of Computer Science at University of California, Davis (UCD) from 2008 to 2011. He joined the Department of Computer and Information Science at University of Michigan Dearborn as an assistant professor in 2011. He is a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2012. He won Excellence in Postdoctoral Research Award at UCD in 2011 and Sigma Xi Outstanding Ph.D. Dissertation Award at WPI in 2008. His current research interests are in wireless network security, physical layer security, cognitive radio networks, energy efficiency, and cyber-physical systems.

Weidong Xiang received his M.S. and Ph.D. degrees from Tsinghua University, Beijing, China, in 1996 and 1999, respectively. From 1999 to 2004, he worked as a Postdoctoral Fellow and then a Research Scientist in the Software Radio Laboratory (SRL) at Georgia Institute of Technology, Atlanta, USA. In 2004, he joined the ECE Department, University of Michigan, Dearborn (UMD) where he currently is an Associate Professor. His research interest includes LTE, vehicular communications and networks, smart grid, software radio/cognitive radio, ultra-wideband (UWB), and wireless networked control systems. He established and leads the Center for Vehicular Communications and Network Laboratory at UMD focusing on dedicate short range communications (DSRC), machine type communications (MTC), LTE for high mobility applications and UWB positioning. He serves as an Associate Editor/Editor for IEEE Communications Magazine, EURASIP Journal on Wireless Communications and Networking and others. He has successfully held several tutorials in IEEE Globecom, IEEE CCNC, IEEE WCNC, IEEE Tutorial Now and many others. He has published 50+ technical papers in relevant international journals and conferences. He has served as the leading guest editor for a special issue on WAVE technology on EURASIP Journal on Wireless Communications and Networking and the General Chair/Co-Chair for WAVE conference 2008/2009. His current research is widely supported by NSF, DoE, China Government, CISCO Research and University of Michigan. He also found and operates the Vehicom LLC.

Paul Richardson received the B.S.E. degree in computer engineering, the M.S.E. degree in computer and electrical engineering, and the Ph.D. degree in systems engineering, all from Oakland University, Rochester, MI. He is a Professor in the Department of Electrical and Computer Engineering, University of Michigan, Dearborn. He is a Principal Investigator for ultra-wideband applications with the U.S. Army Research Development, and Engineering Center, Warren, MI, and a Consultant for the U.S. Marine Corps regarding command and control networks. His interests include embedded real-time systems, vehicular networks and communications systems, and ultra-wideband applications.

Yan Dong (M'08) received the B.S. and M.S. degrees from Xidian University, Xian, China, and the Ph.D. degree from Huazhong University of Science and Technology, Wuhan, China, in 2007. She currently works in the Department of Electronics and Information Engineering, Huazhong University of Science and Technology, as an Associate Professor. Her research interests include signal processing and coding for high performance wireless networks.