Physical Layer Challenge-Response Authentication in Wireless Networks with Relay

Xianru Du*, Dan Shan*, Kai Zeng* and Lauren Huie†
*Department of Computer and Information Science, University of Michigan - Dearborn, MI 48128
Email: {duxianru, danshan, kzeng}@umich.edu
†Air Force Research Laboratory, Rome, NY, 13441
Email: Lauren.Huie@us.af.mil

***Abstract*—Exploiting physical layer characteristics to enhance or complement authentication strength in wireless networks has been attracting research attention recently. Existing physical layer authentication mechanisms mainly tackle single-hop communications. In this paper, we propose two physical layer challenge-response authentication mechanisms for wireless networks with relay. One mechanism, named PHY-CRAMR, is an extension of the existing PHY-CRAM protocol. It fully utilizes the randomness, reciprocity, and location decorrelation features of the wireless fading channel to hide/encrypt the challenge response messages at the physical layer, and is immune to outside attacks with a trusted relay. The other novel mechanism, named PHY-AUR, exploits randomness, coherence, and location decorrelation properties of wireless fading channel to securely convey the product of the channel state information on consecutive links and uses the fading channel to encrypt challenge and response messages. PHY-AUR is immune to both outside and inside attacks with an untrusted relay. Both PHY-CRAMR and PHY-AUR adopt OFDM technique to modulate the authentication key and challenge-response messages on subcarriers. Physical layer pilots and preambles are eliminated to prevent an attacker from gaining knowledge about the channel state information, and as a result prevent the authentication key from being revealed to untrusted attackers. We analyze the security strength of both mechanisms and conduct extensive simulations to evaluate them. It shows that both PHY-CRAMR and PHY-AUR can achieve both a high successful authentication rate and low false acceptance rate, and the performance improves as the signal to noise ratio (SNR) increases.**

***Index Terms*—Physical-layer security, challenge-response authentication, relay network, wireless fading channel, OFDM**

I. Introduction

With the rapid advancement of wireless communication technology and ever-increasing mobile and pervasive applications, it becomes increasingly important and challenging to secure wireless communications. Authentication is usually the first step to establish a secure communication between two parties. Recently, there has been an increasing interest in complementing or enhancing authentication in wireless networks by exploiting unique physical layer characteristics [1]–[11]. Physical layer authentication/identification benefits a number of wireless applications such as wireless forensics [12], identity-based attack detection [13], access control [14], malfunctioning detection [15], and tracking [16] etc.

Existing works on physical layer authentication [1]–[11] mainly focus on single-hop wireless communications, where the verifier and prover can communicate with each other directly. In wireless networks, however, many communications happen in two hops, such as the communication between two WLAN clients via an access point, two cellular phones via a base station, or two ad hoc nodes through a relay. To the best of our knowledge, there is no existing work tackling physical layer authentication in multihop wireless networks.

In this paper, we propose two physical layer challenge-response authentication mechanisms for two-hop wireless networks involving a relay. We first propose a mechanism, named PHY-CRAMR (PHYsical layer Challenge Response Authentication Mechanism with Relay), which is an extension of the existing PHY-CRAM protocol [11]. It fully utilizes the randomness, reciprocity, and location decorrelation features of the wireless fading channel to hide/encrypt the challenge response messages at the physical layer, and is immune to outside attacks assuming the relay is trustworthy. The basic idea of PHY-CRAMR is to use a random number and channel fading to mask the authentication key, and exploit channel reciprocity to cancel out the channel effect using inverse operations such that the verifier can decode the secret without knowing the channel state information.

In order to tackle an untrusted relay node, who attempts to break the authentication key or impersonate legitimate users, we further propose a novel authentication mechanism, named PHY-AUR (PHYsical layer Authentication with Untrusted Relay). It exploits randomness, coherence, and location decorrelation properties of the wireless fading channel to securely convey the product of the channel state information on the two relay links and use the fading channel to encrypt challenge and response messages. PHY-AUR is secure against both outside and inside attacks with an untrusted relay.

PHY-CRAMR and PHY-AUR share a unique feature that, it eliminates channel coding, channel estimation and frequency offset compensation in the challenge-response messages. This feature not only simplifies the baseband design, but also prevents the outside and inside attackers from knowing the channel state information, thus provides strong security strength.

We summarize our major contributions as follows:

- We propose two physical layer challenge-response authentication mechanisms, PHY-CRAMR and PHY-AUR, for two-hop wireless networks with a relay in section IV and V.
- We conduct extensive simulation to evaluate the performance of proposed two mechanisms under different channel conditions, key lengths, and signal to noise ratios (SNRs), as reported in section VI.
- The security strength of PHY-CRAMR and PHY-AUR are analyzed and evaluated under various attacks in section IV-E and V-C.

II. Related Work

A. Physical Layer Authentication/Identification

Existing physical layer authentication/identification schemes mainly focus on single-hop wireless communications, and can be generally categorized into four types: (1) the ones based on transceiver hardware differences, i.e., RF fingerprinting [6]–[8],

(2) the ones based on wireless channels [1]–[5], (3) physical layer signal watermarking [9], [10], and (4) physical layer challenge response authentication [11].

1) RF Fingerprinting for Device Identification: Most wireless devices have unique and uncloneable impairments that could be used for device identification. These impairments, with the name RF fingerprinting, may be caused by either transient behaviours of amplifiers [6] or imperfection of constellation [7].

Unfortunately, RF fingerprinting is unsafe under impersonation attack [8]. To attack the existing RF fingerprinting schemes, an attacker does not necessarily reproduce a legitimate radio, but only needs to reproduce/replay the signal used for RF fingerprint verification. Furthermore, measurements on RF fingerprinting is expensive, since it needs a high-end signal analyzer to extract the subtle differences in the signals. Lastly, it usually requires a relatively stationary channel condition in order to accurately extract the RF fingerprint. That is, its performance tends to deteriorate in a dynamic environment.

2) Wireless Channel Based Authentication: Channel state information (CSI) between different transmitter-receiver (Tx-Rx) pairs are different, and may be used for authentication [2], [3]. This type of authentication requires that locations and CSI of legitimate users are known, channel sounding are fast enough compared with channel coherence time T_C, or the number of channel sounding samples is large enough to overcome the time-varying effect. Moreover, false acceptance rate of such method is high when mimicry attackers are very close to legitimate users [17].

In our protocols, PHY-CRAMR does not require channel sounding, while PHY-AUR conducts channel sounding on-the-fly. Both protocols neither require legitimate users to be at specific locations nor need to measure CSI of legitimate users first. Our protocols exchange only two messages during authentication, and can be finished well within time interval T_C to ensure channel reciprocity.

In time-varying channels, CSI or received signal strength (RSS) may be used for message authentication [1], [4], while the proposed protocols in this paper study user authentication.

3) Physical Layer Signal Watermarking: Physical layer signal watermarking or fingerprinting embeds a cryptography based authentication code or tag into the original data signal [9], [10]. By doing this, conventional wireless communication systems have the ability of message authentication with no extra bandwidth consumption. Again, this technique studies message authentication while we focus on user authentication.

4) Physical Layer Challenge Response Authentication: Recently, a physical layer challenge response authentication mechanism, named PHY-CRAM, was proposed [11]. It utilizes the randomness of the fading channel to hide the shared secret used for authentication. PHY-CRAM does not require the legitimate user to be at a fixed location. It does not require a high-end signal analyzer or signature training. It is impossible for an attacker to pass the authentication by replaying the signal since a fresh nonce is used for every new authentication. It also favors dynamic environments.

PHY-CRAMR is an extension of PHY-CRAM to support authentication for two-hop wireless networks with a relay. It is secure when the relay is trustworthy. PHY-AUR uses a different methodology to tackle the problem of untrusted relay.

B. Conventional Challenge Response Authentication

Conventional challenge-response authentication mechanisms (such as CRAM-MD5 [18], CHAP [19]) use hash function to hide shared secret for authentication. The authentication mechanisms proposed in this paper is fundamentally different from the conventional ones. The fundamental difference lies in that PHY-CRAMR and PHY-AUR utilize physical layer properties to mask the shared secret used for authentication while conventional challenge-response protocols rely on cryptographic functions to hide the shared secret. The security strength of PHY-CRAMR and PHY-AUR depend on the randomness of the fading channel and the relative geographic location among the attacker, relay and legitimate users, but not depend on the computation complexity. As a result, both mechanisms do not suffer the threat of ever-increasing computing power, while this does not hold for conventional authentication schemes (such as CRAM-MD5 [18] and CHAP [19]). It is anticipated that cryptography-based authentication requires longer keys in the future, while longer keys usually imply higher computation overhead, communication overhead, energy consumption, and storage overhead.

Neither PHY-CRAMR nor PHY-AUR intends to replace the existing conventional challenge-response authentication protocol, but they can serve as attractive alternatives that do not depend on computational security.

III. System Model

A. Application Model

Real-world wireless communications usually involve two hops, such as two WLAN clients communicate with each other via an access point, or two mobile phones talk to each other through a base station. This paper provides new challenge-response authentication solutions at the physical layer for two-hop wireless networks.

The general application model is shown in figure 1. We consider two legitimate users $Alice$ (A) and Bob (B), who communicate with each other with the assistance of $Relay$ (R). An attacker may listen to the wireless channel, try to steal some useful information and impersonate a legitimate user.

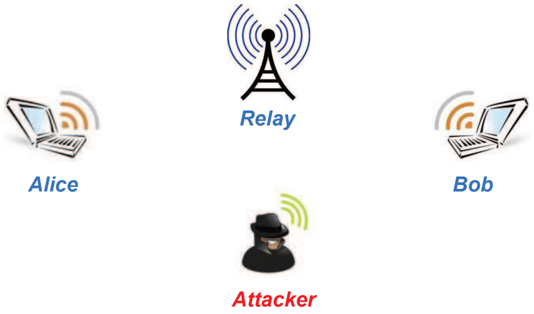


Fig. 1. System model

In this paper, we mainly focus on one-way authentication in which A needs to authenticate B. We assume A and B share a secret key K. The security of the authentication mechanisms rely on the shared secret key and the unique characteristics of the wireless fading channel.

B. Physical Layer Communication

At physical layer, we assume Orthogonal Frequency Division Multiplexing (OFDM) is adopted. OFDM is widely used in current WLAN and cellular networks, such as WiFi 802.11a/n, LTE (4G), etc.

In OFDM systems, the bandwidth is shared by N independent narrow band sub-carriers which can be multiplexed easily by Fast Fourier Transform (FFT) or Inverse Fast Fourier Transform (IFFT) operations. Due to this feature, it is convenient to conduct reciprocal and multiplication operations in the frequency domain. If not specified, all wireless signals and their operations are expressed in frequency domain in this paper.

Some sub-carriers in OFDM symbols are usually used as pilots for channel estimation. However, we eliminate pilots to avoid revealing the channel state information to the attacker. In fact, in the two protocols proposed, all OFDM symbols do not include pilots, synchronization preambles or any other reference signals, so that any receivers cannot estimate the channel and cannot get the original message further. In this case, autocorrelation on energy and cyclic prefix (CP) [20] is used for time synchronization at the receiving side.

In order to be close to the practical situation, both Rayleigh fading channel and Additive White Gaussian Noise (AWGN) channel are taken into account in the simulations.

C. Attack Model

The attackers can be either passive or active. A passive attacker can overhear all the signals transmitted from A, B, or R, and attempts to determine the authentication key. An active attacker not only can eavesdrop all the signals from A, B, or R, but also can inject or replay signals into the network.

The attacker can be inside or outside of the communication system. Relay node R can be an inside attacker, who can record all the signals received from A or B, and replay the signals later on or inject any signals into the network. R may attempt to determine the authentication key or pass the authentication procedure by injecting specific signals without being noticed.

We do not consider jamming or denial of service attack (DoS) in this paper. All wireless communications are subject to this kind of attack, and counter jamming methodologies, such as frequency hopping [21], [22], can be incorporated into the physical layer authentication mechanisms proposed in this paper.

IV. PHY-CRAMR Protocol

In this section, we propose PHY-CRAMR to provide physical layer authentication in wireless networks with relay. PHY-CRAMR actually is the extension of the existing PHY-CRAM protocol [11].

A. Basics

From the physical communication model described in section III-B, we denote H_{AB} as the frequency domain channel response of fading channel and W_{AB} as the AWGN for the wireless link from A to B. H_{AB} is the multiplicative factor to the frequency domain signal, while W_{AB} is additive. Due to the use of IFFT/FFT in OFDM, we can always operate the signal in frequency domain conveniently. Equation (1) expresses the relationship between the received signal and transmitted signal.

$$RX_{AB} = TX_{AB} H_{AB} + W_{AB} \tag{1}$$

where RX_{AB} and TX_{AB} represent received and transmitted signals in the frequency domain respectively. H_{AB} is a random process and provides a natural mask for the protocol messages.

In the design, we assume the channels are symmetric which means $H_{AB} = H_{BA}$ and keep correlated during the processing time. This is feasible because the processing time can be much smaller than channel coherent time T_C in the real world. For example, we can adopt $2.4GHz$ RF carrier, same as Wi-Fi frequency band. When transmitter and receiver have low relative speed $1m/s$, the Doppler frequency $f_d = v/\lambda = vf/c = 1 * 2.4 * 10^9/(3 * 10^8) = 8Hz$. Empirically, coherent time is related to maximum Doppler frequency shift and can be calculated as $T_C = \frac{9}{16\pi f_d} = \frac{9}{16\pi * 8} = 0.02239s = 22.4ms$. In the mobile environment with relative speed $v = 60km/h$, the corresponding coherent time is $1.3ms$ calculated in the same way. On the other hand, the total process time may include transmitting time T_t, propagation time T_p and operation delay T_d in each nodes. If we take $10MHz$ sampling rate, an OFDM symbol with 64 sub-carriers and 16 CP samples takes $T_t = 8\mu s$ to transmit. The propagation time will be $1\mu s$ if the distance is $300m$. The operation delay is usually in the same order of transmitting time. Then totally the processing time can be much smaller than coherent time in the above two cases.

B. Protocol Description

PHY-CRAMR is a challenge-response protocol with only one round procedure, as illustrated in figure 2. For easy understanding and description purpose, we ignore AWGN and assume channel reciprocity holds in the illustration. Noise and non-perfect channel reciprocity will be taken into account in the later analysis.

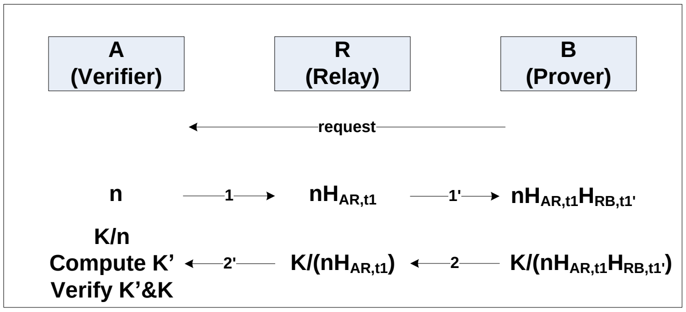


Fig. 2. PHY-CRAMR protocol

Step (0) At time t_0, B sends one OFDM frame with the authentication request. Only one symbol is needed to identify the request command. This starts the protocol.

Step (1-1') After receiving the authentication request from B, A randomly generates a random number n (i.e., challenge) to modulate amplitudes of sub-carriers in one OFDM symbol, and sends it to R. What R receives is $nH_{AR,t_1} + W_{AR}$, where H_{AR,t_1} is the wireless channel at time t_1 between A and R and W_{AR} is the AWGN. R further forwards the received signal to B.

Step (2-2') After B receives the signal from R, it calculates the reciprocal (inverse) of the received signal, multiplies it by the shared key K, and then transmits the resulting signal to R. In the same way, R forwards the signal to A.

C. Verifying Scheme

After the frame is arrived, A verifies the authentication message from B. If AWGN is ignored, the signal received by A can be expressed as the first half part in equation (2).

$$RX_{A,t_{2'}} = \frac{K}{nH_{AR,t_1} H_{RB,t_{1'}}} H_{BR,t_2} H_{RA,t_{2'}} \approx \frac{K}{n} \tag{2}$$

If the processing time is smaller than the channel coherent time T_C, which can be ensured in practice, the channel effects can be further cancelled out due to the symmetric correlated channel. That is $H_{AR,t_1} = H_{RA,t_{2'}}$ and $H_{RB,t_{1'}} = H_{BR,t_2}$. Then, after the last step, A can calculate the approximate shared key $K' = nRX_{A,t_{2'}} \approx K$. Finally, A can verify the message by comparing K' and K. However, because of non-perfect channel reciprocity and especially AWGN, the estimated K' will be different from the real one, but should be highly correlated. Therefore, we use the method of correlation to evaluate the similarity between K and K'. Then verifier can make the judgement whether it is talking to B according to the predefined threshold and the correlation result between calculated K' and K. The correlation of two variables i and j is defined in equation (3).

$$Corr(i,j) = \frac{Cov(i,j)}{\sqrt{Cov(i,i)Cov(j,j)}} \tag{3}$$

Here, Cov is the covariance of two variables.

$$Cov(x_1, x_2) = E[(x_1 - \mu_1)(x_2 - \mu_2)] \tag{4}$$

where E is the mathematical expectation, $\mu_1 = E(x_1)$ and $\mu_2 = E(x_2)$.

The absolute value of correlation result ranges from 0 to 1. As we know, the higher the correlation is, the more similar the two values are. A parameter, $0 < C_0 < 1$, can be set as the threshold. If the equation (5) is satisfied, A believes the counterpart B is really what it claims. Then B passes the authentication.

$$Corr(nRX_{A,t_{2'}}, K) > C_0 \tag{5}$$

The selection of threshold C_0 is critical. A large C_0 may lead to a high false negative rate, which means many legal users may not pass the authentication. On the other hand, a small C_0 may lead to a high false positive rate, which means many illegal users may pass the authentication. Therefore, we should make a trade-off to balance them. The Receiver Operating Characteristic (ROC) curve, which reflects the relationship between successful authentication rate (the rate of legitimate users who pass the authentication) and false acceptance rate (the rate of illegal users who pass the authentication), will be used to evaluate the protocol's performance.

For the ideal case, when AWGN is ignored and channel symmetrical characteristic is considered, that is $H_{XY} = H_{YX}$, we can easily get $Corr(nRX_A(ideal), K) = Corr(K, K) = 1$. Therefore the verification scheme is correct. Actually, the performance will be worsened mainly by AWGN, because we can consider the channel is symmetric between two nodes as long as the processing time is smaller than T_C which can be ensured in practice. The performance with different SNR will be shown in our simulation in section VI-E to examine the effects of AWGN.

D. Data Mapping

Figure 3 shows the general OFDM system. The original bit stream is mapped to sub-carriers in OFDM symbols before IFFT operation for multiplex. In this subsection, we will mainly discuss the data format used and the data mapping.

In the one round challenge-response message exchanges described above, the shared key and random challenge number are the authentication messages. The length of K and n can be different, but it will be convenient to use the same bit length L. Then $K = \{K^0, K^1, ..., K^{L-1}\}$ and $n = \{n^0, n^1, ..., n^{L-1}\}$, where $K^l \in \{0,1\}, n^l \in \{0,1\}$ for $l \in \{0, 1, ..., L-1\}$.

In practice, there are mainly three kinds of sub-carriers in an OFDM symbol: data sub-carriers used to transmit data, pilot sub-carriers used for channel estimation, and null sub-carriers to protect side band and DC sub-carrier. For different modulation mapping scheme, different number of bits from original messages are mapped to each data sub-carrier sequentially in OFDM symbols. Usually, a complex value, in which the real part and imaginary part represent In-phase and Quadrature component respectively, is used as the mapped signal for each sub-carrier in OFDM systems. For example, in QPSK mapping, a frequently-used method, two bits are mapped to a complex number for each sub-carrier, and then there are totally four states.

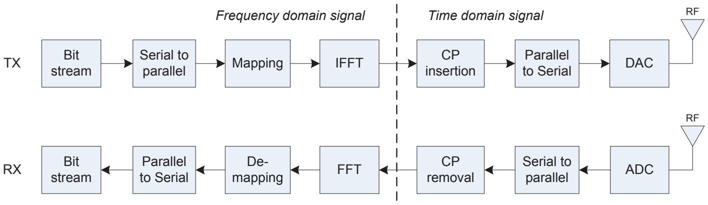


Fig. 3. General OFDM system

In this paper, we adopt AM as the mapping scheme. We assume there are S bits per sub-carrier. Then the number of total data sub-carriers used for K or n is $M = \lceil L/S \rceil$, where $\lceil \rceil$ denotes the operation that rounds a number toward positive infinity. Then $\lceil M/N \rceil$ symbols in one transmitting frame are needed to accommodate all the information in K or n if there are N data sub-carriers in each OFDM symbol. For simplicity, we choose $M < N$ so that only one symbol can carry all bits in K or n. In this following description, we take the sub-carrier number M as the key length. A brief mapping relationship for the case of $M < N$ is shown in figure 4.

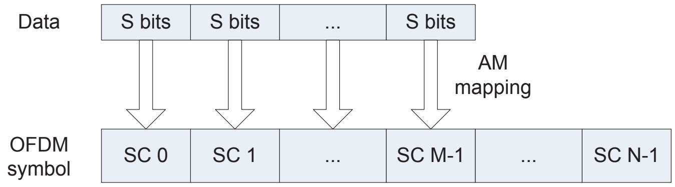


Fig. 4. Data mapping in OFDM symbol ($M < N$, SC represents sub-carrier)

In fact, both the length of the shared key M and the bit number for a sub-carrier SC will affect the correlation results in the verifying scheme and further influence the overall performance. Different M will be examined in our simulations for comparison.

We can define an AM mapping rule which can reflect the relationship between S-bit data and the mapped complex number. However, as a simplification, we can generate $M = \lceil L/S \rceil$ complex numbers with random absolute values and random phases to represent original message K and n directly.

Since we only exploit the amplitude components in AM, the phase components are ignored. The amplitude component is the real absolute value of the complex number in each sub-carrier, which ranges from A_1 to A_2. Because we do the reciprocal in PHY-CRAMR, A_1 and A_2 cannot be too large or too small so as to avoid signal peaks and high transmission power at some sub-carriers. Meanwhile, A_2/A_1 should be large enough to keep a good discrimination and hide the channel state information. In fact, the distribution range of the amplitudes in sub-carriers should be in accordance with channel's magnitude response.

E. Security Analysis

The use of random challenge number n in *step (1-1')* can ensure different messages for each authentication and prevent simple replay attack. Due to the missing of pilots, synchronization preambles and any pre-known reference signals in transmitting signals, an attacker cannot estimate the channel information to extract the authentic message. Legitimate users A and B in the system share one secret key. All of these ensure the security of the protocol. For any attacker E, we denote the wireless channel between E and A, B and R as H_{AE}, H_{BE} and H_{RE}, respectively.

1) Passive Attacks: A passive attacker E_P only monitors the network traffic and try to obtain useful information such as shared key K, for the further attack. Passive attacker will not inject additional signals during the authentication process. Different locations will result in different abilities for attacks.

(1) *The naive E_P:* When passive attacker E_P is far away from A, B and R, the exchanged messages between A and B are masked by the channel naturally. We name this kind of passive attackers as naive E_P, because it can obtain little information about the authentic message. In PHY-CRAMR, E_P can intercept four messages $(nH_{AE}$, $nH_{AR}H_{RE}$, $KH_{BE}/(nH_{AR}H_{RB})$, $KH_{RE}/(nH_{AR}))$ if AWGN is ignored and symmetric channel is assumed, where seven unknown factors (K, n, H_{AE}, H_{BE}, H_{RE}, H_{AR} and H_{BR}) exist. E_P cannot determine K through these messages because it has no knowledge about any channel state information.

(2) *The smart E_P:* Similar to [11], a smart E_P, who is very close to one certain legitimate user, may get more information. If E_P is very close to A, $H_{AE} \approx 1$ because the line-of-sight (LOS) signal is much stronger than any other multipath signals and $H_{RE} \approx H_{AR}$. Then the messages E can receive are simplified as (n, nH_{AR}^2, $KH_{BE}/(nH_{AR}H_{RB})$, K/n). In fact, E who is close to A can get approximate values of n and K in this situation. This is why the protocol security relies on location decorrelation and stochastic property of the wireless channel. If the channel is a pre-known constant, it should not be safe. When E_P is close to B, $H_{BE} \approx 1$ and $H_{RE} \approx H_{BR}$. When E_P is close to R, $H_{RE} \approx 1$. Similar to the case that E_P is close to A, the attacker can derive the approximate value of K in both of these two cases. However, this kind of attack is hard to launch, because as we know, more than half a wavelength ($\lambda/2$) distance is essential to keep the wireless channel uncorrelated. If 2.4 GHz frequency is used, then $\lambda/2 = 6.25$ cm, a very short distance within which an attacker can be easily identified by the legitimate users. Then E_P can only derive a roughly estimated K due to location distinction, while legitimate users have perfect knowledge about K [11].

(3) *Untrusted relay R:* There is a special case that the relay R is an adversary. Because all the message for authentication are relayed by R, it can have more information. Actually, R can easily get the shared K, because it knows nH_{AR,t_1} after step 1 and $K/(nH_{AR,t_1})$ after step 2. Then R can obtain K by multiplying two received signals. In this case, R can forge the protocol signal in step 2' next time. Thus, although the idea may be suitable for one hop, it is not secure for multi-hop cases if the relay is not trustworthy.

2) Active Attacks: The active attacker E_A can inject or replay signals based on what it obtained. As we assumed, we do not talk about the jamming and DoS attacks.

In a replay attack, E_A wants to pass the authentication using the information it intercepts during the process of legal authentication in previous rounds. However, E_A cannot succeed because the challenge n sent from verifier A is randomly selected at each time. The old one cannot be used for the new authentication.

Due to the pilots elimination method, outside users cannot estimate the wireless channel and extract the original message. Then it is also very hard for outside attacker to mimic the authentication signals.

However, an untrusted relay R is a threat to this protocol. As we discussed before, attacker R can derive shared key K. Then in the next time, it can forge a message in step $2'$ based on K and what it received in step 1.

Further more, if the relay R is not honest, outside users can also launch impersonation attack with the assistance of R. What outside attacker E_p can receive after step 1 is $nH_{AR}H_{RE_P}$. Then it does the reciprocal operation and transmits the result to R. R can receive $1/nH_{AR}$. Now that R has the ability to determine K, it can construct the message K/nH_{AR} for E_P. Finally, E_P will pass the authentication. In fact, this kind of joint attacks can be detected if A always sends the challenge n after the legal authentication request. In this case, the legitimate prover B also exists in the system. B will also respond in the authentication process. Therefore, we can keep the received signal strength (RSS) at a certain level. If there are other responses, the RSS will be higher than normal level. Then we can avoid it by maintaining and detecting RSS.

F. Extension for More Hops

Actually, the protocol is not limited for two hops. Figure 5 shows the general case of PHY-CRAMR in multi-hop networks. In each hop, the channel effects will accumulate. Because of more additive noise involved, the performance will get worse with increased hop count. The simulation result for multiple hops is shown in figure 12.

V. PHY-AUR Protocol

As discussed in the previous section, PHY-CRAMR works under the assumption of a trusted relay, but fails when the relay launches an inside attack. In this section, we propose a new protocol, PHY-AUR, to defend against the inside attack from an untrusted relay. In fact, the attack from the untrusted relay is hard to resist because all exchange signals can be recorded or relayed by R. Based on this, A and B should share more secret information which R and other attackers cannot obtain.

A. Protocol Description

In this scheme, we keep the same basic assumptions as in PHY-CRAMR, such as the data mapping method and pilots elimination in OFDM symbols. The difference lies in that two shared key K_1 and K_2 are used and two OFDM symbols are transmitted simultaneously as one signal frame in each step. B requests the authentication first and the protocol still needs only one round message exchange. The protocol is illustrated in figure 6 by ignoring noise.

Step (0) B sends one OFDM frame with the authentication request.

Step (1-1') A generates a random number n, and sends K_1 and n in two consecutive OFDM symbols which will undergo the same channel fading because of short time interval with different AWGN. R just forwards the received signal to B. At B's side, it can calculate n/K_1 by dividing two received symbols and further get the estimated n' easily with the known shared K_1. The same as PHY-CRAMR, AWGN will influence the performance seriously.

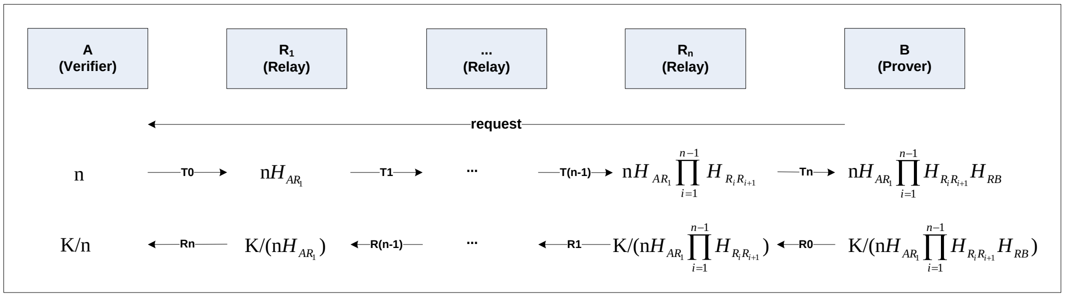

A
(Verifier)
R1
(Relay)
...
(Relay)
Rn
(Relay)
B
(Prover)
request
n
T0
nH_{AR_1}
T1
...
T(n-1)
$nH_{AR_1}\prod_{i=1}^{n-1}H_{R_iR_{i+1}}$
Tn
$nH_{AR_1}\prod_{i=1}^{n-1}H_{R_iR_{i+1}}H_{RB}$
K/n
Rn
$K/(nH_{AR_1})$
R(n-1)
...
R1
$K/(nH_{AR_1}\prod_{i=1}^{n-1}H_{R_iR_{i+1}})$
R0
$K/(nH_{AR_1}\prod_{i=1}^{n-1}H_{R_iR_{i+1}}H_{RB})$

Fig. 5. General case of PHY-CRAMR in multi-hop networks

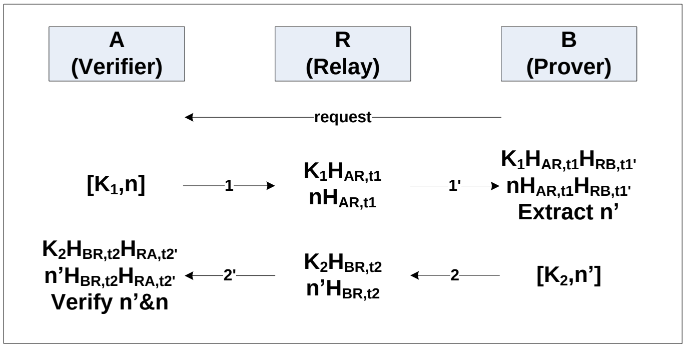


Fig. 6. PHY-AUR protocol

Step (2-2') B can solve out n', and sends back K_2 and n' in the same way as A does. R just forwards the received signal to A. A then extracts n' and verify the authentication according to calculated n' and true n generated by itself.

B. Verifying Scheme

The similar verifying scheme using correlation is adopted. What A receives is one OFDM frame including two symbols expressed in equation (6). The authentication is passed if equation (7) is satisfied. C_1, ranging from 0 to 1, is a threshold.

$$\begin{aligned} RX_{A,t_{2'}} &= \{RX_{A1}, RX_{A2}\} \\ &= \{K_2 H_{AR,t_2} H_{RB,t_{2'}}, nH_{AR,t_2} H_{RB,t_{2'}}\} \end{aligned} \tag{6}$$

$$Corr(K_2(RX_{A2}/RX_{A1}), n) > C_1 \tag{7}$$

C. Security Analysis

1) Passive Attacks: A passive attacker E_P only monitors the traffic from wireless channel in order to acquire some information about shared key K, and does not transmit signals during the authentication process.

(1) *The naive E_P:* Messages what E_P can receive are

$$\begin{cases} K_1 H_{AE}, K_1 H_{AR} H_{RE}, K_2 H_{BE}, K_2 H_{BR} H_{RE} \\ nH_{AE}, nH_{AR} H_{RE}, nH_{BE}, nH_{BR} H_{RE} \end{cases} \tag{8}$$

For naive attackers, E_P still has no way to guess the shared key K_1 and K_2 from the received messages in PHY-AUR, because the original messages are masked by random channels and attackers cannot obtain the channel information, as discussed in IV-E. As a result, both PHY-CRAMR and PHY-AUR are safe under this kind of passive attacks. The correlation distributions in the verifying step of two protocols for legitimate users and attackers are compared in figure 11 in our simulation section.

(2) *The smart E_P:* If E_P is very close to A, we can assume $H_{AE} \approx 1$ because of the LOS signal and $H_{RE} \approx H_{AR}$. Then smart E_P can obtain the following signals from equation (8).

$$\begin{cases} K_1, K_1 H_{AR}^2, K_2 H_{BE}, K_2 H_{BR} H_{AR} \\ n, nH_{AR}^2, nH_{BE}, nH_{BR} H_{AR} \end{cases} \tag{9}$$

In fact, the attacker can derive the approximate K_1, K_2, and n. When E_P is very close to B, the situation is similar because the messages A and B transmitted are symmetric. When E_P is very close to R, $H_{RE} \approx 1$, $H_{AE} \approx H_{AR}$ and $H_{BE} \approx H_{BR}$. Then equation set (8) can be simplified as $(K_1 H_{AR}, nH_{AR}, K_2 H_{BR}, nH_{BR})$ with five unknown values $(K_1, K_2, n, H_{AR}, H_{BR})$. Therefore, E_P cannot solve the equation set. The smart attack is hard to launch since distinct locations make wireless channels uncorrelated.

(3) *Untrusted relay R:* Untrusted relay is a special case when the smart attacker E_P is right at the position of R, that is $H_{RE} = 1$, $H_{AE} = H_{AR}$ and $H_{BE} = H_{BR}$. From discussions above, the untrusted relay cannot obtain shared key K_1 and K_2. Even when we use one same shared key $K_1 = K_2 = K$, R can only compute $K_1/n = K_2/n = K/n$ and H_{AR}/H_{BR} at most, without individual information about K_1, K_2, n, H_{AR}, and H_{RB}. That is PHY-AUR can prevent the passive attacks even if the relay is not honest, which is different from PHY-CRAMR.

2) Active Attacks: Different from passive attacks, an active attacker E_A may pretend to be an legitimate user even it has no knowledge about the shared key.

In our initial design, we use one shared key $K = K_1 = K_2$ instead of two individual keys. In that case, passive attacks can be avoided from the discussion above. However, the untrusted relay R and other outside attackers may impersonate the legitimate user. As we know, R can receive $RX_{R1} = (KH_{AR}, nH_{AR})$ after step 1 and $RX_{R2} = (KH_{BR}, nH_{BR})$ after step 2. Then $RX_{R2} = RX_{R1}X$ is what R forwards in step $2'$, where X is a coefficient. In fact, the untrusted R can multiply the received signal RX_{R1} by any coefficient and send the result to A in step $2'$, because any coefficient can be cancelled out after A does the division operation. Finally, A can still extract correct n and pass the authentication. Furthermore, for an outside attack E_A, he can receive $RX_{E_A} = (KH_{AR}H_{RE}, nH_{AR}H_{RE})$. In the same way, he can impersonate legitimate user B and forge a message by multiplying RX_{E_A} and any coefficient. Then A can also derive the right challenge n even with a trusted relay. Base on this observation, two individual shared keys are used to prevent the impersonation and replay attack, because RX_{R1} and RX_{R2} keep the multiplicative relationship no longer. The prover needs to calculate the challenge n first and then send back (K_2, n). Any other users cannot forge the message in step $2'$ and cannot succeed in the authentication.

Actually, PHY-AUR defends against an active attacker E_A through three features: (1) two different shared key are used; (2)

all signals defined in the protocol do not have pilots or pre-known preambles for channel estimation; (3) legitimate users maintain the received signal strength (RSS) of all signals except for the authentication request, within the expected range. Feature (3) is feasible because path-loss in both directions at all links are identical during channel coherence time, and the path-loss from prover to relay and from relay to verifier are measured during the transmission of request which has constant power.

If E_A pretends to be the verifier A, it must wait until a legitimate prover initiates a conversation with it coincidentally. However, since the real verifier also exists in the network, both the verifier and E_A will respond to the prover, the RSS at relay exceeds the expected range, and the relay can easily detect E_A. Similarly, the prover can detect E_A who pretends to be the relay.

3) Others: The challenge and response messages do not necessarily travel the reversal path, since A and B can decode the messages using the share key. This is different from PHY-CRAMR. However, the interval between the challenge and response messages should be short to avoid unnecessary security issues. After all steps are finished, n and $H_{AR}H_{RB}$ are shared by two participants and can also be used to generate session key $SK = \mathcal{F}(n, H_{AR}H_{RB})$ for the further secure communications. We do not intend to discuss key generation function $\mathcal{F}$ in depth here, which is out of the scope of our considerations. The protocol can implement authentication and key generation simultaneously with two shared keys K_1 and K_2 between A and B in multi-hop wireless networks. Even if the authentication is false accepted, the shared session key SK originated from n and $H_{AR}H_{RB}$ cannot be obtained by the adversary.

D. Extension for More Hops

PHY-AUR is also scalable and can be extended to networks with more hops. The general case of PHY-AUR in multi-hop networks is shown in Figure 5. Similar to PHY-CRAMR, the channel effects will accumulate in each link. The simulation result for multiple hops is shown in figure 12.

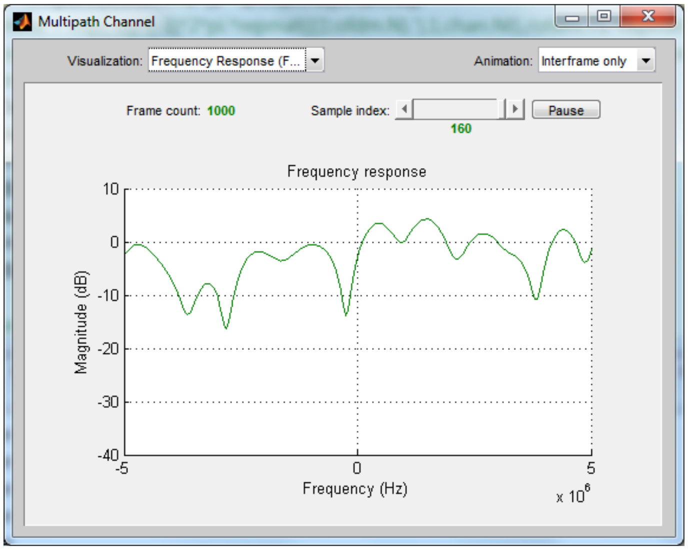
PHY-AUR utilizes the dividing operations to cancel out the channel effects, while PHY-CRAMR makes it by the reciprocal of channel response. Both of them do not employ channel estimation to prevent the information be revealed. Meanwhile, they can be easily extended to more hops due to the natural products of channel state information after each hop.

VI. Performance Evaluation

The random wireless fading channel and AWGN will affect the performance of the protocols. PHY-CRAMR requires short processing time to limit the time-varying nature of the channel, while PHY-AUR is not sensitive to it. Both the fading and AWGN can worsen the signal quality, and the stochastic property and location decorrelation of the channel make the attacks difficult. The performance of the proposed protocols is evaluated by the ROC, which reflects the relationship between successful authentication rate and false acceptance rate. The steeper (higher) the ROC curve is, the better the performance.

A. Simulation Settings

We conduct our simulations in MATLAB. The sample rate is fixed to be 10 MHz. Each OFDM symbol includes $N = 64$ data sub-carriers and Guard Interval has $GI = 16$ samples. The shared key K and the random challenge n are both complex vectors with the same length $M(< N)$. They are put into OFDM symbols sequentially. The ROC curve comes from 1000 iterations which represent 1000 pairs of authentication procedures. SNR ranges from 10 dB to 30 dB. The statistical Rayleigh fading channel model is adopted and can be configured conveniently in MATLAB. The rural and urban channels are differentiated by $MP = 10$ and $MP = 20$ multi-paths, respectively. The delays for multi-paths are randomly selected and the corresponding gains are normalized. The maximum delay spread is $\Delta = \frac{16Sa}{10MSa/s} = 1.6\mu s$, the same time span of GI. Figure 8 shows an example of frequency response of the channel with 20 multi-paths.


Multipath Channel

Visualization: Frequency Response (F...

Animation: Interframe only

Frame count: 1000

Sample index: 160

Fig. 8. Frequency response of the channel

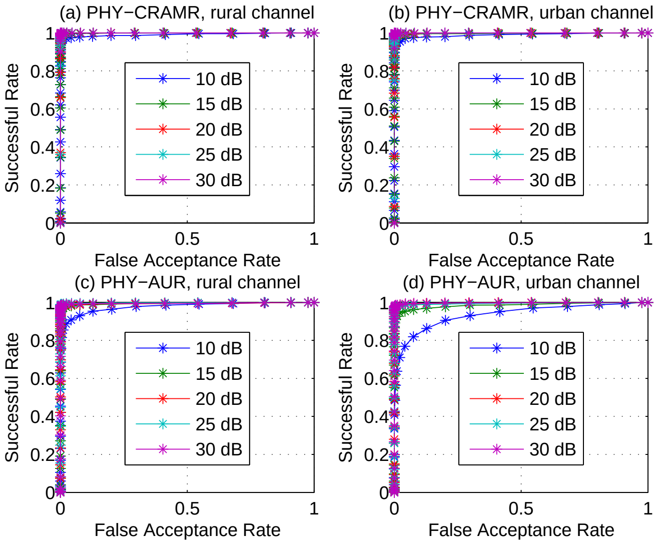


Fig. 9. ROC curve for PHY-CRAMR (a)(b) and PHY-AUR(c)(d) at different SNR in rural(a)(c) and urban(b)(d) area, when key length M=60

B. Impact of Channel

When key length $M = 60$, at different SNR, the ROC curves for PHY-CRAMR in rural and urban channel models are shown in figure 9(a) and 9(b), while PHY-AUR are shown in figure 9(c) and 9(d). The performance in the rural environment is better than in the urban area, because of fewer multi-paths which impact signal quality. Higher SNR results in better performance for both channel models. As we expected, more AWGN leads

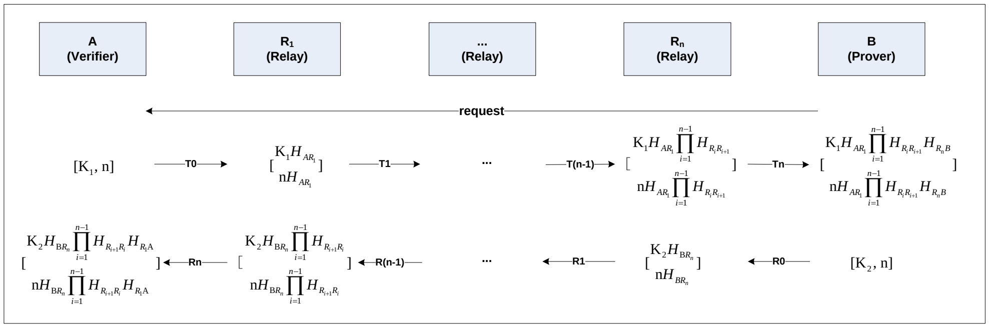
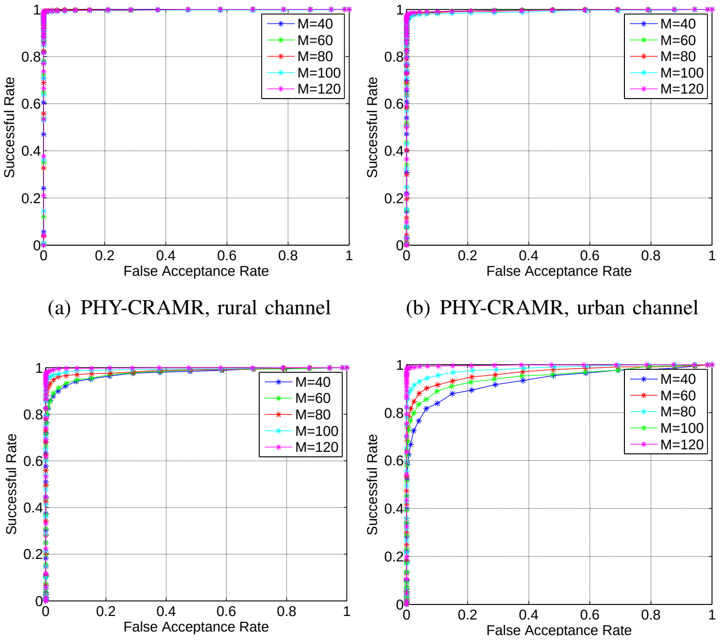

A
(Verifier)
R_1
(Relay)
...
(Relay)
R_n
(Relay)
B
(Prover)
request
$[K_1, n]$
T0
$[K_1 H_{AR_1}; nH_{AR_1}]$
T1
...
T(n-1)
$[K_1 H_{AR_1} \prod_{i=1}^{n-1} H_{R_i R_{i+1}}; nH_{AR_1} \prod_{i=1}^{n-1} H_{R_i R_{i+1}}]$
Tn
$[K_1 H_{AR_1} \prod_{i=1}^{n-1} H_{R_i R_{i+1}} H_{R_n B}; nH_{AR_1} \prod_{i=1}^{n-1} H_{R_i R_{i+1}} H_{R_n B}]$
$[K_2 H_{BR_n} \prod_{i=1}^{n-1} H_{R_{i+1} R_i} H_{R_1 A}; nH_{BR_n} \prod_{i=1}^{n-1} H_{R_{i+1} R_i} H_{R_1 A}]$
Rn
$[K_2 H_{BR_n} \prod_{i=1}^{n-1} H_{R_{i+1} R_i}; nH_{BR_n} \prod_{i=1}^{n-1} H_{R_{i+1} R_i}]$
R(n-1)
...
R1
$[K_2 H_{BR_n}; nH_{BR_n}]$
R0
$[K_2, n]$

Fig. 7. General case of PHY-AUR in multi-hop networks

to worse performance. As the figures illustrate, the successful authentication rates almost reach 100% for both protocols under both channel models when $M = 60$ and SNR$>$ 10 dB.

C. Impact of Key Length

The length M of K and n is also a parameter that affects the performance. In figure 10(a) and 10(b), we can see that the impact of key length on the performance of PHY-CRAMR is not significant when SNR=20 dB. Under this condition, a key length of 40 already achieves almost 100% successful rate. However, figure 10(c) and 10(d) show that the performance of PHY-AUR improves with increased key lengths. This may be due to the operation of correlation when verifying authentication. The longer length results in a more accurate estimation of the correlation.



(a) PHY-CRAMR, rural channel

(b) PHY-CRAMR, urban channel

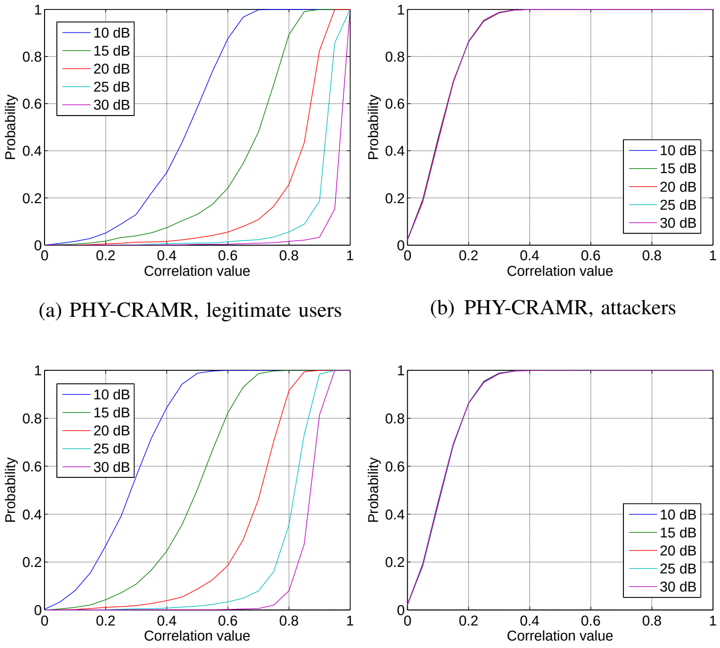
(c) PHY-AUR, rural channel

(d) PHY-AUR, urban channel

Fig. 10. ROC curves with different key length M when SNR=20 dB

D. Correlation Distribution

We can also take a look at the distribution of correlations calculated in the verifying steps further. Figure 11 shows the cumulative distribution function (CDF) curves of correlation distributions in two protocols with multipath number $MP = 10$, key length $M = 60$ and different SNRs. When SNR increases, both protocols can gain relative higher correlations for legitimate users. The attackers, who can only guess the shared key shared, keeps a constant correlation distribution under different SNR, and the value is much lower than the results from legitimate users.



(a) PHY-CRAMR, legitimate users

(b) PHY-CRAMR, attackers

(c) PHY-AUR, legitimate users

(d) PHY-AUR, attackers

Fig. 11. CDF of correlation distributions under different SNRs (MP=10, M=60)

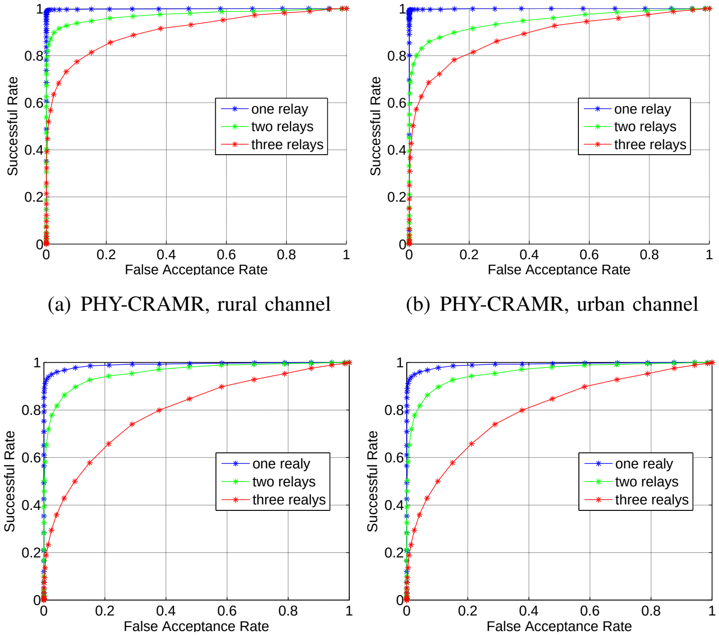
E. Impact of Relay Number

Both PHY-CRAMR and PHY-AUR have the potential to be extended to wireless networks with more hops. We also conduct simulations with more relays in the wireless networks. Figure 12 shows the simulation result for different number of relays when SNR=20 dB. When the hop count increases, the performances of both mechanisms degrade due to signal path loss and accumulated noise. Signal amplification and noise mitigation mechanisms can be integrated to improve the performance.

VII. Discussion

A. Two-way Authentication

Secure communications usually require the participants to authenticate each other. Although only the one-way authentication mechanism is discussed, the two-way authentication can be implemented in the same way. The communication overhead can be doubled.



(a) PHY-CRAMR, rural channel (b) PHY-CRAMR, urban channel

(c) PHY-AUR, rural channel (d) PHY-AUR, urban channel

Fig. 12. ROC curve with different numbers of relays (M=60, SNR=20 dB)

B. *MIMO Enhancement*

MIMO technology can be used to further improve the security strength since longer authentication keys can be conveyed using the same amount of time. Beamforming mechanism can be applied to achieve energy efficiency and tackle channel diversity.

C. *Heterogeneous Network*

Both PHY-CRAMR and PHY-AUR can be applied to heterogeneous networks or cognitive radio networks while different hops may use different channels or frequencies. The transmission rate at different hops may need to change in order to adapt to different channel conditions and bandwidths.

VIII. Conclusions

We proposed two authentication protocols based on challenge-response mechanism, named PHY-CRAMR and PHY-AUR, at the physical layer for wireless networks with a relay. OFDM technique is adopted to modulate the challenge and response messages. They both exploit the unique properties of wireless fading channel, such as randomness and location decorrelation, to hide the authentic message. By eliminating pilots, pre-known synchronous headers, and any reference signals, the attacker cannot gain any knowledge about the channel state information and the secret messages between legitimate users. PHY-CRAMR provides a secure authentication solution when the trusted relay is assumed, while PHY-AUR is immune to both outside and inside attacks with an untrusted relay.

Both protocols are analyzed and simulated to verify the performance. The simulation results show that both PHY-CRAMR and PHY-AUR can obtain a high successful authentication rate and a low false acceptance rate under various channel environments.

Comparing with previous work, our schemes are simple, secure, robust and scalable in multi-hop wireless networks. Although unilateral procedures of the protocols are performed, the mutual authentication can be implemented further.

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 *Proceedings of the 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 *Proceedings of the 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: Proceedings of the 3th ACM Conference on Wireless Network Security*. ACM, 2010, pp. 89–98.

[9] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *Information Forensics and Security, IEEE Transactions on*, 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," *Wireless Communications, IEEE Transactions on*, vol. 10, no. 12, pp. 4270 –4281, december 2011.

[11] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "Phy-cram: Physical layer challenge- response authentication for wireless networks," *IEEE Journal on Selected Areas in Communications - Signal Processing Techniques for Wireless Physical Layer Security*, to appear.

[12] 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.

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

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

[15] 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.

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

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

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

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

[20] D. Lee and K. Cheun, "A new symbol timing recovery algorithm for ofdm systems," in *Consumer Electronics*, vol. 43, no. 3. IEEE Transactions, Aug 1997, p. 767775.

[21] M. Strasser, C. Pöpper, and S. Čapkun, "Efficient uncoordinated fhss anti-jamming communication," in *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, ser. MobiHoc '09. New York, NY, USA: ACM, 2009, pp. 207–218. [Online]. Available: http://doi.acm.org/10.1145/1530748.1530778

[22] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential dsss: Jamming-resistant wireless broadcast communication," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–9.