Channel-Based Authentication Game in MIMO Systems

Liang Xiao*‡, Tianhua Chen*, Guoan Han*, Weihua Zhuang†, Limin Sun‡
*Dept. of CE, Xiamen University, China. Email: lxiao@xmu.edu.cn
†Dept. of ECE, University of Waterloo, Canada. Email: wzhuang@uwaterloo.ca
‡Beijing Key Laboratory of IOT Information Security Technology,
Institute of Information Engineering, CAS, China. sunlimi@iie.ac.cn

***Abstract*—In this paper, we investigate the PHY-layer authentication that exploits the spatial decorrelation property of radio channel information to detect spoofing attacks in multiple-input multiple-output (MIMO) systems. We formulate the interactions between a receiver that applies the PHY-layer MIMO authentication technique and a spoofing node as a zero-sum game. In this game, the receiver chooses the test threshold of the hypothesis test of the PHY-layer authentication to maximize its utility based on the Bayesian risk in the spoofing detection. The adversary chooses its attack frequency, i.e., how often a spoofing packet is sent over multiple antennas. The unique Nash equilibrium of the static MIMO authentication game is derived and the condition for its existence is presented regarding the number of antennas. We also investigate the dynamic authentication game, and propose a PHY-layer MIMO authentication based on Q-learning to achieve the optimal test threshold in the spoofing detection via trials, and implement it over universal software radio peripherals. The performance of the spoofing detection algorithm is evaluated via experiments in indoor environments.**

***Index Terms*—MIMO, PHY-layer authentication, spoofing detection, game theory, learning**

I. Introduction

Multiple-input multiple-output (MIMO) techniques can improve the capacity and reliability of wireless communications, and enhance the resistance against eavesdropping [1]. However, MIMO transmissions are vulnerable to spoofing attacks, in which a spoofing node with multiple transmit antennas claims to be another transmitter by using a faked identity such as a faked MAC address. Spoofing attacks can not only result in illegal advantages and access rights of the adversary, but also lead to man-in-the-middle attacks and denial-of-service attacks [2]. Therefore, physical (PHY)-layer authentication techniques have been proposed to exploit the PHY-layer properties of radio propagations, such as received signal strengths [2], [3] and channel impulse responses [4] to detect spoofing attacks in wireless networks.

Game theoretic study on PHY-layer spoofing detection in [5] investigates the interactions between an attacker and a receiver that applies the PHY-layer authentication scheme. If radio nodes are unaware of the channel model in dynamic wireless networks, the receiver can apply Q-learning, the model-free reinforcement learning techniques [6], to derive the optimal hypothesis test policy to maximize its expected long-term accumulative utility via trial-and-error [7].

In this paper, we extend the game theoretic study on PHY-layer authentication to MIMO systems and formulate a channel-based MIMO authentication game. In the zero-sum game, a spoofing node chooses how frequently to send spoofing signals to maximize its utility based on the Bayesian risks in the spoofing detection. The receiver determines its test threshold in the hypothesis test of the channel-based spoofing detection. The Nash equilibrium (NE) of the static MIMO authentication game is presented, showing that the number of antennas affects the spoofing frequency and detection.

We also investigate a dynamic MIMO authentication game, in which the receiver exploits the received signal strength indicators (RSSIs) without being aware of the radio channel model and the spoofing policy. Based on Q-learning, a receiver decides its test threshold in the hypothesis test by updating a quality function of each state-action combination and can achieve the optimal policy if this selection is a finite Markov decision process.

The contributions of our work can be summarized as follows:

(1) We formulate the interactions between a receiver performing PHY-layer spoofing detection and a spoofing node with multiple antennas as a zero-sum MIMO authentication game. The NE of the game is derived. The condition and the uniqueness of the NE are discussed.

(2) We propose a PHY-layer MIMO spoofing detection based on Q-learning in dynamic wireless networks, and perform experiments over universal software radio peripherals (USRPs) in indoor environments to validate its efficacy.

The rest of this paper is organized as follows. We review related work in Section II, and present the system model in Section III. We formulate the PHY-layer MIMO authentication game in Section IV, and present dynamic PHY-layer MIMO game with Q-learning in Section V. Experiment results are presented in Section VI. In Section VII, we conclude this work.

This work was supported by 863 high technology plan (Grant No. 2015AA01A707).

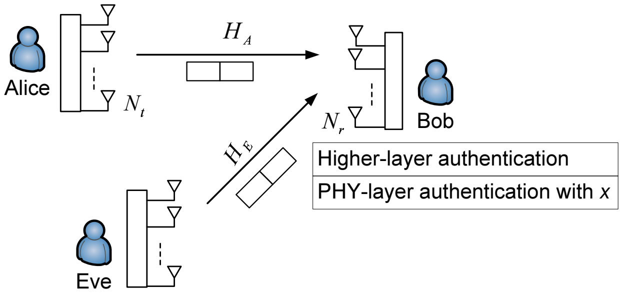
II. Related Work

The spatial decorrelation property of wireless medium has been exploited in [8] to detect spoofing attacks in MIMO systems. Secrecy beamforming and artificial noise transmission have been applied in [9] to enhance the PHY-layer secrecy in multiple antennas wireless systems. A channel responses based detection scheme for MIMO systems was developed in [10] to detect primary user emulation attacks in cognitive radio networks. A channel-based authentication scheme over MIMO fading channels proposed in [11] can address multiple impersonation attack strategies.

A game-theoretic study of channel assignment performed in [12] investigated the MIMO transmissions in time-varying wireless channels, and a learning-based algorithm was proposed to approach to the NE strategy. A cooperative game formulated in [13] investigates the path loss and the transmit power for power budget for all the transmit radars to track a target in MIMO networks. An MIMO transmission game introduced in [14] investigates the dual-threat attacker that performs both eavesdropping and jamming.

We have formulated a zero-sum authentication game in [5] to investigate the interactions between a legitimate receiver and a spoofing node in a single antenna system. Compared with our previous work in [5], we extend the study to MIMO systems and investigate the impacts of the number of antennas on the PHY-layer authentication game. We also provide the NE condition of the MIMO PHY-layer authentication game, considering the spoofing cost in the utility function, which was omitted in [5].

III. System Model



H_A
Alice
N_t
N_r
Bob
H_E
Higher-layer authentication
PHY-layer authentication with *x*
Eve

Fig. 1. Illustration of a spoofing detection game consisting of a legal transmitter Alice with N_t antennas, a spoofing node Eve, and a receiver Bob with N_r antennas.

As shown in Fig. 1, we consider the spoofing detection of a receiver called Bob (B), the legal transmitter called Alice (A) and spoofing node called Eve (E) in a $N_t \times N_r$ MIMO system. The signals are sent over N_t antennas each at center frequency f_0 with bandwidth W.

Based on the training symbols or preambles of the signal, Bob estimates the channel gain and compares it with the channel record of Alice to determine whether the corresponding signal is actually send by Alice. More specifically, Bob obtains the channel vector at time k denoted by $\mathbf{H}_t^k = \left[h_t^k(m,n)\right]_{1\leq m\leq N_t,\ 1\leq n\leq N_r}$, and the channel record of Alice denoted by $\hat{\mathbf{H}} = \left[\hat{h}(m,n)\right]_{1\leq m\leq N_t,\ 1\leq n\leq N_r}$, where $h_t(m,n)$ is the channel gain from the m-th transmit antenna to the n-th receive antenna at time k, while $\hat{h}(m,n)$ is the corresponding channel record of Alice in the previous transmission. Bob estimates the channel gains at M tones for each of the $N_t N_r$ antenna pairs.

Let $\mathbf{x}_{A/E}^k$ denote the N_t-dimensional transmitted signal from Alice (or Eve) at time k, $\mathbf{H}_{A/E}^k$ be the $N_t \times N_r$ matrix of channel gain between Alice (or Eve) and Bob, and $\mathbf{z}_{A/E}$ be the corresponding N_r-dimensional noise at the receiver. The signal from Alice (or Eve) received by Bob at time k is denoted by $\mathbf{y}_{A/E}^k$ and given respectively by

$$\begin{aligned} \mathbf{y}_A^k &= \mathbf{x}_A^k \mathbf{H}_A^k + \mathbf{z}_A \\ \mathbf{y}_E^k &= \mathbf{x}_E^k \mathbf{H}_E^k + \mathbf{z}_E. \end{aligned} \tag{1}$$

Let σ^2 be the average power gain along the path from Alice to Bob, ρ be the average signal-to-noise ratio (SNR) of the signal received by Bob, α indicate the channel time variation due to the radio environment changes, and β present the average ratio of the SNR of the signal sent by Eve to that of Alice. For ease of reference, the commonly used notations are summarized in TABLE 1.

TABLE I
SUMMARY OF SYMBOLS AND NOTATIONS

α	Channel gain time variation
β	Average ratio of the SNR of Eve to that of Alice
ρ	Average SNR of the received signal
$N_{t/r}$	Number of transmit/receive antennas
$H_{A/E}^k$	Channel gain from Alice/Eve to Bob at time k
$\mathbf{H}_t^k$	Channel vector under test at time k
$\hat{\mathbf{H}}$	Channel record of signals from Alice
M	Number of frequency samples
$x \in [0,\infty)$	Test threshold
$y \in [0,1]$	Spoofing frequency
$u_{B/E}$	Immediate utility of Bob/Eve
$G_{1/0}$	Gain of Bob to accept/reject a signal from Alice/Eve
$C_{1/0}$	Cost of Bob to reject/accept a signal from Alice/Eve
C_s	Cost of Eve to send a spoofing signal
$p_{f/m}$	False alarm rate/miss detection rate

IV. MIMO PHY-Layer Authentication Game

Based on the spatial decorrelation of radio channel states, Bob detects spoofing attacks by comparing the estimated channel matrix at time k, $\mathbf{H}_t^k$ with the channel record of Alice $\hat{\mathbf{H}}$. In the spoofing detection, the null hypothesis $\mathcal{H}_0$ indicates that the signal is indeed sent by Alice, while the alternative hypothesis $\mathcal{H}_1$ indicates that the claimant terminal is Eve. The spoofing detection builds the hypothesis test given by

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{H}_t^k = \mathbf{H}_A^k \\ \mathcal{H}_1 &: \mathbf{H}_t^k \neq \mathbf{H}_A^k. \end{aligned} \tag{2}$$

The hypothesis test is based on the sampled channel frequency responses over the N_tN_r antenna pairs at M frequencies. According to (2), the channel responses are significantly different from the channel records of Alice, Bob reports an spoofing alarm at time k. Otherwise, there is every reason to believe that the transmitter is Alice. Bob calculates the statistic, denoted by L, that was chosen by [5] as the normalized Euclidean distance between the channel response $\mathbf{H}_t^k$ and the channel record $\hat{\mathbf{H}}$. Thus, we have

$$L\left(\mathbf{H}_t^k, \hat{\mathbf{H}}\right) = \frac{\left\|\mathbf{H}_t^k - \hat{\mathbf{H}}\right\|^2}{\left\|\hat{\mathbf{H}}\right\|^2}, \tag{3}$$

where $\|\cdot\|$ is the Frobenius norm. Bob compares the test threshold $x \in [0, \infty)$ with the test statistic L. More specifically, if the test statistic is less than x, Bob accepts the null hypothesis $\mathcal{H}_0$; otherwise, Bob accepts $\mathcal{H}_1$. Thus the hypothesis test in the PHY-layer spoofing detection is given by

$$L\left(\mathbf{H}_t^k, \hat{\mathbf{H}}\right) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} x. \tag{4}$$

The detection accuracy of the PHY-layer authentication in (4) depends on the test threshold x. A small test threshold increases the probability to successfully detect Eve, and the probability for Bob to take Alice as Eve. The false alarm rate, denoted by p_f, is the probability that Alice's signal is viewed as a spoofing one, i.e.,

$$p_f(x) = \Pr\left(\mathcal{H}_1|\mathcal{H}_0\right) = \Pr\left(L\left(\mathbf{H}_A^k, \hat{\mathbf{H}}\right) > x\right), \tag{5}$$

where $\Pr(\cdot|\cdot)$ is the conditional probability. It is clear that the probability for Bob to accept a signal from Alice is $1 - p_f$. Similarly, the miss detection rate, denoted by p_m, is defined as the probability that a spoofing signal passes the detection, which is given by

$$p_m(x) = \Pr\left(\mathcal{H}_0|\mathcal{H}_1\right) = \Pr\left(L\left(\mathbf{H}_E^k, \hat{\mathbf{H}}\right) \leq x\right). \tag{6}$$

The probability for Bob to reject a signal from Eve is $1 - p_m$.

Bob applies the higher-layer authentication methods such as [15], [16] to process the signal that passes the PHY-layer authentication. A signal is accepted by Bob if and only if it passes both the PHY-layer and higher-layer authentications. In this case, the channel record of Alice is updated with $\hat{\mathbf{H}} \leftarrow \mathbf{H}_t^k$.

The PHY-layer spoofing detection can be formulated as a zero-sum game denoted by $\mathbf{G}$ consisting of a receiver (Bob) and a spoofing node (Eve). Eve sends faked frames and pretends to be a legal transmitter Alice, while Bob applies the PHY-layer authentication to discriminate the spoofing signals. The action of Eve, denoted by $y \in [0, 1]$, is the probability that Eve sends a spoofing frame. Bob chooses the test threshold in the hypothesis test, $x \in [0, \infty)$, in the spoofing detection. In the zero-sum game, the utility of Bob and that of Eve, denoted by u_B and u_E, respectively, satisfy $u_E(x, y) = -u_B(x, y)$.

The payoff for Bob to accept a legitimate signal (or reject a faked one) is denoted by G_1 (or G_0). The cost for Bob to falsely reject a legitimate signal (or accept a faked one) is denoted by C_0 (or C_1), while the cost for Eve to send a spoofing signal is denoted by C_s. Based on the detection accuracy and the power consumption in the spoofing detection in the time slot, the utility of Bob, denoted by u_B, can be defined as

$$\begin{aligned} u_B(x, y) = C_s y + \Big(G_1\big(1 - p_f\left(x\right)\big) - C_1 p_f(x)\Big)(1 - y) \\ + \Big(G_0\big(1 - p_m\left(x\right)\big) - C_0 p_m(x)\Big)y = -u_E(x, y). \end{aligned} \tag{7}$$

In summary, we consider a PHY-layer authentication zero-sum game, $\mathbf{G} = \langle\{B, E\}, \{x, y\}, \{u_B, u_E\}\rangle$, in which Bob chooses its test threshold $x \in [0, \infty)$, while Eve determines its spoofing frequency $y \in [0, 1]$.

As a concrete example, we assume that Bob detects spoofing based on the estimated channel frequency responses of the radio signals $\mathbf{H}_t^k$ and the channel record of Alice $\hat{\mathbf{H}}$. For simplicity, we also assume zero phase shift between channel measurements. In the frequency-selective Rayleigh channel models, Bob performs the generalized likelihood ratio test, in which the test statistic in [8] is replaced by L', as

$$L'\left(\mathbf{H}_t^k, \hat{\mathbf{H}}\right) = \left\|\mathbf{H}_t^k - \hat{\mathbf{H}}\right\|^2 \sim \chi^2\left(2N_tN_rM\right), \tag{8}$$

where $\chi^2(m)$ is a Chi-square distribution with m degrees of freedom.

Based on the test statistic in (8), it is shown in [8] that the false alarm rate and the miss detection rate of the hypotheses test in the spoofing detection are given by

$$p_f(x) = 1 - F_{\chi^2}\left(\frac{2x\rho}{\sigma^2\left(2 + \alpha\rho\right)}, 2N_tN_rM\right) \tag{9}$$

$$p_m(x) = F_{\chi^2}\left(\frac{2x\rho}{\sigma^2(2 + \rho + \beta\rho)}, 2N_tN_rM\right), \tag{10}$$

where $F_{\chi^2}(\cdot, m)$ is the cumulative distribution function of a Chi-square distribution with m degrees of freedom.

The Nash equilibrium of the static PHY-layer authentication game $\mathbf{G}$ is denoted by (x^*, y^*). By definition, neither the receiver nor the adversary can increase its utility by unilaterally choosing a different strategy, i.e.,

$$x^* = \arg\max_{x \geq 0}\ u_B\left(x, y^*\right) \tag{11}$$

$$y^* = \arg\min_{0 \leq y \leq 1}\ u_B\left(x^*, y\right). \tag{12}$$

Theorem 1. *If the channel gains over M frequencies are independent and identically distributed, and*

$$\begin{cases} C_s < G_1 + C_0 & \text{(13a)} \\ \alpha \leq \beta + 1, & \text{(13b)} \end{cases}$$

the static MIMO PHY-layer authentication game $\mathbf{G}$ has a unique NE (x^*, y^*), given by (14) and (15).

Proof. By (9) and (10), we have $p_f(0) = 1$, $p_m(0) = 0$, $\lim_{x\to\infty} p_f(x) = 0$ and $\lim_{x\to\infty} p_m(x) = 1$. By (7), we have

$$\frac{\partial u_E}{\partial y} = G_1 - G_0 - (G_1 + C_1)p_f(x) + (G_0 + C_0)p_m(x) - C_s, \tag{16}$$

$$(G_1 + C_1) F_{\chi^2}\left(\frac{2\rho x^*}{\sigma^2(2+\alpha\rho)}, 2N_tN_rM\right) = G_0 + C_s + C_1 - (G_0+C_0) F_{\chi^2}\left(\frac{2\rho x^*}{\sigma^2(2+\rho+\beta\rho)}, 2N_tN_rM\right) \tag{14}$$

$$y^* = \left(1 + \frac{G_0+C_0}{G_1+C_1}\left(\frac{2\rho^{-1}+\alpha}{2\rho^{-1}+1+\beta}\right)^{N_tN_rM} e^{\frac{(\beta+1-\alpha)\rho^2 x^*}{\sigma^2(2+\alpha\rho)(2+\rho+\beta\rho)}}\right)^{-1} \tag{15}$$

indicating that if $G_1 + C_0 > C_s$,

$$\frac{\partial u_E(0,y)}{\partial y} = -G_0 - C_1 - C_s < 0 \tag{17}$$

$$\lim_{x\to\infty} \frac{\partial u_E(x,y)}{\partial y} = G_1 + C_0 - C_s > 0. \tag{18}$$

Let $\hat{x}$ be the solution of $\partial u_E(x,y)/\partial y = 0$. By (16), (9) and (10), we have (14) after simplication, showing that $\hat{x}$ is unique and positive. If $x > \hat{x}$, we have $\partial u_E(x,y)/\partial y > 0$; Otherwise, if $0 \leq x < \hat{x}$, we have $\partial u_E(x,y)/\partial y < 0$. By (9) and (10), we have

$$\frac{\partial p_f(x)}{\partial x} = -\frac{x^{N_tN_rM-1}e^{-\frac{x\rho}{\sigma^2(2+\alpha\rho)}}}{\left(\sigma^2(2/\rho+\alpha)\right)^{N_tN_rM}\Gamma\left(N_tN_rM\right)} \tag{19}$$

$$\frac{\partial p_m(x)}{\partial x} = \frac{x^{N_tN_rM-1}e^{-\frac{x\rho}{\sigma^2(2+\rho+\beta\rho)}}}{\left(\sigma^2(2/\rho+1+\beta)\right)^{N_tN_rM}\Gamma\left(N_tN_rM\right)}, \tag{20}$$

where $\Gamma(\cdot)$ is the Gamma function.

By (19), (20) and (7), we have

$$\frac{\partial u_B(x,y)}{\partial x} = \frac{x^{N_tN_rM-1}e^{-\frac{x\rho}{\sigma^2(2+\alpha\rho)}}}{\sigma^{2N_tN_rM}\Gamma\left(N_tN_rM\right)} \left(\frac{(G_1+C_1)(1-y)}{(2/\rho+\alpha)^{N_tN_rM}} - \frac{(G_0+C_0)ye^{\frac{(\beta+1-\alpha)x\rho^2}{(2+\alpha\rho)(2+\rho+\beta\rho)\sigma^2}}}{(2/\rho+1+\beta)^{N_tN_rM}}\right). \tag{21}$$

As $\partial u_E(\hat{x},y)/\partial y = 0$, $u_E(\hat{x},y)$ is constant, $\forall y \in [0,1]$. Let $\hat{y}$ be the solution of $\partial u_B(\hat{x},y)/\partial x = 0$, which can be simplified by (21) into (15). By (21), if $\beta + 1 \geq \alpha$, we have $\partial u_B(x,\hat{y})/\partial x \geq 0$ for $0 < x < \hat{x}$ and $\partial u_B(x,\hat{y})/\partial x \leq 0$ for $x > \hat{x}$. Thus, (11) and (12) hold for $(x^*,y^*) = (\hat{x},\hat{y})$.

Next, we consider the uniqueness of the NE by assuming that there exists another NE, denoted by $(x',y') \neq (x^*,y^*)$. If $0 \leq x' < x^*$, we have $\partial u_E(x',y)/\partial y < 0$ and thus $y' = 0$. By (21), we have $\partial u_B(x,y')/\partial x \geq 0$, indicating that $u_B(x',y') < u_B(x^*,y')$, contradicting to the assumption that (x',y') is an NE. If $x' > x^*$, we have $\partial u_E(x',y)/\partial y > 0$, yielding $y' = 1$. By (21), we have $\partial u_B(x,y')/\partial x \leq 0$, and thus $u_B(x',y') < u_B(x^*,y')$, contradicting to the assumption. Thus $(x^*,y^*) = (\hat{x},\hat{y})$ is a unique NE in the game. □

Theorem 2. *The static MIMO PHY-layer authentication game* $\mathbf{G}$ *has no NE, if*

$$C_s \geq G_1 + C_0 \tag{22}$$

or

$$\begin{cases} C_s < G_1 + C_0 & (23a) \\ \alpha > \beta + 1. & (23b) \end{cases}$$

Proof. If $C_s \geq G_1 + C_0$, we have $\partial u_E(x,y)/\partial y < 0$, and thus $y^* = 0$. By (21), we have $\partial u_B(x,0)/\partial x \geq 0$, i.e., $x^* \to \infty$, and thus no NE exists.

If $C_s < G_1 + C_0$, similar to the proof to Theorem 1, no NE exists if $x^* \neq \hat{x}$, with $\hat{x}$ given by (14). Otherwise, if $x^* = \hat{x}$, we can infer from (21) and (11) that $\partial u_B(x^*,y^*)/\partial x = 0$, $\partial u_B(x,y^*)/\partial x > 0$, $\forall 0 < x < \hat{x}$, and $\partial u_B(x,y^*)/\partial x < 0$, $\forall x > \hat{x}$. However, if $\alpha > \beta + 1$, by (21) and (15), we have $\partial u_B(x,y^*)/\partial x < 0$, $\forall 0 < x < \hat{x}$, and $\partial u_B(x,y^*)/\partial x > 0$, $\forall x > \hat{x}$, indicating that $x^* \neq \hat{x}$. Thus, no NE exists in this case. □

By (14) and (15), the NE of game $\mathbf{G}$ depends on the spoofing cost and the relative channel time variation. Under a small spoofing cost and relative small channel gain time variation, i.e., (13), Bob chooses his test threshold and Eve decides her spoofing probability based on the gain, cost and channel conditions by (14) and (15) to maximize their individual payoffs. If the channel gain time variation is large, i.e., (23b), the channel responses change too fast to form a stable radio fingerprint for spoofing detection and thus no NE exists. Otherwise, under a large spoofing cost, i.e., (22), the attack motivation of Eve is suppressed and Bob chooses to use a high test threshold to avoid false alarm in the spoofing detection.

V. PHY-Layer MIMO Authentication with Q-Learning

The repeated interactions between Bob and Eve, who cannot accurately estimate the environment model and the action of the opponent in dynamic wireless networks can be formulated as a dynamic MIMO PHY-layer authentication game. The receiver Bob builds the hypothesis test in (4) to discriminate Alice from Eve. When receiving T frames in a time slot, Bob has an expected sum utility, denoted by U^k and defined as

$$U^k = \sum_{n=(k-1)T+1}^{kT} u_B^n(x,y), \tag{24}$$

where u_B^n is his immediate utility from the n-th frame given by (7).

For simplicity, both the false alarm rate and miss detection rate in each time slot are quantized into $X+1$ levels, i.e., $p_f^k, p_m^k \in \{l/X\}_{0\leq l\leq X}$. The state observed by Bob at time slot k, denoted by s^k, consists of both the false alarm rate and miss detection rate at the last time slot, i.e., $\mathrm{s}^k = \left[p_f^{k-1}, p_m^{k-1}\right] \in \{l/X, m/X\}_{0\leq l,m\leq X}$. The feasible test threshold in the spoofing detection is quantized into $K+1$ levels, i.e., $x^k \in \{l/K\}_{0\leq l\leq K}$.

Algorithm 1 MIMO PHY-layer authentication with Q-learning.

```
Set $Q(\mathbf{s}, x) = \mathbf{0}$, $V(\mathbf{s}) = \mathbf{0}$, $\forall x \in \{l/K\}_{0 \le l \le K}$, $\mathbf{s} \in \mathbf{S}$
for $k = 1, 2, 3, \ldots$ do
    Set $x^k$ via (25)
    for $n = 1$ to $T$ do
        Read the MAC address of packet $n$ at time $k$
        Channel estimation to obtain $\mathbf{H}_t$
        Calculate $L$ via (3)
        if $L \le x^k$ then
            Perform the higher-layer authentication
            if packet $n$ is accepted then
                $\hat{\mathbf{H}} \leftarrow \mathbf{H}_t$
            else
                Send spoofing alarm for packet $n$
            end if
        end if
    end for
    Observe $p_f$ and $p_m$ at time $k$
    $\mathbf{s}^{k+1} = [p_f, p_m]$
    Update $U^k$ via (24)
    $Q(\mathbf{s}^k, x^k) \leftarrow (1-\mu) Q(\mathbf{s}^k, x^k) + \mu \left(U^k + \delta V(\mathbf{s}^{k+1})\right)$
    $V(\mathbf{s}^k) \leftarrow \max_{x \in \{\frac{l}{K}\}_{0 \le l \le K}} Q(\mathbf{s}^k, x)$
end for
```

Let $Q(\mathbf{s}, x)$ be the Q-function at state $\mathbf{s}$ and action x. The value function, denoted by $V(\mathbf{s})$, represents the highest value of state $\mathbf{s}$. The test threshold is chosen by ϵ-greedy policy given by

$$\Pr(x = \dot{x}) = \begin{cases} 1 - \epsilon, & \dot{x} = \arg \max\limits_{x \in \{\frac{l}{K}\}_{0 \le l \le K}} Q(\mathbf{s}, x) \\ \frac{\epsilon}{K}, & \text{o.w.}, \end{cases} \tag{25}$$

with $0 < \epsilon \le 1$.

After choosing test threshold x^k, Bob builds the hypothesis test in (3) to authenticate the transmitter at time k. If a frame is rejected, Bob sends a spoofing alarm, calculates the spoofing detection accuracy at time k, and updates the expected sum utility U^k via (24).

The Q function is updated at a learning rate denoted by $\mu \in (0, 1]$, which represents the extent to which the new detection experience overrides the existing knowledge on the Q function. The discount factor $\delta \in (0, 1]$ indicates the uncertainty on the rewards in the future interaction. The Q function is updated based on the current system state $\mathbf{s}^k$ and test threshold x^k, as summarized in Algorithm 1.

VI. Performance Evaluation

Experiments have been performed to evaluate the performance of the proposed PHY-layer authentication in the dynamic games, in which 20 radio nodes each equipped with laptops and USRPs were placed in a $12 \times 9.5 \times 3$ m^3 office room as shown in Fig. 2, with $G_1 = C_1 = 6$, $G_0 = 9$, $C_0 = 4$, $C_s = 1$, $M = 3$, $f_0 = 2.42$ GHz, $W = 20$ MHz, $y = 0.5$, $\mu = 0.8$, $\delta = 0.7$ and $\epsilon = 0.1$. Each transmitter equipped with up to 5 antennas acted as either Alice or Eve, while Bob received signals with 3 antennas in the experiments. As comparison, we used the PHY-layer spoofing detection with a randomly selected threshold as a benchmark.

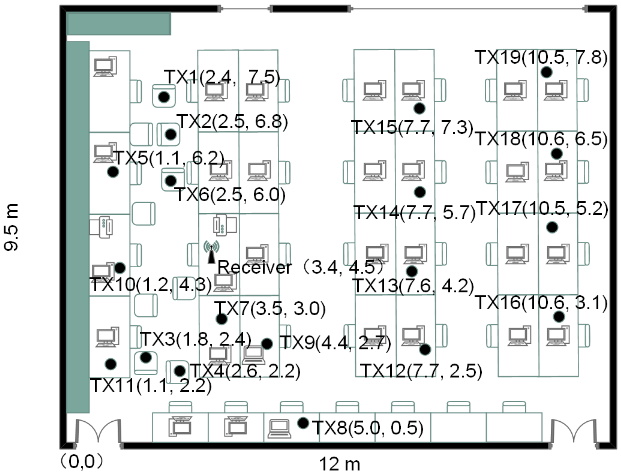


Fig. 2. Network topology of the experiments in a $12 \times 9.5 \times 3$ m^3 office room, consisting of 19 transmitter location, with $f_0 = 2.42$ GHz, $M = 3$ and $W = 20$ MHz.

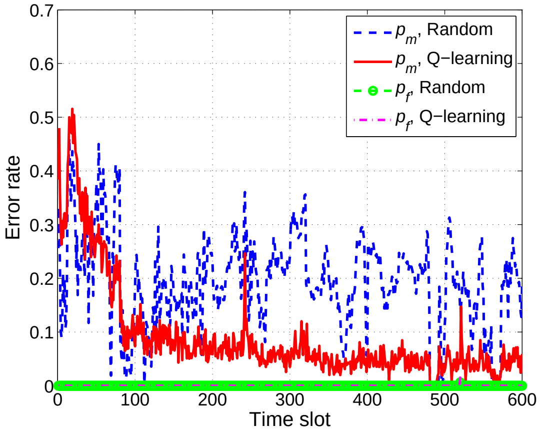
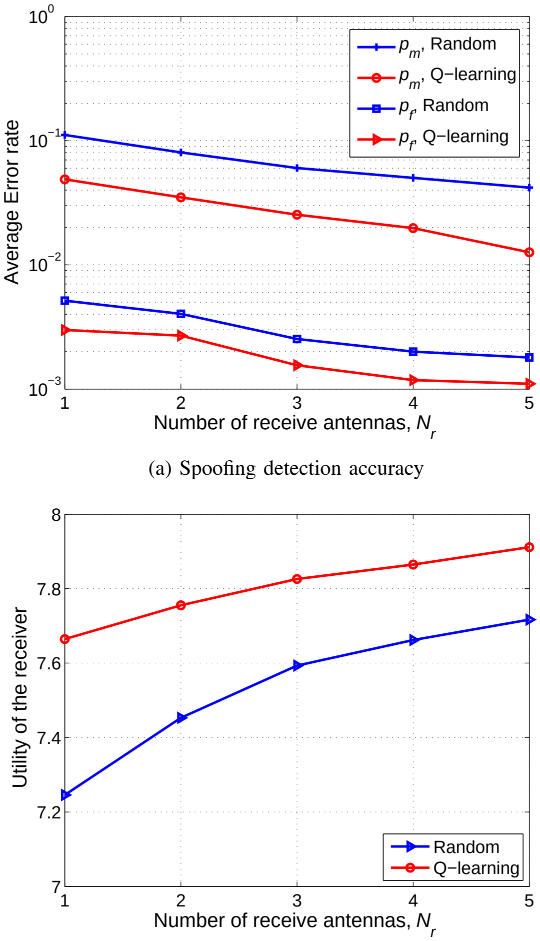


Fig. 3. Spoofing detection accuracy of the PHY-layer authentication in 5×3 MIMO systems, with $M = 3$, $f_0 = 2.42$ GHz and $W = 20$ MHz, in which Alice is at TX3 and Eve locates at TX16, in the wireless network with topology as shown in Fig. 2.

As shown in Fig. 3, the proposed spoofing detection improves the detection accuracy at a fast convergence speed. For example, if Alice and Eve are located at TX3 and TX 16, respectively, the miss detection rate decreases to 5% after 400 time slots, which is 38.9% less than the benchmark, and the false alarm rate is as small as 3×10^{-5}, which is 17.9% lower than that of the benchmark strategy.

As shown in Fig. 4(a), the spoofing detection accuracy improves with the number of receive antennas. For example, the miss detection rate decreases by 74.2%, and the false alarm rate decreases by 63.1%, if the number of receive



(a) Spoofing detection accuracy

(b) Utility of the receiver

Fig. 4. Average spoofing detection performance of the $5 \times N_r$ MIMO transmission with $M = 3$, $f_0 = 2.42$ GHz and $W = 20$ MHz in the experiments with topology as shown in Fig. 2.

antennas changes from 1 to 5. In addition, the proposed spoofing detection exceeds the benchmark strategy with higher detection accuracy and the performance gain increases with the number of receive antennas. For instance, the miss detection rate of the proposed authentication reduces by 60.7% and the false alarm rate decreases by 41.0%, in the 5×4 MIMO system. The performance gain regarding the miss detection rate rises from 56.5% to 69.9%, and the gain regarding the false alarm rate rises from 33.2% to 38.6%, if the number of receive antennas changes from 2 to 5.

Fig. 4(b) indicates that the average utility of the receiver increases with the number of receive antennas, e.g., the average utility increases by 3.2%, if N_r changes from 1 to 5. Finally, the proposed spoofing detection has performance gain regarding the utility compared with the benchmark scheme, e.g., the utility gain is 3.1% in the 3×5 MIMO system.

VII. Conclusions

In this work, we have investigated the PHY-layer authentication game in MIMO systems between a receiver and a spoofing node, and presented the unique NE of the game. We have also evaluated the dynamic PHY-layer authentication game with reinforcement learning, in which the test threshold in the spoofing detection is chosen via Q-learning. We have performed USRP-based experiments to validate the efficacy of the proposed Q-learning based PHY-layer authentication. For example, in the 5×3 MIMO transmission against an adversary with 20 MHz bandwidth at 2.42 GHz, the proposed PHY-layer spoofing detection can reduce the miss detection rate to 5%, which is 38.9% less than the benchmark spoofing detection scheme, and the false alarm rate is below 3×10^{-5}.

References

[1] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless Personal Commun.*, vol. 6, pp. 311–335, Mar. 1998.

[2] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, pp. 56–62, Oct. 2010.

[3] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 24, pp. 44–58, Jan. 2013.

[4] F. Liu, X. Wang, and S. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int'l Conf. Commun. (ICC)*, pp. 4724–4728, Budapest, Jun. 2013.

[5] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "PHY-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Vehicular Technology*, 2016, in press.

[6] C. J. Watkins and P. Dayan, "Q-learning," *Machine learning*, vol. 8, pp. 279–292, May 1992.

[7] L. Xiao, Y. Li, G. Liu, Q. Li, and W. Zhuang, "Spoofing detection with reinforcement learning in wireless networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1–5, San Diego, CA, Dec. 2015.

[8] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in *Proc. IEEE Information Sciences and Systems (CISS)*, pp. 642–646, Princeton, NJ, Mar. 2008.

[9] Y. W. P. Hong, P. C. Lan, and C. C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Trans. Signal Process. Mag.*, vol. 30, pp. 29–40, Sep. 2013.

[10] H. Wen, S. Li, X. Zhu, and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," *IEEE Network*, vol. 27, pp. 34–39, May 2013.

[11] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 2564–2573, Jul. 2012.

[12] L. C. Tseng, F. T. Chien, R. Y. Chang, W. H. Chung, C. Huang, and A. Marzouki, "Distributed channel assignment for network MIMO: Game-theoretic formulation and stochastic learning," *Wireless Networks*, vol. 21, pp. 1211–1226, May 2015.

[13] H. Chen, S. Ta, and B. Sun, "Cooperative game approach to power allocation for target tracking in distributed MIMO radar sensor networks," *Wireless Networks*, vol. 15, pp. 5423–5432, Oct. 2015.

[14] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, pp. 1695–1700, San Jose, CA, Oct. 2010.

[15] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, "Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 23, pp. 32–43, Jan. 2012.

[16] S. L. Yeo, W. Yap, J. K. Liu, and M. Henricksen, "Comments on "analysis and improvement of a secure and efficient handover authentication based on bilinear pairing functions"," *IEEE Commun. Lett.*, vol. 17, pp. 1521–1523, Aug. 2013.