Spoofing Detection with Reinforcement Learning in Wireless Networks

Liang Xiao*, Yan Li*, Guolong Liu*, Qiangda Li*, Weihua Zhuang†
*Dept. of Communication Engineering, Xiamen University, Xiamen, China. Email: lxiao@xmu.edu.cn
†Dept. of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. Email: wzhuang@uwaterloo.ca

***Abstract*—In this paper, we investigate the PHY-layer authentication in wireless networks, which exploits PHY-layer channel information such as the received signal strength indicators to detect spoofing attacks. The interactions between a legitimate receiver node and a spoofer are formulated as a PHY-authentication game. More specifically, the receiver chooses the test threshold in the hypothesis test of the spoofing detection to maximize its expected utility based on Bayesian risk to detect the spoofer. On the other hand, the spoofing node decides its attack strength, i.e., the frequency to send a spoofing packet that claims to use another node's MAC address, based on its individual utility in the zero-sum game. As it is challenging for most radio nodes to obtain the exact channel models in advance in a dynamic radio environment, we propose a spoofing detection scheme based on reinforcement learning techniques, which achieves the optimal test threshold in the spoofing detection via Q-learning and implement it over universal software radio peripherals (USRP). Experimental results are presented to validate its efficiency in spoofing detection.**

***Index Terms*—PHY-authentication, Spoofing detection, Game theory, Reinforcement learning.**

I. Introduction

Wireless networks have to address spoofing attacks, in which an attacker claims to be another node by using the faked MAC address and thus obtains illegal advantages and further performs man-in-the-middle or denial of service attacks. Traditional authentication techniques, such as digital signatures, cannot fully address spoofing attacks in wireless networks.

Recently, physical-layer authentication techniques are proposed to detect spoofing attacks by exploiting the physical layer properties of wireless channels. Received signal strength (RSS) [1]–[3], channel impulse response (CIR) [4], [5], channel state information (CSI) [6]–[8] and channel frequency response (CFR) [9], [10] have been used as the fingerprints of wireless channels to authenticate users. In [9], a binary hypothesis test was performed to compare the channel frequency response of the transmitter with its record. The test threshold in the hypothesis test of the spoofing detection determines the authentication accuracy; however, it is challenging to choose a proper threshold value under unknown channel parameters in a dynamic environment.

In this paper, a PHY-authentication scheme is proposed for a dynamic wireless network, which exploits the received signal strength indicator (RSSI) of the radio packets and builds a binary hypothesis test to detect spoofing attacks. The interactions between a receiver and a spoofing attacker are modeled as a zero-sum authentication game, in which utilities of the receiver and the spoofing attacker are based on Beyesian risk. The optimal test threshold in the binary hypothesis test of the spoofing detection is achieved by a reinforcement learning technique to maximize authentication accuracy. The proposed spoofing detection scheme is implemented over universal software radio peripherals (USRP) and verified via experimental results.

The contributions of this work lie in three aspects: (1) We propose the PHY-authentication scheme that exploits the received signal strength indicators of the message as a basis of spoofing detection, and formulate the interactions between a receiver and a spoofing attacker as a zero-sum authentication game in which Beyesian risk is introduced to describe the utilities of both players; (2) The optimal threshold in the hypothesis test of the spoofing detection is achieved via reinforcement-learning for a dynamic environment; (3) The proposed spoofing detection scheme is implemented over USRP and its performance is verified via field tests.

The rest of this paper is organized as follows. We briefly review related work in Section II. In Section III, we describe the system model and present the spoofing detection scheme. We formulate a PHY-authentication game in Section IV and present a reinforcement learning-based spoofing detection scheme in Section V. Experimental results are presented in Section VI. Finally, Section VII concludes this work.

II. Related Work

Physical layer authentication in wireless networks has attracted extensive attentions from the research community. In [2], the spatial correlation of RSS inherited from wireless nodes is used to detect spoofing attacks. A proximity-based authentication is proposed in [3], in which the RSS variations are used to test the proximity of radio nodes.

Properties of the channel impulse response are used in authentication in [4]. In [6], a CSI-based authentication framework is proposed, in which a machine-learning technique is applied to distinguish two users even with similar signal fingerprints. In [11], the time-varying carrier frequency offset between each transmit-receive pair is exploited to distinguish transmitters. The channel-phase response over multi-carrier channels is exploited to authenticate users in [12]. In [13], an

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

978-1-4799-5952-5/15/$31.00 ©2015 IEEE

enhanced cross-layer authentication scheme based on packet error rate and RSSI is proposed. A single-carrier time-domain approach via either residual testing or time-domain CSI comparison is studied in [14]. Different from the existing studies, in this work, we focus on the spoofing detection that applies the reinforcement learning technique to determine the test threshold in the hypothesis test for dynamic radio environments.

III. System Model

We consider a single-hop radio network, where a receiver obtains packets from N transmitters which can impersonate another node to perform spoofing attacks. For simplicity, the i-th transmitter is assumed to have the MAC address i, $i \in \mathcal{L}$, where $\mathcal{L}$ is the possible MAC address set. After receiving a packet, the receiver applies a PHY-authentication technique based on the channel response to detect spoofing attacks in the wireless network. The receiver utilizes the pilots or preambles of the packets to estimate the channel response of the corresponding transmitter. The nodes are assumed to have the information of the center frequency f_0 and bandwidth W. By sampling the channel response at M different tones in $f \in [f_0 - W/2, f_0 + W/2]$, the receiver obtains a resulting received signal strength indicator (RSSI) vector of the k-th packet claimed to have the MAC address i, denoted by $\mathbf{r}_i^k = \left[r_{i,m}^k\right]_{1 \le m \le M}$, where $r_{i,m}^k$ is the RSSI of the m-th tone for the i-th transmitter. The receiver has a reference channel record when receiving the k-th packet for the MAC address i, $\hat{\mathbf{r}}_i^k = \left[\hat{r}_{i,m}^k\right]_{1 \le m \le M}$, where $\hat{r}_{i,m}^k$ is the record of the RSSI at the m-th tone for the i-th transmitter. The probability that the received packet is a spoofing packet is denoted by p.

The receiver applies a simple hypothesis test to determine whether a packet with a channel vector $\mathbf{r}_i^k$ is indeed sent by the node with MAC address i. Let $f(\mathbf{r}_i^k)$ be the MAC address of the node which sends the k-th packet with channel vector $\mathbf{r}_i^k$. The null hypothesis $\mathcal{H}_0$ indicates that the k-th packet is sent by the node with MAC address i. The alternative hypothesis $\mathcal{H}_1$ represents that the MAC address of the transmitter of the k-th packet is not i, i.e., the new packet is sent by a spoofer. Thus, the hypothesis test is given by

$$\mathcal{H}_0 : f(\mathbf{r}_i^k) = i \tag{1}$$

$$\mathcal{H}_1 : f(\mathbf{r}_i^k) \neq i. \tag{2}$$

The false alarm rate in the spoofing detection, i.e., the probability that a legitimate packet is classified as a spoofing one, denoted by α, is given by

$$\alpha = \Pr\left(\mathcal{H}_1 \,|\mathcal{H}_0\right) \tag{3}$$

where $\Pr\left(A\,|B\right)$ is the conditional probability that the receiver chooses the hypothesis A under the occurrence of the hypothesis B. Similarly, the miss detection rate, i.e., the probability that a spoofing packet is viewed as a legitimate one by the receiver, denoted by β, is given by

$$\beta = \Pr\left(\mathcal{H}_0 \,|\mathcal{H}_1\right). \tag{4}$$

According to (3) and (4), we see that the probability for a receiver to accept a legitimate packet is $\Pr\left(\mathcal{H}_0\,|\mathcal{H}_0\right) = 1 - \alpha$ and the probability to reject a spoofing packet is $\Pr\left(\mathcal{H}_1\,|\mathcal{H}_1\right) = 1 - \beta$.

IV. PHY-authentication Game

In this section, the interactions between a receiver and a spoofer are formulated as an authentication game. In this game, the receiver aims to detect spoofing attacks, while the spoofer aims to increase its illegal advantage.

After receiving the k-th packet claimed to have MAC address i, the receiver utilizes the above mentioned hypothesis test to detect spoofing attacks. Based on the uniqueness of the channel responses, the receiver discriminates the k-th packet by comparing the new channel vector, $\mathbf{r}_i^k$, with its reference channel vector, $\hat{\mathbf{r}}_i^k$. If the distance between the two vectors is small, the receiver considers the new packet is indeed from the node with MAC address i; otherwise, the k-th packet is a spoofing packet. Therefore, the test statistic of the hypothesis test, denoted by $L\left(\mathbf{r}_i^k, \hat{\mathbf{r}}_i^k\right)$, is given by

$$L\left(\mathbf{r}_i^k, \hat{\mathbf{r}}_i^k\right) = \frac{\left\|\mathbf{r}_i^k - \hat{\mathbf{r}}_i^k\right\|^2}{\left\|\hat{\mathbf{r}}_i^k\right\|^2} \tag{5}$$

where $\|\cdot\|$ is the Frobenius norm. The test statistic can be viewed as the normalized Euclidean distance between $\mathbf{r}_i^k$ and $\hat{\mathbf{r}}_i^k$. If the test statistic is below a threshold, denoted by θ, the receiver accepts the null hypothesis $\mathcal{H}_0$. Otherwise, the receiver accepts $\mathcal{H}_1$. Thus the receiver performs the hypothesis test given by

$$L \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \theta. \tag{6}$$

The test threshold θ directly impacts the spoofing accuracy. If the test threshold is too large, the miss detection rate is high, while the false alarm rate is large if θ is too small. Therefore it is critical for the receiver to choose a proper test threshold.

In the game, the receiver chooses its test threshold θ in the hypothesis test of the spoofing detection, while the spoofer chooses its spoofing probability p. Let $C_{x,y}$ denote the payoff that the receiver chooses hypothesis $\mathcal{H}_x$ in the case of hypothesis $\mathcal{H}_y$, $x, y \in \{0, 1\}$. The costs of the PHY-layer and high-layer authentications are denoted by C and G, respectively. The gain of accepting a packet sent by the node with MAC address i is denoted by g_i^l, while the cost of rejecting a legitimate packet sent by the node with MAC address i is denoted by γ_i. In addition, let g_i^s denote the gain of rejecting a spoofing packet claimed to have MAC address i. Thus, we have

$$C_{0,0} = g_i^l - G - C \tag{7}$$

$$C_{0,1} = -G - C \tag{8}$$

$$C_{1,0} = -\gamma_i - C \tag{9}$$

$$C_{1,1} = g_i^s - C. \tag{10}$$

As the probability that a received packet is a spoofing packet is p (i.e., $\Pr\left(\mathcal{H}_1\right) = p$), the Bayesian risk of the spoofing

detection for a packet from transmitter i, denoted by $R(i)$, which is the expected payoff in the spoofing detection, is given by

$$\begin{aligned} R(i) &= \sum_{x=0}^{1}\sum_{y=0}^{1} C_{x,y}\Pr\left(\mathcal{H}_x\,|\mathcal{H}_y\right)\Pr\left(\mathcal{H}_y\right) \\ &= (g_i^l - G - C)(1-\alpha)(1-p) - (G+C)\beta p \\ &\quad - (\gamma_i + C)\alpha(1-p) + (g_i^s - C)(1-\beta)p. \end{aligned} \tag{11}$$

The authentication is formulated as a zero-sum game, in which the utility of the receiver (or the spoofer) is the Bayesian risk in the spoofing detection, denoted by $u_r(\theta, p)$ (or $u_s(\theta, p)$), and is given by

$$\begin{aligned} u_r(\theta,p) &= -u_s(\theta,p) = R(i) \\ &= (g_i^l - G - C)(1-\alpha)(1-p) - (G+C)\beta p \\ &\quad - (\gamma_i + C)\alpha(1-p) + (g_i^s - C)(1-\beta)p. \end{aligned} \tag{12}$$

The optimal threshold, denoted by θ^*, is defined as

$$\theta^* = \arg\max_{\theta\geq 0} u_r(\theta, p). \tag{13}$$

The receiver applies the higher-layer authentication process for the packets that pass the PHY-authentication to reduce the costs by spoofing packets. The reference channel vector, $\hat{\mathbf{r}}_i$, is updated once the packet of node i is accepted, i.e., $\hat{\mathbf{r}}_i^k = \mathbf{r}_i^k$; otherwise, $\hat{\mathbf{r}}_i^k = \hat{\mathbf{r}}_i^{k-1}$. A packet is accepted if and only if both the PHY-layer and higher-layer authentications accept it.

V. Spoofing Detection with Reinforcement Learning

For dynamic radio environments with unknown system parameters such as the distribution of channels, the test threshold in the hypothesis test of the spoofing detection can be chosen via reinforcement learning. More specifically, the optimal authentication threshold as in (13) depends on the channel model of the environment and the spoofing model, which are not always known by the receiver. As a special case, if $p = 0$, the optimal authentication threshold is very large to make all the packets passing the authentication. Otherwise, if all the packets are spoofing, i.e., $p = 1$, the optimal threshold has to be small. Therefore reinforcement learning can be applied to determine the test threshold under a dynamic unknown environment. The receiver applies a Q-learning process to obtain the optimal threshold in the PHY-authentication based on its observation of the radio environment.

Without loss of generality, we assume that the receiver obtains T packets in each time slot. The test threshold is assumed to be one of K levels and the action set is denoted by $\mathbf{A} = [\theta_l]_{1\leq l\leq K}$. The state observed by the receiver in the n-th time slot, denoted by $\mathbf{s}_n$, consists of the false alarm rate and miss detection rate of authentication in the previous time slot, i.e., $\mathbf{s}_n = [\alpha_{n-1}, \beta_{n-1}]$, which have X and Y levels, respectively. The receiver chooses its action a_n based on state $\mathbf{s}_n$.

Algorithm 1. Spoofing detection scheme with Q-learning.

Initialize: ε, μ, δ, $Q(\mathbf{s}, a) = \mathbf{0}$, $V(\mathbf{s}) = \mathbf{0}$, $\forall a \in \mathbf{A}$.
Repeat (for each episode)
  For $n = 1, 2, 3, ...$ (for each time slot)
    Observe the current state $\mathbf{s}_n$.
    Select a threshold a_n via (18).
    For $k = 1, 2, ..., T$ (for each packet)
      Authenticate the k-th packet:
        Read MAC address i of the k-th packet.
        Extract $\mathbf{r}_i$ and $\hat{\mathbf{r}}_i$.
        Calculate test statistic L via (5).
        If $L \leqslant a_n$ and this packet passes higher-layer authentication
          Update $\hat{\mathbf{r}}_i$: $\hat{\mathbf{r}}_i^k = \mathbf{r}_i^k$.
          Accept this packet.
        Else
          Keep $\hat{\mathbf{r}}_i$: $\hat{\mathbf{r}}_i^k = \hat{\mathbf{r}}_i^{k-1}$.
          Send a spoofing alarm.
        End If
    End For
    Observe next state, $\mathbf{s}_{n+1}$, and utility U_n.
    Update $Q(\mathbf{s}_n, a_n)$ via (15).
    Update $V(\mathbf{s}_n)$ via (16).
  End For
End Repeat

According to (12), the utility of the receiver after receiving T packets, denoted by U_n, is given by

$$U_n = \sum_{k=(n-1)T+1}^{nT} u_r^k(a_n, p_n). \tag{14}$$

In the spoofing detection scheme, the learning rate, denoted by $\mu \in (0, 1]$, indicates the weight of the current Q-function, denoted by $Q(\mathbf{s}_n, a_n)$, in the update process. The discount factor denoted by $\delta \in (0, 1]$ indicates the uncertainty about rewards to be received in the future. Let $V(\mathbf{s})$ represent the maximum Q value of the receiver in state $\mathbf{s}$. The receiver updates the Q-function as follows,

$$Q(\mathbf{s}_n, a_n) \leftarrow (1-\mu)Q\left(\mathbf{s}_n, a_n\right) + \mu\left(U_n + \delta V(\mathbf{s}_{n+1})\right) \tag{15}$$

$$V\left(\mathbf{s}_n\right) \leftarrow \max_{a\in\mathbf{A}} Q\left(\mathbf{s}_n, a\right). \tag{16}$$

By applying the ε-greedy policy for choosing its action, the receiver tries all actions in all the states repeatedly, i.e., the action to maximize the Q value is chosen with a large probability $1-\varepsilon$ while the other $K-1$ actions are taken with a small probability $\varepsilon/(K-1)$. The optimal threshold, denoted by a^*, is given by

$$a^* = \arg\max_{x\in\mathbf{A}} Q\left(\mathbf{s}, x\right). \tag{17}$$

Therefore, the receiver chooses its test threshold a according to the following

$$\Pr\left(a = a'\right) = \begin{cases} 1-\varepsilon, & a' = a^*, \\ \frac{\varepsilon}{K-1}, & a' \in \mathbf{A}, a' \neq a^*. \end{cases} \tag{18}$$

The spoofing detection process is shown in detail in Algorithm 1.

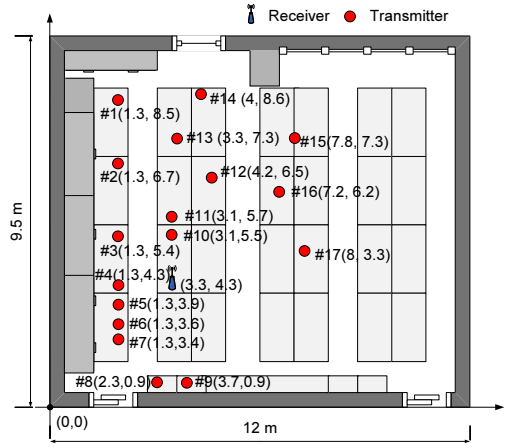


Fig. 1. The network topology of the experiments in a $12 \times 9.5 \times 3m^3$ office room, consisting of 17 transmitters and a receiver.

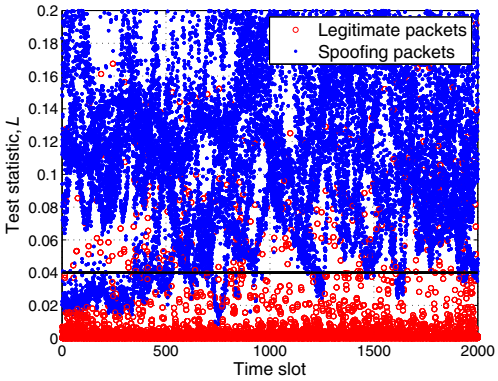
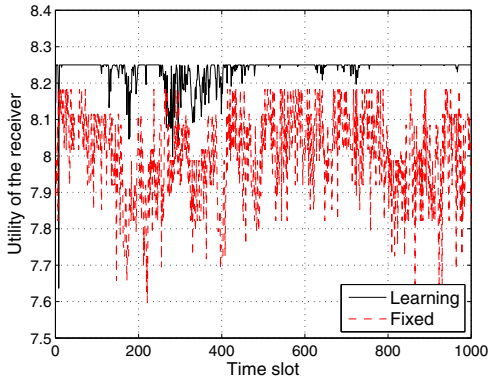
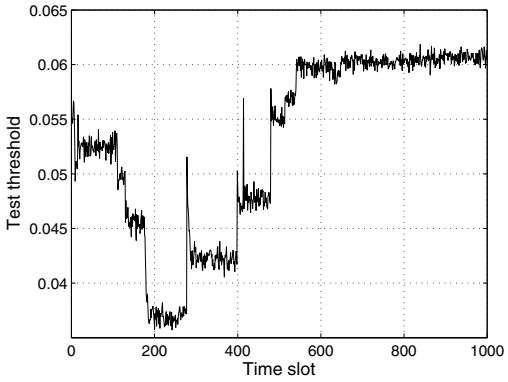


Fig. 2. Test statistic of the spoofing dection in the situation that Node 1-6 pretend to be another in a topology as shown in Fig. 1.



(a) Utility of the receiver



(b) Threshold in the spoofing detection

Fig. 3. Performance of the spoofing detection in the situation that Node 2, 15 and 17 claim to be Node 13 in a topology as shown in Fig. 1.

VI. Experimental Results

Experiments have been performed to analyze the performance of the proposed spoofing detection scheme, which is compared with a PHY-authentication scheme with a fixed threshold. In the experiments, we consider $N = 17$ transmitters and a receiver in a $12 \times 9.5 \times 3m^3$ office room, as shown in Fig. 1, $p = 0.75$, $C = 1$, $G = 3$, $g_i^l = 10$, $\gamma_i = 20$, $g_i^s = 10$ $(1 \leq i \leq 17)$, $f_0 = 2.4$ GHz, $W = 200$ MHz and $M = 5$.

An example of the test statistic of the spoofing detection with 6 transmitters is shown in Fig. 2. Most of spoofing attacks can be detected by the authentication with $\theta = 0.04$. Thus, the test threshold is fixed as 0.04 for the case without learning.

In addition, we set $\mu = 0.8$, $\delta = 0.7$, $\varepsilon = 0.1$, $X = Y = 29$ levels, $\alpha = \beta = \{0 : 0.01 : 0.1, 0.15 : 0.05 : 1\}$, $K = 10$ levels and $\mathbf{A} = \{0.01 : 0.01 : 0.1\}$.

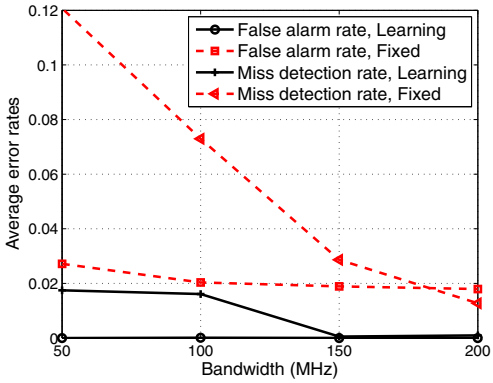
As shown in Fig. 3, the optimal threshold in the spoofing detection is about 0.06, and the proposed strategy has a higher utility and is more stable than the fixed threshold strategy in most situations.

Both the false alarm rate and miss detection rate of the scheme decrease with the bandwidth, as shown in Fig. 4 (a). For example, both the false alarm rate and miss detection rate are close to 0, if the bandwidth is 200 MHz. If the bandwidth is 150 MHz, the false alarm rate and miss detection rate of the fixed threshold strategy are up to 1.89% and 2.86%, respectively, while that of the proposed strategy are only 0.03% and 0.05%. The average utility of the receiver in Fig. 4 (b) increases by 5.12% if the bandwidth is 150 MHz.

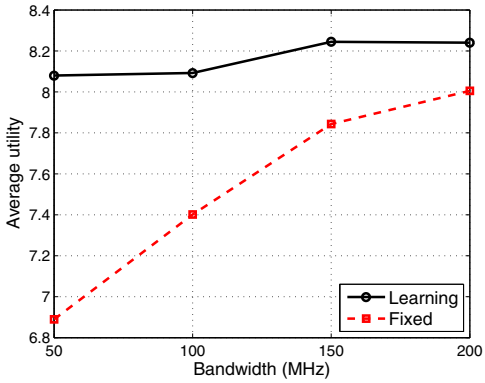
As shown in Fig. 5 (a), the miss detection rate in the proposed strategy increases with the number of nodes, because the optimal threshold a^* may not match the optimal one for the specific spoofer. As the cost of accepting a spoofing packet (i.e., the cost of high-layer authentication) is smaller than that to reject a legitimate packet, the receiver in the learning process has to restrict the false alarm. On the other hand, the average utility of the receiver in both strategies decreases with the number of nodes from Fig. 5 (b), as the detection error rate increases.

VII. Conclusion

In this work, we have investigated the PHY-authentication technique in wireless networks. The repeated interactions between a receiver and a spoofer have been formulated as

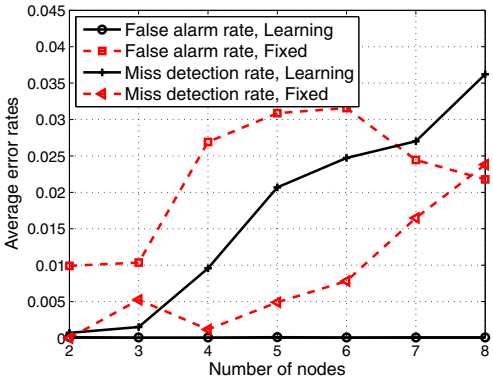


(a) Average error rates

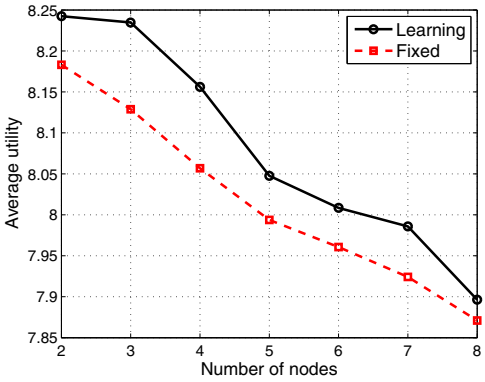


(b) Average utility of the receiver

Fig. 4. Performance of the proposed PHY-authentication vs. that with a fixed threshold in which Node 2, 15 and 17 pretend to be Node 13 in a topology as shown in Fig. 1.



(a) Average error rates



(b) Average utility of the receiver

Fig. 5. Performance of the proposed PHY-authentication vs. that with a fixed threshold in which Node 1, 2, 11, 12, 14-17, pretend to be Node 13 in a topology as shown in Fig. 1.

a zero-sum spoofing detection game. A PHY-authentication method has been proposed for enhancing authentication accuracy in a dynamic radio environment, in which the optimal test threshold in the spoofing detection hypothesis test is achieved via Q-learning technique. Experimental results demonstrate that the proposed PHY-authentication method can efficiently improve the authentication performance. For example, if the bandwidth is 200 MHz, the average error rate of the proposed spoofing detection scheme is less than 0.1%.

REFERENCES

[1] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, 2010.

[2] 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, no. 1, pp. 44–58, 2013.

[3] A. Kalamandeen, A. Scannell, E. Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proc. Int'l Conf. Mobile systems, applications and services*, pp. 331–344, 2010.

[4] F. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. Military Commun. Conf.*, pp. 538–542, 2011.

[5] F. J. 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, 2013.

[6] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information(CSI)," in *Proc. ACM Symp. Inform., computer and commun. security*, pp. 389–400, 2014.

[7] J. Tugnait, "Wireless user authentication via comparison of power spectral densities," *IEEE J. Selected Areas in Commun.*, vol. 31, no. 9, pp. 1791–1802, 2013.

[8] Z. Jiang, J. Zhao, X. Li, J. Han, and W. Xi, "Rejecting the attack: Source authentication for WiFi management frames using CSI information," in *Proc. IEEE Int'l Conf. Computer Commun. (INFOCOM)*, pp. 2544–2552, 2013.

[9] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. IEEE Int'l Conf. Commun.*, pp. 4646–4651, 2007.

[10] L. Xiao, A. Reznik, W. Trappe, and et al., "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, pp. 6–10, 2010.

[11] W. Hou, X. Wang, J. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658–1667, 2014.

[12] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, 2015.

[13] P. Hao, X. Wang, and A. Refaey, "An enhanced cross-layer authentication mechanism for wireless communications based on PER and RSSI," in *Proc. IEEE Canadian Workshop on Informa. Theory (CWIT)*, pp. 44–48, 2013.

[14] J. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. IEEE Int'l Conf. Commun. Systems and Networks (COMSNETS)*, pp. 1–9, 2010.