SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

December 2020, Vol. 63 222302:1–222302:14
https://doi.org/10.1007/s11432-019-2802-x

An area based physical layer authentication framework to detect spoofing attacks

Na LI, Shida XIA, Xiaofeng TAO*, Zhiyuan ZHANG & Xiaohui WANG

National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing 100876, *China*

Received 20 August 2019/Revised 15 January 2020/Accepted 18 February 2020/Published online 28 October 2020

Abstract In this paper, we propose an area-oriented authentication framework, which aims to provide a light-weight first authentication by reducing the complexity in acquiring and maintaining many different reference vectors as in the traditional one-by-one authentication framework. Under the proposed framework, we first derive the missing detection probability and the false alarm probability, respectively. Then we quantitatively evaluate the average risks that a spoofer is successfully detected or a legitimate user is falsely alarmed, at any position in a certain area. And correspondingly three kinds of areas are defined as the clear area where the spoofers prefer not to attack, the danger area where the spoofers have pretty high probabilities to attack successfully, and the warning area where the legitimate users are much likely to be falsely reported as attackers. These results depict the security situation distribution of a region, and provide useful insights for network operators to take proper following strategies. Finally, simulations are given to verify our analytical derivations and show the impacts of system parameters.

Keywords physical layer authentication, light weight authentication, security situation distribution, spoofing, area authentication

Citation Li N, Xia S D, Tao X F, et al. An area based physical layer authentication framework to detect spoofing attacks. Sci China Inf Sci, 2020, 63(12): 222302, https://doi.org/10.1007/s11432-019-2802-x

1 Introduction

Wireless channels are much vulnerable to jamming, eavesdropping, spoofing and many other attacks, which greatly damage the availability of wireless networks. Among various types of wireless attacks, spoofing is easy to launch, and is usually viewed as the springboard to launch a variety of other attacks [1–3], like denial of service (DoS), man-in-the-middle, data modification, and sniffing. Authentication of the broadcast signals is an effective countermeasure for defending spoofing attacks, and is considered as the important first step in securing the wireless communication [3, 4]. Meanwhile, as the development of the fifth generation (5G) mobile communication, many capacity-limited devices and users demanding latency-sensitive services [4, 5] require light-weight authentication techniques [4–7].

Cryptographic light-weight authentication techniques and protocols have been proposed [6–8]. Meanwhile, physical (PHY)-layer authentication provides light-weight solutions [1–3, 9, 10], because complex signaling exchanges are not required. The inherent idea is to utilize the difference of the physical attributes between legitimate signals and spoofing signals. Based on the timeliness, PHY authentication methods can be divided into two categories. One is to verify each current message by the instant physical information. This method can verify the source timely, but the efficiency could be limited in some practical scenarios with massive connections or frequently moving users, because maintaining lots of reference

* Corresponding author (email: taoxf@bupt.edu.cn)

vectors (RVs) or frequently updating RVs is very heavy work [2]. The other method is to verify multiple messages over a period of time, based on the statistical properties of the large amount of physical information. This method can provide a macroscopical insight in the security of the entire communication, which is an important first step to handle the spoofing problem.

Channel based attributes are often used in PHY authentication, like channel state information (CSI) [11], received signal strength (RSS) [12–17], and angle of arrival (AoA) [18–20]. As easily to be obtained in practice, RSS is the most popular option, and has been used either independently [12–14], or jointly with other attributes [15]. Multiple RSSs from many sources can be combined to enhance the authentication performance [16]. In [17], the statistical property over time of RSS is observed to determine whether the source is legitimate or is under attack ever. Except for the temporal property, the spatial property of RSS is also very useful in practice, like in positioning [21–23], range estimation [24–26], and detection [27–29]. In [27–29], the authors used RSS information to detect and localize the attackers.

Different from current researches, we use the spatial property of RSS in the PHY authentication framework to observe the spatial distribution of the network security situation. This study provides an important first authentication, after which further authentications can be added as necessary. In our previous work [30], we first considered a simple scenario where the spoofer attacks a silent user. In this paper, we further consider a practical case that the spoofer tries to force the destination to accept its spoofing messages even when the victim user is also active. Moreover, we provide a more detailed analysis and design a framework for the area authentication, and extended simulations are added to better show the characteristics of different areas. Specifically, the main work and contributions are as follows.

(1) We propose the area-based authentication framework, which can dramatically reduce the complexity in acquiring and maintaining many different reference vectors, by verifying whether a signal comes from a certain area instead of a certain position, as in the traditional one-by-one authentication framework.

(2) Under the proposed framework, we evaluate the authentication performance for two different spoofing models, by deriving the average miss detection probability (MDP) and the average alarm probability (FAP). We also provide the general derivation framework for the average transmission rates.

(3) Based on the derived probabilities and average rates, we can describe the spatial distribution of different areas intuitively depicting the network security situation, which provides useful insights for network governors, so that proper solutions can be adopted to different areas. We also study the area properties through analytical and simulation results.

The rest of this paper is organized as follows. In Section 2, the two dimensional area model is presented and the area-based hypothesis test model is introduced. Then in Section 3, the authentication performance is evaluated by deriving the closed-form expressions of the detecting probabilities, respectively for two practical spoofing models. Three different kinds of security areas are further defined and studied to show the distribution property of the security situations. In Section 4, simulations are performed to verify our derivations, and to show the impacts of system parameters. Finally, the paper is concluded in Section 5.

2 Proposed scheme

In this section, we show the system model and the proposed area authentication framework.

2.1 The system model

As shown in Figure 1, the destination denoted by the star is at the origin of the coordinates. The users denoted by circles locate in the annular area with the inner radius d_i and the outer radius d_o. We denote this area as the legitimate area where only legitimate users are inside[1)]. The possible spoofers denoted by

1) This could be many practical scenarios. For example, the sensors are distributed in a certain area, or the vehicles move within a certain area. This area could be a room, a factory, a plaza and other places within physical isolations or under the control and supervision of the network operator. Note that the shape of the area is not necessarily a two-dimensional annular area. Without loss of generality, we use the annular area for analytical convenience. And this work can be easily extended to any area models in practice by adjusting the RSS thresholds and combining with other attributes, like arrival of angles.

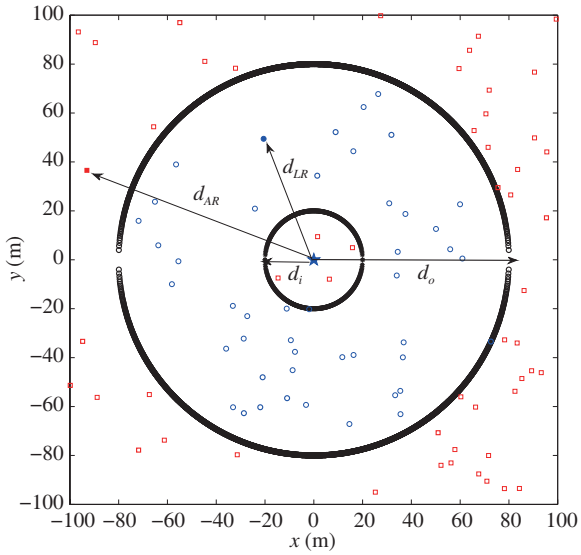

Figure 1 (Color online) The system model.

square markers distribute randomly outside. For the convenience of analysis, we consider a typical user with the distance d_{LR} and its corresponding spoofing attacker with distance d_{AR}, and assume that other user-and-spoofer pairs with distances d_L and d_A use different channels. All nodes are equipped with a single antenna.

To obtain a baseline performance, we assume the spoofer is so smart that it can always find a best time and best way to transmit spoofing messages. The spoofing attack is called to be successful when the destination accepts the spoofer as legitimate, and decodes the spoofing message successfully. The spoofer may take two strategies. One strategy is that it attacks when the victim user is silent. In this case, the spoofer monitors the communication of the victim user, and waits for a proper idle time. The other strategy is that the spoofer jams the transmission of the victim user and compels the destination to accept the spoofing message as legitimate. In our previous work [30], we have studied the former case. In this paper, we consider both situations with an emphasis on the latter one.

2.2 Area authentication model

The hypothesis test model is usually used in PHY layer authentication. Given a physical attribute (vector) v_r between two legitimate users, the conventional hypothesis testing decides whether is the successive attribute (vector) v_m from the legitimate transmitter or not. It can be simply represented by

$$\begin{cases} \mathcal{H}_0 : v_m = v_r, \\ \mathcal{H}_1 : v_m \neq v_r, \end{cases} \tag{1}$$

where v_r describes the reference attribute (vector) of the legitimate transmitter. We extend this model to a general case that

$$\begin{cases} \mathcal{H}_0 : v_m \in \Phi_v, \\ \mathcal{H}_1 : \text{otherwise}, \end{cases} \tag{2}$$

where Φ_v denotes a set or a range of the reference attribute (vector). In this case, the new hypothesis testing decides whether is the successive attribute (vector) v_m from a specific group of users. Here we use "area" to define the group of users.

In this paper, we use the easily obtained RSS information. Based on the path-loss model, we can approximately transform RSS into the distance between the source and the destination. That is, an area

oriented decision criterion is given by

$$\begin{cases} \mathcal{H}_0 : r_o \leqslant r \leqslant r_i, \\ \mathcal{H}_1 : \text{otherwise}, \end{cases} \Rightarrow \begin{cases} \mathcal{H}_0 : d_i \leqslant d \leqslant d_o, \\ \mathcal{H}_1 : \text{otherwise}, \end{cases} \tag{3}$$

where r denotes the RSS, $r_i > r_o \geqslant 0$ describes the legitimate value region of RSS, and d is the distance between the transmitter and the receiver[2)].

The above framework is beneficial in lightweight authentications. (i) Realtime channel and location information of users are not required. This information may be constantly changing in wireless environments, and is hard to be correctly obtained. (ii) The threshold value plays an important role in the hypothesis test theory. The optimal value changes with channel variations, which is a big challenge in practice. In the proposed framework, only the thresholds for the area are required to be optimized and refreshed, which greatly reduced the complexity. (iii) If the users move around, as long as they keep within the same area, the detector does not need to update the RVs, which further reduces the complexity and also improves the robustness with respect to movements.

3 Performance analysis

In this section, we study the authentication performance under the above proposed area authentication framework. Since the spoofer may take different strategies, we discuss three cases separately as follows.

3.1 The spoofer forges a silent user

Here we consider the case that the attacker transmits spoofing messages by claiming to be a legitimate user who is actually silent.

The spoofer first determines whether to spoof or not, and then chooses an optimal spoofing power. The principle for the spoofer to launch a attack is that the spoofing rate should be larger than zero. Thus, the spoofer first estimates the RSS at the receiver as $\hat{r}_A = P_A d_A^{-2\alpha}|h_A|^2 + \sigma_n^2$ [30], where P_* is the transmit power, d_* is the distance to the receiver, h_* is the small-scale fading channel, the subscript $* = A$ means attacker, and σ_n^2 is the variance of the receiver's thermal noise n following complex Gaussian distribution with zero mean. And to successfully cheat the destination, the spoofer has to set $r_o \leqslant \hat{r}_A \leqslant r_i$, and restricts the spoofing power as $P_1 \leqslant P_A \leqslant \min\{P_2, P_m\}$, where $P_1 \triangleq \frac{r_o - \sigma_n^2}{d_A^{-2\alpha}|h_A|^2}$, $P_2 \triangleq \frac{r_i - \sigma_n^2}{d_A^{-2\alpha}|h_A|^2}$, and P_m is the maximum spoofing power.

(1) If $P_m < P_1$, there is no possibility that the spoofing is not detected. In this case, the best policy is not to attack. The silent probability for the spoofer is

$$p_1 \triangleq \Pr\{P_m < P_1\} = \Pr\left\{Y < \frac{d_A^{2\alpha}(r_o - \sigma_n^2)}{P_m}\right\} = \int_0^{\frac{d_A^{2\alpha}(r_o - \sigma_n^2)}{P_m}} f_Y(y)\mathrm{d}y, \tag{4}$$

where $Y \triangleq |h_A|^2$ follows a distribution with the probability density function (PDF) $f_Y(y)$. If Rayleigh fading[3)] is assumed, the channels are independent complex Gaussian variables, i.e., $Y \sim \chi_2^2$, where χ_2^2 denotes the chi-square distribution with the degree of two, and the corresponding PDF and cumulative density function (CDF) are e^{-y} and $1 - \mathrm{e}^{-y}$, respectively, and then p_1 can be calculated as [30] $p_1 = 1 - \mathrm{e}^{-(\frac{d_A}{d_o})^{2\alpha}\frac{P_t}{P_m}}$, which increases with d_A but decreases with P_m. That is, when the spoofer is far away or the spoofing power is small, the attacker is more likely to keep silent.

When the silent probability is larger than a threshold ϵ_1, we assume there are no active attackers, and the corresponding area is viewed as the clear area.

2) Here we use the average RSS values at the area boundaries as thresholds. In this case, the relationship between r_i and r_o and the distances can be well described by the path-loss models. When $d_i = 0$, it reduces to a scenario where the users are within a circular region. When $d_o = d_i \pm \delta_d$ with δ_d as the offset threshold, it reduces to the conventional hypothesis test model for a specific legitimate user.

3) Without loss of generality, we assume Rayleigh fading throughout the paper. Other fading models can also be considered in our framework by substituting the random distribution features.

Definition 1. The ϵ_1-clear area describes an area where the spoofers have a silent probability larger than ϵ_1. That is,

$$\mathcal{A}_{\epsilon_1}^{\mathrm{clr}} \triangleq \mathrm{Area}\left\{p_1 > \epsilon_1\right\}. \tag{5}$$

As shown in Figure 2, the area marked with 'o' denotes the clear area where the system assumes that the spoofers keep silent with a probability larger than $\epsilon_1 = 90\%$.

(2) If $P_m > P_1$, the spoofer tries to transmit spoofing messages. Only when the actual RSS at the receiver $r_A = P_A d_A^{-2\alpha}|h_A|^2 + |n|^2$ satisfies $r_o \leqslant r_A \leqslant r_i$, the destination accepts the spoofing message as legitimate. As a result, the successful spoofing probability is defined as

$$p_2 = \Pr\left\{ P_1 \leqslant P_A \leqslant \min\{P_2, P_m\}, r_o \leqslant P_A d_A^{-2\alpha} Y + \sigma_n^2 Z \leqslant r_i \right\}, \tag{6}$$

where $Z \triangleq \frac{|n|^2}{\sigma_n^2} \sim \chi_2^2$. The corresponding successful spoofing rate is defined as

$$R_A = \mathrm{E}_{Y,Z}\log_2\left(1 + \frac{P_A d_A^{-2\alpha} Y}{\sigma_n^2 Z}\right) \mathbb{1}\left\{ r_o \leqslant P_A d_A^{-2\alpha} Y + \sigma_n^2 Z \leqslant r_i, P_1 \leqslant P_A \leqslant \min\{P_2, P_m\} \right\}, \tag{7}$$

where E denotes the expectation.

When the maximal power $P_A = \min\{P_2, P_m\}$ is adopted, p_2 can be calculated as [30]

$$p_2 = \Pr\left\{ P_1 \leqslant P_A = \min\{P_2, P_m\}, r_o \leqslant P_A d_A^{-2\alpha} Y + \sigma_n^2 Z \leqslant r_i \right\} \tag{8}$$

$$= \begin{cases} \int_{\beta(\hat{r}_i-1)}^{\infty} \mathrm{e}^{-y} \int_{\hat{r}_o-\hat{r}_i+1}^{1} \mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y + \int_{\beta(\hat{r}_o-1)}^{\beta(\hat{r}_i-1)} \mathrm{e}^{-y} \int_{\hat{r}_o-\frac{y}{\beta}}^{\hat{r}_i-\frac{y}{\beta}} \mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y, & \Delta r \leqslant 1, \\ \int_{\beta(\hat{r}_i-1)}^{\infty} \mathrm{e}^{-y} \int_{0}^{1} \mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y + \int_{\beta\hat{r}_o}^{\beta(\hat{r}_i-1)} \mathrm{e}^{-y} \int_{0}^{\hat{r}_i-\frac{y}{\beta}} \mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y + \int_{\beta(\hat{r}_o-1)}^{\beta\hat{r}_o} \mathrm{e}^{-y} \int_{\hat{r}_o-\frac{y}{\beta}}^{\hat{r}_i-\frac{y}{\beta}} \mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y, & \Delta r > 1, \end{cases}$$

$$= \begin{cases} \left(\mathrm{e}^{-\hat{r}_o} - \mathrm{e}^{-\hat{r}_i}\right)\left(\frac{1}{1-\beta}\mathrm{e}^{\xi_i} - \frac{1}{v}\mathrm{e}^{\xi_o}\right), & \Delta r \leqslant 1, \\ \mathrm{e}^{-\beta(\hat{r}_i-1)}\left(2 + \frac{v-1}{v}\mathrm{e}^{-1}\right) + \frac{\mathrm{e}^{-\beta\hat{r}_o}}{1-\beta} + \frac{1}{v}\mathrm{e}^{\xi_o}\left(\mathrm{e}^{-\hat{r}_i} + \mathrm{e}^{-\hat{r}_o}\right), & \Delta r > 1, \end{cases} \tag{9}$$

where $\beta \triangleq \frac{\sigma_n^2}{P_m d_A^{-2\alpha}}$, $v \triangleq \frac{1-\beta}{\beta}$, $\hat{r}_i \triangleq \frac{r_i}{\sigma_n^2}$, $\hat{r}_o \triangleq \frac{r_o}{\sigma_n^2}$, $\Delta r \triangleq \hat{r}_i - \hat{r}_o$, $\xi_o \triangleq (1-\beta)(\hat{r}_o - 1)$, and $\xi_i \triangleq (1-\beta)(\hat{r}_i - 1)$.

The closed-form expression for R_A can be straightforwardly derived using similar integrals as in (9) [30]. In this paper, we omit this result owing to the space limitation.

Based on the above results, the area with $p_2 > \epsilon_2$ or (and) $R_A > \epsilon_A$ is defined as the danger area where the spoofer is active and can get a pretty good spoofing performance.

Definition 2. The danger area consists of locations where the spoofer can achieve a relatively higher successful spoofing probability $p_2 > \epsilon_2$ or (and) larger average successful spoofing rate $R_A > \epsilon_A$. That is,

$$\mathcal{A}_{\epsilon_2}^{\mathrm{danger}} \triangleq \mathrm{Area}\left\{p_2 > \epsilon_2\right\} \quad \text{or (and)} \quad \mathcal{A}_{\epsilon_A}^{\mathrm{danger}} \triangleq \mathrm{Area}\left\{R_A > \epsilon_A\right\}. \tag{10}$$

In Figure 3, the danger area is marked with '□', adjoining to the legitimate annular area from the outside, the successful spoofing probability is larger than 10% or the average spoofing rate is larger than 0.1 bps/Hz. Note the thresholds can be chosen according to the practical requirements. The danger area describes the spoofers' vantage locations, and should be paid additional attentions.

3.2 The legitimate communication under no spoofing attacks

When no spoofing attack is launched, the destination receives the legitimate message with the RSS $r_L = P_t d_L^{-2\alpha}|h_L|^2 + |n|^2$, where subscript '$* = L$' indicates the legitimate transmitter. This transmission can be viewed as legitimate only when $r_o \leqslant r_L \leqslant r_i$, and the corresponding successful probability is defined as $p_3 \triangleq \Pr\{r_o \leqslant r_L \leqslant r_i\}$. Similarly, by assuming $X \triangleq |h_A|^2 \sim \chi_2^2$, p_3 can be calculated by [30]

$$p_3 = \Pr\left\{r_o \leqslant P_t d_L^{-2\alpha} X + \sigma_n^2 Z \leqslant r_i\right\} \tag{11}$$

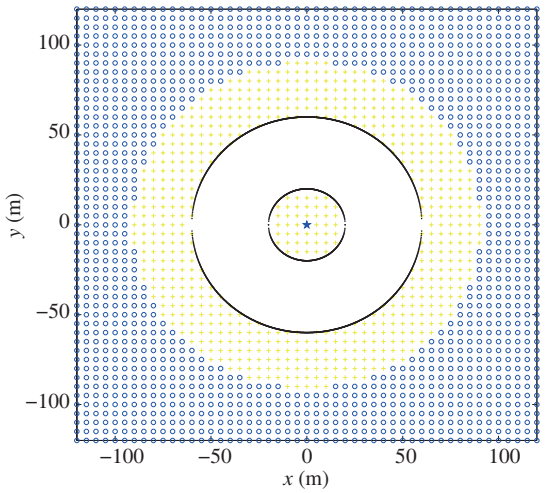

Figure 2 (Color online) The clear area with $\epsilon_1 = 0.9$. We set $P_t = P_m = 20$ dB, $\alpha = 1$, $d_i = 20$ m, $d_o = 60$ m. The legitimate users locate in the blank area. The spoofers distribute outside the blank area.

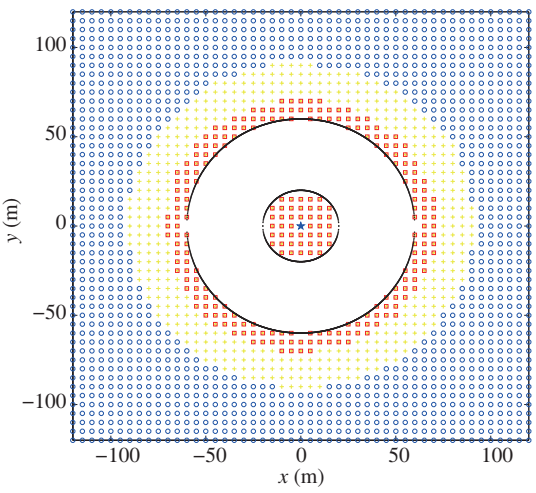

Figure 3 (Color online) The danger area with $\epsilon_2 = 0.1$ or $\epsilon_A = 0.1$ bps/Hz.

$$
\begin{aligned}
&= \int_0^{\frac{r_o}{\sigma_n^2}} \mathrm{e}^{-z} \int_{\frac{r_o-\sigma_n^2 z}{d_L^{-2\alpha}P_t}}^{\frac{r_i-\sigma_n^2 z}{d_L^{-2\alpha}P_t}} \mathrm{e}^{-x}\mathrm{d}x\mathrm{d}z + \int_{\frac{r_o}{\sigma_n^2}}^{\frac{r_i}{\sigma_n^2}} \mathrm{e}^{-z} \int_0^{\frac{r_i-\sigma_n^2 z}{d_L^{-2\alpha}P_t}} \mathrm{e}^{-x}\mathrm{d}x\mathrm{d}z \\
&= \frac{1}{1-\bar{\beta}} \left(\mathrm{e}^{-\bar{\beta}\hat{r}_o} - \mathrm{e}^{-\bar{\beta}\hat{r}_i}\right) - \frac{1}{\bar{v}} \left(\mathrm{e}^{-\hat{r}_o} - \mathrm{e}^{-\hat{r}_i}\right), \qquad (12)
\end{aligned}
$$

where $\bar{\beta} \triangleq \frac{\sigma_n^2}{P_t d_L^{-2\alpha}}$, and $\bar{v} = \frac{1-\bar{\beta}}{\bar{\beta}}$. And the successful legitimate transmission rate is calculated as

$$
R_L = \mathrm{E}_{X,Z} \log_2 \left(1 + \frac{P_A d_A^{-2\alpha} X}{\sigma_n^2 Z}\right) \mathbb{1}\left\{r_o \leqslant P_t d_L^{-2\alpha} X + \sigma_n^2 Z \leqslant r_i\right\}. \qquad (13)
$$

The closed-form expression for R_L can be derived using similar integrals as (12), which is omitted in this paper.

Definition 3. The warning area satisfies $p_3 < \epsilon_3$ or (and) the average successful transmission rate $R_L < \epsilon_L$. That is,

$$
\mathcal{A}_{\epsilon_3}^{\text{warning}} \triangleq \text{Area}\left\{p_3 < \epsilon_3\right\} \quad \text{or (and)} \quad \mathcal{A}_{\epsilon_L}^{\text{warning}} \triangleq \text{Area}\left\{R_L < \epsilon_L\right\}. \qquad (14)
$$

The warning area describes an area that the users may have very high probability to be falsely detected as a spoofer, or the average successful transmission rate is smaller than an expected threshold. It is necessary to warn users never enter this area, or on the other hand, users in this area should be protected with additional measures.

We observe the warning area in Figure 4. The warning area covered by markers '□' has the average successful rate smaller than 1 bps/Hz, and the warning area covered by '+' denotes the area where the successful legitimate probability is smaller than 90%. We can see that the warning area is internally close to the boundaries of the legitimate area. That is, the relatively safe locations for legitimate users are usually in the middle part of the legitimate area.

To now, we can describe the security situation distribution using three different areas: (i) the clear area where the spoofers choose not to attack because of the high risk of being detected; (ii) the danger area where the spoofers have great chances to attack successfully; (iii) the warning area where the legitimate users are much likely to be falsely reported as attackers. The spatial distribution of different areas intuitively depicts the network security situation, which provides useful insights for network governors, so that proper solutions can be adopted to different areas. For example, beamforming can be used to

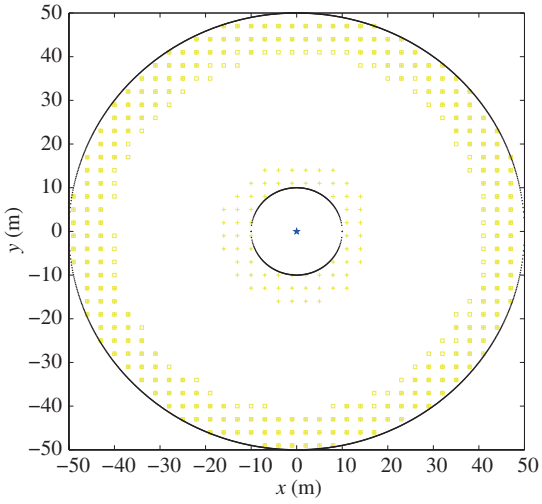

Figure 4 (Color online) The warning area with $\epsilon_3 = 0.9$ or $\epsilon_L = 1$ bps/Hz.

physically isolate the danger area, and stronger authentication measures should be adopted for users in danger or warning areas, and simple authentication measures can be adopted for users in the secure areas. From these points, we enhance the overall security of the wireless network, and at the same time, can reduce the average cost in authentication.

3.3 The spoofer forges an active user

If the spoofer attacks when the victim user is active, the received signal is

$$y = \sqrt{P_A} d_A^{-\alpha} h_A x + \sqrt{P_t} d_L^{-\alpha} h_L s + n, \tag{15}$$

and the RSS becomes $r_c = P_A d_A^{-2\alpha} |h_A|^2 + P_t d_L^{-2\alpha} |h_L|^2 + |n|^2$.

In this case, the spoofer tries to ensure not only that the joint signal is verified to be legitimate, but also that the spoofing message x is successfully decoded instead of the legitimate symbol s. Generally, the maximal symbol is decoded. Thus, the spoofer has to control the power P_A according to

$$\begin{cases} r_o \leqslant \hat{r}_c \leqslant r_i \Rightarrow P_{1,c} \leqslant P_A \leqslant P_{2,c}, \\ P_A d_A^{-2\alpha} |h_A|^2 > P_t d_L^{-2\alpha} |h_L|^2 \Rightarrow P_A > \tilde{P}_1, \end{cases} \Rightarrow \max\left\{P_{1,c}, \tilde{P}_1\right\} < P_A < \min\left\{P_{2,c}, P_m\right\}, \tag{16}$$

where $\hat{r}_c = P_A d_A^{-2\alpha} |h_A|^2 + P_t d_L^{-2\alpha} |h_L|^2 + \sigma_n^2$ is the estimated RSS, $P_{1,c} \triangleq \frac{r_o - \sigma_n^2 - P_t d_L^{-2\alpha} |h_L|^2}{d_A^{-2\alpha} |h_A|^2}$, $\tilde{P}_1 \triangleq \frac{P_t d_L^{-2\alpha} |h_L|^2}{d_A^{-2\alpha} |h_A|^2}$, and $P_{2,c} \triangleq \frac{r_i - \sigma_n^2 - P_t d_L^{-2\alpha} |h_L|^2}{d_A^{-2\alpha} |h_A|^2}$. To make sure that Eq. (16) holds, $\min\{P_{2,c}, P_m\} > \max\{P_{1,c}, \tilde{P}_1\}$ should be satisfied. Otherwise, either the spoofer will be detected or the spoofing symbol will not be decoded, and thus it is better for the spoofer to keep silent. The silent probability is then redefined as

$$\hat{p}_1 = 1 - \Pr\left\{\min\left\{P_{2,c}, P_m\right\} > \max\left\{P_{1,c}, \tilde{P}_1\right\}\right\} \tag{17}$$

$$\begin{aligned} &= 1 - \int_0^{\frac{\hat{r}_o - 1}{2}\bar{\beta}} \mathrm{e}^{-x} \int_{\beta(\hat{r}_o - 1) - \frac{\beta x}{\bar{\beta}}}^{\infty} \mathrm{e}^{-y} \mathrm{d}y \mathrm{d}x - \int_{\frac{\hat{r}_o - 1}{2}\bar{\beta}}^{\frac{\hat{r}_i - 1}{2}\bar{\beta}} \mathrm{e}^{-x} \int_{\frac{\beta x}{\bar{\beta}}}^{\infty} \mathrm{e}^{-y} \mathrm{d}y \mathrm{d}x \\ &= 1 - \begin{cases} \frac{1}{\psi} \mathrm{e}^{-\phi_o} \left(\mathrm{e}^{\psi \varphi_o} - 1\right) + \frac{1}{\psi + 2} \left[\mathrm{e}^{-(\psi+2)\varphi_o} - \mathrm{e}^{-(\psi+2)\varphi_i}\right], & \beta \neq \bar{\beta}, \\ \mathrm{e}^{-\phi_o} \varphi_o + \frac{1}{2} \left(\mathrm{e}^{-2\varphi_o} - \mathrm{e}^{-2\varphi_i}\right), & \beta = \bar{\beta}, \end{cases} \end{aligned} \tag{18}$$

where $\psi \triangleq \frac{\beta}{\bar{\beta}} - 1$, $\phi_i \triangleq \beta(\hat{r}_i - 1)$, $\phi_o \triangleq \beta(\hat{r}_o - 1)$, $\varphi_i \triangleq \frac{1}{2}\bar{\beta}(\hat{r}_i - 1)$, and $\varphi_o \triangleq \frac{1}{2}\bar{\beta}(\hat{r}_o - 1)$.

To obtain a maximal spoofing rate, the spoofer uses a maximal power $P_A = \min\{P_{2,c}, P_m\}$. In this case, the successful spoofing probability is defined as

$$\hat{p}_2 = \Pr\left\{ P_A = \min\{P_{2,c}, P_m\} > \max\left\{P_{1,c}, \tilde{P}_1\right\}, r_o \leqslant P_t d_L^{-2\alpha} X + P_A d_A^{-2\alpha} Y + \sigma_n^2 Z \leqslant r_i \right\}, \tag{19}$$

and the closed-form expression is derived as follows.

(1) When $\Delta r \leqslant 1$, we have

$$\begin{aligned}
\hat{p}_2 =& \int_0^{\varphi_i} \mathrm{e}^{-x} \int_{\phi_i - \frac{\beta}{\bar{\beta}}x}^{\infty} \mathrm{e}^{-y} \int_{\hat{r}_o - \hat{r}_i + 1}^{1} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x + \int_0^{\varphi_o} \mathrm{e}^{-x} \int_{\phi_o - \frac{\beta}{\bar{\beta}}x}^{\phi_i - \frac{\beta}{\bar{\beta}}x} \mathrm{e}^{-y} \int_{\hat{r}_o - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}}^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x \\
&+ \int_{\varphi_o}^{\varphi_i} \mathrm{e}^{-x} \int_{\frac{\beta x}{\bar{\beta}}}^{\phi_i - \frac{\beta x}{\bar{\beta}}} \mathrm{e}^{-y} \int_{\hat{r}_o - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}}^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x \\
=& \frac{1}{\psi}\left(\mathrm{e}^{-\hat{r}_o} - \mathrm{e}^{-\hat{r}_i}\right)\left[\mathrm{e}^{\phi_i v}\left(\mathrm{e}^{\psi\varphi_i} - 1\right) + \frac{1}{v}\left(\mathrm{e}^{\phi_o v} - \mathrm{e}^{\phi_i v}\right) + \frac{2(\psi+1)}{2v(\psi+1)+\psi}\left(\mathrm{e}^{\psi\varphi_i + \phi_i v} - \mathrm{e}^{\psi\varphi_o + \phi_o v}\right)\right].
\end{aligned} \tag{20}$$

(2) When $\Delta r > 1$, we have

$$\begin{aligned}
\hat{p}_2 =& \int_0^{\varphi_i} \mathrm{e}^{-x} \int_{\phi_i - \frac{\beta}{\bar{\beta}}x}^{\infty} \mathrm{e}^{-y} \int_0^{1} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x + \int_0^{\varphi_o} \mathrm{e}^{-x} \int_{\phi_o - \frac{\beta}{\bar{\beta}}x}^{\beta\hat{r}_o - \frac{\beta}{\bar{\beta}}x} \mathrm{e}^{-y} \int_{\hat{r}_o - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}}^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x \\
&+ \int_0^{\varphi_o} \mathrm{e}^{-x} \int_{\beta\hat{r}_o - \frac{\beta}{\bar{\beta}}x}^{\phi_i - \frac{\beta}{\bar{\beta}}x} \mathrm{e}^{-y} \int_0^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x + \int_{\varphi_o}^{\frac{\bar{\beta}\hat{r}_o}{2}} \mathrm{e}^{-x} \int_{\frac{\beta x}{\bar{\beta}}}^{\beta\hat{r}_o - \frac{\beta x}{\bar{\beta}}} \mathrm{e}^{-y} \int_{\hat{r}_o - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}}^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x \\
&+ \int_{\varphi_o}^{\frac{\bar{\beta}\hat{r}_o}{2}} \mathrm{e}^{-x} \int_{\beta\hat{r}_o - \frac{\beta x}{\bar{\beta}}}^{\phi_i - \frac{\beta x}{\bar{\beta}}} \mathrm{e}^{-y} \int_0^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x + \int_{\frac{\bar{\beta}\hat{r}_o}{2}}^{\varphi_i} \mathrm{e}^{-x} \int_{\frac{\beta}{\bar{\beta}}x}^{\phi_i - \frac{\beta}{\bar{\beta}}x} \mathrm{e}^{-y} \int_0^{\hat{r}_i - \frac{x}{\bar{\beta}} - \frac{y}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x \\
=& \frac{1}{\psi}\left(1 + \frac{1}{v}\right)\left(\mathrm{e}^{-1-\phi_i} - \mathrm{e}^{-\beta\hat{r}_o}\right) + \frac{\mathrm{e}^{-1}}{v}\left[\frac{1}{\psi}\mathrm{e}^{-\phi_o} + \left(\frac{1}{2\bar{v} - \psi} - \frac{1}{\psi}\right)\mathrm{e}^{-\frac{\phi_o}{2} - \varphi_o}\right]\left(1 - \mathrm{e}^{-\Delta r}\right) \\
&+ \left[\frac{1}{v}\left(\frac{1}{2\bar{v} - \psi} - \frac{1}{\psi}\right) - \frac{1}{\psi}\right]\left(\mathrm{e}^{-1 - \frac{\phi_i}{2} - \varphi_i} - \mathrm{e}^{-\frac{\beta+\bar{\beta}}{2}\hat{r}_o}\right) + \frac{1}{\psi + 2}\left(\mathrm{e}^{-\frac{\beta+\bar{\beta}}{2}\hat{r}_o} - \mathrm{e}^{-\frac{\phi_i}{2} - \varphi_i}\right).
\end{aligned} \tag{21}$$

Correspondingly, the successful spoofing rate is derived as

$$R_A = \mathrm{E}_{X,Y,Z}\log_2\left(1 + \frac{P_A d_A^{-2\alpha} Y}{P_t d_L^{-2\alpha} X + \sigma_n^2 Z}\right) \mathbb{1}\left\{ \begin{array}{l} P_A = \min\{P_{2,c}, P_m\} > \max\left\{P_{1,c}, \tilde{P}_1\right\}, \\ r_o < P_A d_A^{-2\alpha} Y + P_t d_L^{-2\alpha} X + \sigma_n^2 Z < r_i \end{array} \right\}. \tag{22}$$

The closed-form expression can be derived by similar manipulations in (20) and (21).

As for the legitimate user, the successful communication happens when the spoofer chooses to be silent. That is, the successful legitimate communication probability is defined as

$$\hat{p}_3 = \Pr\left\{ \min\{P_{2,c}, P_m\} < \max\left\{P_{1,c}, \tilde{P}_1\right\}, r_o \leqslant P_t d_L^{-2\alpha} X + \sigma_n^2 Z \leqslant r_i \right\}, \tag{23}$$

and the closed-form expression is derived as follows.

(1) When $2\hat{r}_o < \hat{r}_i - 1$, we have

$$\begin{aligned}
\hat{p}_3 =& \int_0^{\varphi_o} \mathrm{e}^{-x} \int_0^{\phi_o - \frac{\beta}{\bar{\beta}}x} \mathrm{e}^{-y} \int_{\hat{r}_o - \frac{x}{\bar{\beta}}}^{\hat{r}_i - \frac{x}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x + \int_{\varphi_i}^{\bar{\beta}\hat{r}_i} \mathrm{e}^{-x} \int_0^{\infty} \mathrm{e}^{-y} \int_0^{\hat{r}_i - \frac{x}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x \\
&+ \int_{\bar{\beta}\hat{r}_o}^{\varphi_i} \mathrm{e}^{-x} \int_0^{\frac{\beta}{\bar{\beta}}x} \mathrm{e}^{-y} \int_0^{\hat{r}_i - \frac{x}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x + \int_{\varphi_o}^{\bar{\beta}\hat{r}_o} \mathrm{e}^{-x} \int_0^{\frac{\beta x}{\bar{\beta}}} \mathrm{e}^{-y} \int_{\hat{r}_o - \frac{x}{\bar{\beta}}}^{\hat{r}_i - \frac{x}{\bar{\beta}}} \mathrm{e}^{-z} \mathrm{d}z\mathrm{d}y\mathrm{d}x, \\
=& \frac{1}{1 - \bar{\beta}}\left(\mathrm{e}^{-\bar{\beta}\hat{r}_o} - \mathrm{e}^{-\bar{\beta}\hat{r}_i}\right) + \left(\mathrm{e}^{-\hat{r}_o} - \mathrm{e}^{-\hat{r}_i}\right)\left\{\frac{\mathrm{e}^{(\bar{\beta}^{-1} - \psi - 2)\varphi_o}}{\bar{\beta}^{-1} - \psi - 2} - \frac{1}{\bar{v}} - \frac{\mathrm{e}^{-\phi_o}}{\bar{\beta}^{-1} + \psi}\left[\mathrm{e}^{(\bar{\beta}^{-1} + \psi)\varphi_o} - 1\right]\right\}
\end{aligned}$$

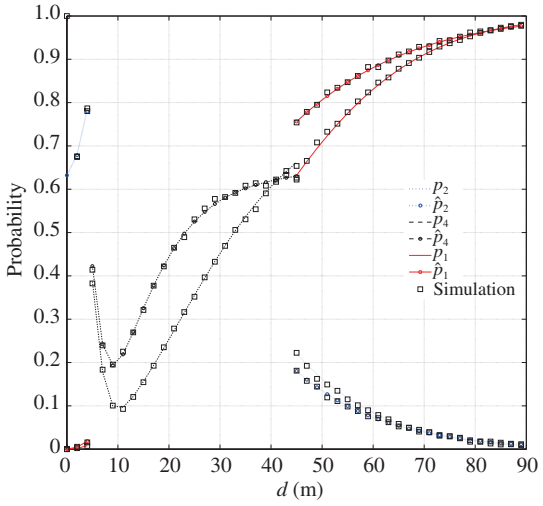

Figure 5 (Color online) Simulation and numerical results of the probabilities. The parameters are $P_t = P_m = 20$ dB, $d_i = 5$ m, and $d_o = 45$ m. For $\hat{p}_1$ and $\hat{p}_2$, we set $d_{LR} = 30$ m, and d indicates d_A. For $\hat{p}_4 = 1 - \hat{p}_3$, we use $d_{AR} = 60$ m, and d indicates d_L.

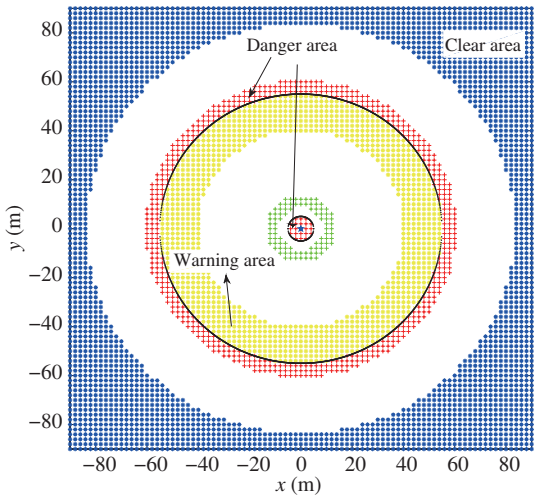

Figure 6 (Color online) The area distribution when the spoofer attacks a silent user. The parameters are $P_t = P_m = 20$ dB, $d_i = 5$ m, $d_o = 55$ m, $\epsilon_A = 0.1$ bps/Hz, $\epsilon_L = 0.5$ bps/Hz, $\epsilon_1 = 0.9$ and $\epsilon_3 = 0.9$.

$$+\left(\frac{\mathrm{e}^{-\frac{\hat{r}_i+1}{2}}}{\bar{\beta}^{-1}-\psi-2}+\frac{1}{\psi+2}\right)\mathrm{e}^{-(\psi+2)\varphi_i}-\left(\frac{1}{\bar{\beta}^{-1}-\psi-2}+\frac{1}{\psi+2}\right)\mathrm{e}^{-(\psi+2)\bar{\beta}\hat{r}_o}. \tag{24}$$

(2) When $2\hat{r}_o > \hat{r}_i - 1$, we have

$$\begin{aligned}\hat{p}_3 =& \int_0^{\varphi_o}\mathrm{e}^{-x}\int_0^{\phi_o-\frac{\beta}{\bar{\beta}}x}\mathrm{e}^{-y}\int_{\hat{r}_o-\frac{x}{\bar{\beta}}}^{\hat{r}_i-\frac{x}{\bar{\beta}}}\mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y\mathrm{d}x+\int_{\bar{\beta}\hat{r}_o}^{\bar{\beta}\hat{r}_i}\mathrm{e}^{-x}\int_0^{\infty}\mathrm{e}^{-y}\int_0^{\hat{r}_i-\frac{x}{\bar{\beta}}}\mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y\mathrm{d}x\\ &+\int_{\varphi_i}^{\bar{\beta}\hat{r}_o}\mathrm{e}^{-x}\int_0^{\infty}\mathrm{e}^{-y}\int_{\hat{r}_o-\frac{x}{\bar{\beta}}}^{\hat{r}_i-\frac{x}{\bar{\beta}}}\mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y\mathrm{d}x+\int_{\varphi_o}^{\varphi_i}\mathrm{e}^{-x}\int_0^{\frac{\beta}{\bar{\beta}}x}\mathrm{e}^{-y}\int_{\hat{r}_o-\frac{x}{\bar{\beta}}}^{\hat{r}_i-\frac{x}{\bar{\beta}}}\mathrm{e}^{-z}\mathrm{d}z\mathrm{d}y\mathrm{d}x,\\ =&\frac{1}{1-\bar{\beta}}\left(\mathrm{e}^{-\bar{\beta}\hat{r}_o}-\mathrm{e}^{-\bar{\beta}\hat{r}_i}\right)+\left(\mathrm{e}^{-\hat{r}_o}-\mathrm{e}^{-\hat{r}_i}\right)\left\{\frac{\mathrm{e}^{\left(\bar{\beta}^{-1}-\psi-2\right)\varphi_o}}{\bar{\beta}^{-1}-\psi-2}-\frac{1}{\bar{v}}-\frac{\mathrm{e}^{-\phi_o}}{\bar{\beta}^{-1}+\psi}\left[\mathrm{e}^{\left(\bar{\beta}^{-1}+\psi\right)\varphi_o}-1\right]\right\}\\ &-\frac{\mathrm{e}^{-\hat{r}_o}-\mathrm{e}^{-\hat{r}_i}}{\bar{\beta}^{-1}-\psi-2}\mathrm{e}^{\left(\bar{\beta}^{-1}-\psi-2\right)\varphi_i}.\end{aligned} \tag{25}$$

Correspondingly, the successful legitimate rate is derived as

$$R_L = \mathrm{E}_{X,Y,Z}\log_2\left(1+\frac{P_t d_L^{-2\alpha}X}{\sigma_n^2 Z}\right)\mathbb{1}\left\{\min\left\{P_{2,c},P_m\right\}<\max\left\{P_{1,c},\tilde{P}_1\right\},r_o\leqslant P_t d_L^{-2\alpha}X+\sigma_n^2 Z\leqslant r_i\right\}. \tag{26}$$

The closed-form expression can be derived by similar manipulations in (24) and (25).

4 Simulations

In this section, simulations are performed to verify our previous derivations, and study the impacts of system parameters, which are given in details respectively for Figures 5–12.

4.1 Verification of derivations

Without loss of generality, we set $r_i = P_t d_i^{-2\alpha} + \sigma_n^2$, $r_o = P_t d_o^{-2\alpha} + \sigma_n^2$, and $\alpha = 1$ unless otherwise stated. In Figures 6–8, the marker '★' is the destination, the marker '♦' denotes the typical user, and the marker '■' denotes the typical spoofer.

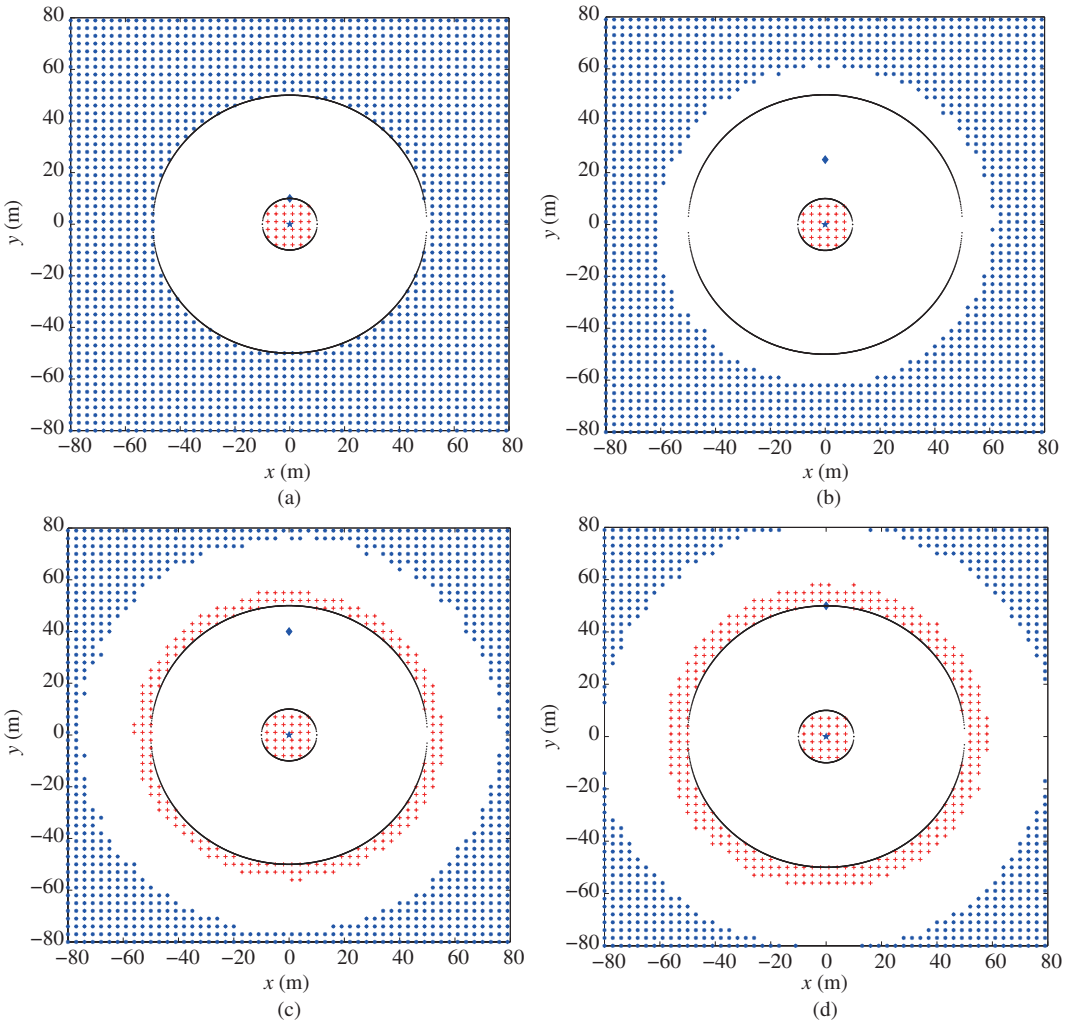

Figure 7 (Color online) The area distribution for different users. (a) $d_{LR} = 10$ m; (b) $d_{LR} = 25$ m; (c) $d_{LR} = 40$ m; (d) $d_{LR} = 50$ m. The parameters are $P_t = P_m = 20$ dB, $d_i = 10$ m, $d_o = 50$ m, $\epsilon_A = 0.1$ bps/Hz, and $\epsilon_1 = 0.9$.

In Figure 5, we find that the numerical curves obtained from the closed-form derivations match well with the monte carlo simulations, which verify that the analytical derivations are accurate. As a result, we use numerical curves in Figures 9–12 unless otherwise stated.

Figure 6 shows the area distribution as defined in previous sections. Two dark circles separate the legitimate users and spoofers. The area outside the annular region marked with '+' denotes the danger area with parameter $\epsilon_A = 0.1$ bps/Hz, while the area marked with 'o' denotes the clear area with $\epsilon_1 = 0.9$. The area inside of the annular region and close to the outer boundary denotes the warning area with $\epsilon_L = 0.5$ bps/Hz, while in the area close to the inner boundary, both the successful transmission probability and the successful data rate are larger than the given thresholds, i.e., $\epsilon_L = 0.5$ bps/Hz and $\epsilon_3 = 0.9$, respectively.

Figure 7 shows different spoofing distributions for users with distances 10 m, 25 m, 40 m, and 50 m, respectively. We find when the user is far away from the destination, the clear area shrinks and the danger area expands. Figure 8 shows the security distribution of the users when the spoofer is with a specific distance to the destination. We find when the spoofer is far away from the destination, the warning area shrinks to a pretty small area. These results indicate that under the proposed framework, the spoofers or the legitimate users close to the boundaries are hard to be distinguished. For messages from this area, we should further perform more detailed authentication.

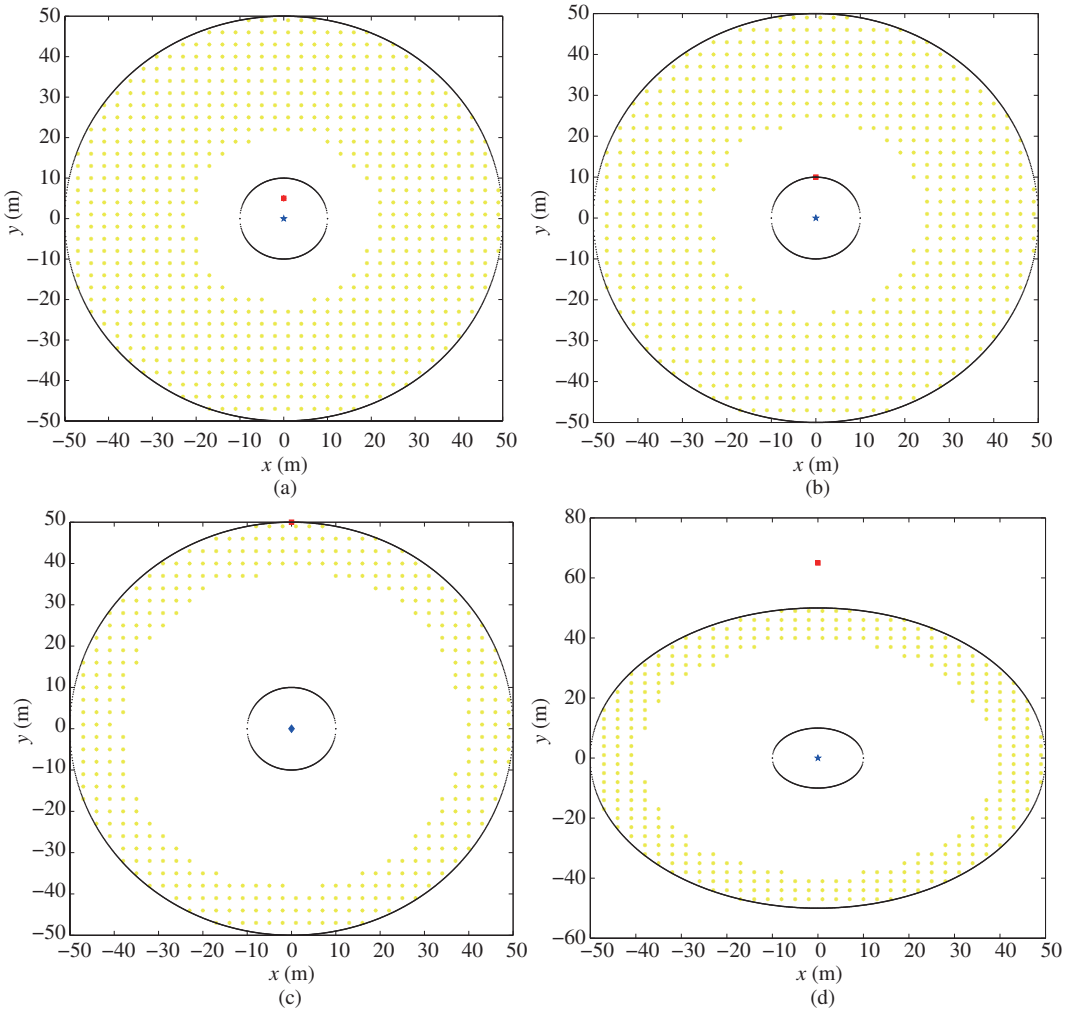

Figure 8 (Color online) The area distribution for different spoofers. (a) $d_{AR} = 5$ m; (b) $d_{AR} = 10$ m; (c) $d_{AR} = 50$ m; (d) $d_{AR} = 65$ m. The parameters are $P_t = P_m = 20$ dB, $d_i = 10$ m, $d_o = 50$ m, $\epsilon_L = 0.5$ bps/Hz and $\epsilon_3 = 0.9$.

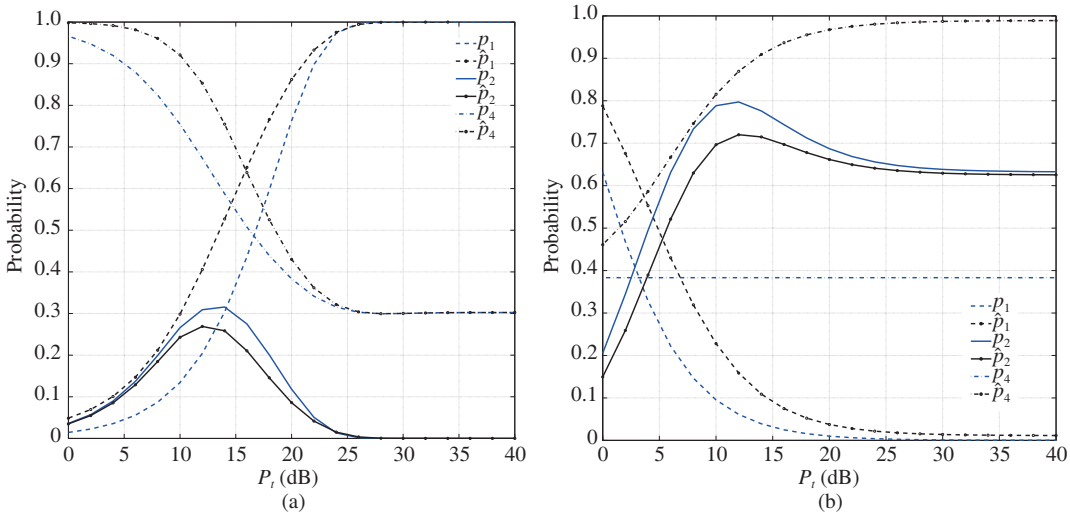

Figure 9 (Color online) The probability comparison over P_t. (a) $d_{AR} = 60$ m; (b) $d_{AR} = 5$ m. The parameters are $d_i = 10$ m, $d_o = 50$ m, and $d_{LR} = 30$ m.

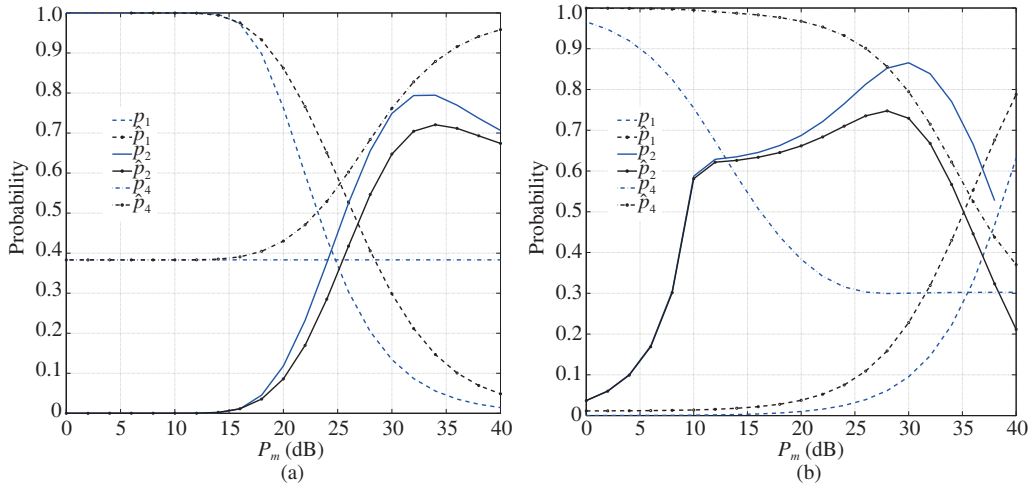

Figure 10 (Color online) The probability comparison over P_m. (a) $d_{AR} = 60$ m; (b) $d_{AR} = 5$ m. The parameters are $d_i = 10$ m, $d_o = 50$ m, and $d_{LR} = 30$ m.

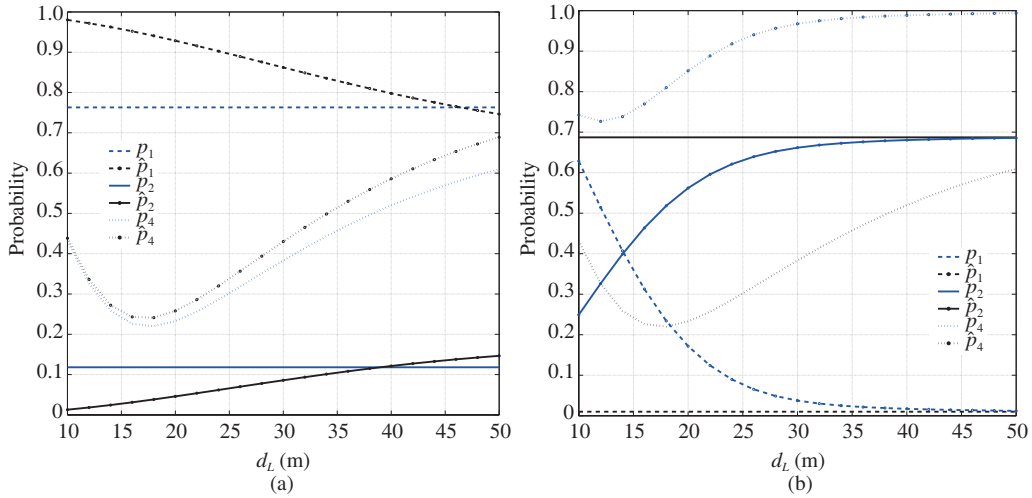

Figure 11 (Color online) The probability comparison over d_L. (a) $d_{AR} = 60$ m; (b) $d_{AR} = 5$ m. The parameters are $P_t = P_m = 20$ dB, $d_i = 10$ m, and $d_o = 50$ m.

4.2 Impact of system parameters

Figures 9–12 compare the probabilities for both cases with silent and active legitimate users, respectively. We find when the legitimate user is active, it is generally harder for the spoofer to launch a successful attack. That is, the spoofer is more likely to attack a silent user.

In Figure 9, we fix $P_m = 20$ dB, and for Figure 10, we fix $P_t = 20$ dB. Figure 9 shows that improving the legitimate power P_t can reduce the false alarm probability for legitimate users, i.e., p_4 and $\hat{p}_4$. However, it converges to a non-zero constant value at the high transmit power. This is mainly caused by the fading effects of wireless channels and also the power of thermal noise at the receiver. And when the transmit power P_t is larger than the maximal power P_m of the spoofer, it trends to be impossible for the spoofer to launch a successful attack, and thus the silent probability, i.e., p_1 and $\hat{p}_1$, tends to be one.

Figure 10 shows the impacts of the transmit powers on the probabilities. We find that p_2 is generally large when P_m is large, especially when the spoofers are quite close to the receiver. That is, strict power restriction on P_A (i.e., smaller P_m) is suggested to be performed by the network operator. Meanwhile, when the spoofer is close to the receiver, the legitimate transmit power P_t can take a small or medium value. Otherwise, P_t should be sufficiently enlarged.

From Figures 9 and 10, we also find that generally a larger transmit power is preferred by both spoofers

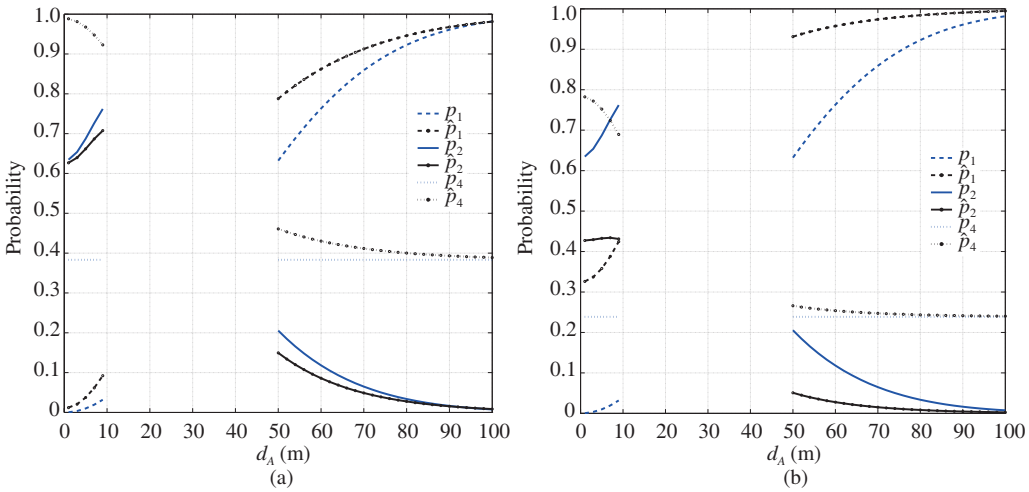

Figure 12 (Color online) The probability comparison over d_A. (a) $d_{LR} = 30$ m; (b) $d_{LR} = 15$ m. The parameters are $P_t = P_m = 20$ dB, $d_i = 10$ m, and $d_o = 50$ m.

and users. When the spoofing power is limited to $P_m = 20$ dB, relatively weak threat can be obtained at slightly larger legitimate power, i.e., $P_t = 20 - 25$ dB. While when the legitimate power is limited to a certain value, e.g., $P_t = 20$ dB, stronger threat will happen if the spoofing power is relatively large, e.g., $P_m = 30 - 35$ dB. We conclude that an optimal solution to avoid spoofing attacks is that the spoofing power is restricted to a value no larger than the legitimate transmit power. From this point of view, an efficient power control policy is necessary to restrict the transmit power of the overall network.

In Figures 11 and 12, we find that both the false alarm probability p_4 or $\hat{p}_4$ of users, and the successful spoofing probability p_2 or $\hat{p}_2$, increase as the transmitter is close to the inner and outer boundaries. These results imply that (1) the users at the center of the legitimate region are more safe than those close to the boundaries. (2) the spoofers close to the boundaries are more likely to launch attacks successfully. (3) the fuzzy area, i.e., the area where the false detection of both legitimate users and spoofers are so large that it is hard to distinguish between a user and a spoofer, is usually at the boundaries. We also find that the silent probability increases with the distance between the spoofer and the destination. These results are also verified in Figures 6–8.

5 Conclusion

In this paper, we propose a light-weight area-based authentication framework, potentially applicable to wireless communications with massive dynamic connections or low-capability devices. We considered two practical behavior models of the spoofers, and respectively derived the miss detection probabilities and the false alarm probabilities. We then evaluated the average security risks of the network by defining three different security areas. These results can provide insights for network operators.

In this paper, we considered a simple two-dimension space model with omnidirectional azimuth angles. And RSS is simply chosen as the authentication variable. To further enhance the security performance and support more general scenarios, we may introduce more physical variables into the framework, such as the azimuth angle and the altitude angle. These are under study as further work.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61941114, 61601051), Beijing Municipal Science and Technology Project (Grant No. Z181100003218005), and the 111 Project of China (Grant No. B16006).

References

1 Yilmaz M H, Arslan H. A survey: spoofing attacks in physical layer security. In: Proceedings of IEEE Local Computer Networks Conference Workshops, Clearwater Beach, 2015. 812–817

2 Xiao L, Sheng G, Wan X, et al. Learning-based PHY-layer authentication for underwater sensor networks. IEEE Commun Lett, 2019, 23: 60–63
3 Zeng K, Govindan K, Mohapatra P. Non-cryptographic authentication and identification in wireless networks. IEEE Wirel Commun, 2010, 17: 56–62
4 Aman M N, Chua K C, Sikdar B. Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet Things J, 2017, 4: 1327–1340
5 Namal S, Georgantas K, Gurtov A. Lightweight authentication and key management on 802.11 with Elliptic Curve Cryptography. In: Proceedings of 2013 IEEE Wireless Communications and Networking Conference, Shanghai, 2013. 1830–1835
6 Johansson N A, Wang Y P E, Eriksson E, et al. Radio access for ultra-reliable and low-latency 5G communications. In: Proceedings of 2015 IEEE International Conference on Communication Workshop (ICCW), London, 2015. 1184–1189
7 Kamal M, Tariq M. Light-weight security and data provenance for multi-hop Internet of Things. IEEE Access, 2018, 6: 34439–34448
8 Yang J, Ji X, Huang K, et al. Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet. IET Commun, 2019, 13: 144–152
9 Suzan S, Babak D B. A survey on lightweight cryptographic algorithms. In: Proceedings of TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, 2018. 1784–1789
10 Challa S, Wazid M, Das A K, et al. Secure signature-based authenticated key establishment scheme for future IoT applications. IEEE Access, 2017, 5: 3028–3043
11 Xiao L, Greenstein L, Mandayam N, et al. Channel-based spoofing detection in frequency-selective rayleigh channels. IEEE Trans Wirel Commun, 2009, 8: 5948–5956
12 Shi L, Li M, Yu S, et al. BANA: body area network authentication exploiting channel characteristics. IEEE J Sel Areas Commun, 2013, 31: 1803–1816
13 Zhang K, Liang X, Lu R, et al. Sybil attacks and their defenses in the Internet of Things. IEEE Internet Things J, 2014, 1: 372–383
14 Demirbas M, Song Y. An RSSI-based scheme for sybil attack detection in wireless sensor networks. In: Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, Buffalo-Niagara Falls, 2006. 564–570
15 Wang X, Hao P, Hanzo L. Physical-layer authentication for wireless security enhancement: current challenges and future developments. IEEE Commun Mag, 2016, 54: 152–158
16 Xiao L, Wan X, Han Z. PHY-layer authentication with multiple landmarks with reduced overhead. IEEE Trans Wirel Commun, 2018, 17: 1676–1687
17 Mohamed M, Cheffena M. Received signal strength based gait authentication. IEEE Sens J, 2018, 18: 6727–6734
18 Li J, Halder B, Stoica P, et al. Computationally efficient angle estimation for signals with known waveforms. IEEE Trans Signal Process, 1995, 43: 2154–2163
19 Wang Y, Guan X, Cai Y. The impacts of mobility on performance of physical layer secret key based on angle of arrival. In: Proceedings of IEEE International Conference on Wireless Communications and Signal Processing, Yangzhou, 2016. 1–5
20 Abdelaziz A, Burton R, Koksal C E. Message authentication and secret key agreement in VANETs via angle of arrival. In: Proceedings of 2016 IEEE Vehicular Networking Conference, Columbus, 2016. 1–2
21 Zanella A. Best practice in RSS measurements and ranging. IEEE Commun Surv Tut, 2016, 18: 2662–2686
22 Zhao Y, Liu Y, Yu T, et al. FREDI: robust RSS-based ranging with multipath effect and radio interference. Comput Netw, 2018, 147: 49–63
23 Zanella A, Bardella A. RSS-based ranging by multichannel RSS averaging. IEEE Wirel Commun Lett, 2014, 3: 10–13
24 Stoyanova T, Kerasiotis F, Efstathiou K, et al. Modeling of the RSS uncertainty for RSS-based outdoor localization and tracking applications in wireless sensor networks. In: Proceedings of 2010 4th International Conference on Sensor Technologies and Applications, Venice, 2010. 45–50
25 Achroufene A, Amirat Y, Chibani A. RSS-based indoor localization using belief function theory. IEEE Trans Automat Sci Eng, 2019, 16: 1163–1180
26 Waadt A E, Wang S, Kocks C, et al. Positioning in multiband OFDM UWB utilizing received signal strength. In: Proceedings of Positioning Navigation and Communication, Dresden, 2010. 308–312
27 Bhargava V, Sichitiu M L. Physical authentication through localization in wireless local area networks. In: Proceedings of IEEE Global Telecommunications Conference, St. Louis, 2005. 2658–2662
28 Chen Y, Yang J, Trappe W, et al. Detecting and localizing identity-based attacks in wireless and sensor networks. IEEE Trans Veh Technol, 2010, 59: 2418–2434
29 Yang J, Chen Y Y, Trappe W, et al. Detection and localization of multiple spoofing attackers in wireless networks. IEEE Trans Parallel Distrib Syst, 2013, 24: 44–58
30 Li N, Geng H, Xia S, et al. An area description framework for physical layer authentication. In: Proceedings of 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakech, 2019. 1–6