A Two Dimensional Quantization Algorithm for CIR-Based Physical Layer Authentication

Fiona Jiazi Liu, Xianbin Wang, and Serguei L. Primak
Dept. of Electrical and Computer Engineering,
The University of Western Ontario, London, Canada

Abstract—**Recently, channel impulse response (CIR) based physical layer authentication has been studied to enhance the security of wireless communications. However, the reliability of CIR-based authentication is substantially reduced at low signal-to-noise ratio (SNR) conditions due to the presence of communications noise, channel estimation error and mobility induced channel variation. To this end, we integrate additional multipath delay characteristics into the CIR-based physical layer authentication and propose a two dimensional quantization scheme to tolerate these random errors of CIRs for reduced false alarm rate and more reliable spoofing detection. Instead of directly comparing the estimated CIRs from different transmitters for authentication purpose, we first quantize the CIR estimates in two dimensions (i.e., the amplitude dimension and multipath delay dimension) and then differentiate transmitters based on the quantizer outputs with a binary hypothesis testing. More specifically, the quantization intervals are determined by using a searching algorithm based on a guaranteed miss probability of detection of the presence of spoofing attack. A logarithmic likelihood ratio test (LLRT) is used to evaluate the authentication performance, and a threshold with a constant value is used for the decision-making of authentication under the binary hypothesis testing. To verify the effectiveness of proposed algorithm, an orthogonal frequency division multiplexing (OFDM) system is considered in our simulation.**

I. Introduction

Due to the open as well as the broadcast nature of radio signal propagation, secure transmission has received significant amount of research attentions in addressing the security weaknesses of wireless systems and networks. Wireless security is traditionally achieved on the higher layers of protocol stack through cryptography approaches, which leads to a transparent and unprotected communications environment at the physical layer. As a result, various physical layer security schemes have been explored for further security enhancement against malicious interception and spoofing attacks on the communication links [1].

Physical layer authentication, one major aspect of physical layer security, is generally formulated as a binary hypothesis testing problem by exploiting the physical layer characteristics of wireless channels [2]–[5]. Specifically, received signal strength (RSS) and channel state information (CSI) have been investigated for physical layer authentication in [2] due to their temporal correlation in the propagation environment. However, the performance of RSS based authentication is limited by the channel stability and communications noise. Other channel characteristics, e.g. channel frequency response (CFR), have been explored to improve the reliability of physical layer authentication [3]–[5], where multiple antennas are further exploited to combat the mobility of wireless terminals. Nevertheless, the drawbacks of CFR-based physical layer authentication include the high implementation complexity in broadband systems and the omission of the spatial information on the signal propagation environment.

As an alternative, time-domain channel characteristics have also been investigated for authentication enhancement. In [6], a channel impulse response (CIR)-based authentication scenario has been proposed for a simple time-invariant wireless environment. In [7], an improved CIR-based physical layer authentication algorithm has been proposed by considering a time-varying channel, where the inherent properties of CIR are explored and an adaptive threshold is derived for spoofing detection. Nevertheless, the movement of mobile terminals and the presence of noise and channel estimation error lead to the temporal variation of CIR (especially in high mobility environments), which results in the low detection probability and high false alarm rate of CIR-based authentication approaches. In contrast to the rapid temporal variation of CIR, the multipath delay spread is relatively stable at different time slots, which, however, varies significantly at different spatial locations. This can be exploited as a significant feature for the physical-layer authentication, since the legitimate users and spoofing attacks are typically spatially separated with distinct multipath delay spread profiles. In addition, in order to achieve a robust authentication performance, an adaptive threshold for decision-making of CIR-based authentication needs to be derived under various channel conditions before the communication links are established, otherwise the performance of spoofing detection would be decreased.

As a result, we consider the integration of multipath delay characteristics into the CIR-based authentication framework and propose a two dimensional quantization scheme for the physical layer authentication to mitigate the negative impact of communications noise, channel estimation error and mobility induced path amplitude and delay variations. In particular, since the variations of both channel amplitude and path delay affect the decision-making of CIR-based authentication, the estimated CIRs are quantized in two dimensions, i.e., amplitude dimension and multipath delay dimension. Considering an appropriate miss detection rate, a searching-based algorithm is proposed to derive different step sizes of quantization corresponding for different channel taps. To verify the effectiveness of proposed quantization approach, an averaged logarithmic

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

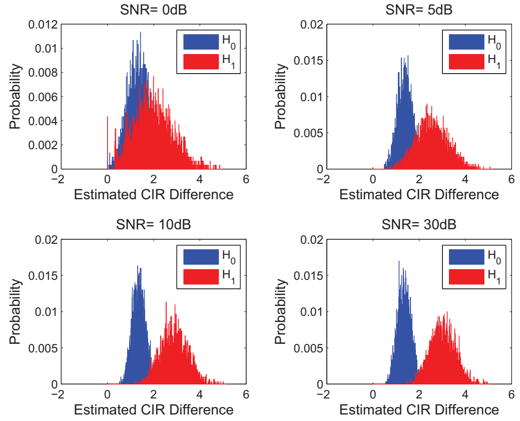

Fig. 1. Probability histograms of the difference between CIR estimates in consecutively time slots with four different SNRs under the two hypotheses H_0 and H_1.

likelihood ratio test (LLRT) is developed based on the difference between two consecutively quantized CIR estimates, and a threshold with constant value is used to simplify the procedure of decision making for authentication. In addition, the proposed authentication scheme is applied to an OFDM system in the simulation section. The performance of our proposed authentication scheme is evaluated and compared with that of CIR-based authentication without quantization.

The rest of this paper is organized as follows. In Section II, we introduce the system model and channel estimation method. Our proposed CIR quantization scheme is presented in Section III. In order to evaluate the performance of proposed CIR authentication scheme, we provide the simulation results in Section IV. Lastly, this paper is concluded in Section V.

II. System Modeling

Our proposed physical layer authentication scheme can be illustrated in three steps. Specifically, CIRs needed for the authentication process are obtained from noise-eliminated channel estimation using the method in [7], and then a two dimensional quantization scheme is applied to these CIRs. The quantized CIR estimates are used for decision-making based on the likelihood ratio test under a binary hypothesis testing. For theoretical analysis and numerical simulation, an OFDM system is employed. Additionally, the ubiquitous “Alice-Bob-Eve” scenario is used to explain the concept of authentication, where Alice, Bob and Eve are at different locations in space. Alice and Bob as the legitimate users, require secure communications, while eavesdropper Eve intends spoofing Bob. The objective of proposed authentication is to determine if a spoofing attack is present (or absent).

A. Channel Model

A time-varying multipath fading channel is considered in this paper, and modeled as

$$h(n) = \sum_{i=0}^{K-1} a_i(n)\delta(n-\tau_i(n)), \tag{1}$$

where n is the time-domain sample index with sampling period T_s. $a_i(n)$ and $\tau_i(n)$ are the time-varying amplitude and multipath propagation delay of the i^{th} multipath component at time nT_s, respectively. K is the total number of channel paths. In a Rayleigh fading channel, the attenuation of each path $a_i(n)$ can be modeled as a zero-mean complex Gaussian random variable with variance σ_i^2, i.e., $a_i(n) \sim \mathcal{N}_c(0, \sigma_i^2)$, and $\sum_{i=0}^{K-1} \sigma_i^2 = 1$. Additionally, the statistical independence between the multipath components is assumed.

B. Channel Estimation

As for channel estimation, a sparse channel model with a few significant paths is adopted in this paper, and comb-type pilots are embedded in the OFDM symbols (consisting of N subcarriers) for CIR estimation [7]. Specifically, we assume that the number of pilots N_p is at least equal to that of ideal paths K to avoid any loss of the information of CIR. Without any knowledge of the channel at receiver, the CIR estimation algorithm can be written by

$$\hat{h}_i(n) = \begin{cases} h_i(n) + w(n), & if\ 0 \le i \le N_p - 1 \\ 0, & if\ N_p \le i \le N, \end{cases} \tag{2}$$

where w is a white complex Gaussian noise with mean zero and variance σ_w^2. Since both strong and weak multipath components are contaminated by noise, and noise components are also introduced to the original zero-valued channel paths, the presence of noise increases the difficulty of determining the true channel variations on all paths. To mitigate the effect of noise on estimated CIRs, a noise-dependent threshold is derived [7]. Specifically, the absolute value of each path is compared with some threshold. All paths with absolute value less than the threshold are specified as zero-valued taps.

III. Quantized CIR-based Authentication

A. Quantization Scheme

Based on the system model, a CIR-based physical layer authentication has been proposed in [7], where the unique characteristics of CIR are exploited and the difference between two adjacent CIR estimates is used to develop test statistics for evaluating the authentication performance. Fig. 1 shows four histograms generated from the proposed authentication scheme in [7], which indicates that CIR-based authentication cannot guarantee a robust performance at low SNR due to large overlapped portion under a binary hypothesis testing (H_0 and H_1). Since the overlapping parts are caused by the presence of noise, channel estimation error and terminal movement, and channel variations are represented by the terms of channel amplitude and path delay variation, we propose a two dimensional quantization scheme applied to CIR estimates to tolerate these negative impacts on CIRs. Due to the statistical independence between multipath components, we just consider one path in our quantization scheme. Therefore, the superscript “i”, which stands for the i^{th} path, can be removed. A sample of quantized

CIR estimate is described in two dimensions, i.e., channel amplitude $a_q(n)$ and path delay $\tau_q(n)$,

$$\begin{aligned} a_q(n) &= |\hat{a}(n)|+e_x(n), && (3)\\ \tau_q(n) &= \hat{\tau}(n)+e_y(n), && (4) \end{aligned}$$

where $e_i(n) = e_{x,i}(n) + je_{y,i}(n)$ is the quantization noise, and assumed as additive Gaussian noise with variance of $\sigma^2_{e,i}$. $|\hat{a}(n)|$ and $\hat{\tau}(n)$ are the estimated amplitude and path delay. Since $\hat{a}(n)$ follows zero-mean complex Gaussian distribution with variance $\sigma^2 + \sigma^2_w$, the distribution of $|\hat{a}(n)|$ is Rayleigh with parameter $\sqrt{(\sigma^2 + \sigma^2_w)/2}$. Additionally, as for our proposed quantization scheme, a multi-level quantization algorithm is developed with the number of quantization level L. We also define that $\{x_1, x_2, \ldots, x_L\}$ and $\{y_1, y_2, \ldots, y_L\}$ are two vectors of quantization boundary points in the dimensions of amplitude and path delay respectively.

To determine the boundary points of quantization intervals $\{x_v\}^L_{v=1}$ and $\{y_v\}^L_{v=1}$, a searching-based algorithm is proposed based on the missed detection rate (MDR) P_{MD}, which is formulated as a joint probability, i.e., the probability of CIR estimate from Eve dropping in same quantization interval as that from Alice. In particular, since $|\hat{a}^A(n)|$ achieved from the legitimate transmitter is independence of $|\hat{a}^E(n)|$ obtained from the eavesdropper, the MDR in the dimension of channel amplitude $P_{MD,1}$ can be derived as

$$\begin{aligned} P_{MD,1} &= P\left\{x_v < |\hat{a}^E(n)| \leq x_{v+1}, x_v < |\hat{a}^A(n)| \leq x_{v+1}\right\}\\ &= P\left\{x_v < |\hat{a}^E(n)| \leq x_{v+1}\right\} \cdot P\left\{x_v < |\hat{a}^A(n)| \leq x_{v+1}\right\}\\ &= \left[e^{\frac{-x_v^2}{\sigma^2_E+\sigma^2_w}} - e^{\frac{-x_{v+1}^2}{\sigma^2_E+\sigma^2_w}}\right]\left[e^{\frac{-x_v^2}{\sigma^2_A+\sigma^2_w}} - e^{\frac{-x_{v+1}^2}{\sigma^2_A+\sigma^2_w}}\right] \qquad (5) \end{aligned}$$

where $v = \{1, 2, \ldots, L\}$. The superscripts "A" and "E" stand for transmitters Alice and Eve. Similarly, in this paper, we assume that the distribution of path delay is exponential, and $\hat{\tau}^E(n)$ is independence of $\hat{\tau}^A(n)$. Therefore, the MDR in the dimension of path delay $P_{MD,2}$ can be written as

$$\begin{aligned} P_{MD,2} &= P\left\{y_v < \hat{\tau}^E(n) \leq y_{v+1}, y_v < \hat{\tau}^A(n) \leq y_{v+1}\right\}\\ &= P\left\{y_v < \hat{\tau}^E(n) \leq y_{v+1}\right\} \cdot P\left\{y_v < \hat{\tau}^A(n) \leq y_{v+1}\right\}\\ &= [e^{-\lambda_E y_v} - e^{-\lambda_E y_{v+1}}][e^{-\lambda_A y_v} - e^{-\lambda_A y_{v+1}}] \qquad (6) \end{aligned}$$

where λ_A and λ_E are the rate parameters of the distributions.

For secure communications, low MDR is required and set to be 0.1 in our case. Consequently, the searching-based algorithm determines the values $\{x_v\}^L_{v=1}$ and $\{y_v\}^L_{v=1}$, and guarantees the MDR is exactly 0.1, which can be described as follows:

Step 1: Initialization, set $v = 1$, $x_1 = 0$ and $y_1 = 0$.

Step 2: For each v, search for the unique quantization step sizes x_{v+1} and y_{v+1}, which satisfy:

$$\begin{aligned} P_{MD,1} &= 0.1, && (7)\\ P_{MD,2} &= 0.1. && (8) \end{aligned}$$

Step 3: If $v < L$, set $v = v+1$ and go to Step 2; otherwise, go to next step.

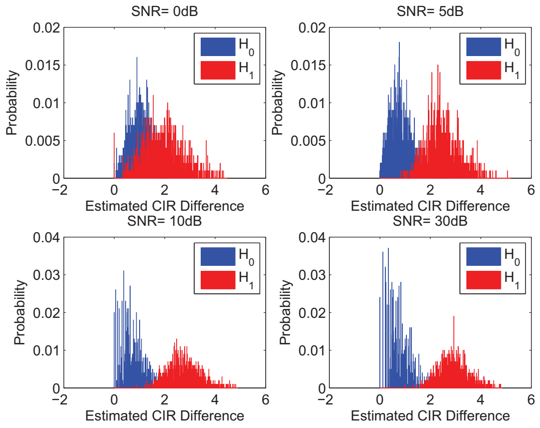

Fig. 2. Probability histograms of the difference between quantized CIR estimates in consecutively time slots with four different SNRs under the two hypotheses H_0 and H_1.

Step 4: Set $x_{v+1} = +\infty$ and $y_{v+1} = +\infty$.

Looking into this searching-based algorithm, it indicates that difference boundary points of quantization are achieved under difference channel conditions.

Due to the impact of quantization noise on CIR estimates, the objective of our proposed quantization scheme is to minimize the variation between two adjacently quantized CIR estimates from same transmitter, but still maintain the difference between them from disparate transmitters. Additionally, since we just consider the difference between current quantized CIR and the previous one in the analysis of authentication, we are not interested in the specific value of each quantized CIR. Therefore, based on the derived quantization boundary points $\{x_v\}^L_{v=1}$ and $\{y_v\}^L_{v=1}$, we define the differences of two successively quantized CIRs corresponding to the two dimensions, i.e., Δa_q and $\Delta\tau_q$, as

$$\Delta a_q(n) = \begin{cases} 0, & if\ x_v < |\hat{a}(n)|, |\hat{a}(n+1)| \leq x_{v+1},\\ |\hat{a}(n+1) - \hat{a}(n)|, & otherwise, \end{cases} \qquad (9)$$

$$\Delta\tau_q(n) = \begin{cases} 0, & if\ y_v < \hat{\tau}(n), \hat{\tau}(n+1) \leq y_{v+1},\\ \min\left\{\hat{\tau}(n), \hat{\tau}(n+1)\right\}, & otherwise, \end{cases} \qquad (10)$$

From Fig. 2, a set of histograms corresponding to them shown in Fig. 1 are drawn using same simulation parameters in [7]. It illustrates that the proportion of overlapping part is significantly decreased under severe channel conditions.

B. Authentication Scheme

In our proposed authentication scheme, the likelihood ratio test (LRT) is developed based on the variation between two successive CIRs, which is further expressed under two cases. First of all, without the quantization process, since both CIR estimate and its difference between two consecutive CIRs follow complex Gaussian distribution [7], an averaged logarithmic likelihood ratio test (LLRT), defined as $\mathbf{L}$, can be formulated by

$$\mathbf{L} = \frac{1}{M}\sum_{n=0}^{M-1} T_n, \qquad (11)$$

where

$$T_n = \ln\left\{ \frac{1}{2\pi N_p} \sum_{i=0}^{N_p-1} \frac{1}{\sigma_i^2} \exp\left[\frac{-1}{2\sigma_i^2} \left| \hat{h}_i(n+1) - \hat{h}_i(n) \right|^2 \right] \right\}, \tag{12}$$

where σ_i^2 is the variance of difference between estimated CIRs on the i^{th} path under a certain SNR, and M is the number of achieved CIR estimates. Similarly, when our proposed quantization scheme is considered into the system, a test statistic of the difference between two quantized CIRs using the averaged LLRT function, i.e., $\mathbf{L_q}$, can be written as

$$\mathbf{L_q} = \frac{1}{M} \sum_{n=0}^{M-1} T_{q,n}, \tag{13}$$

where

$$\begin{aligned} T_{q,n} = \alpha \times \ln & \left\{ \frac{1}{2\pi N_p} \sum_{i=0}^{N_p-1} \frac{1}{\sigma_{q,i}^2} \exp\left[\frac{\Delta a_{q,i}(n)^2}{-2\sigma_{q,i}^2} \right] \right\} + \\ & \beta \times \ln \left\{ \frac{1}{N_p} \sum_{i=0}^{N_p-1} \lambda_q^2 \exp\left[-\lambda_q \Delta\tau_{q,i}(n) \right] \right\}, \end{aligned} \tag{14}$$

where $\sigma_{q,i}^2$ and λ_q are respectively the variance of Δa_q on the i^{th} tap, and the rate parameter of $\Delta\tau_q$ at a specific SNR. α and β are assigned weights.

In order to evaluate the performance of our proposed authentication scheme, these two test statistics based on the averaged LLRT function, i.e., $\mathbf{L}$ and $\mathbf{L_q}$, are analyzed and calculated in the next subsection.

C. Analysis of Authentication Performance

Note that physical layer authentication is generally considered as a hypothesis testing problem, which is formulated to verify the performance of proposed authentication scheme. Specifically, first of all, without the preprocessing procedure of quantization, an adaptive threshold is derived in [7] for analyzing the authentication performance. The binary hypothesis testing problem is correspondingly expressed as

$$\begin{aligned} H_0 &: T_n < \delta \\ H_1 &: T_n > \delta, \end{aligned} \tag{15}$$

where H_0, the null hypothesis, denotes Alice as the sender, while the alternative hypothesis, H_1, stands for that the eavesdropper Eve is involved in the communications. The adaptive threshold δ is derived based on the distribution of the test statistic under the hypothesis H_0, where the false alarm rate (FAR) is set to be a constant less than 0.1 for military communications. The value of δ is varying with the number of paths of two successive CIRs from the legitimate transmitter.

In contrast, considering our proposed quantization algorithm given in the equations (9) and (10), the majority of significant variations between consecutive CIRs from the legitimate transmitter are reduced to zero, while original distinction between two CIRs from unauthenticated transmitters are remained.

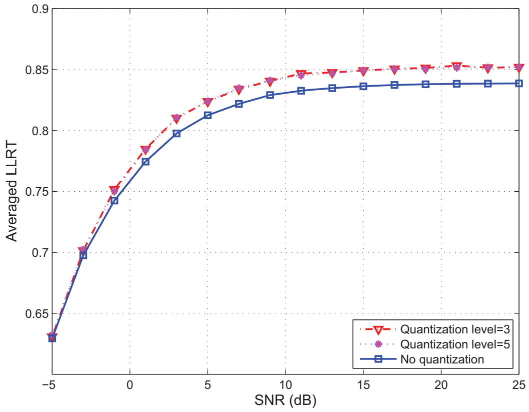

Fig. 3. Under the hypothesis H_0, the two averaged LLRTs ($\mathbf{L}$ and $\mathbf{L_q}$) versus SNRs under two different quantization levels. The AR coefficient ζ is fixed as 0.8.

Thus, based on our quantization scheme, we can define a binary hypothesis testing as

$$\begin{aligned} H_0 &: T_{q,n} < \delta_q \\ H_1 &: T_{q,n} > \delta_q, \end{aligned} \tag{16}$$

where δ_q is a threshold defined as a constant. Comparing these two hypothesis testing problems, no threshold needs to be derived adaptively when the proposed quantization is considered in our authentication scheme. In addition, most of differences between two CIRs from the legitimate user are eliminated after quantization, thereby the processing procedure of our authentication system is simplified. To evaluate the performance of our proposed authentication scheme, False alarm rate (FAR) and probability of detection (PD) are employed.

Additionally, referring to the theoretical analysis in [7] and the assumption of high correlation between two adjacent CIRs on the same path, the variance σ_i^2 in (12) under the two hypotheses can be expressed as $\sigma_{H_0,i}^2 = 2(1-\zeta)\sigma_{A,i}^2 + 2\sigma_w^2$ and $\sigma_{H_1,i}^2 = \sigma_{E,i}^2 + \sigma_{A,i}^2 + 2\sigma_w^2$ respectively. ζ is the AR correlation coefficient and considered as a constant. Therefore, based on the expressions of variance σ_i^2, $\sigma_{q,i}^2$ in (14) can be derived under the two hypotheses as $\sigma_{q,H_0,i}^2 = \sigma_{H_0,i}^2 + \sigma_{e,i}^2$ and $\sigma_{q,H_1,i}^2 = \sigma_{H_1,i}^2 + \sigma_{e,i}^2$. Similarly, under the two hypotheses, we can obtain that $\lambda_{q,H_0} = 2\lambda_A$ and $\lambda_{q,H_1} = \lambda_A + \lambda_E$.

IV. Simulation Results

A. Simulation Scenarios

In this section, the effectiveness of proposed authentication scheme is verified by numerical simulations. An OFDM system with total subcarrier number of 1024 is employed and modulated by QPSK technique on each subcarrier, and the length of CP is 256. Comb-type pilots with number of 64 are inserted into each OFDM symbol for channel estimation. As for the channel model, a random Rayleigh fading channel is developed with six sparse sample-spaced significant paths and uniform power delay profile. In contrast, the number of significant paths communicating between Eve and Bob is

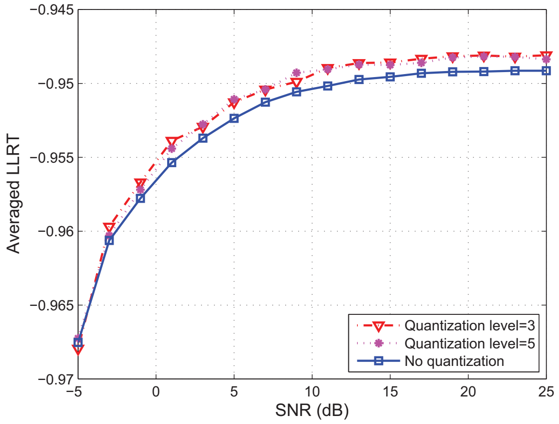

Fig. 4. Under the hypothesis H_1, the two averaged LLRTs ($\mathbf{L}$ and $\mathbf{L_q}$) versus SNRs under two different quantization levels. Herein ζ is 0.8.

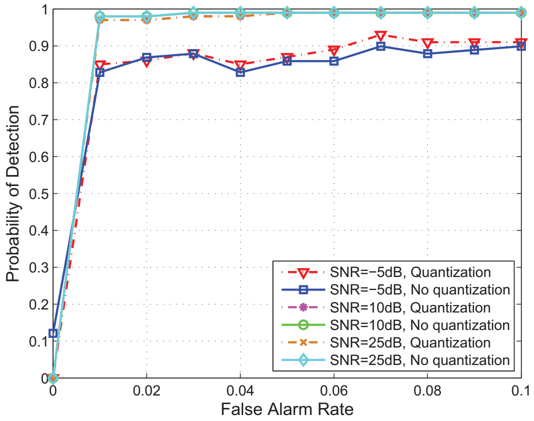

Fig. 5. Probability of detection versus false alarm rates under three different SNRs. Herein the number of quantization levels is three.

randomly chosen from 1 to 10. Additionally, different delayed paths are statistically independent of each other.

B. Numerical Results and Discussion

Fig. 3 shows the effects of different quantization levels on values of $\mathbf{L_q}$, and which are compared with $\mathbf{L}$ at different SNRs. It shows that the values of $\mathbf{L}$ and $\mathbf{L_q}$ under H_0 are all dramatically increasing when SNR increases, and $\mathbf{L_q}$ under various quantization levels are slightly larger than $\mathbf{L}$. In other words, under H_0, the significant variations between two CIRs are partially eliminated based on the proposed quantization scheme, and the proportion becomes larger at high SNRs. In addition, different quantization levels hardly impact on the values of $\mathbf{L_q}$.

In Fig. 4, the values of the two averaged LLRTs are calculated versus SNRs under two different quantization levels, when the eavesdropper Eve is present. Fig. 4 illustrates that the presence of Eve decreases the values of both $\mathbf{L_q}$ and $\mathbf{L}$, as the difference between two consecutive CIRs under H_1 is larger than that under H_0. The values of $\mathbf{L}$ and $\mathbf{L_q}$ are also increasing but slightly, when the SNR value increases. Additionally, comparing Fig. 4 with Fig. 3, the difference between $\mathbf{L}$ and $\mathbf{L_q}$ is decreased. Overall, the performance of detecting spoofing attacks is maintained.

The performance of spoofing detection is sketched versus FARs under three different SNR values in Fig. 5, which compares the CIR-based authentication scheme with the proposed quantization-based CIR authentication, and the number of quantization levels is set to be three. It shows that, under different SNRs, the performance of authentication based on our proposed quantization scheme can maintain to a great level, which is slightly greater than the performance of authentication scheme without quantization under high FARs (for example, when SNR is at a low value of -5dB, the PD can reach to 0.9 at FAR=0.1). Additionally, the performance of detection gets better under high SNR values.

V. Conclusion

In this paper, we have proposed a physical layer authentication scheme using a two dimensional quantization under a binary hypothesis testing, where estimated CIRs are quantized in two dimensions to eliminate the impacts of noise, channel estimation error and mobility induced channel variation. Specifically, a noise-eliminated channel estimation is utilized to preprocess the achieved CIRs at receiver. The proposed quantization algorithm is then applied to the CIR estimates in the dimensions of amplitude and path delay respectively, where different step sizes of quantization are derived based on a searching algorithm. An OFDM system has been employed to evaluate the performance of authentication based on the LLRT. The numerical results show the effectiveness of our proposed authentication scheme.

Acknowledgement

The authors would like to thank Dr. Peter Mason and Dr. Helen Tang from Defense Research and Development Canada (DRDC) for their constructive comments and helpful suggestions.

References

[1] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*,vol.5. Foundations and Trends in Comms. and Info. Theory, 2009.

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

[3] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. IEEE International Conference on Communications (ICC)*, May 2008, pp. 1520-1524.

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

[5] F. He, H. Man, D. Kivanc and B. McNair, "EPSON: enhanced physical security in OFDM networks," in *Proc. IEEE International Conference on Communications (ICC)*, 2009, pp. 1-5.

[6] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. IEEE International Conference on Communication systems and networks (COMSNETS)*, Mar. 2010, pp. 1-9.

[7] F. J. Liu, X. Wang and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. IEEE Military Communications Conference (MILCOM)*, Nov.2011, pp.538-542.