Complementary Authenticator Design for Ground Control Station to Identify Unmanned Aerial Vehicles Based on Channel-tap Power

Trong Nghia Le, Lan Anh Nguyen Thi, Trong Khanh Nghiem, Hong Viet Nguyen,
Dang Khoa Truong, Tran Hiep Nguyen, Van Cong Hoang, and Minh Dong Pham

Abstract—This work proposes a novel authentication method for identifying Unmanned Aerial Vehicles (UAVs) based on a channel-tap power. A ground control station utilized the channel-tap power as a radio-frequency fingerprint (RFF) to directly detect UAVs via physical (PHY) layer. The proposed authentication method uses the Neyman-Pearson test to discriminate between two UAVs, UAV_I and UAV_A, which are controlled by the ground control station. The proposed methods helps the ground control station completely detect UAV_I and UAV_A using PHY layer. Finally, the performances are analyzed, and simulations are conducted to evaluate the performance of the proposed authenticator. From simulation results, for SNR=-5 dB and the false alarm probability of 0.2, the ground control station can detect the UAV with the detection probability of 0.90 under the UAV speed of 70 km/h.

Keywords—Channel-tap Power, Unmanned Aerial Vehicles (UAVs), Complementary Authenticator.

I. Introduction

In recent years, the detection of Unmanned Aerial Vehicles (UAVs) using PHY layer has been treated as one aspect of issue in the more general research problem of identifying radio-frequency fingerprint (RFF). Complementary authenticator design for ground control station to identify UAV is very important when the GPS is not available temporarily or permanently. In this work, the channel-tap power is estimated over the multipath Rayleigh fading channels, which will be employed for UAVs detection. The change of channel-tap powers depends on the motion of UAV and the ground control station utilized as the RFF, which is a one-to-one relation between the UAV and the ground control station, to detect UAVs. A channel-based detection by PHY layer is proposed. In the scheme, the Neyman-Pearson test is performed to discriminate between two UAVs, UAV_I and UAV_A, which are controlled by the ground control station.

II. System Model

A. Channel Model

The uniqueness of a channel between two locations in the multipath environment of wireless communications has been proven [1]. Our system consists of two UAVs, UAV_I and UAV_A, a satellite and a ground control station, which uses a wireless network based on orthogonal frequency-division multiplexing (OFDM) technology. The ground control station might detect the UAV using the proposed detection method when the GPS is not available temporarily or permanently. In this study, $h_m(n,l)$ denotes the lth channel impulse response of multipath channels at time n with (L+1) uncorrelated taps, undergone by the mth OFDM symbol. The wireless channels are assumed to be Rayleigh fading [2]. The channel taps are assumed to be stationary within an OFDM symbol; however, they are randomly generated across symbols to capture the randomness of wireless channels. Based on the assumption of wide-sense stationary and uncorrelated scattering, the cross-correlation of the channel response within a symbol can be expressed as

$$\begin{aligned} E[h_m(n_1,l_1)h_m^*(n_2,l_2)] &= E[h_m(n_1,l_1)h_m^*(n_2,l_2)]\delta(l_1-l_2) \\ &= J_0(\beta\Delta)\sigma^2_{h_m(l)}|_{l=l_1=l_2} \end{aligned} \quad (1)$$

where $\delta(\cdot)$ is the Dirac delta function; $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind; $\Delta \equiv n_2 - n_1$; $\sigma^2_{h_m(l)} \equiv E\left[|h_m(l)|^2\right]$ is the lth channel-tap power, and $\beta = 2\pi f_d T_s$, f_d is the maximum Doppler shift, T_s is the sampling interval, and $(\cdot)^*$ denotes the complex conjugate.

B. Correlation characteristics of OFDM

In the following discussion, since the time-domain correlation characteristics of OFDM symbols are related to neighboring symbols, the signal model will consider three symbols, which are the previous, the current, and the next symbols. We consider an OFDM with N subcarriers using burst-mode transmission that includes M consecutive symbols. The complex data are modulated onto the N subcarriers by means of the inverse discrete Fourier transform (IDFT). A cyclic prefix (CP) of length N_{CP} is inserted at the beginning of each OFDM symbol to prevent ISI and preserve the mutual orthogonality of subcarriers. Following serial-to-parallel conversion, the current mth OFDM symbol $x_m(n)$, $n \in \{0,1,\ldots,N+N_{CP}-1\}$, is finally transmitted through a multipath channel $h_m(n,l)$. Because of CP, the transmitted data have the following characteristics. If $n_2 \neq n_1$ and $n_2 \neq n_1 + N$, then the correlation of $x_m(n)$ is $E[x_m(n_1)x_m^*(n_2)] = 0$; otherwise $E[x_m(n_1)x_m^*(n_2)] = \sigma_x^2$, where σ_x^2 is the signal power.

At the ground control station side, given the previous OFDM symbol $x_{m-1}(n)$ before the current symbol, the received

This work was not supported by any organization.

Trong Nghia Le is with Technical Office, Le Quy Don Technical University, Hanoi, Vietnam (Email: nghiahp79@gmail.com).

The rest of authors are with Department of Control Engineering, Le Quy Don Technical University, Hanoi, Vietnam (Email: lananhbk@yahoo.com; khoahn@yahoo.com; hiepnguyentran@vnn.vn)

978-1-5386-3422-6/17/$31.00 ©2017 IEEE

sampled data $\tilde{x}_m(n)$ can be written as

$$\begin{aligned}\tilde{x}_m(n) &= \sum_{l=0}^{L} h_{m-1}(n,l)\, x_{m-1}(n-l) \\ &+ \sum_{l=0}^{L} h_m(n,l)\, x_m(n-l) + \omega(n) \end{aligned} \tag{2}$$

where $\omega(n)$ is the additive white Gaussian noise (AWGN) with zero mean and variance σ_ω^2. Next, to obtain the correlation characteristics of separated-by-N data, $\tilde{x}_m(n+N)$ should be obtained,

$$\begin{aligned}\tilde{x}_m(n+N) = &\sum_{l=0}^{L} h_m(n+N,l)\, x_m(n+N-l) \\ &+ \sum_{l=0}^{L} h_{m+1}(n+N,l)\, x_{m+1}(n+N-l) \\ &+ \omega(n+N)\end{aligned} \tag{3}$$

As $x_{m-1}(\cdot)$, $x_m(\cdot)$, $x_{m+1}(\cdot)$, $h_{m-1}(\cdot)$, $h_m(\cdot)$, $h_{m+1}(\cdot)$, and $\omega(\cdot)$ are mutually uncorrelated, the correlation between $\tilde{x}_m(n)$ and $\tilde{x}_m(n+N)$ can be expressed as,

$$E\left[\tilde{x}_m(n)\,\tilde{x}_m^*(n+N)\right] = \begin{cases} \mu \sum_{l=0}^{n} \sigma_{h_m(l)}^2 & , n \in I_1 \\ \mu \sum_{l=0}^{L} \sigma_{h_m(l)}^2 & , n \in I_2 \\ \mu \sum_{l=n-N_{CP}+1}^{L} \sigma_{h_m(l)}^2 & , n \in I_3 \\ 0 & , n \in I_4 \end{cases} \tag{4}$$

where $\mu = \sigma_x^2 J_0(\beta N)$ is a constant when the coherent time is larger than the symbol duration, and

$$\begin{aligned} &I_1 \equiv \{0, 1, ..., L-1\} \\ &I_2 \equiv \{L, L+1, ..., N_{CP}-1\} \\ &I_3 \equiv \{N_{CP}, N_{CP}+1, ..., N_{CP}+L-1\} \\ &I_4 \equiv \{N_{CP}+L, N_{CP}+L+1, ..., N_{CP}+N-1\} \end{aligned} \tag{5}$$

III. PROPOSED ESTIMATION OF CHANNEL-TAP POWER FOR DESIGNING COMPLEMENTARY AUTHENTICATOR

Based on equation (4), the correlation can be written in matrix form as,

$$\mathbf{r} = \mu \mathbf{D} \mathbf{p} \tag{6}$$

where the correlation vector

$$\begin{aligned}\mathbf{r} &= [r(0), r(1), ..., r(N+N_{CP}-1)]^T \\ &\equiv E\left[\tilde{\mathbf{x}}_m(0) \otimes \tilde{\mathbf{x}}_m^*(N)\right]\end{aligned} \tag{7}$$

$\otimes$ and $[\cdot]^T$ denote the Hadamard product and transpose, respectively.

$$\tilde{\mathbf{x}}_m(i) = [\tilde{x}_m(i), \tilde{x}_m(i+1), \cdots, \tilde{x}_m(i+N+N_{CP}-1)]^T \tag{8}$$

$$\mathbf{p} = \left[\sigma_{h_m(0)}^2, \sigma_{h_m(1)}^2, \cdots, \sigma_{h_m(L)}^2\right]^T \tag{9}$$

$$\mathbf{D} \equiv \begin{bmatrix} \mathbf{D}_1 \\ \mathbf{D}_2 \\ \mathbf{D}_3 \\ \mathbf{D}_4 \end{bmatrix}_{(N+N_{CP})\times(L+1)} \tag{10}$$

$$\mathbf{D}_1 \equiv \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}_{L\times(L+1)} \tag{11}$$

$$\mathbf{D}_2 \equiv \mathbf{1}_{(N_{CP}-L)\times(L+1)} \tag{12}$$

$$\mathbf{D}_3 \equiv \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 1 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}_{L\times(L+1)} \tag{13}$$

$$\mathbf{D}_4 \equiv \mathbf{0}_{(N-L)\times(L+1)} \tag{14}$$

$\mathbf{1}_{(N_{CP}-L)\times(L+1)}$/$\mathbf{0}_{(N-L)\times(L+1)}$ are matrices with all-unity/all-zero elements.

The CP is responsible for the non-zero correlation values of separated-by-N samples. Owing to the linear convolution of transmitted data with channels, the length of non-zero correlation values is $N_{CP}+L$. Next, the statistical properties of equation (4) are considered.

According to equation (6), the proposed channel-tap power estimation of the ground control station, $\hat{\mathbf{p}}$, can be obtained

$$\hat{\mathbf{p}} = \mu^{-1} \mathbf{D}^\dagger \hat{\mathbf{r}} \tag{15}$$

where $\mathbf{D}^\dagger$ denotes the pseudo-inverse of $\mathbf{D}$ and $\hat{\mathbf{r}}$ is the maximum likelihood estimate of $\mathbf{r}$ with Gaussian distribution. Since the estimate (15) is a linear combination of $\hat{\mathbf{r}}$, $\hat{\mathbf{p}}$ is also Gaussian distribution with

$$\hat{\mathbf{p}} \sim \mathcal{N}_r(\bar{\mathbf{p}}, \mathbf{C}) \tag{16}$$

where $\bar{\mathbf{p}} \equiv \mu^{-1} E\left[\mathbf{D}^\dagger \hat{\mathbf{r}}\right]$ and $\mathbf{C} \equiv \mu^{-2} \mathrm{Cov}\left(\mathbf{D}^\dagger \hat{\mathbf{r}}\right)$ are the mean vector and covariance matrix of $\hat{\mathbf{p}}$, respectively.

The proposed time-domain estimation of channel-tap power equation (15) requires the multiplication with a constant matrix, which can be easily implemented using additions. The estimation can be applied in those systems with repeated signal structures, instead of relying on conventional channel estimations, which are considered to be time consuming and complex. Additionally, UAV detection based on channel-tap power is insensitive to the unknown channel phase.

According to equation (1), the correlation of channel response is critical. The ground control station estimates channel-tap power according to equation (15). The change of channel-tap powers depends on the motion of UAVs and the ground control station; however, the estimated channel-tap power statistics, mean $\bar{\mathbf{p}}$ and covariance $\mathbf{C}$, do not change within the channel coherent time. Hence, these statistics are utilized as the RFFs to detect UAVs. We use a timer in the ground control station, once its timer achieves the maximum lifetime, which should be less than the channel coherence time, the ground control station will estimate a new channel-tap power and then performs channel-based detection to detect the UAV. The maximum lifetime is configured as approximately the inverse of Doppler frequency [3].

IV. Complementary Authenticator Design for Ground Control Station

Section III estimates the channel-tap power over the multipath Rayleigh fading channel, which will be employed for complementary authenticator to detect UAVs using the channel-based detection by PHY layer in this section. In the scheme, the Neyman-Pearson test with a constant probability of false alarm is performed to discriminate between the UAV_I and UAV_A. The ground control station uses a hypothesis test to determine whether the transmission terminal is UAV_I or UAV_A.

$$\begin{cases} \mathcal{H}_0 : \hat{\mathbf{p}} & \text{is} \quad \text{UAV}_\text{I} \\ \mathcal{H}_1 : \hat{\mathbf{p}} & \text{is} \quad \text{UAV}_\text{A} \end{cases} \tag{17}$$

From (16) and (17), the properties of the hypotheses are

$$\begin{cases} \mathcal{H}_0 : \hat{\mathbf{p}} & \sim & \mathcal{N}_r\left(\overline{\mathbf{p}}_I, \mathbf{C}_I\right) \\ \mathcal{H}_1 : \hat{\mathbf{p}} & \sim & \mathcal{N}_r\left(\overline{\mathbf{p}}_A, \mathbf{C}_A\right) \end{cases} \tag{18}$$

where subscripts I and A refer to UAV_I and UAV_A, respectively. $\overline{\mathbf{p}}$ and $\mathbf{C}$ represent the mean vector and covariance matrix of estimated channel-tap powers, respectively. The likelihood ratio test (LRT) can be expressed as

$$\begin{aligned} \Lambda &= \frac{f(\hat{\mathbf{p}}|\mathcal{H}_1)}{f(\hat{\mathbf{p}}|\mathcal{H}_0)} \\ &= \sqrt{\frac{\det(\mathbf{C}_I)}{\det(\mathbf{C}_A)}} \times \exp\{\tfrac{1}{2}\left(\hat{\mathbf{p}} - \overline{\mathbf{p}}_I\right)^T \mathbf{C}_I^{-1}\left(\hat{\mathbf{p}} - \overline{\mathbf{p}}_I\right) \\ &\quad - \left(\hat{\mathbf{p}} - \overline{\mathbf{p}}_A\right)^T \mathbf{C}_A^{-1}\left(\hat{\mathbf{p}} - \overline{\mathbf{p}}_A\right)\} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_1 \end{aligned} \tag{19}$$

where η_1 is the threshold, $f\left(\hat{\mathbf{p}}|\mathcal{H}_0\right)$ and $f\left(\hat{\mathbf{p}}|\mathcal{H}_1\right)$ are conditional pdfs of $\hat{\mathbf{p}}$ under the two hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. The log-likelihood ratio (LLR) test can be expressed as

$$\begin{aligned} \zeta \quad = \quad & \log\left(\sqrt{\frac{\det \mathbf{C}_I}{\det \mathbf{C}_A}}\right) \\ & + \frac{1}{2}\hat{\mathbf{p}}^T\left(\mathbf{C}_I^{-1} - \mathbf{C}_A^{-1}\right) + \hat{\mathbf{p}}^T\left(\mathbf{C}_A^{-1}\overline{\mathbf{p}}_A - \mathbf{C}_I^{-1}\overline{\mathbf{p}}_I\right) \\ & + \frac{1}{2}\left(\overline{\mathbf{p}}_I^T\mathbf{C}_I^{-1}\overline{\mathbf{p}}_I - \overline{\mathbf{p}}_A^T\mathbf{C}_A^{-1}\overline{\mathbf{p}}_A\right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_2 \end{aligned} \tag{20}$$

where η_2 is the logarithm of η_1.

According to (**??**) and (**??**), and for simplicity $\mathbf{C}_I \approx \mathbf{C}_A \equiv \mathbf{C}$ at low SNRs, the equation (20) can be approximated as

$$\begin{aligned} \zeta = \ & \hat{\mathbf{p}}^T\mathbf{C}^{-1}\left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right) \\ & - \frac{1}{2}\left(\overline{\mathbf{p}}_A + \overline{\mathbf{p}}_I\right)^T\mathbf{C}^{-1}\left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right) \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta_2 \end{aligned} \tag{21}$$

According to equations (18) and (21),

$$\begin{cases} \mathcal{H}_0 : \zeta \sim \mathcal{N}_r\left(m_0, \sigma_\zeta^2\right) \\ \mathcal{H}_1 : \zeta \sim \mathcal{N}_r\left(m_1, \sigma_\zeta^2\right) \end{cases} \tag{22}$$

where

$$\begin{aligned} m_0 &= \frac{1}{2}\left(\overline{\mathbf{p}}_I - \overline{\mathbf{p}}_A\right)^T\mathbf{C}^{-1}\left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right) \\ m_1 &= \frac{1}{2}\left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right)^T\mathbf{C}^{-1}\left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right) \\ \sigma_\zeta^2 &= \left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right)^T\mathbf{C}^{-1}\left(\overline{\mathbf{p}}_A - \overline{\mathbf{p}}_I\right) \end{aligned} \tag{23}$$

The Neyman-Pearson detector is adopted to achieve a constant probability of false alarm, P_{fa}, which is given by

$$P_{fa} = P\left(\zeta \geq \eta_2|\mathcal{H}_0\right) = \frac{1}{2}\text{erfc}\left(\frac{\eta_2 - m_0}{\sqrt{2}\sigma_\zeta}\right) \tag{24}$$

where $\text{erfc}(\cdot)$ is the complementary error function. Therefore, the threshold at the detector can be calculated as,

$$\eta_2 = \sqrt{2}\sigma_\zeta\text{erfc}^{-1}\left(2P_{fa}\right) + m_0 \tag{25}$$

Finally, the probability of detection, P_d, is given by

$$\begin{aligned} P_d &= P\left(\zeta \geq \eta_2|\mathcal{H}_1\right) = \frac{1}{2}\text{erfc}\left(\frac{\eta_2 - m_1}{\sqrt{2}\sigma_\zeta}\right) \\ &= \frac{1}{2}\text{erfc}\left(\frac{\sqrt{2}\sigma_\zeta\text{erfc}^{-1}\left(2P_{fa}\right) + m_0 - m_1}{\sqrt{2}\sigma_\zeta}\right) \end{aligned} \tag{26}$$

V. Performance Evaluation

This section verifies the analytical results by simulations and confirms the advantages of the proposed scheme under the Doppler effect. An OFDM system with $N = 64$ and $N_{CP} = 16$ is considered. The simulated modulation scheme is quadrature phase shift keying (QPSK). The signal bandwidth is 0.8 MHz, and the radio frequency is 2.4 GHz. The subcarrier spacing is 12.5 kHz. The OFDM symbol duration is 80 μs. The channel taps are randomly generated using independent complex Gaussian variables with zero-mean and unity-variance. The Doppler effect is verified using vehicular test environment of International Mobile Telecommunications-2000 (IMT-2000) standard with recommendation ITU-R M.1225 [4]. The parameters of channel B from Table 5 in [4] with the number of taps L = 4 and velocity of the UAV equal to 70 km/h are utilized in the following simulations. All the results are obtained by averaging over 5000 simulation runs.

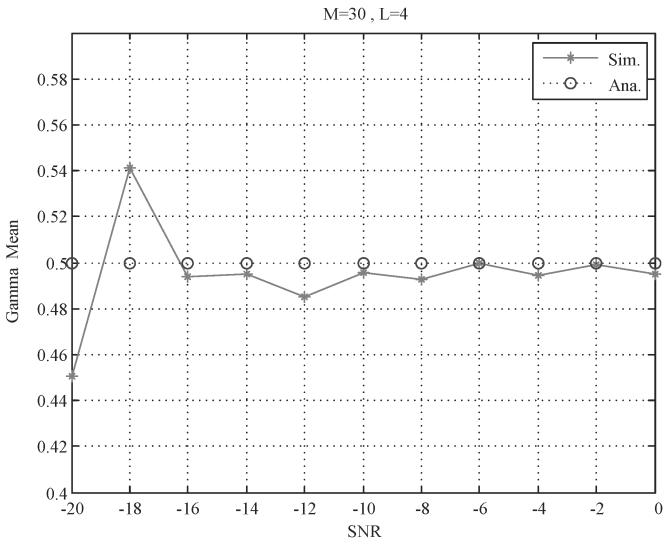

Fig. 1. Mean of estimates of $r(n)$.

First, the performance of the proposed channel-tap power estimation using (16) is verified. Channels between UAV and

the ground control station are randomly generated, so the SNR can be expressed as

$$\text{SNR} \equiv \frac{\sigma_x^2 \sum_l |h_m(l)|^2}{\sigma_\omega^2} = \frac{\sigma_x^2 \sum_l \sigma_{h_m(l)}^2}{\sigma_\omega^2} \tag{27}$$

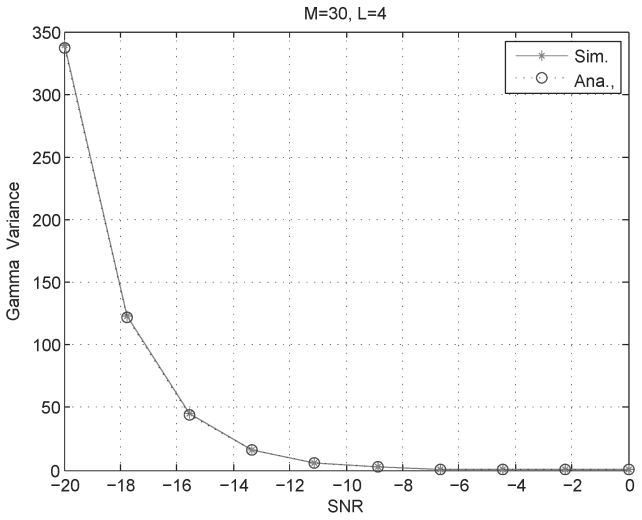

Fig. 2. Variance of estimates of $r(n)$.

The theoretical mean and variance of $\hat{r}(n)$ are evaluated. Figures 1 and 2 plot the actual mean and variance of $\hat{r}(n)$, respectively, under various SNRs with $M = 30$ and $L = 4$. As shown, the mean and variance of $\hat{r}(n)$ are close to their respective theoretical values especially at high SNR. The theoretical $r(n)$, $E[r(n)]$, is 0.5 for all SNRs, because it depends only on channel conditions. However, the variance quadratically decreases with increasing SNR.

Figures 3(a) and 3(b) plot the mean of channel-tap power estimate $\hat{\mathbf{p}}$ in equation (15) with SNR=-10 dB for different numbers of symbols $M = 10$ and $M = 30$, respectively. The simulation results indicate that as M increases, the mean of $\hat{\mathbf{p}}$ approaches the theoretical value, because more samples are being used for estimation; however, the detection time also increases. This indicates that the proposed authenticator works is very well.

Figure 4 plots the probability of detection against false-alarm probability under various SNRs, with $M = 30$ and $L = 4$. The result demonstrates that the proposed method works very well at low SNRs. Increasing the SNR considerably improves the detection probability.

Figure 5 plots the probability of detection versus false-alarm probability for various M at SNR= -5 dB. At $P_{fa} = 0.2$, a detection probability of $P_d = 0.90$ can be achieved with $M = 30$, while only $P_d = 0.60$ can be achieved with $M = 8$. Notably, the performance can be improved by increasing M but the detection time also increases. Figures 5 and 6 suggest that doubling M improves the probability of detection more than does doubling SNR.

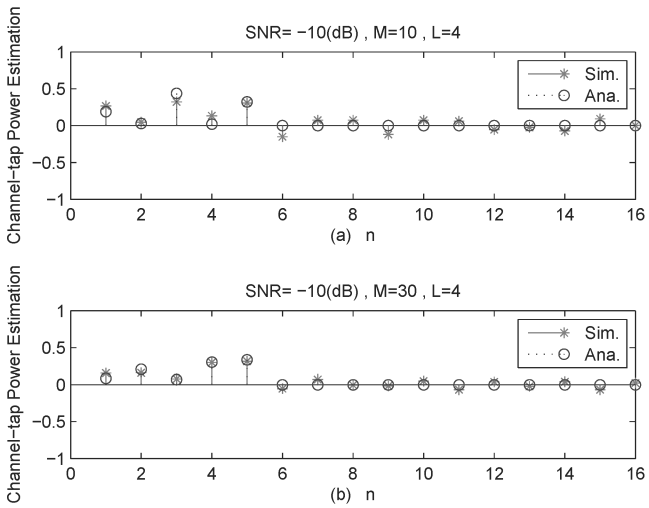

Fig. 3. Estimation of channel-tap power for different numbers of symbols; (a) $M = 10$, (b) $M = 30$.

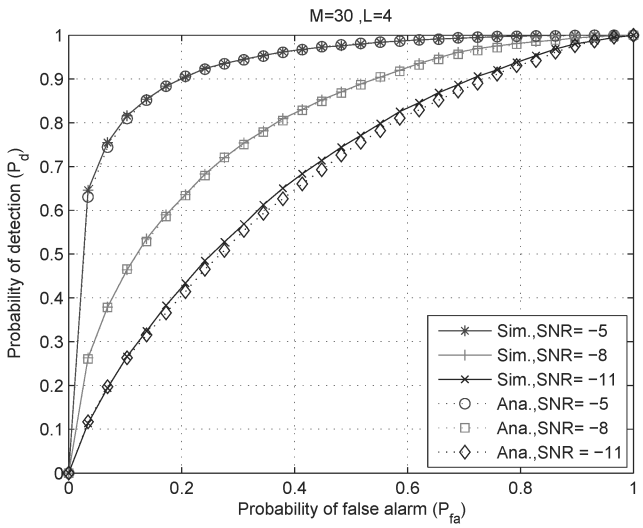

Fig. 4. Probability of detection as a function of P_{fa} for various SNRs.

VI. CONCLUSIONS

This study proposes a complementary authenticator for detecting UAVs in the fading and shadowing environments when the GPS is not available temporarily or permanently. The uniqueness and diversity of channel-tap powers between the UAV and the ground control station is utilized as a RFF to detect UAVs. Simulations demonstrate that the proposed authenticator perform well and can reliably differentiate UAV_I and UAV_A at low SNRs.

REFERENCES

[1] J. Tugnait, H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proceedings of Second International Conference on Communication Systems and Networks-COMSNETS'10*, pp. 1-9, 2010.

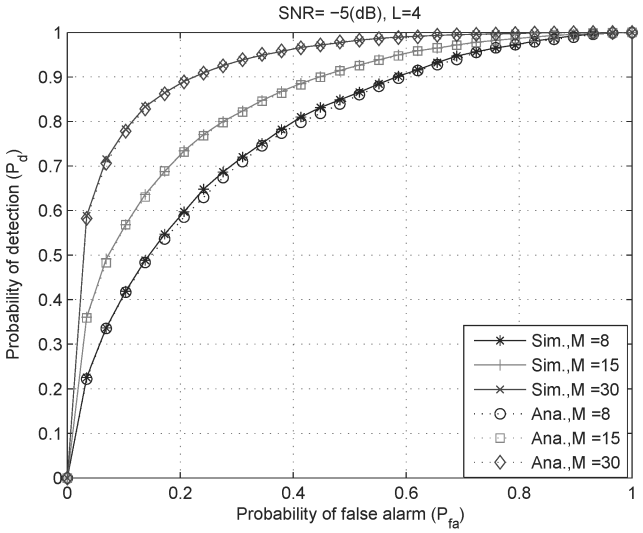

Fig. 5. Probability of detection versus P_{fa} for various M.

[2] T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice-Hall, 1996.
[3] A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, 2005.
[4] International Telecommunication Union, "Guidelines for evaluation of radio transmission technologies for IMT-2000," *Recommendation ITU-R M.1225*, 1997.