Active Spoofing Attack Detection: An Eigenvalue Distribution and Forecasting Approach

Ning Gao*† Xiaojun Jing* Qiang Ni† Binbin Su†
*School of Information and Communication Engineering,
Beijing University of Posts and Telecommunications, Beijing, China.
†School of Computing and Communications, InfoLab21, Lancaster University, Lancaster, UK.
Emails: {ngao, jxiaojun}@bupt.edu.cn, {q.ni, b.su}@lancaster.ac.uk

***Abstract*—Physical-layer security has drawn ever-increasing attention in the next generation wireless communications. In this paper, we focus on studying the secure communication in an HPN-to-devices (HTD) network, in which a new type of MAC spoofing attack is considered. To detect the malicious attack, we propose a novel algorithm, namely, eigenvalue test using random matrix theory (ETRMT) algorithm, which needs no prior information about the channel. In particular, when the number of samples is finite at the receiver or the number of devices is large, the sampled signal is the biased estimation of the actual signal, which inspires us to use the random matrix theory to analyze the spoofing attack detection. The closed-form expressions of the detection probability, the false alarm probability, and the Neyman-Pearson threshold are derived based on eigenvalue distribution of the spiked population model. In addition, taking the channel time-varying into consideration, we provide an adaptive threshold tracking method by using Bayesian forecasting. Finally, the simulations are conducted to validate our proposed method and some insightful conclusions are obtained.**

***Index Terms*—Active MAC spoofing attack detection, random matrix theory, Bayesian forecasting.**

I. Introduction

Thanks to the next generation wireless communications, the high-speed data communication is gradually becoming reality. However, owing to the broadcast nature of wireless communications, they are vulnerable to MAC spoofing attack, in which the spoofer claims himself as a legitimate user by eavesdropping and then modify its MAC address to legitimate user's. Because of the management and control frame are usually *not protected* in existing security techniques [1], such attack can further launch significant denial of service (DoS) or man-in-the-middle (MITM) attack.

Many previous work exploited the physical layer characteristics derived from intrinsic channel randomness to verify the identities of terminals. received signal strength indicator (RSSI) [2], [3], channel state information (CSI) [4], [5], channel impulse response (CIR) [6]–[8] have been widely used. However, reference [9] shown that the intrinsic channel randomness is time-varying, i.e., doppler frequency shift, location, scattered multi-path environment etc, thus, limits the design of physical-layer (PHY-layer) security. With the consideration of channel time-varying, many related work has been explored. In [10], the authors modeled the variable part of the channel response as a wide sense stationary uncorrelated scattering process and utilized an autoregressive model of order 1 to characterize the temporal process. Game theory and Q-learning based authentication was proposed in [8] to determine the optimal threshold for spoofer detection in a dynamic unknown channel model. In addition, the authors proposed a logistic regression based authentication to remove the assumption on the known channel model and used a distributed Frank-Wolfe based authentication method to reduce the communication overhead in [3]. In light of the aforementioned work, some intense interests mainly focused on time-varying channel spoofing attack detection. However, there are still some urgent problems need to be solved. The main motivations of this paper are based on the following considerations:

1) Most of existence work only consider the *passive MAC spoofing attack* which launches when transmitter is in idle state, and they have to store the genuine user's PHY-layer fingerprint in the off-line phase, i.e., [3]–[5], [8], [10].
2) The prior channel information is needed, which introduces a high overhead and estimation error. If the attacker mimics the legitimate channel information (no spatial diversity), many landmark methods may not work well, i.e., [4]–[8].

In this paper, we study the multi-user cooperative detection for *active MAC spoofing attack* in an HPN-to-devices (HTD) network, and the channel time-varying is considered. In this attack, the attacker eavesdrops the legitimate channels information and MAC address in HTD uplink transmission, and then fabricating both of them in HTD downlink transmission. In this case, if the forged management or control frame signal (aliased as control signal) and legitimate control signal are trans-

mitted synchronously and the transmission power of the forged one is higher than the legitimate one, then the receivers would accept the spoofing codewords and reject the HPN's codewords [11]. Hence, such attacker is more of threat to the network services than passive spoofer, i.e., availability refers to communication continuity and timeliness, besides launching DoS or MITM attack. It becomes even more worse, specifically in multiple access systems, i.e., non-orthogonal multiple access (NOMA) system. Due to all the serious damages this attack could cause, first of all, it is important for the user to be able to detect it. In general, the design for the above stated active spoofing attack and its detection approach are non-trivial, the main contributions of this work are summarized as follows

- Unlike the passive MAC spoofing attack detection, we propose an eigenvalue test using random matrix theory (ETRMT) algorithm to cooperative detect active MAC spoofing attack. Our proposed ETRMT algorithm is a "location freely" and "online" method, which needs no prior information about the channel and do not have to store any PHY-layer fingerprint in the off-line phase.
- Different from existing energy detection based methods [2], [3], we consider the impact of estimation error caused by finite number of samples and use the RMT to compensate this error. The closed-form expressions of detection probability and false alarm probability are derived. We prove the minimum eigenvalue distribution with the presence of signals. The adaptive threshold tracking method is proposed using Bayesian forecasting.
- The proposed cooperative detection algorithm can detect the attacker in a pure PHY-layer approach (relative to cross-layer security design means), which makes the mobile device save a large amount of time and overhead. In addition, this method requires no modification to the current transmit-receive structure and can be integrated with traditional authentication mechanisms to enhance wireless communication security.

Notation: Boldface uppercase and lowercase letters denote matrix and vector, such as $\mathbf{A}$ and $\mathbf{a}$, respectively. $\mathbf{A}^\top$ and $\mathbf{A}^\dagger$ represent transpose and conjugate transpose, respectively. $\mathbf{I}_M$ is the identity matrix of order $M \times M$ and $\mathbf{R}_\mathbf{A}$ is the covariance matrix of matrix $\mathbf{A}$. $\mathbb{E}[\cdot]$ is the expectation operator. $\mathbb{C}^{m\times n}$ denotes the complex space of order $m \times n$.

II. SYSTEM MODEL

A. Attack Model

We consider a PHY-layer active MAC spoofing attack that the malicious spoofer can eavesdrop the legitimate channels information and HPN's MAC address in uplink orthogonal channels, i.e., the attacker deploys a "helper node" who stays close to the receiver to passive eavesdropping the reverse training phase [12], then attacker emulates the legitimate channels information and transmits the deceiving signal, i.e., the illegitimate control signal, using HPN's MAC address in downlink transmission[1]. We assume that the spoofer and HPN are separated by a reasonable security distance and can emulate the legitimate channels (compensate channel differences) by equipping a circular smart antennas array to design signal precode [13].

B. Network Model

We assume that the network consists of one location fixed HPN, M free moving devices, one fusion center (FC), all of them are equipped with single antenna. In addition, one location free spoofer are equipped with a smart antenna array and uses a low power single antenna helper node to eavesdropping and transmission. Let b denote the HPN, $m \in \{1, \cdots, M\}$ denote the m-th device, and s denote the spoofer. Let $x(t)$ be the time continuous downlink frame signal with bandwidth W, the sampling rate is $f_s \geq W$, and the sampling period is $T_s = 1/f_s$. For the N_s samples of signal $x(t)$, we write it as $\mathbf{x} = \{x_{n_s T_s} | n_s = 1, \cdots, N_s\}$. The channel between transmitter and the m-th receiver is reciprocal and orthogonal, which is defined as $h_{tm} = \sqrt{d_{tm}^{-\eta}}\widetilde{h}_{tm}$, where d_{tm} represents the distance between transmitter and the m-th receiver, η is the path loss exponent and $\widetilde{h}_{tm}$ represents small-scale fading follows zero-mean complex Gaussian processes of unit-variance. Specifically, we treat h_{tm} as a wide sense stationary uncorrelated scattering process with the classical Jakes' power spectrum of maximum Doppler frequency f_d and the channel is time-varying but correlated between the time t and the next time $t+T$. In addition, during time slot T, we assume the channel is quasi-static. To this end, we model the channel as an autoregressive of order 1 random process follows

$$h_{tm}(t+T) = \rho h_{tm}(t) + u(t), \tag{1}$$

where ρ is the correlation coefficient of the time-varying channel with respect to the zero-th order Bessel function of the first kind and $u(t)$ is independent of the channel $h_{tm}(t)$, following zero-mean complex Gaussian distribution with variance $1-\rho^2$. For all devices M, the N samples of the received signal in downlink can be denoted as a matrix form[2]

$$\mathbf{Y} = \sqrt{\mathcal{P}_b}\mathbf{h}_{bd}\mathbf{x}_b + \Phi\sqrt{\mathcal{P}_s}\mathbf{h}_{sd}\mathbf{x}_s^p + \mathbf{N}, \tag{2}$$

where $\mathbf{Y} \in \mathbb{C}^{M\times N_s}$ ($N_s \gg M$), $\mathcal{P}_b, \mathcal{P}_s$ ($\mathcal{P}_b < \mathcal{P}_s$) are the power budget of HPN and spoofer, $\mathbf{h}_{bd}, \mathbf{h}_{sd} \in$

[1]Each receiver knows the normal signal power by estimating using HTD uplink, i.e., reverse training, and the attacker knows the legitimate channels information by eavesdropping HTD uplink.

[2]Note that this argument assumes perfect synchronization of HPN and spoofer's transmissions when $\Phi = 1$.

$\mathbb{C}^{M\times 1}$, $\mathbf{x}_b^\top \in \mathbb{C}^{N_s\times 1}$ is the sampled unit-energy genuine control signal, $\mathbf{x}_s^{p\top} \in \mathbb{C}^{N_s\times 1}$ is the sampled illegitimate control signal with precode, i.e., the spoofer sends $x_s^p(t) = \mathbf{w}_m x_s(t)$ to the m-th device via precode $\mathbf{h}_{sd}^\top \mathbf{w}_m = h_{mb}$, $\mathbf{N} \in \mathbb{C}^{M\times N_s}$ is independent of signal, each term is i.i.d. complex Gaussian random variable with zero-mean and variance σ^2, and $\Phi = 1$ or $\Phi = 0$ represents the active spoofer is present or absent.

III. Cooperative PHY-Layer Spoofing Detection

According to (2), when the spoofer is present ($\Phi = 1$), the spoofer and the HPN are co-existence. Hence, the control signals are underlay and the power is obviously larger than normal (no attack). The larger the signal power is, the higher risk the attacker will be detected. Hence, we use this interesting phenomenon to detect the active attacker. Since the channel and the noise variance are time-varying, the samples are finite, which make channel information difficult to estimate accurately, thus, we propose the ETRMT algorithm.

A. Eigenvalue Test Using Random Matrix Theory

After broadcasting the control signal, each device transmits N_s samples of the received control signal to a fusion center (FC), then FC calculates the sample covariance matrix

$$\mathbf{R}_{\mathbf{Y}(N_s)} = \mathbb{E}[\mathbf{Y}\mathbf{Y}^\dagger]. \tag{3}$$

Since signal covariance matrix is full-rank, the sample covariance matrix $\mathbf{R}_{\mathbf{Y}(N_s)}$ can be denoted as a diagonal form

$$\mathbf{E}^\dagger \mathbf{R}_{\mathbf{Y}(N_s)} \mathbf{E} = \sigma^2 \mathbf{I}_M + diag(\lambda_0, \cdots, \lambda_m, 0 \cdots, 0),$$

where $\mathbf{E}$ is the eigenvector matrix corresponding to the eigenvalue matrix. Let $\lambda_0 \geq \cdots \geq \lambda_m$ denote the eigenvalues in the descending order, we find that the signal power is almost concentrated on $\lambda_{max}(\mathbf{R}_{\mathbf{Y}(N_s)}) = \lambda_0$ and the noise power can be estimated by the minimum eigenvalue $\lambda_{min}(\mathbf{R}_{\mathbf{Y}(N_s)}) = \sigma^2$. We use the maximum eigenvalue ratio the minimum eigenvalue to detect the spoofer's state. The cooperative spoofing attack detection can be transformed into the hypothesis test

$$\frac{\lambda_{max}(\mathbf{R}_{\mathbf{Y}(N_s)})}{\lambda_{min}(\mathbf{R}_{\mathbf{Y}(N_s)})} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} \gamma. \tag{4}$$

Where $\mathcal{H}_0$ indicates the attacker is absent and $\mathcal{H}_1$ indicates the attacker is present. If the test statistic is less than a threshold γ, which is derived from the statistic of the initial normal signal, the device accepts $\mathcal{H}_0$. Otherwise, the device accepts $\mathcal{H}_1$.

However, the number of samples is finite in practice, the sample covariance matrix $\mathbf{R}_{\mathbf{Y}(N_s)}$ is the biased estimate of the statistical covariance matrix $\mathbf{R}_{\mathbf{Y}}$. Let us rewrite (2) with $\Phi = 0$ as

$$\mathbf{Y} = \underbrace{\begin{bmatrix} h_{b,1} & \sigma & & 0 \\ \vdots & & \ddots & \\ h_{b,M} & 0 & & \sigma \end{bmatrix}}_{\mathbf{T}_b} \begin{bmatrix} x_{b,1} & \cdots & x_{b,N_s} \\ n_1 & \cdots & n_{N_s} \\ \vdots & & \vdots \\ n_1 & \cdots & n_{N_s} \end{bmatrix}$$

where $h_{b,m} \triangleq \sqrt{\mathcal{P}_b} h_{bm}$ represents the channel of the m-th device, and n_k is the noise with unit variance at sample k. Note that $\mathbf{T}_b \mathbf{T}_b^\dagger$ has clearly one eigenvalue $\rho_{b,0} = \sum_{m=1}^{M} |h_{b,m}|^2 + \sigma^2$ and the rest eigenvalues are σ^2. It inspires us to analyze the behavior of the eigenvalue of $\mathbf{R}_{\mathbf{Y}(N_s)}$ using random matrix theory. This behavior is related to the eigenvalue of large sample covariance matrix of spiked population model $\mathbf{T}_b$ [14]. In the following, the symbol $\sum_{m=1}^{M}$ is omitted to $\sum$ and $\lambda_{max}(\mathbf{R}_{\mathbf{Y}(N_s)})$ to λ_{max}, if no confusion occurs.

Theorem 1: Let $\mathbf{R}_{\mathbf{Y}(N_s)}$ denote the sample covariance matrix of N_s samples with a single signal of strength $\sum |h_{b,m}|^2$ from (2) ($\Phi = 0$). Then, if $N_s, M \to \infty$, with $\frac{M}{N_s}$ fixed, the largest eigenvalue of $\mathbf{R}_{\mathbf{Y}(N_s)}$ converges w.p.1 to [15]

$$\lambda_{b,max} = (\sum |h_{b,m}|^2 + \sigma^2)\big(1 + \frac{M\sigma^2}{N_s \sum |h_{b,m}|^2}\big) \tag{5}$$

Similarly, we rewrite (2) with $\Phi = 1$ as

$$\mathbf{Y} = \underbrace{\begin{bmatrix} h_{b,1} & h_{s,1} & \sigma & & 0 \\ \vdots & \vdots & & \ddots & \\ h_{b,M} & h_{s,M} & 0 & & \sigma \end{bmatrix}}_{\mathbf{T}_s} \begin{bmatrix} x_{b,1} & \cdots & x_{b,N_s} \\ x_{s,1} & \cdots & x_{s,N_s} \\ n_1 & \cdots & n_{N_s} \\ \vdots & & \vdots \\ n_1 & \cdots & n_{N_s} \end{bmatrix}$$

where $h_{s,m} \triangleq \sqrt{\mathcal{P}_s} h_{sm}$ represents the m-th forged channel. If the eigenvalues are arranged in the descending order, we find $\mathbf{T}_s \mathbf{T}_s^\dagger$ has two eigenvalues $\rho_{s,0} \geq \rho_{s,1}$, and the rest eigenvalues are σ^2. The following theorem describes the behavior of the largest eigenvalue $\lambda_{s,max}$ of $\mathbf{R}_{\mathbf{Y}(N_s)}$, i.e., (2) with $\Phi = 1$, with K sufficiently strong signals, i.e., $\rho_{s,0} - \sigma^2 > \sigma^2 (\frac{M}{N_s})^{1/2}$ [16].

Theorem 2: Let $\mathbf{R}_{\mathbf{Y}(N_s)}$ denote the sample covariance matrix of N_s samples from (2) ($\Phi = 1$) with K signals. Then, if $N_s, M \to \infty$, with $\frac{M}{N_s}$ fixed, the eigenvalue $\lambda_{s,m}$ of $\mathbf{R}_{\mathbf{Y}(N_s)}$ can converge w.p.1 to

$$\lambda_{s,k} = \begin{cases} \rho_{s,k}\left(1 + \frac{M\sigma^2}{N_s(\rho_{s,k} - \sigma^2)}\right), & k = 0, \cdots, K-1; \\ \sigma^2[1 + (\frac{M}{N_s})^{1/2}]^2, & \text{otherwise.} \end{cases}$$

and the largest eigenvalue is

$$\lambda_{s,max} = \rho_{s,0}\left(1 + \frac{M\sigma^2}{N_s(\rho_{s,0} - \sigma^2)}\right). \tag{6}$$

Corollary 1: Assuming each term $h_{b,m}$ with respect to channel vector $\mathbf{h}_{bd}$ is an i.i.d complex random process with zero-mean and variance σ_b^2. Then, when N_s, M

is large, i.e., $N_s = 1000$, $M = 50$, the single signal of strength $\frac{\sum |h_{b,m}|^2}{M}$ can converge w.p.1 to a Gaussian distribution with mean $\mu_\infty = \sigma_b^2$ and variance $\sigma_\infty^2 = \frac{\sigma_b^4}{M}$ for complex random variable.

Proof: Using central limit theorem, the variance can be denoted as

$$\begin{aligned}\sigma_\infty^2 &= \mathbb{E}\left[\left(\frac{\sum |h_{b,m}|^2}{M}\right)^2\right] - \mathbb{E}\left[\frac{\sum |h_{b,m}|^2}{M}\right]^2 \\ &= \frac{1}{M}\mathbb{E}\left[|h_{b,m}|^4 - \sigma_b^4\right]. \end{aligned} \quad (7)$$

For complex random variable $h_{b,m} = h_r + jh_j$ with variance σ_b^2, we obtain

$$\begin{aligned}\mathbb{E}[|h_{b,m}|^4] &= \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \frac{|h_{b,m}|^4}{\pi\sigma_b^2} \\ &\times \exp\left[-\frac{h_r^2 + h_j^2}{\sigma_b^2}\right] dh_r dh_j \\ &= 2\sigma_b^4. \end{aligned} \quad (8)$$

Substituting (8) into (7), the proof is completed. ■

When the terms of $\mathbf{Y}$ are zero-mean i.i.d. Gaussian noise, $\mathbf{R_Y}$ is commonly referred to as a Wishart random matrix [14]. However, the matrix form of (2) is no longer a Wishart random matrix, which is difficult to obtain the eigenvalue distribution of λ_{min}. To solve it, we prove the theorem 3.

Theorem 3: Let $\lambda'_{min} = \frac{N_s}{\sigma^2}\lambda_{min}$ denote the minimum eigenvalue of the normalized statistical covariance matrix. For a setting with K signals (sufficiently strong), if $N_s, M \to \infty$, $\frac{\lambda'_{min} - \mu_K}{\phi_K}$ converges w.p.1 to the Tracy-Widom distribution of order 2 [17], with $\mu_K = (N_s^{1/2} - (M-K)^{1/2})^2$, $\phi_K = ((M-K)^{1/2} - N_s^{1/2})((M-K)^{-1/2} - N_s^{-1/2})^{1/3}$.

Proof: See Appendix A for details. ■

B. Detection Probability and False Alarm Probability

Since the finite number of samples and time-vary noise, observation will exist estimation error, which lead to imperfect detection. We estimate the performance of our proposed ETRMT method by detection probability and false alarm probability. That is, if a spoofer is observed, while the actual state is null (spoofer is absent), we say a false alarm occurs and denote this probability as P_f, otherwise we have a correct detection probability P_d. Using theorem 3, the actually detection probability can be calculated by

$$\begin{aligned}P_d &= Pr\left(\frac{\lambda_{s,max}}{\lambda_{s,min}} > \gamma | \mathcal{H}_1\right) \\ &= Pr\left(\frac{\lambda'_{s,min} - \mu_1}{\phi_1} < \frac{N_s\lambda_{s,max}}{\sigma^2\gamma\phi_1} - \frac{\mu_1}{\phi_1}\right) \\ &= F_{TW2}\left(\frac{N_s\rho_{s,0}^2 - N_s\rho_{s,0}\sigma^2 + M\sigma^2}{\sigma^2\gamma\phi_1\rho_{s,0} - \sigma^4\gamma\phi_1} - \frac{\mu_1}{\phi_1}\right). \end{aligned}$$

Correspondingly, false alarm probability is calculated by

$$\begin{aligned}P_f &= Pr\left(\frac{\lambda_{b,max}}{\lambda_{b,min}} > \gamma | \mathcal{H}_0\right) \\ &= Pr\left(\frac{\lambda_{b,min} - \mu_2}{\phi_2} < \frac{N_s\lambda_{b,max}}{\sigma^2\gamma\phi_2} - \frac{\mu_2}{\phi_2}\right) \\ &= F_{TW2}\left(\frac{N_s\rho_{b,0}^2 - N_s\rho_{b,0}\sigma^2 + M\sigma^2}{\sigma^2\gamma\phi_2\rho_{b,0} - \sigma^4\gamma\phi_2} - \frac{\mu_2}{\phi_2}\right), \end{aligned}$$

where $\rho_{b,0} = \sum |h_{b,m}|^2 + \sigma^2$, $F_{TW2}(\cdot)$ is the cumulative distribution function (CDF) of the Tracy-Widom distribution of order 2 ($n = 1, 2$), and $\mu_n = (N_s^{1/2} - (M-n)^{1/2})^2$, $\phi_n = ((M-n)^{1/2} - N_s^{1/2})((M-n)^{-1/2} - N_s^{-1/2})^{1/3}$. For a specified P_f, i.e., $P_f = 0.1$ with respect to $F_{TW2}^{-1}(0.1) = -2.78$, the Neyman-Pearson threshold can be determined by

$$\gamma = \frac{N_s\lambda_{b,max}}{\sigma^2\phi_2 F_{TW2}^{-1}(P_f) + \mu_2\sigma^2}, \quad (9)$$

where $F_{TW2}^{-1}(\cdot)$ is the inverse function of Tracy-Widom distribution $F_{TW2}(\cdot)$.

C. Adaptive Tracking Using Bayesian Forecasting

Because of the channel is time-varying, which makes the threshold extremely difficult to choice for FC with time. Fortunately, according to (1) and corollary 1, we can regard the channel gain $\sum |h_{b,m}|^2$ at time $T-1$ and T approximately as correlated Gaussian variables. In this case, we adaptively predict the current threshold recursively based on the past channel gain using Kalman filter [18], a special case of Bayesian forecasting[3]. The channel gain $\mathcal{G} = \sum |h_{b,m}|^2$ can be well approached by an autoregressive of order 1 random process

$$\mathcal{G}(T) = f(T)\mathcal{G}(T-1) + w(T), \quad (10)$$

which represents the state transition equation for the system, describing the variation of $\mathcal{G}$ at time $T-1$ and T. Where $\mathcal{G}(T)$ is the state of gain power at time T, $w(T)$ is the process noise following zero-mean Gaussian distribution with variance $r_{w(T)}$, $f(T)$ is the state transition probability. Both $f(T)$ and $w(T)$ can be computed by the set of the Yule-Walker equations defined as

$$f(T) = r^{(1)}\left(r^{(0)}\right)^{-1}, \quad (11)$$

$$w(T) = r^{(0)} - f(T)r^{(-1)}, \quad (12)$$

where the variance is given by $r^{(g)} = \mathbb{E}[\mathcal{G}(T)\mathcal{G}(T-g)]$ for lag $g \in \{-1, 0, 1\}$. The channel gain observed by the receiver at time T is related to the state by the measurement equation

$$\mathbf{z}(T) = \mathbf{H}\mathcal{G}(T) + \mathbf{v}(T). \quad (13)$$

[3]The initialization channel gain is available by means of reverse training.

Where vector $\mathbf{z}(T)$ represents the observed gain of time T, $\mathbf{v}(T)$ is the measurement noise following zero-mean Gaussian distribution with covariance matrix $\mathbf{R}_{v(T)}$ and $\mathbf{H} = [0, f(T)]^\top$ is the measurement that maps the state transition probability into the measurement domain. The Kalman equation that allow us to recursively calculate $\hat{\mathcal{G}}(T)$ by combining past knowledge, prediction from system model and noisy measurement. At time T, the receiver predicts power before receiving the measurement with the equations

$$\begin{aligned} \hat{\mathcal{G}}(T-) &= f(T)\hat{\mathcal{G}}(T-1), \\ \mathbf{M}(T-) &= \mathbf{H}\mathbf{M}(T-1)\mathbf{H}^\top + \mathbf{R}_{w(T)}. \end{aligned} \quad (14)$$

Where $\mathbf{M}(\cdot)$ is the state estimation mean square error matrix of $T-1$-th term, and $\mathbf{R}_{w(T)}$ is the covariance matrix with respect to $r_{w(T)}$. After observing the measurement from $\mathbf{z}(T)$, receiver updates the Kalman gain $\mathbf{K}(T)$ and corrects the state estimate and correlation coefficient according to the equations

$$\begin{aligned} \hat{\mathcal{G}}(T) &= \hat{\mathcal{G}}(T-) + \mathbf{K}(T)(\mathbf{z}(T) - \mathbf{H}\hat{\mathcal{G}}(T-)), \\ \mathbf{M}(T) &= [\mathbf{I}_2 - \mathbf{K}(T)\mathbf{H}]\mathbf{M}(T-), \end{aligned} \quad (15)$$

where $\mathbf{K}(T) = \mathbf{M}(T-)\mathbf{H}^\top[(\mathbf{H}\mathbf{M}(T-)\mathbf{H}^\top\mathbf{R}_{w(T)}]^{-1}$. Then, FC updates the power gain $\hat{\mathcal{G}}(T)$ with respect to the threshold via (14) and (15), recursively.

IV. Simulation and Performance Analysis

In this section, we verify the theory and analyze the performance of the proposed algorithm by simulation. In the simulation, we set the number of devices be $M = 20$, maximum Doppler frequency $f_d = 20$Hz. Without loss of generality, we set the large-scale fading coefficients to be one and the normal transmission power $\mathcal{P}_b = 1W$. Hence, the signal is transmitted through a multi-path Rayleigh fading channel. At the receivers, the users send the signal samples to FC to cooperative detect whether the active spoofing attack is present or not. Fig. 1 shows three instances of our proposed time-varying channel gain tracking algorithm with time in different SNRs. As shown in the figure, the tracked channel gain is fluctuate around actual channel gain in each time slot. Moreover, when the measurement noise increases, the algorithm can still effectively track the power gain across time through the recursive update.

Fig. 2 illustrates how the Neyman-Pearson threshold γ change with the number of samples N_s increasing. It shows that the threshold γ decreases as the number of samples increases, and this threshold will converge w.p.1 to an approximate fixed point no matter what the noise power is. This is an meaningful insight, which guides us to stably track the threshold via choosing a proper sample number. For example, we do not need to set the sample number N_s to be extremely large, actually, we can get a good detection performance by setting it to $N_s = 200$ or less. Furthermore, the higher the noise power is, the lower the threshold will be. Next, we conduct 10000 times of Monte-Carlo simulations and plot the receiver operating characteristic (ROC) curves, in which detection probability are plotted with respect to the false alarm probability. In Fig. 3, we compare our method with power spectral density (PSD) method [5] in an OR role with different parameters, i.e., the number of devices and spoofer's power. We find that the performance of the proposed ETRMT method is better than PSD method in the same parameters. Both PSD and ETRMT method's detection performances are improved with the increasing of device number and spoofer power. In particular, we observe that our proposed method has an apparent performance boost with $\mathcal{P}_s = 2W$ for $M = 8$ than PSD method, which thanks to the compensation for finite sample number via RMT. Moreover, when the device number is fixed, we see that a larger transmit power is, the higher risk the attacker will be detected, which shows a tradeoff between the transmit power and the detection probability.

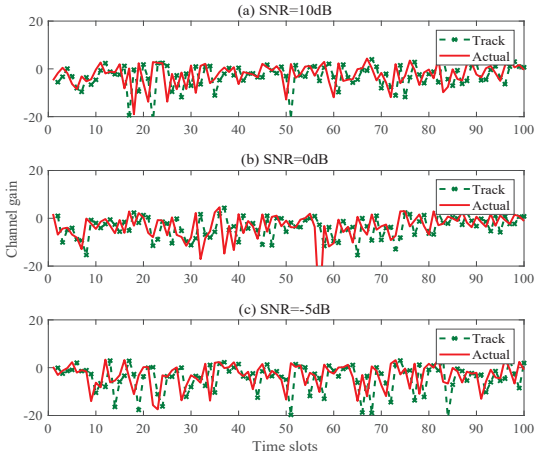

Fig. 1. The time-varying channel gain tracking using Kalman filter.

V. Conclusion

In this paper, we introduced a new type of MAC spoofing attack and proposed the ETRMT algorithm to cooperative detect this attack. This approach needs no prior information about the channel and do not have to store the genuine user's PHY-layer fingerprint in the off-line phase. We used the random matrix theory to analyze the detection performance of the proposed algorithm and provided an depth analysis on the behavior of the maximum and minimum eigenvalue distribution of the sample covariance matrix. The closed-form expression of the detection probability, false alarm probability and the Neyman-Pearson threshold were derived. According to the channel time-varying, we proposed an adaptive threshold tracking method. Finally, the simulation results

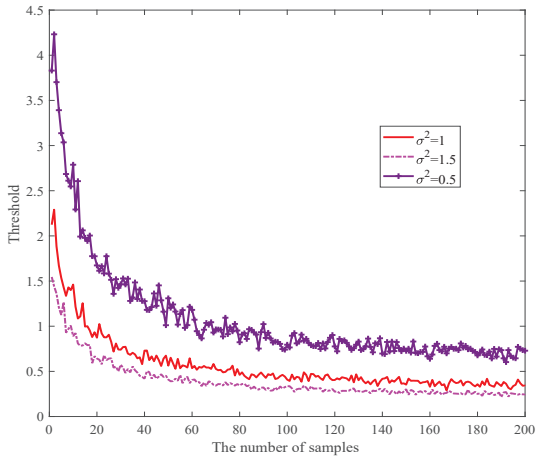

Fig. 2. The number of samples vs. threshold with different noise power.

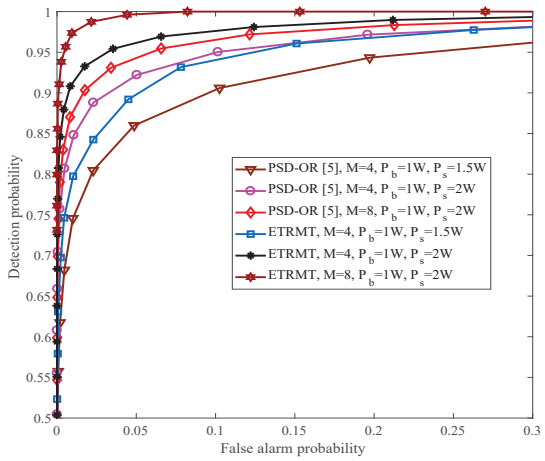

Fig. 3. The ROC of PSD-OR [5] vs. the proposed ETRMT.

showed that our proposed algorithm can effectively detect the attacker with a good performance.

APPENDIX A
PROOF OF THEOREM 3

Lemma 1: For a N_s sample Wishart random matrix of the Gaussian noise, if $N_s, M \to \infty$, the normalized minimum eigenvalue $\frac{\lambda'_{min}-\mu_K}{\phi_K}$ converges to the Tracy-Widom distribution of order 2. Where $\mu_K = (N_s^{1/2} - M^{1/2})^2$, and $\phi_K = (M^{1/2}-N_s^{1/2})(M^{-1/2}-N_s^{-1/2})^{1/3}$ [17].

Lemma 2: Consider a setting with K signals, if $N_s, M \to \infty$, with $\frac{M}{N_s}$ fixed, the rest of the eigenvalue with respect to noise and $(K+1)$-th eigenvalue as the maximum eigenvalue of this noise Wishart random matrix [15].

Recall that the minimum eigenvalue of the sample covariance matrix is denoted as λ_{min}. According to lemma 2, we get λ_{min} is the minimum eigenvalue of the Wishart random matrix. Let $\lambda'_{min} = \frac{N_s}{\sigma^2}\lambda_{min}$ denote the minimum eigenvalue of the normalized statistical covariance matrix. Combining lemma 1, we obtain the theorem 3, and the proof is completed.

REFERENCES

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

[2] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Optimal information-theoretic wireless location verification," *IEEE Trans. Vehic. Tech.*, vol. 63, no. 7, pp. 3410–3422, Jul. 2014.

[3] L. Xiao, X. Wan, and Z. Han, "Phy-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676–1687, Mar. 2018.

[4] N. Gao, X. Jing, H. Huang, and J. Mu, "Robust collaborative spectrum sensing using phy-layer fingerprints in mobile cognitive radio networks," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1063–1066, May 2017.

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

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

[7] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171–4182, Jun. 2016.

[8] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Trans. Vehic. Tech.*, vol. 65, no. 12, pp. 10 037–10 047, Dec. 2016.

[9] P. L. Yu, G. Verma, and B. M. Sadler, "Wireless physical layer authentication via fingerprint embedding," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 48–53, Jun. 2015.

[10] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, Dec. 2009.

[11] Z. Ding, P. Fan, and H. V. Poor, "On the coexistence between full-duplex and noma," *IEEE Wireless Commun. Lett.*, vol. 7, no. 4, pp. 1–1, Mar. 2018.

[12] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proc. IEEE Symposium on Security and Privacy*, May 2010, pp. 286–301.

[13] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2778–2786.

[14] Z. D. Bai, "Methodologies in spectral analysis of large dimensional random matrices, a review," in *Advances In Statistics*. World Scientific, 2008, pp. 174–240.

[15] S. Kritchman and B. Nadler, "Non-parametric detection of the number of signals: Hypothesis testing and random matrix theory," *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 3930–3941, Oct. 2009.

[16] J. Baik and J. W. Silverstein, "Eigenvalues of large sample covariance matrices of spiked population models," *J. Multivariate Anal.*, vol. 97, no. 6, pp. 1382–1408, 2006.

[17] O. N. Feldheim and S. Sodin, "A universality result for the smallest eigenvalues of certain sample covariance matrices," *Geometric And Functional Analysis*, vol. 20, no. 1, pp. 88–123, Jan. 2010.

[18] R. Faragher, "Understanding the basis of the Kalman filter via a simple and intuitive derivation," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 128–132, May 2012.