Is Link Signature Dependable for Wireless Security?

Xiaofan He† and Huaiyu Dai†
†Department of ECE
North Carolina State University, USA
Email: {xhe6,hdai}@ncsu.edu

Wenbo Shen‡ and Peng Ning‡
‡Department of CSC
North Carolina State University, USA
Email: {wshen3,pning}@ncsu.edu

***Abstract*—Link signature, which refers to the unique and reciprocal wireless channel between a pair of transceivers, has gained significant attentions recently due to its effectiveness in signal authentication and shared secret construction for various wireless applications. A fundamental assumption of this technique is that the wireless signals received at two locations separated by more than half a wavelength are essentially uncorrelated. However, it has been shown in literatures that in certain circumstances, e.g., when there is poor scattering and/or a strong line-of-sight (LOS) component, this assumption is invalid. In this paper, a Correlation ATtack (CAT) is proposed to demonstrate the potential vulnerability of the link signature based security mechanisms in such circumstances. Based on statistical inference, CAT explicitly exploits the spatial correlations to recover the legitimate link signature from the observations of multiple adversary receivers deployed in vicinity. The effectiveness of CAT is verified both through theoretical analysis and well-known channel correlation modeling. Our findings are corroborated by experiments on USRP platforms and GNURadio.**

I. Introduction

Wireless physical layer security is becoming increasingly important as wireless devices permeate not only people's daily life but also critical national infrastructures and systems. Link signature based security mechanism is one of the prominent advances in this area recently, where the radio channel characteristics between two wireless devices are explored to provide security protection complementary to traditional cryptographic approaches. While various link signature schemes have been proposed (e.g., [1–4]), the success of them relies crucially on the uniqueness of link signatures due to assumed fast spatial decorrelation of wireless channels.

As discussed in [2], a link signature should provide integrity protection of the wireless signals so that the adversary will not have the same link signature as the legitimate receiver unless it is at exactly the same location. This conclusion is made due to a common assumption that the channel impulse responses of two transceivers spatially separated by more than half a wavelength are essentially uncorrelated. Built upon this optimistic assumption, various secret key extraction and signal authentication techniques are developed in literature using link signature. In [5], the amplitude ratio between the first and the second multipath components is used to provide wireless channel authentication. A methodology based on detecting deep fades in the received signal amplitude is adopted in [6] to extract correlated bitstrings between transceivers. The level-crossing of the channel impulse response amplitude is used in [7] to establish secured communication between two wireless parties. In [8], a multi-bit quantization scheme is proposed to construct secret keys between two wireless nodes by exploring the shared channel characteristics.

This work was supported in part by the National Science Foundation under Grants CCF-0830462, ECCS-1002258 and CNS-1016260.

However, insufficient attention has been paid on the following two critical questions. First, does the common "half-wavelength decorrelation" assumption always hold in all circumstances? Second, when the half-wavelength decorrelation assumption is violated, is the current link signature technique still able to provide security protection to wireless applications? Unfortunately, the answer to the first question is negative. In fact, as pointed out in [9–11], the spatial channel correlation is mainly determined by the angular spread (AS) of the incoming signal, which characterizes how spread out in the angular domain the receive power is. When two receivers are surrounded by rich scatterers, their corresponding AS is usually large and the half-wavelength decorrelation conclusion holds. But when a line-of-sight (LOS) component exits or the waveguide propagation effect dominates, the AS is small and will induce high spatial channel correlation. In fact, high spatial channel correlations have already been observed in real-world experiments [12].

As to the second question, there have been a few works in literature that study whether the current link signature technique is secure when high spatial channel correlation exists. In [13], it is shown that if the received symbols of the adversary receiver is very similar to those of the legitimate receiver, then the adversary can successfully mimic the legitimate link signature. Through experiments, it shows that the received symbols at the legitimate and the adversary receivers are indeed similar, i.e., highly correlated, even when the spatial separation is beyond half a wavelength. In [14], strong space-time channel correlation is also observed, and it is shown that the adversary party can use their channel samples to spoof the legitimate link signature with significant successful rate. However, to the best of our knowledge, none of the existing literatures answers the second question in quantifiable measures built on a solid theoretical basis. Specifically, how severely can the increased spatial channel correlation degrade the performance of link signature schemes, and how much can the adversary party gain from a given channel correlation?

Motivated by the above questions, a Correlation ATtack (CAT) is presented in this work to show the potential vulnerability of link signatures. In particular, CAT adopts statistical inference techniques to recover the legitimate link signature from observations of multiple adversary receivers in the vicinity,

by taking advantage of the spatial correlations between their channels. As compared to previous works, the contributions of this work are given as follows:

- Based on statistical inference, CAT is proposed to show that the adversary can quantitatively use the spatial channel correlation to infer the legitimate link signature in sufficient accuracy.
- The effectiveness of CAT is verified both through theoretical analysis and well-known channel correlation modeling.
- Practical experiments using USRP platforms and GNU-Radio are conducted to support the theoretical analysis, which shed lights on the environment characteristics that may lead to link signature vulnerability.

The rest of this paper is organized as follows. The spatial channel correlation models and the potential vulnerability of link signature are presented in Section II. Section III analyzes how the adversary can apply the proposed CAT to forge the legitimate link signature. To support the theoretical analysis, experiments are conducted in Section IV. Conclusions are drawn in Section V.

II. Potential Vulnerability of Link Signature

A. Spatial Channel Correlation Models

Wireless channel modeling has been extensively studied in literature [15, 16]. Here we introduce two widely adopted ones, the Durgin-Rappaport's model [9] and the one-ring model [17]. Throughout this work, we will focus on narrowband fading channels [18], i.e., only the main (unresolvable) path is considered while other paths are ignored. Therefore, each channel is represented by a scalar (complex) random variable h; in particular, we mainly consider the fading envelope $|h|$. This is a common practice in literature (e.g., [6, 7, 13]), and the extension to the vector case is straightforward. The envelope correlation coefficient between two channels is defined as

$$\rho_{1,2}^{env} \triangleq \frac{E\left[|h_1||h_2|\right] - E\left[|h_1|\right]E\left[|h_2|\right]}{\sqrt{\mathrm{Var}(|h_1|)\mathrm{Var}(|h_2|)}}. \quad (1)$$

In particular, it is related to the complex correlation coefficient $\rho_{1,2}^{complex} \triangleq \frac{E[h_1 h_2^*]-E[h_1]E[h_2^*]}{\sqrt{\mathrm{Var}(h_1)\mathrm{Var}(h_2^*)}}$ through $\rho_{1,2}^{env} \approx |\rho_{1,2}^{complex}|^2$ [19].

In the Durgin-Rappaport's model, the angular spread (AS) Δ, which describes how spread out in the angular domain the receive power is, is an important factor characterizing the channel correlation. The AS itself is determined by the distribution of the power azimuth spectrum (PAS) $p(\theta)$, where θ is the angle of arrival. In literature, various types of PAS have been proposed, such as the $\cos^n(\theta)$ function PAS [20], the uniform PAS [21], the truncated normally distributed PAS [22], the Gaussian PAS [10], the von-Mises PAS [23], and the multimodal truncated Laplacian PAS [11]. Given a specific PAS, the AS Δ can be evaluated as [9]:

$$\Delta \triangleq \sqrt{1 - \frac{|F_1|^2}{|F_0|^2}}, \quad (2)$$

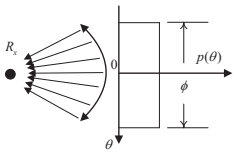


Fig. 1. A uniform PAS at the receiver in the Durgin-Rappaport's model. (R_x: the receiver.)

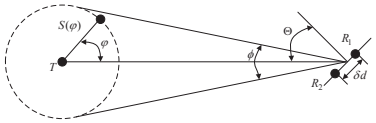


Fig. 2. Illustration of the "one-ring" model. (T: the transmitter, R_1, R_2: two receivers separated by δd, ϕ: angular range, $S(\varphi)$: the scatterer located at direction φ, Θ: receiver orientation.)

where $F_n = \int_0^{2\pi} p(\theta)\exp(jn\theta)d\theta$ is the nth complex Fourier coefficient of $p(\theta)$. The angular spread Δ ranges from 0 to 1 where $\Delta = 0$ corresponds to signal incidence from a single direction and $\Delta = 1$ corresponds to all-around arrivals. As an exmaple, Fig. 1 shows a uniform PAS spreading out in an angular range of ϕ, and the corresponding angular spread is given by $\Delta = \frac{\sqrt{\phi^2-2+2\cos\phi}}{\phi}$ according to (2). In particular, Durgin and Rappaport model the channel envelope correlation coefficient of two receivers $\rho_{1,2}^{env}$ as a function of receiver spatial separation δd parameterized by the AS Δ in the following form [9]:

$$\rho_{1,2}^{env}(\delta d) \approx \exp\left[-\frac{2\pi^2}{4-\pi}\Delta^2\left(\frac{\delta d}{\lambda}\right)^2\right]. \quad (3)$$

Fig. 3 shows how this correlation varies with the receiver separation (normalized with respect to (w.r.t.) the wavelength λ) for different angular spread for a uniform PAS. As shown, the channel envelopes of two receivers are highly correlated for small angular spread even when the receiver separation is much larger than half a wavelength.

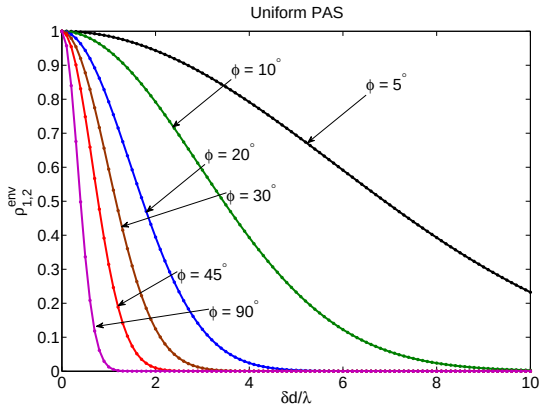


Fig. 3. Channel envelope correlation v.s. receiver separation (based on the Durgin-Rappaport's model).

Another well-known model for channel correlation is the one-ring model [17, 23] depicted in Fig. 2, which represents the scenario where one communication end is surrounded by rich scatterers while the other end experiences much less diffusion. By applying the approximation $\rho_{1,2}^{env} \approx |\rho_{1,2}^{complex}|^2$,

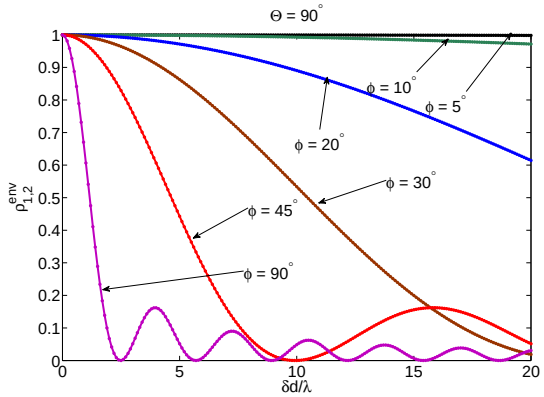


Fig. 4. Channel envelope correlation v.s. receiver separation (based on the one-ring model).

the envelope correlation coefficient between the two receivers separated by δd, when the scatterer ring is on the transmitter side and $\Theta = 90°$, is given by [17]:

$$\rho_{1,2}^{env}(\delta d) \approx \left| J_0\left(2\pi\frac{\phi^2}{16}\frac{\delta d}{\lambda}\right) e^{-2\pi j\frac{\delta d}{\lambda}\left(1-\frac{\phi^2}{16}\right)}\right|^2 = J_0^2\left(2\pi\frac{\phi^2}{16}\frac{\delta d}{\lambda}\right), \quad (4)$$

where $J_0()$ is the first kind Bessel function of order zero. Fig. 4 shows how this correlation varies with the receiver separation for different angular spreads. Again, it is observed that, when the angular spread is small, two channels remain highly correlated for $\delta d \gg \lambda/2$.

Both the Durgin-Rappaport's model and the one-ring model indicate that strong channel correlation exists even when the receivers are separated well beyond half a wavelength. The experiments in [12] also verifies the existence of high spatial channel correlations.

B. Potential Vulnerability of Link Signature

The success of the link signature technique relies on the assumption that the channel between the legitimate transmitter (t) and the adversary receiver (a), $h_{t,a}$,[1] is not the same as $h_{t,r}$, the channel between the legitimate transmitter and receiver (r). In particular, the legitimate transmitter and receiver can construct a common secret $s(h_{t,r})$ based on the shared reciprocal channel $h_{t,r}$, while the adversary cannot obtain this secret because $s(h_{t,a}) \neq s(h_{t,r})$ when $h_{t,a} \neq h_{t,r}$. However, if the adversary can construct an estimate $\hat{h}_{t,r}$ of $h_{t,r}$ based on channel measurement $h_{t,a}$ with sufficient precision, all existing physical layer authentication and key extraction schemes that solely rely on wireless link signature will fail. A common optimistic belief is that the adversary cannot do so if it is spatially restricted beyond half a wavelength away from the legitimate receiver. However, as shown in the above subsection, both well-known channel models and real-world experiments point out that this benign half-wavelength decorrelation assumption is not always valid. Furthermore, as will be shown in the next section, with the collaboration of multiple adversaries, better estimation can be obtained with even larger spatial separation. This may post severe threats to the link signature based security mechanisms. In the following section, we will first demonstrate the effectiveness of the proposed CAT through theoretical analysis; then we will show how potential attacks can be launched based on the one-ring model and the Durgin-Rappaport's model. Supporting experiment results will be presented in Section IV.

[1]The magnitude sign $|\cdot|$ is omitted for simplicity.

III. Link Signature Forging

A. Theoretical Analysis

This subsection shows how the adversary party can apply the proposed CAT to infer the legitimate receiver channel $h_{t,r}$ so as to forge the corresponding link signature. In the proposed CAT, multiple adversary receivers deployed in the vicinity of the legitimate receiver first measure their own channels h_{t,a_i}'s, and then, based on these measurements, construct an estimate $\hat{h}_{t,r}$ of $h_{t,r}$ through linear minimum mean square error (LMMSE) estimation, which explicitly exploits the potential high spatial channel correlations. The LMMSE estimator is optimal when the random variables involved are jointly Gaussian (often assumed in communications when the central limit theorem can be invoked), and widely adopted in practice due to its simplicity and good performance [24]. Specifically, the LMMSE estimator of an unknown random variable x based on measurement y, is given by $\hat{x} = E[x] + [Cov(y,y)^{-1}Cov(x,y)]^T(y - E[y])$, where $E[u]$ denotes the expectation of u, T represents the transpose operation, and $Cov(u,v) \triangleq E[uv] - E[u]E[v]$ is the covariance between u and v; $\hat{x}$ is no worse than y in the MSE sense [25].

Proposition 1: The LMMSE estimate of the legitimate receiver channel based on the multiple ($n \geq 2$) adversary channels $h_{t,a} = [h_{t,a_1}, h_{t,a_2}, ..., h_{t,a_n}]^T$ is given by

$$\hat{h}_{t,r} = E[h_{t,r}] + B^T C^{-1}(h_{t,a} - E[h_{t,a}]), \quad (5)$$

where $B_{n\times 1} \triangleq Cov(h_{t,r}, h_{t,a}) = [b_i]_{i=1}^n$ is the correlation vector between the legitimate receiver channel and the adversary channels, $C_{n\times n} \triangleq Cov(h_{t,a}, h_{t,a}) = [c_{i,j}]_{i,j=1}^n$ is the symmetric correlation matrix of the adversary channels. This estimator is always no worse than that based on any single ($n = 1$) adversary channel, in the MSE sense.

Proof: See Appendix A. ■

Proposition 2: The MSE of the LMMSE estimate $\hat{h}_{t,r}$ is given by $\frac{\det(\Gamma)}{\det(C)}$, where $\Gamma = \begin{bmatrix} A & B^T \\ B & C \end{bmatrix}$ and $A_{1\times 1} \triangleq Cov(h_{t,r}, h_{t,r}) = Var(h_{t,r})$ is the variance of the legitimate receiver channel.

Proof: Let $S = A - B^T C^{-1} B$ be the Schur complement of block C in Γ. Then,

$$MSE(\hat{h}_{t,r}) = E\left[(\hat{h}_{t,r} - h_{t,r})^2\right] = A - B^T C^{-1} B = \det(A - B^T C^{-1} B) = \det(S) = \frac{\det(\Gamma)}{\det(C)}. \quad (6)$$

■

The above propositions are general as no further knowledge about the correlation matrix structure is assumed. A special theoretical model is considered in the following to show how the mutual correlations between the legitimate receiver channel and adversary channels affect the inference quality, and that in some circumstances the adversary is even capable of obtaining a perfect inference.

Corollary 1: Assume that the correlation between any adversary channel and the legitimate receiver channel is b, and the correlation between any two adversary channels is a. Then, the resulting MSE of deploying n adversary receivers is given by $\frac{1+(n-1)a-nb^2}{1+(n-1)a}$.[2]

Corollary 2: If $a < b^2$, then $\exists n = \frac{1-a}{b^2-a}$, s.t. the MSE of deploying n adversary receivers is zero. If $a \geq b^2$, the limit of MSE is $\frac{a-b^2}{a}$ as $n \to \infty$.

Remark: Some interesting observations can be made from the above results. If $a < b^2$, there exists an $n = \frac{1-a}{b^2-a}$ such that the MSE of the LMMSE estimator can be driven down to zero when employing n adversary receivers. For example, when $b = 0.9$, the measurement from one adversary receiver would (in principle for the ideal case of $a = 0$) lead to an MSE of $1-b^2 = 0.19$, and the minimum number of adversary receivers required for zero MSE is $1/b^2 \approx 2$. In Fig. 5, a more realistic case where $a = 0.8$ is considered[3], for which 20 adversary receivers are needed for a perfect inference in theory. We also conduct 10000 Monte Carlo simulations in which $h_{t,r}$ and $h_{t,a}$ are Gaussian with the above given correlations, and provide the average MSE (denoted by circle) as well as the 90% confidence interval of the simulated results (denoted by cross). It is found that the average MSE of the simulation matches well with the theoretical results. However the instantaneous MSE exhibits large deviation for single and a small number of adversary receivers, which favorably decreases with the increase of n. In this scenario, 8 to 10 adversary receivers will result in satisfactory estimation quality, which in turn severely degrades the security of link signature based mechanisms.

B. Potential Attacks Based on Channel Correlation Models

In the above discussion, we have demonstrated the vulnerabilities of link signatures through theoretical analysis. In this subsection, we move one step further by proposing two potential attacks based on the two well-known channel correlation models discussed in II-A.

In the first attack, we consider the one-ring model and the line placement of adversary receivers as depicted in Fig. 6(a). The corresponding achievable normalized MSE is plotted numerically in Fig. 7 according to Proposition 2 and the one-ring model. As shown in Fig. 7, when the AS is small ($\phi = 10°$), a single adversary receiver placed around 5 wavelengths away from the legitimate receiver is able to achieve a target normalized MSE 0.05. If the adversary has two collaborative receivers, both of them may be put at least 10 wavelengths away, and for eight adversary receivers the target is still achieved even if the legitimate receiver has a guard zone of 20 wavelengths.

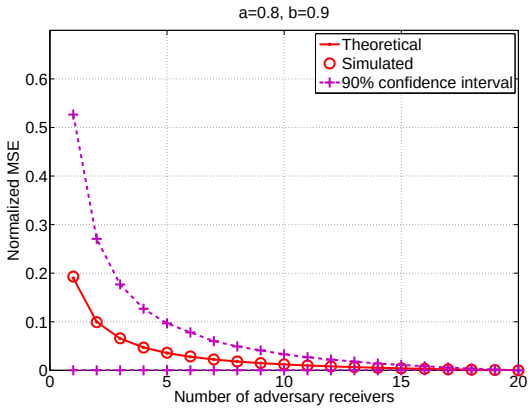


Fig. 5. Normalized MSE comparison of using single and multiple adversary receivers.

In the second attack, the Durgin-Rappaport's model is considered, and the adversary receivers are deployed on a ring as shown in Fig. 6(b). The following corollary gives a closed-form expression for the achievable normalized MSE.

Corollary 3: If the correlation between any two receivers (either legitimate or adversary) with spatial separation δd is $\rho(\delta d)$, i.e., the channel correlation is insensitive to the absolute position, and all the adversary receivers are uniformly deployed around the legitimate receiver as a ring with radius r, then the normalized MSE of using n adversary receivers is given by[4]

$$MSE(\hat{h}_{t,r}) = 1 - \frac{n \cdot \rho^2(r)}{\sum_{k=0}^{n-1} \rho(2r \cdot \sin(\frac{\pi k}{n}))}. \quad (7)$$

Proof: See Appendix B. ■

As shown in Fig. 8 (plotted according to Corollary 3 and the Durgin-Rappaport's model), for small AS ($\phi = 5°$), as few as 3 adversary receivers, which may be confined 4 wavelengths away from the legitimate receivers, are capable of achieving a target normalized MSE 0.05.

The above analysis indicates that collaborative adversary receivers placed much further away than the commonly believed safe distance, e.g., half a wavelength, may still be capable of inferring the legitimate channel with high accuracy, which reveals the potential threat to existing wireless link signature schemes.

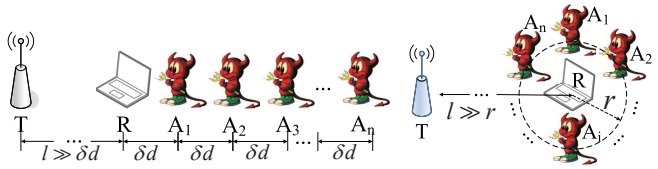
IV. Experiment Results

In this section, experiments using Universal Software Radio Peripheral (USRP) platforms and GNURadio are conducted to support analytical results and demonstrate the potential

[2]The covariance matrix Γ exists (or it is non-negative-definite) iff $1+(n-1)a-nb^2 \geq 0$.

[3]In practice, it is difficult for the adversary receivers to simultaneously maintain a high correlation with the legitimate receiver and a low correlation among themselves, due to spatial constraints.

[4]Without out loss of generality, it is assumed that all the channels ($h_{t,r}$ and h_{t,a_i}'s) have variance 1.



(a) line placement (b) Ring placement

Fig. 6. Two deployment patterns of the adversary receivers. (T: legitimate transmitter, R: legitimate receiver, $A_1 - A_n$: adversary receivers, l: transmission distance, δd: receiver separation, r: radius of the ring.)

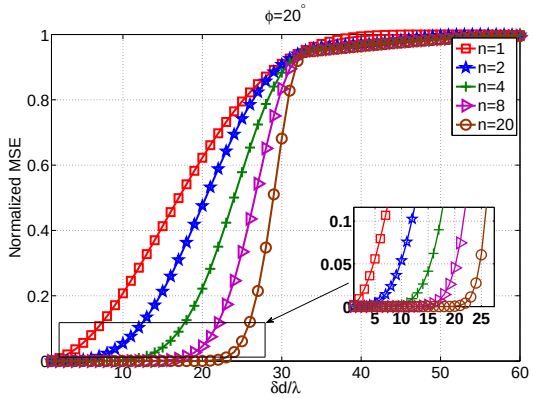


Fig. 7. Achievable normalized MSE of n adversary receivers aligned in a line (based on the one-ring model).

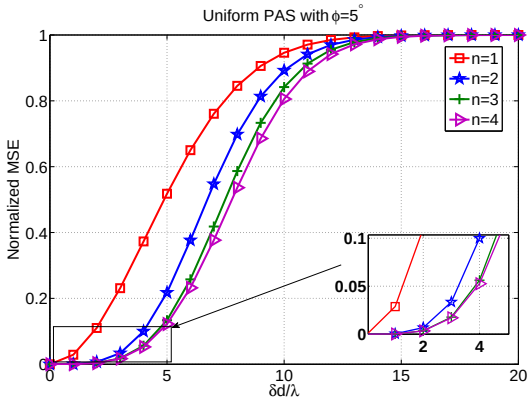


Fig. 8. Achievable normalized MSE of n adversary receivers placed on a ring (based on the Durgin-Rappaport's model).

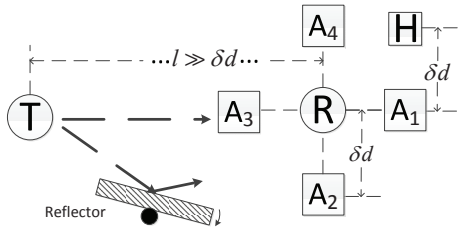


Fig. 9. The experiment setting for $n = 4$. (T: legitimate transmitter, R: legitimate receiver, A_1–A_4: four adversary receivers, H: adversary helper, l: transmission distance.)

vulnerability of the link signature based security mechanisms. The carrier frequency is 2.4 GHz with corresponding wavelength $\lambda = 12.5$ cm. Four experiments are conducted with different number of adversary receivers n and different receiver separations δd. Specifically, $n = 2$ and $\delta d = 2\lambda$ in experiment I, $n = 3$ and $\delta d = 4\lambda$ in experiments II and III, and $n = 4$ and $\delta d = 6\lambda$ in experiment IV. All these experiments are conducted indoor, and a strong LOS component exists. The adversary receivers are placed at an equal distance δd to the legitimate receiver. The channel envelope is used as the link signature.

A. Measuring Channel Correlation

The procedure of measuring the channel envelope correlation between two receivers is described in this subsection.

For the indoor environment, if both the transmitter and receiver are static, the channel is quasi-static, and thus small environment disturbances are required to randomize the channels for the correlation measurement. To do so, the transceivers move through a grid centered at the nominal measurement point with grid points being separated by λ in [12]. However, this approach is not suitable here because the legitimate transmitter may be static in practice and will not collaborate with the adversary. In our experiment, a flat reflector is deployed nearby, and randomly rotated to randomize the channels. After K rotations, K pairs of channel samples $\{|h_1^{(k)}|, |h_2^{(k)}|\}$ ($k = 1, ..., K$) are recorded.[5] Then, the estimate of the envelope correlation coefficient between two receivers can be evaluated as

$$\hat{\rho}_{1,2}^{env} = \frac{\frac{1}{K}\sum_{k=1}^{K}(|h_1^{(k)}| - \hat{\mu}_1)(|h_2^{(k)}| - \hat{\mu}_2)}{\hat{\sigma}_1\hat{\sigma}_2}, \tag{8}$$

where $\hat{\mu}_i = \frac{1}{K}\sum_{k=1}^{K}|h_i^{(k)}|$ and $\hat{\sigma}_i^2 = \frac{1}{K}\sum_{k=1}^{K}(|h_i^{(k)}| - \hat{\mu}_i)^2$.

[5]In the experiment, undesired temporal variation and measurement noise are eliminated by averaging over 100 channel samples per $h_i^{(k)}$, as suggested in literature [12].

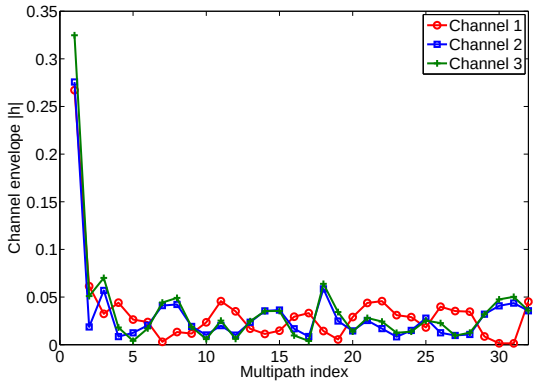


Fig. 10. An example of measured channels.

TABLE I
COMPARISON OF THE SPATIAL CHANNEL CORRELATION COEFFICIENTS.

	$\hat{\rho}_{A_1,R}$	$\hat{\rho}_{A_2,R}$	$\hat{\rho}_{A_3,R}$	$\hat{\rho}_{A_4,R}$	$\hat{\rho}_{A_1,H}$
Exp. I	0.88	0.84	/	/	0.79
Exp. II	0.84	0.78	0.86	/	0.80
Exp. III	0.86	0.64	0.50	/	/
Exp. IV	0.76	0.69	0.70	0.88	/

In the experiments, the least square (LS) method is used to obtain the channel estimates [13]. Fig. 10 shows an example of measured channels, which indicates that indeed the measured channels are dominated by one path component.

B. Known Statistics

In this subsection, it is assumed that all the required statistics are available for the adversary. That is, 1) C the correlation matrix of adversary channels, 2) B the correlation vector between adversary channels and the legitimate receiver channel, and 3) $E[|h_{t,r}|]$ the mean of the legitimate receiver channel envelope, are all known.

In Fig. 11–Fig. 14, the link signatures of the legitimate receiver channel, the adversary channels, and the adversary collaboratively estimated channel are shown for these four experiments, respectively. For each experiment, 30 samples are recorded per channel where the variations of channels are caused by the random rotations of the reflector. The corresponding channel spatial correlation coefficients are summarized in Table I, and the normalized (w.r.t. the mean of legitimate channel envelope) root-mean-square-error (RMSE) of the adversary channels and the estimated channels are summarized in Table II, where $\hat{\rho}_{A_i,R}$ denotes the estimated correlation coefficient (from the 30 samples) between the channels of the adversary receiver A_i and the legitimate receiver R. Several observations are in order:

- Strong correlations ($\rho > 0.8$) exist between the adversary channels and the legitimate receiver channel even though the spatial separation δd is significantly larger than half a wavelength, as shown in Table I.
- When channel statistics are known apriori, the adversary can launch CAT and obtain a link signature estimate with normalized RMSE around 10%, as shown in Table II.
- When the adversaries are being confined further away, they can maintain a similar estimation accuracy through increasing the number of adversary receivers. For example, in experiment I where $\delta d = 2\lambda$, using two adversary receivers can achieve a normalized RMSE 8%. In experiment IV where $\delta d = 6\lambda$, when only the first two adversary receivers A_1 and A_2 are used, the resulting normalized RMSE is around 17%; if the first three adversary receivers are used, the corresponding normalized RMSE is reduced to 15%; if all the four adversary receivers are used, the normalized RMSE can be further reduced to 11%.

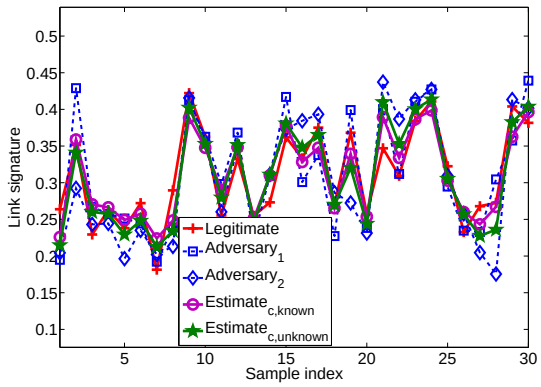


Fig. 11. Forged and true link signatures in experiment I ($n = 2$ and $\delta d \approx 2\lambda$).

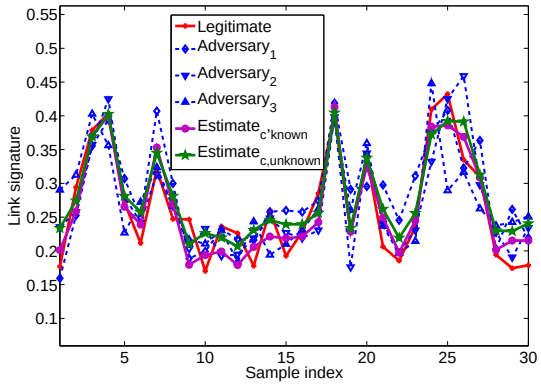


Fig. 12. Forged and true link signatures in experiment II ($n = 3$ and $\delta d \approx 4\lambda$).

C. Unknown Statistics

The assumption that all the statistics are known is reasonable for certain practical situations. For example, the adversary party can deploy the transceivers in a similar environment to obtain estimates of these statistics (and build databases), or they can infer from specific physical models, e.g., [9, 17] when

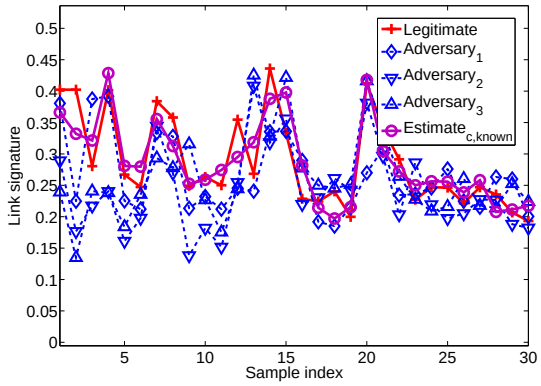


Fig. 13. Forged and true link signatures in experiment III ($n = 3$ and $\delta d \approx 4\lambda$).

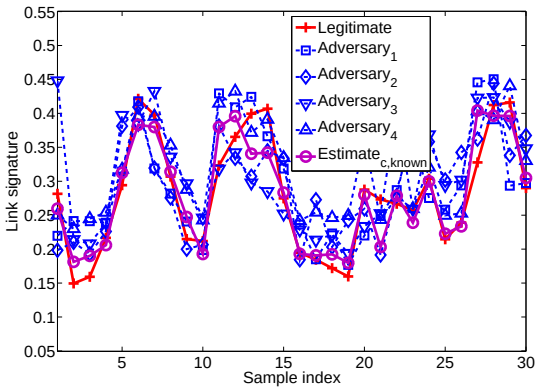


Fig. 14. Forged and true link signatures in experiment IV ($n = 4$ and $\delta d \approx 6\lambda$).

TABLE II
THE NORMALIZED (W.R.T. THE MEAN) RMSE.

	A_1	A_2	A_3	A_4	$\text{Est.}_{\text{known}}$	$\text{Est.}_{\text{unknown}}$
Exp. I	12%	15%	/	/	8%	9%
Exp. II	18%	19%	16%	/	11%	13%
Exp. III	27%	21%	29%	/	11%	/
Exp. IV	21%	23%	24%	19%	11%	/

these models are known to match the environment of interest well. In the following, it is shown that a simple approximation approach may work for the adversary to launch CAT in certain circumstances.

In particular, two interesting properties are observed in the first two experiments:

- The correlation coefficients $\{\hat{\rho}_{A_i,R}\}$ between the channels of any of the adversaries (A_i) and the legitimate receiver (R) are similar, as shown in Table I. In addition, the correlation coefficient $\hat{\rho}_{A_1,H}$ between the channels of A_1 and an adversary helper (H), which is placed at an equal distance (δd) away from A_1 as the legitimate receiver as shown in Fig. 9, is also close to $\{\hat{\rho}_{A_i,R}\}$. This implies that, in these two experiments, the spatial correlation between two receivers is mainly determined by their spatial separation δd but not sensitive to their absolute positions.[6] Similar phenomenon has been observed in [12] as well.
- The sample mean of the legitimate receiver's channel envelopes ($\hat{E}[|h_R|]$) is close to those of the adversary receivers ($\hat{E}[|h_{A_i}|]$), as shown in Table III.

[6]The two channel models discussed in II-A conform to this setting when the angular range is fixed.

TABLE III
COMPARISON OF THE SAMPLE MEAN OF CHANNEL ENVELOPES.

	$\hat{E}[\lvert h_{A_1}\rvert]$	$\hat{E}[\lvert h_{A_2}\rvert]$	$\hat{E}[\lvert h_{A_3}\rvert]$	$\hat{E}[\lvert h_{A_4}\rvert]$	$\hat{E}[\lvert h_R\rvert]$
Exp. I	0.31	0.30	/	/	0.31
Exp. II	0.28	0.27	0.27	/	0.27
Exp. III	0.22	0.26	0.24	/	0.29
Exp. IV	0.29	0.29	0.30	0.31	0.29

TABLE IV
THE PERCENTAGE OF CORRECTLY INFERRED SECRET BITS.

	A_1	A_2	A_3	A_4	$\text{Est.}_{\text{known}}$	$\text{Est.}_{\text{unknown}}$
Exp. I	82%	87%	/	/	97%	97%
Exp. II	90%	95%	88%	/	99%	99%
Exp. III	80%	83%	77%	/	83%	/
Exp. IV	70%	78%	73%	90%	97%	/

In environments with the above two properties, the adversary party can approximate the unknown statistics as

$$E[|h_R|] \approx \frac{1}{n}\sum_{i=1}^{n} \hat{E}[|h_{A_i}|], \tag{9}$$

and

$$B \approx \hat{\rho}_{A_1,H} \times [\hat{\sigma}^2_{|h_{A_1}|}, ..., \hat{\sigma}^2_{|h_{A_n}|}]^T, \tag{10}$$

to launch CAT.[7] With these approximations, the estimated link signatures are shown in Fig. 11 and Fig. 12. As summarized in Table II, the estimation accuracy degrades only slightly ($1 \sim 2$ percentages).

However, it should be admitted that these properties are not universal. As observed in the third and forth experiments that are conducted in a corridor, the correlations are not close enough for different adversary receivers even though the spatial separation is identical, which, we conjecture, is due to the asymmetry of the physical environment. In such circumstances, the adversary may rely on the two approaches mentioned above to compute the correlation, and the success of CAT will depend on how accurate the physical correlation model or the database is.

D. Secret Key Extraction

The adversary can effectively reproduce the secret key based on the forged link signature if the estimation is sufficiently accurate. In our experiments, a 2-bits quantization key extractor[8] is used. Table IV shows the percentage of correctly inferred secret bits for the four experiments, respectively, where each receiver extracts 60 secret bits based on its own 30 channel samples and the adversary party will further extract secret bits based on their collaboratively estimated link signature. As can be seen, when high spatial channel correlation exists, even a single adversary is capable of correctly inferring the secret bits with a significant accuracy. By adopting CAT, the adversary party successfully recover 97% and 99% of the secret bits in the first and second experiments, respectively, without requiring any prior information.

V. CONCLUSIONS

A correlation attack, which explicitly exploits the channel correlations to recover the legitimate link signature, is

[7]The adversaries can always measure the correlation matrix C through collaboration.

[8]A high granularity extractor distinguishes the legitimate and the forged link signatures more accurately but will also increase the key mismatch rate between the transmitter and receiver. Finding an optimal key extractor is beyond the scope of this paper.

proposed to demonstrate the potential vulnerability of the link signature based security mechanisms. Through theoretical analysis and channel modeling, it is shown that a close replication of the legitimate link signature is possible, even if the adversary receivers are deployed well beyond what is commonly believed as a safe distance. Experiments conducted on USRP platforms and GUNRadio support the theoretical analysis and lead to two important conclusions: 1) significant spatial correlation exists between wireless channels in various circumstances, which can be exploited by the adversary party to forge the legitimate link signature through the correlation attack; 2) a physical environment where the spatial correlation is high and not sensitive to position shift is especially unsafe for wireless applications solely relying on link signature based security mechanisms.

APPENDIX A
PROOF OF PROPOSITION 1

Proof: According to the well-known orthogonality principle, the LMMSE estimator $\hat{h}_{t,r}$ of $h_{t,r}$ can be found as

$$\hat{h}_{t,r} = E[h_{t,r}] + \xi^T (h_{t,a} - E[h_{t,a}]), \tag{11}$$

where ξ is the coefficient vector of the estimator that satisfies $C\xi = B$.

Then, it is going to be shown that the estimator of the legitimate channel based on multiple adversary channels is no worse than that based on any single adversary channel. For clarity, let $x = h_{t,r} - E[h_{t,r}]$, $y_i = h_{t,a_i} - E[h_{t,a_i}]$, and $y = [y_1, y_2, ..., y_n]^T$. Consequently, $E[x] = 0$, and $E[y_i] = 0$ $(i = 1, ..., n)$. It is clear that, the covariance matrices corresponding to $h_{t,r}$ and $h_{t,a}$ are identical to those corresponding to x and y. That is, $Cov(y, y) = C$ and $Cov(x, y) = B$. As a result, the coefficient vector in the estimator of x based on measurement y is also ξ. Specifically, the estimator $\hat{x}_m$ of x based on multiple adversary channels can be expressed as

$$\hat{x}_m = \xi^T y. \tag{12}$$

Similarly, the estimator $\hat{x}_s$ based on a single adversary channel[9] is in the form of $\hat{x}_s = \varphi y_1$, where the corresponding coefficient scalar φ satisfies $c_{1,1}\varphi = b_1$. Since $C\xi = B$, it is readily to see that

$$C_1^{(r)} \xi = c_{1,1}\varphi, \tag{13}$$

where $C_1^{(r)}$ denotes the first row of matrix C.

It can be verified that $MSE(\hat{x}) = MSE(\hat{h}_{t,r})$, thus we will only prove $MSE(\hat{x}_m) \leq MSE(\hat{x}_s)$ in the following, and the same conclusion can be applied to $\hat{h}_{t,r}$. According to (12), the MSE of $\hat{x}_m$ is given by

$$\begin{aligned} MSE(\hat{x}_m) &= E[(\hat{x}_m - x)^2] \\ &= E[x^2] - Cov(x, y)^T Cov^{-1}(y, y) Cov(x, y) \\ &= E[x^2] - B^T C^{-1} B. \end{aligned} \tag{14}$$

[9]Without loss of generality, assume that the first adversary channel is used.

Similarly, the MSE of $\hat{x}_s$ is given by

$$\begin{aligned} MSE(\hat{x}_s) &= E[(\hat{x}_s - x)^2] \\ &= E[x^2] - Cov(x, y_1) Cov^{-1}(y_1, y_1) Cov(x, y_1) \\ &= E[x^2] - \frac{b_1^2}{c_{1,1}}. \end{aligned} \tag{15}$$

Considering (14), (15), $C\xi = B$, and $c_{1,1}\varphi = b_1$, it can be seen that $MSE(\hat{x}_m) \leq MSE(\hat{x}_s)$ iff $\xi^T C \xi \geq \varphi c_{1,1} \varphi$, which will be shown next.

To this end, partition matrix C into $C = \begin{bmatrix} c_{1,1} & G^T \\ G & F \end{bmatrix}$ where $G_{(n-1)\times 1} = Cov(y_1, [y_2, ..., y_n]^T)$ and $F_{(n-1)\times(n-1)} = Cov([y_2, ..., y_n]^T, [y_2, ..., y_n]^T)$. Noting that $C_1^{(r)} = [c_{1,1}\ G^T]$, it can be verified that $\xi^T C \xi \geq \varphi c_{1,1} \varphi$ iff $\xi^T \begin{bmatrix} c_{1,1} & G^T \\ G & F \end{bmatrix} \xi \geq \frac{1}{c_{1,1}} \xi^T \begin{bmatrix} c_{1,1} \\ G \end{bmatrix} [\, c_{1,1}\ G^T \,] \xi$ using (13). Thus, it only needs to show $\begin{bmatrix} 0 & 0_{1\times(n-1)} \\ 0_{(n-1)\times 1} & c_{1,1} \cdot F - GG^T \end{bmatrix}$ is a positive-semidefinite (PSD) matrix, which is equivalent to that $c_{1,1} \cdot F - GG^T$ is PSD.

To show $c_{1,1} \cdot F - GG^T$ is PSD, consider the eigenvalue decomposition $C = [\, \tilde{u}_1 \ ... \ \tilde{u}_n \,] \begin{bmatrix} \lambda_1 & & \\ & \cdots & \\ & & \lambda_n \end{bmatrix} \begin{bmatrix} \tilde{u}_1^T \\ \cdots \\ \tilde{u}_n^T \end{bmatrix}$, where $\tilde{u}_i = \begin{bmatrix} u_{1,i} \\ u_i \end{bmatrix}$, $u_i = [u_{2,i}, ..., u_{n,i}]^T$, and all the eigenvalues λ_i's are non-negative because the covariance matrix C is always PSD. It can be verified that $c_{1,1} = \sum_{i=1}^{n} \lambda_i u_{1,i} u_{1,i}$, $G = \sum_{i=1}^{n} \lambda_i u_{1,i} u_i$ and $F = \sum_{i=1}^{n} \lambda_i u_i u_i^T$. For any vector α, it has

$$\begin{aligned} &\alpha^T (c_{1,1} \cdot F - GG^T) \alpha \\ &= \alpha^T \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j u_{1,i} u_{1,i} u_j u_j^T \right. \\ &\quad \left. - \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j u_{1,i} u_{1,j} u_i u_j^T \right) \alpha \\ &= \alpha^T \left(\sum_{i=1}^{n} \sum_{j=1}^{n} \widetilde{\lambda}_i \widetilde{\lambda}_j v_j v_j^T - \sum_{i=1}^{n} \sum_{j=1}^{n} \widetilde{\lambda}_i \widetilde{\lambda}_j v_i v_j^T \right) \alpha \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} \widetilde{\lambda}_i \widetilde{\lambda}_j \beta_j \beta_j - \sum_{i=1}^{n} \sum_{j=1}^{n} \widetilde{\lambda}_i \widetilde{\lambda}_j \beta_i \beta_j \\ &= \left(\sum_{i=1}^{n} \widetilde{\lambda}_i \right) \left(\sum_{j=1}^{n} \widetilde{\lambda}_j \beta_j^2 \right) - \left(\sum_{i=1}^{n} \widetilde{\lambda}_i \beta_i \right)^2 \geq 0, \end{aligned} \tag{16}$$

where $v_i = \frac{u_i}{u_{1,i}}$, $\widetilde{\lambda}_i = \lambda_i u_{1,i}^2 \geq 0$, $\beta_i = \alpha^T v_i$, and the last step in (16) is due to the Cauchy-Schwartz inequality, which shows that $c_{1,1} \cdot F - GG^T$ is PSD. Therefore, $MSE(\hat{x}_m) \leq MSE(\hat{x}_s)$ for $\hat{x}$ and so is $\hat{h}_{t,r}$. ■

APPENDIX B
PROOF OF COROLLARY 3

Proof: Based on the geometry, it can be seen that the correlation between the legitimate channel and any of the adversary channels is $\rho(r)$, and the correlation between the ith and the jth adversary channels is $\rho(2r \cdot \sin(\frac{\pi |i-j|}{n}))$. For clarity, denote $\rho(r)$ by b and $\rho(2r \cdot \sin(\frac{\pi k}{n}))$ by $g(k)$, respectively, then the determinant of Γ (defined in Proposition 2) is given by

$$
\begin{aligned}
&\det(\Gamma)\\
&= \left| \begin{bmatrix} 1 & b & b & \cdots & \cdots & b \\ b & 1 & g(1) & \cdots & \cdots & g(n-1) \\ b & g(n-1) & 1 & g(1) & \cdots & g(n-2) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \cdots & \ddots & \vdots \\ b & g(1) & g(2) & \cdots & g(n-1) & 1 \end{bmatrix}_{(n+1)\times(n+1)} \right| \\
&= \left| \begin{bmatrix} 1 & b & b & \cdots & \cdots & b \\ 0 & 1-b^2 & g(1)-b^2 & \cdots & \cdots & g(n-1)-b^2 \\ 0 & g(n-1)-b^2 & 1-b^2 & g(1)-b^2 & \cdots & g(n-2)-b^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \ddots & \vdots \\ 0 & g(1)-b^2 & g(2)-b^2 & \cdots & g(n-1)-b^2 & 1-b^2 \end{bmatrix} \right| \\
&= \left| \begin{bmatrix} 1-b^2 & g(1)-b^2 & \cdots & \cdots & g(n-1)-b^2 \\ g(n-1)-b^2 & 1-b^2 & g(1)-b^2 & \cdots & g(n-2)-b^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ g(1)-b^2 & g(2)-b^2 & \cdots & g(n-1)-b^2 & 1-b^2 \end{bmatrix}_{n\times n} \right| \\
&= \prod_{i=0}^{n-1} \left(c_0 + c_1\omega_i^1 + \cdots + c_{n-1}\omega_i^{n-1} \right), \qquad (17)
\end{aligned}
$$

where $\omega_k = \exp(j\frac{2\pi k}{n})$ is the nth roots of unity, and $c_0 = 1-b^2$, $c_i = g(n-i)-b^2$ for $i > 0$. The last step is due to the circulant structure of the matrix. Similarly, the determinant of C is given by

$$
\det(C) = \prod_{i=0}^{n-1} \left(c_0' + c_1'\omega_i^1 + \cdots + c_{n-1}'\omega_i^{n-1} \right), \qquad (18)
$$

where $c_0' = 1$ and $c_i' = g(n-i)$ for $i > 0$. According to Proposition 2, the MSE of the estimator $\hat{h}_{t,r}$ based on the channel measurements from these n adversary receivers is given by

$$
\begin{aligned}
&MSE(\hat{h}_{t,r})\\
&= \frac{\det(\Gamma)}{\det(C)} = \prod_{i=0}^{n-1} \left[\frac{c_0 + c_1\omega_i^1 + \cdots + c_{n-1}\omega_i^{n-1}}{c_0' + c_1'\omega_i^1 + \cdots + c_{n-1}'\omega_i^{n-1}} \right] \\
&= \prod_{i=0}^{n-1} \left[\frac{c_0' + c_1'\omega_i^1 + \cdots + c_{n-1}'\omega_i^{n-1} - b^2 \sum_{k=0}^{n-1} \omega_i^k}{c_0' + c_1'\omega_i^1 + \cdots + c_{n-1}'\omega_i^{n-1}} \right] \\
&= \frac{c_0' + c_1' + \cdots + c_{n-1}' - n \cdot b^2}{c_0' + c_1' + \cdots + c_{n-1}'} \\
&= 1 - \frac{n \cdot \rho^2(r)}{\sum_{k=0}^{n-1} \rho(2r \cdot \sin(\frac{\pi k}{n}))}, \qquad (19)
\end{aligned}
$$

where in the second last step the fact $\sum_{k=0}^{n-1} \omega_i^k = \delta(i)$ is applied. ■

REFERENCES

[1] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," *In Proc. of WiSec'06*, Los Angeles, CA, Sep. 2006.

[2] N. Patwari, and S. K. Kasera, "Robust location distinction using temporal link signatures," *In Proc. of Mobicom'07*, pp. 111–122, Montreal, Canada, Sep. 2007.

[3] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," *In Proc. of ACM MobiCom'08*, pp. 26–37, San Francisco, CA, Sep. 2008.

[4] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," *In Proc. of ACM MobiSys'10*, pp. 331–344, San Francisco, CA, Jun. 2010.

[5] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," *IEEE Symposium on SP (Oakland'10)*, pp. 286–301, Oakland, CA, May 2010.

[6] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," *In Proc. of ACM CCS'07*, pp. 401–410, 2007.

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," *In Proc. of ACM MobiCom'08*, pp. 128–139, San Francisco, CA, Sep. 2008.

[8] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[9] G. D. Durgin, and T. S. Rappaport, "Effects of multipath angular spread on the spatial cross-correlation of received voltage envelopes," *In Proc. of IEEE VTC*, pp. 996–1000, Jul. 1999.

[10] J. Fuhl, A. F. Molisch, and E. Bonek, "Unified channel model for mobile radio systems with smart antennas," *In Proc. of IEE Radar, Sonar and Navigation*, vol. 145, no. 1, pp. 32–41, Feb. 1998.

[11] L. Schumacher, and B. Raghothaman, "Closed-form expressions for the correlation coefficient of directive antennas impinged by a multimodal truncated Laplacian PAS," *IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1351–1359, Jul. 2005.

[12] P. Kyritsi, D. C. Cox, R. A. Valenzuela, and P. W. Wolniansky, "Correlation analysis based on MIMO channel measurements in an indoor environment," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 5, pp. 713–720, Jun. 2003.

[13] Y. Liu, and P. Ning, "Mimicry attacks against wireless link signature and defense using time-synched link signature," *In Proc. of IEEE INFOCOM (mini-conference)*, Orlando, FL, Mar. 2012.

[14] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction," *In Proc. of ACM EuroSec'11*, Salzburg, Austria, Apr. 2011.

[15] W. C. Jakes, *Microwave mobile communications*, New York: Wiley, 1974.

[16] A. F. Molisch, *Wireless communications*, New York: Wiley, 2011.

[17] D. S. Shiu, G. J. Foschini, M. J. Gans, and J. M. Kahn, "Fading correlation and its effect on the capacity of multielement antenna systems." *IEEE Trans. Commun.*, vol. 48, no. 3, pp. 502–513, Aug. 2000.

[18] A. Goldsmith, *Wireless Communications*, Cambridge Univ. Press, 2005.

[19] R. O. LaMaire, and M. Zorzi, "Effect of correlation in diversity systems with Rayleigh fading, shadowing, and power capture," *IEEE J. Sel. Areas Commun.*, vol. 14, no. 3, pp. 449–460, Apr. 1996.

[20] W. Lee, "Effects on correlation between two mobile radio base-station antennas," *IEEE Trans. Commun.*, vol. 21, no. 11, pp. 1214–1224, Nov. 1973.

[21] J. Salz, and J. H. Winters, "Effect of fading correlation on adaptive arrays in digital mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 4, pp. 1049–1057, Nov. 1994.

[22] F. Adachi, M. T. Feeney, J. D. Parsons, and A. G. Williamson, "Crosscorrelation between the envelopes of 900 MHz signals received at a mobile radio base station site," *In Proc. of IEE Communications, Radar and Signal Processing*, vol. 133, no. 6, pp. 506–512, Oct. 1986.

[23] A. Abdi, and M. Kaveh, "A space-time correlation model for multielement antenna systems in mobile fading channels," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 3, pp. 550–560, Apr. 2002.

[24] H. V. Poor., *An introduction to signal detection and estimation*, New York: Springer, 1994.

[25] G. R. Grimmett, and D. R. Stirzaker, *Probability and random processes*, Oxford Univ. Press, 2001.