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*—A fundamental assumption of link signature based security mechanisms is that the wireless signals received at two locations separated by more than half a wavelength are essentially uncorrelated. However, it has been observed that in certain circumstances (e.g., with 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 reconstruct the legitimate link signature from the observations of multiple adversary receivers deployed in vicinity. Our findings are verified through theoretical analysis, well-known channel correlation models, and experiments on USRP platforms and GNURadio.**

I. Introduction

Link signature based wireless security mechanisms exploit the radio channel characteristics between two wireless devices to provide security protection complementary to traditional cryptographic approaches. The success of these schemes relies crucially on the uniqueness of link signatures resulting from the assumed fast spatial decorrelation of wireless channels; in particular, it is widely accepted that half a wavelength separation is sufficient for security assurance. Built upon this optimistic assumption, various secret key extraction and signal authentication techniques have been developed based on link signatures (e.g., [1–8]).

However, two critical questions remain unclear. First, does the common "half-wavelength decorrelation" assumption hold in all circumstances? As pointed out in [9–11], the spatial channel correlation is significantly influenced by the angular spread (AS) of the incoming signal. 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 exists 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]. Second, when the half-wavelength decorrelation assumption is violated, is the current link signature technique still able to provide security protection to wireless applications? This question attracts research interest very recently (e.g., [13, 14]). However, to the best of our knowledge, none of the existing literatures answers it in quantifiable measures based on a solid analysis.

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

Motivated by the above questions, a Correlation ATtack (CAT) is presented in this work to show the potential vulnerability of link signatures and associated security schemes. 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. The contributions of this work are: 1) the proposed CAT shows that the adversary can exploit the spatial channel correlation more effectively, through both collaborative sensing and statistical inference, to estimate the legitimate link signature in much higher accuracy than pure observation; 2) the effectiveness of CAT is verified both through theoretical analysis and well-known wireless channel models; 3) practical experiments using USRP platforms and GNURadio are conducted to support the theoretical analysis, and the corresponding results shed lights on the environment characteristics that may lead to link signature vulnerability.

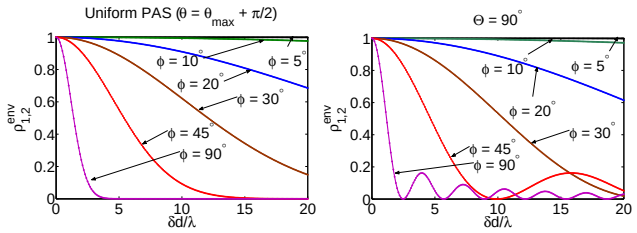
II. Potential Vulnerability of Link Signature

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] and mainly consider the fading envelope $|h|$, which is a common practice in literature (e.g., [6, 7, 13]). Our study can be naturally extended to the more general link signatures. The envelope correlation coefficient between two channels is defined as

$$\rho_{1,2}^{env} \triangleq \frac{E\left[|h_1||h_2|\right] - E\left[|h_1|\right] E\left[|h_2|\right]}{\sqrt{\mathrm{Var}(|\mathrm{h}_1|)\mathrm{Var}(|\mathrm{h}_2|)}}. \quad (1)$$

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) $p(\theta)$. For example, the AS corresponding to a uniform PAS spreading out in an angular range of ϕ is given by $\Delta = \sqrt{\phi^2 - 2 + 2\cos\phi}/\phi$ [9]. In particular, Durgin and Rappaport model the channel envelope correlation coefficient $\rho_{1,2}^{env}$ of two receivers aligned in direction θ as a function of receiver spatial separation δd parameterized by the AS Δ in the following form:



(a) The Durgin-Rappaport's model (b) The one-ring model

Fig. 1. Channel envelope correlation v.s. receiver separation.

$$\rho_{1,2}^{env}(\delta d,\theta) \approx \exp\left[-\frac{2\pi^2}{4-\pi}\Delta^2\left[1+\gamma\cos(2(\theta-\theta_{max}))\right]\left(\frac{\delta d}{\lambda}\right)^2\right], \tag{2}$$

where γ and θ_{max} are the angular constriction and the azimuthal direction of maximum fading, respectively [9]. Fig. 1(a) shows how this correlation varies with the receiver separation (normalized with respect to (w.r.t.) the wavelength λ) for different angular spreads for a uniform PAS when $\theta = \theta_{max} + \pi/2$.

Another well-known model for channel correlation is the one-ring model [17, 19], which represents the scenario where one communication end is surrounded by rich scatterers while the other end experiences much less diffusion. The channel envelope correlation coefficient between two receivers separated by δd and aligned in the x-direction (i.e., $\Theta = 90^\circ$ in [17]), when the scatterer ring is on the transmitter side, is given by:

$$\rho_{1,2}^{env}(\delta d) \approx J_0^2\left(2\pi\frac{\phi^2}{16}\frac{\delta d}{\lambda}\right), \tag{3}$$

where $J_0()$ is the zeroth order first kind Bessel function. Fig. 1(b) shows how this correlation varies with the receiver separation for different angular spreads.

As shown in Fig. 1, 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

Most existing link signature schemes rely on the assumption that the channel between the legitimate transmitter (t) and the adversary receiver (a), $|h_{t,a}|$, 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 from the legitimate receiver. However, as shown in the above subsection, both well-known channel models and real-world experiments indicate 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.

III. Link Signature Forging

A. Theoretical Analysis

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, based on which they construct an estimate $|\hat{h}_{t,r}|$ of $|h_{t,r}|$ through linear minimum mean square error (LMMSE) estimation [20] for link signature forging.

Proposition 1: (a) The LMMSE estimate of the legitimate receiver channel based on 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

$$|\hat{h}_{t,r}| = E[|h_{t,r}|] + B^T C^{-1}(|h_{t,a}| - E[|h_{t,a}|]), \tag{4}$$

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. (b) This estimator is always no worse than that based on any subset of $\{|h_{t,a_1}|, ..., |h_{t,a_n}|\}$ with $k(< n)$ adversary channels, in the MSE sense.

Proof: Please see [21]. ■

Remark: A direct consequence of Proposition 1 is that the estimator based on multiple ($n > 1$) adversary channels is always no worse than that based on any single adversary channel ($k = 1$) among them.

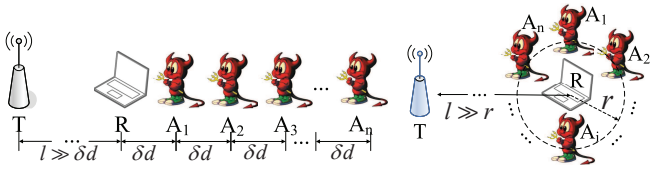
Proposition 2: The MSE of the LMMSE estimate $|\hat{h}_{t,r}|$ is given by $\frac{\det(\Gamma)}{\det(C)}$, where $\Gamma = \left[\begin{smallmatrix} A & B^T \\ B & C \end{smallmatrix}\right]$ and $A_{1\times 1} \triangleq Cov(|h_{t,r}|, |h_{t,r}|) = Var(|h_{t,r}|)$ is the variance of the legitimate receiver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

Proof: Please see [21]. ■

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 corresponding MSE of deploying n adversary receivers is given by $\frac{1+(n-1)a-nb^2}{1+(n-1)a}$.[1]

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



(a) line placement (b) Ring placement

Fig. 3. 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.)

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 $n \to \infty$.

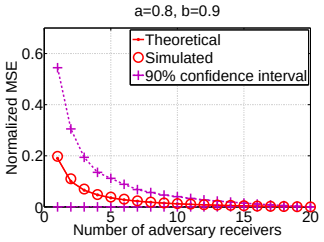


Fig. 2. Normalized MSE comparison of using single and multiple adversary receivers.

Remark: Some interesting observations are in order. 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 $a = 0.8$, $b = 0.9$, $n = 20$ collaborative adversary receivers can achieve perfect inference in theory. We also conduct 10000 Monte Carlo simulations in which $|h_{t,r}|$ and $|h_{t,a}|$ are Rayleigh distributed with the above given correlations. Fig. 2 shows 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 this subsection, we propose 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 (Fig. 3(a)). The corresponding achievable normalized MSE is plotted numerically in Fig. 4 according to Proposition 2 and the one-ring model. As shown in Fig. 4, when the AS is small ($\phi = 20°$), 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.

In the second attack, the Durgin-Rappaport's model is considered, and the adversary receivers are uniformly deployed

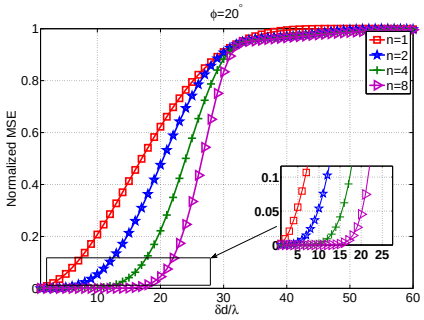


Fig. 4. Achievable normalized MSE of n adversary receivers aligned in a line (based on the one-ring model).

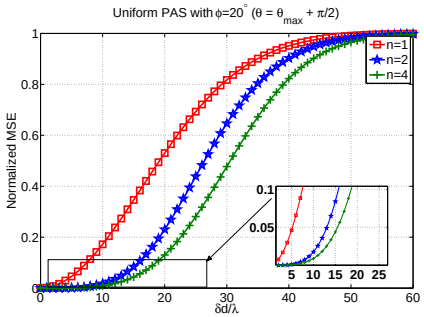


Fig. 5. Achievable normalized MSE of n adversary receivers placed on a ring (based on the Durgin-Rappaport's model).

on a ring with radius r (Fig. 3(b)). As shown in Fig. 5 (plotted according to Corollary 3 of [21] and the Durgin-Rappaport's model), for small AS ($\phi = 20°$), as few as 4 adversary receivers, which may be confined 15 wavelengths away from the legitimate receiver, 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

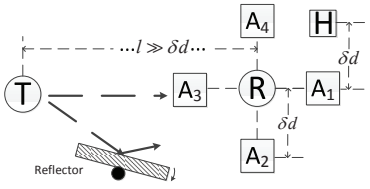


Fig. 6. The experiment setting for $n = 4$. (T: legitimate transmitter, R: legitimate receiver, A_1–A_4: four adversary receivers, H: adversary helper, l: transmission distance.)

In this section, experiments using Universal Software Radio Peripheral (USRP) platforms and GNURadio are conducted to support analytical results and demonstrate the potential vulnerability of the link signature based security mechanisms. The carrier frequency is 2.4 GHz with the corresponding wavelength $\lambda = 12.5$ cm. Two experiments are conducted indoor and a strong LOS component exists. (More experiments can be found in [21].) In experiment I,

$n = 2$ adversary receivers are placed $\delta d = 2\lambda$ away from the legitimate receiver, while $n = 4$ and $\delta d = 6\lambda$ in experiment II. Fig. 6 gives the experiment setting for experiment II, and that for experiment I is similar with A_1 and A_2 only.

A. Measuring Channel Correlation

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 [12]. In our experiments, a flat reflector is deployed nearby, and is 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.[2] Then, the estimate of the channel envelope correlation coefficient between two receivers can be evaluated as $\hat{\rho}_{1,2}^{env} = \sum_{k=1}^K (|h_1^{(k)}| - \hat{\mu}_1)(|h_2^{(k)}| - \hat{\mu}_2)/K\hat{\sigma}_1\hat{\sigma}_2$, where $\hat{\mu}_i = \sum_{k=1}^K |h_i^{(k)}|/K$ and $\hat{\sigma}_i^2 = \sum_{k=1}^K (|h_i^{(k)}| - \hat{\mu}_i)^2/K$. Further, the least square (LS) method is used to obtain the channel estimates [13].

B. Known Statistics

In this subsection, it is assumed that all the required statistics, i.e., C the correlation matrix of adversary channel envelopes, B the correlation vector between adversary channel envelopes and the legitimate receiver channel envelope, and $E[|h_{t,r}|]$ the mean of the legitimate receiver channel envelope, are available for the adversary. This assumption 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 these models are known to match the environment of interest well.

In Fig. 7–8, the link signatures of the legitimate receiver channel, the adversary channels, and the adversary collaboratively estimated channel are shown. For each experiment, $K = 30$ samples are recorded per channel where the variations of channels are caused by the random rotations of the reflector. The corresponding results are summarized in Table I and Table II, where $\hat{\rho}_{A_i,R}$ denotes the estimated envelope correlation coefficient between the channels of the adversary receiver A_i and the legitimate receiver R. Several observations are in order. 1) Strong correlations 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. 2) When channel statistics are known a priori, the adversary can launch CAT and obtain a link signature estimate with normalized RMSE about 10%, as shown in Table II. 3) When the adversaries are confined further away, they can maintain a similar estimation accuracy by increasing the number of adversary receivers. For example, in experiment II where δd is increased to 6λ, when only two adversary receivers A_1 and A_2 are used, the corresponding normalized RMSE is around 17% (not shown in Table II); if all the four adversary receivers are used, the normalized RMSE can be reduced to (11%).

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

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	0.76	0.69	0.70	0.88	/

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	21%	23%	24%	19%	11%	/

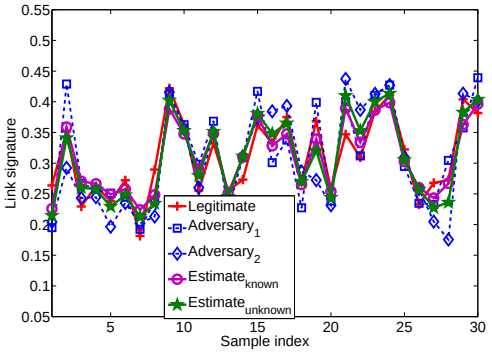


Fig. 7. Forged and true link signatures in experiment I ($n = 2$ and $\delta d \approx 2\lambda$).

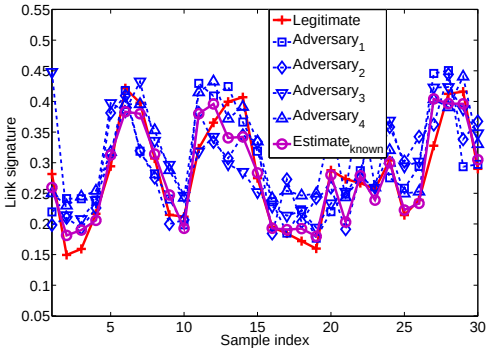


Fig. 8. Forged and true link signatures in experiment II ($n = 4$ and $\delta d \approx 6\lambda$).

C. Unknown Statistics

In the following, it is shown that a simple approximation approach may work for the adversary to launch CAT in certain circumstances even though the statistics are unknown, which is based on two interesting properties observed in the first experiment (conducted in an office): 1) The correlation coefficients $\hat{\rho}_{A_i,R}$'s 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 (Fig. 6), is also close to $\hat{\rho}_{A_i,R}$'s. This implies that, in this experiment, the spatial correlation between two receivers is mainly determined by their spatial separation δd but not

TABLE III
COMPARISON OF THE SAMPLE MEAN OF CHANNEL ENVELOPES.

	$\hat{\mu}_{\lvert h_{A_1}\rvert}$	$\hat{\mu}_{\lvert h_{A_2}\rvert}$	$\hat{\mu}_{\lvert h_{A_3}\rvert}$	$\hat{\mu}_{\lvert h_{A_4}\rvert}$	$\hat{\mu}_{\lvert h_R\rvert}$
Exp. I	0.31	0.30	/	/	0.31
Exp. II	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	70%	78%	73%	90%	97%	/

sensitive to their absolute positions, which conforms to the two channel models discussed in II-A for fixed AS and to the observations in [12] as well. 2) The sample mean of the legitimate receiver channel envelopes ($\hat{\mu}_{|h_R|}$) is close to those of the adversary receivers ($\hat{\mu}_{|h_{A_i}|}$), as shown in Table III.

In environments with the above two properties, the adversary party can approximate the unknown statistics as $E[|h_R|] \approx \frac{1}{n}\sum_{i=1}^{n}\hat{\mu}_{|h_{A_i}|}$ and $B \approx \hat{\rho}_{A_1,H} \times [\hat{\sigma}^2_{|h_{A_1}|},...,\hat{\sigma}^2_{|h_{A_n}|}]^T$ to launch CAT.[3] With these approximations, the estimated link signature is also shown in Fig. 7 (denoted by star). As summarized in Table II, the estimation accuracy degrades only slightly (1 percentage).

However, it should be admitted that these properties are not universal. As observed in the second experiment that is conducted in a corridor, the correlations are not sufficiently close for different adversary receivers, which, we conjecture, is due to the physical environment asymmetry (but not the increase of δd [21]). In such circumstances, the adversary may rely on the two approaches mentioned in Section IV-B 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 proof-of-concept 2-bit quantization key extractor is used. Table IV shows the percentage of correctly inferred secret bits for the two 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 around 97% of the secret bits.

V. CONCLUSIONS

A correlation attack, which explicitly exploits the channel correlations to recover the legitimate link signature, is proposed to demonstrate the potential vulnerability of the link signature based security mechanisms. Through theoretical analysis and verification with well-known wireless channel models, 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 support the theoretical analysis and lead to two conclusions: 1) significant spatial channel correlation exists and can be exploited by the adversary to forge the legitimate link signature; 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.

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

REFERENCES

[1] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. of ACM WiSec*, 2006.

[2] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: Cooperative proximity-based authentication," in *Proc. of ACM MobiSys*, 2010.

[3] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proc. of ACM MobiCom*, 2007.

[4] J. Zhang, M. Firooz, N. Patwari, and S. Kasera, "Advancing wireless link signatures for location distinction," in *Proc. of ACM MobiCom*, 2008.

[5] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *IEEE Symposium on SP (Oakland)*, 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*, 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*, 2008.

[8] N. Patwari, J. Croft, S. Jana, and S. 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, 2010.

[9] T. Rappaport, *Wireless communications: Principles and practice.* Prentice Hall, 2001.

[10] J. Fuhl, A. Molisch, and E. Bonek, "Unified channel model for mobile radio systems with smart antennas," in *Proc. of IEE Radar, Sonar and Navigation*, 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, 2005.

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

[13] Y. Liu and P. Ning, "Enhanced wireless channel authentication using time-synched link signature," in *Proc. of IEEE INFOCOM-mini*, 2012.

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

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

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

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

[18] A. Goldsmith, *Wireless communications*. Cambridge University Press, 2005.

[19] 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, 2002.

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

[21] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" NC State University, Department of Electrical Engineering, Tech. Rep., 2012, available at http://www4.ncsu.edu/∼hdai/linksignature.pdf.