

Fundamental Limits of Passive Attacks on Wireless Link Signatures

Xiaofan He, Huaiyu Dai, Peng Ning

Abstract

The goal of this technical report is to gain a fundamental understanding of the potential vulnerability of existing wireless link schemes subject to passive eavesdropping and inference. From the adversary's perspective, the feasibility and fundamental limit of this new attack is explored. In addition, how the theoretical results are instantiated in various channel models and how the different adversary sensor deployments affect the inference accuracy are also studied for practical interests. Preliminary theoretical study reveals that a high-fidelity estimate of the desired signal is indeed feasible, provided the spatial correlation among the legitimate receiver and sensors satisfies certain conditions.

I. INTRODUCTION

The security of link signature relies on the uniqueness of the the sender-to-receiver channel impulse response. Single attacker may have difficulty in emulating the sender-to-receiver channel due to the spatial de-correlation between the channel she measured, i.e., sender-to-attacker channel, and the sender-to-receiver channel. Does it imply the link signature is secure enough? To answer this question, it is worth exploring beyond the single attack case, which is the interest of this research work. In particular, the vulnerability of link signature under *multiple* attackers will be explored. Specifically, n attackers deployed around the receiver will measure the channels between themselves and the sender, and then based on this set of measured channels they collaboratively estimate the sender-to-receiver channel in order to launch effective attack to link signature authentication. Preliminary theoretical study in this technical report will answer the following fundamental questions: 1) Would multiple attackers be able to obtain more accurate sender-to-receiver channel estimate than single attacker? 2) To what level of accuracy can be achieved by multiple attackers?

The rest of this technical report is organized as follows. Section II briefly reviews the physical models for channel correlation. Section III presents the capability of obtaining high accurate channel inference of multiple cooperative attackers. Section IV instantiates the theoretical results in the physical model. Section V concludes the paper.

II. CHANNEL CORRELATION MODEL

In literature, extensive studies had been done for channel correlation due to physical factors such as multipath propagation and fading. The one-ring model was first introduced in [17] [14] and widely explored in later works such as [13] [20] [26] for multiple antennas systems.

The power azimuth spectrum (PAS) is an important factors characterizing the evolution of the channel correlation as a function of the normalized antenna distance. In literature, several types of PAS are widely used. A PAS with $\cos^n(\varphi)$ function is proposed in [17]; the uniform PAS was discussed in [24]; truncated normally distributed PAS was proposed in [2]; Gaussian PAS was also studied in [7]; the von-Mises PAS was used in [1]; the multimodal truncated Laplacian PAS was explored in [25].

In the one-ring model, it is assumed that the angle of arrival (AoA) uniquely determines the angle of departure (AoD) and thus also known as “non-Kronecker” model [34]. “single-Kronecker” model is also used in literature such as [31] [4]. In the “single-Kronecker” model, the AoA and the AoD is assumed to be loosely correlated or independent such that the normalized MIMO channel covariance matrix can be well approximated by the Kronecker product of the covariance matrices at the transmitter and receiver. To fill the gap between “non-Kronecker” model where AoA and AoD are fully correlated and “single-Kronecker” model where AoA and Aod are loosely correlated, an extend one-ring model was proposed in [34] which allows varying degrees of correlation between AoA and AoD. (Not sure this part is related, because currently we only consider one transmitter.)

A. The One-ring Model

The classical one-ring model is widely used to study the correlation between two channels when one side (either sender or receiver) of the channel is obstructed by rich scatterers. Fig. 1 illustrates the one-ring mode where the ring of scatterers is assumed to be at the transmitter side. Specifically,

- TA_p and TA_q are two transmitter antennas, and RA_m and RA_l are two receiver antennas.
- D is the distance between the transmitter and receiver, and R is the radius of the scatterer ring.
- Θ is the angle of arrive (AoA) at the receiver.
- $S(\theta)$ is the corresponding scatterer located in angle θ .
- Δ is referred to as the angle spread (AS).

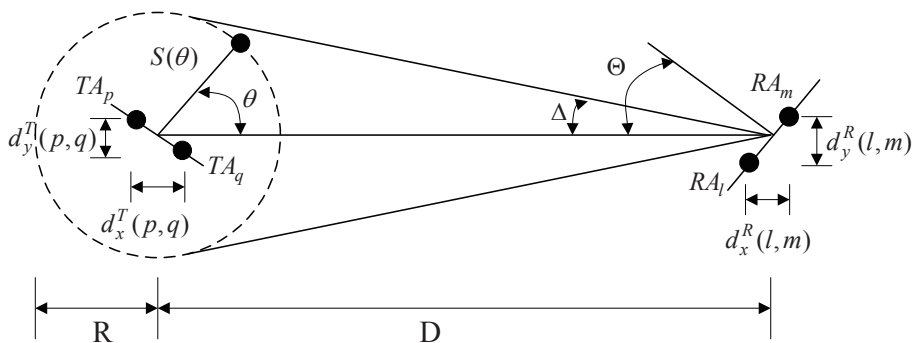


Fig. 1. Illustration of the abstract “one-ring” model.

The “one-ring” model is basically a ray-tracing model. The following assumptions are generally made in this model:

- The channel varies at a rate slow enough.
- It is appropriate in the fixed wireless communication context, where one side is unobstructed by local scatterers and the other side is often surrounded by local scatterers.
- The radius of the scatterer ring R is determined by the root-mean-square (rms) delay spread of the channel.
- Only rays that are reflected by the effective scatterers exactly once are considered.
- All rays that reach the receiving antennas are equal in power.
- Every actual scatterer that lies at an angle to the receiver is represented by a corresponding effective scatterer located at the same angle on the scatterer ring.
- Therefore, rays that are reflected by $S(\theta)$ are all subject to a phase change of $\phi(\theta)$. Statistically, $\phi(\theta)$ is modeled as uniformly distributed in $[-\pi, \pi)$ and i.i.d. in θ .

In particular, suppose that there are K effective scatterers $S(\theta_k)$, then the properly normalized complex path gain connecting transmitting antenna TA_p and receiving antenna RA_l is

$$H_{l,p} = \frac{1}{\sqrt{2\pi}} \int_0^{2\pi} \frac{1}{\sqrt{K}} \sum_{k=1}^K \delta(\theta - \theta_k) \exp \left\{ -j \frac{2\pi}{\lambda} (D_{TA_p \rightarrow S(\theta)} + D_{S(\theta) \rightarrow RA_l}) + j\phi(\theta) \right\} d\theta \quad (1)$$

where $D_{A \rightarrow B}$ denotes the distance between two objects A and B , $\phi(\theta)$, which is assumed to be uniform in $[-\pi, \pi)$ and i.i.d. in θ , is the signal phase change due to the scatter $S(\theta)$. Consequently, by taking the expectation over $\phi(\theta)$ assuming uniform power azimuth spectrum (PAS) and $K \rightarrow \infty$, the covariance between two channels $H_{l,p}$ and $H_{m,q}$ is

$$E[H_{l,p} H_{m,q}^*] = \frac{1}{2\pi} \int_0^{2\pi} \exp \left\{ -j \frac{2\pi}{\lambda} [D_{TA_p \rightarrow S(\theta)} + D_{S(\theta) \rightarrow RA_l} - D_{TA_q \rightarrow S(\theta)} - D_{S(\theta) \rightarrow RA_m}] \right\} d\theta \quad (2)$$

In general, there is no closed-form for the above integral, but when the AS is small, i.e., $\Delta \approx \frac{R}{D}$, an approximation exists.

$$\begin{aligned} E[H_{l,p} H_{m,q}^*] &= \frac{1}{2\pi} \int_0^{2\pi} \exp \left\{ -j \frac{2\pi}{\lambda} [D_{TA_p \rightarrow S(\theta)} + D_{S(\theta) \rightarrow RA_l} - D_{TA_q \rightarrow S(\theta)} - D_{S(\theta) \rightarrow RA_m}] \right\} d\theta \\ &\approx \frac{1}{2\pi} \int_0^{2\pi} \exp \left\{ -j \frac{2\pi}{\lambda} \left[d_x^T(p, q) \cdot \left(1 - \frac{\Delta^2}{4} + \frac{\Delta^2 \cos 2\theta}{4} \right) \right. \right. \\ &\quad \left. \left. + \Delta d_y^T(p, q) \sin \theta + d_x^R(l, m) \sin \theta + d_y^R(l, m) \cos \theta \right] \right\} d\theta \end{aligned} \quad (3)$$

If only one transmitter with single antenna is considered, for example TA_p , and think of RA_l as the receiver and RA_m as an attacker, then the correlation between sender-to-receiver channel $H_{s,r}$ and sender-to-attacker channel $H_{s,a}$ where the sender is surrounded by scatters and the attacker and receiver are in the x-axis can be approximated as

$$E[H_{s,r} H_{s,a}^*] = e^{-j(2\pi/\lambda)d_x(r,a)(1-\Delta^2/4)} J_0 \left(\left(\frac{\Delta}{2} \right)^2 \frac{2\pi}{\lambda} d_x(r, a) \right) \quad (4)$$

where $d_x(r, a)$ is the distance between receiver and attacker. It can be seen from (4) that two channel will de-correlated very slowly if AS is small. Fig. 2–4 show how the relation between channel correlation varies with respect to AS and AoD.

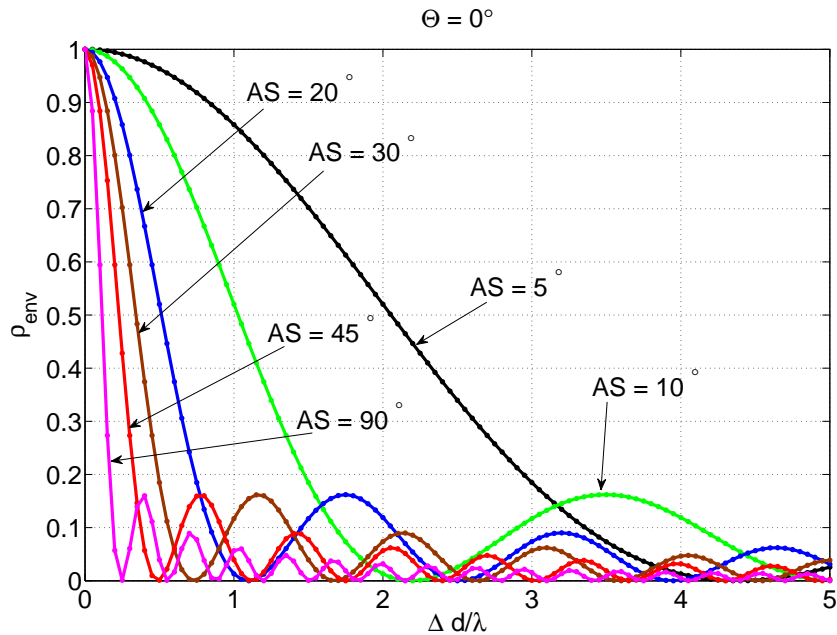


Fig. 2. Envelope correlation for AoD $\Theta = 0^\circ$ with different AS.

B. Correlation of Channel Envelope

The one-ring model characterizes the correlation $\rho_{complex}(h_1(t), h_2^*(t))$ of two channels impulse responses $h_1(t)$ and $h_2(t)$. In literature, the amplitude of the channel impulse response $|h(t)|$ is also usually used [19] [18]. To qualify the correlation of the amplitude of two channels $\rho_{env}(|h_1(t)|, |h_2(t)|)$, [15] [16] show the following:

$$\rho_{env}(|h_1(t)|, |h_2(t)|) \approx |\rho_{complex}(h_1(t), h_2^*(t))|^2 \quad (5)$$

C. Extension of One-ring Model

The one-ring model applies to the situation where only one side of the channel is surrounded by scatterers. Two-ring models are explored to characterize the communication channels where both sides of the channel are surrounded by scatterers. To avoid the technical difficulties of the double-bounced two-ring model [8] [9] as discussed in [32], single-bounced two-ring model was proposed in [30], which was further extended to mobile-to-mobile case in [3].

D. Other Related Channel Model

The Saleh-Valenzuela model was proposed in [23] for wideband SISO multipath indoor scenario on the basis of the indoor measurements, and further extended to MIMO systems in [29].

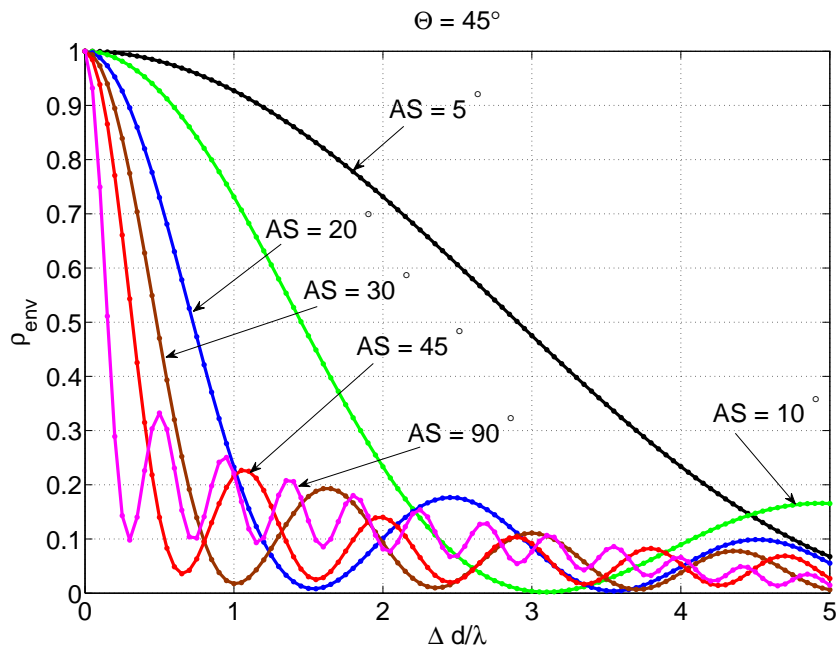


Fig. 3. Envelope correlation for AoD $\Theta = 45^\circ$ with different AS.

E. Shadow Fading

The well known statistic model of shadow fading is the lognormal distribution. The autocorrelation of the shadow fading of a certain channel at different time instances is well studied in [12] where an exponential autocorrelation function was proposed. The cross-correlation of the shadow fading between two links is of our interests. A suitable cross-correlation model was proposed in [10] based on the preliminary work in [28]. Further, it was pointed out in [33] that the cross-correlation mainly depends on two factors: 1) the angle from which the mobile user sees the two base stations; 2) the ratio between the distance from the mobile to each station. In [11], a general correlation model for shadow fading was proposed to includes both autocorrelation and cross-correlation features.

In [27], a protocol of how to use shadow fading to generate secret key was developed.

In [22] [21], the cross-correlation of links due to shadow fading in multi-hop network was explored. In particular, the shadow fading is model by a function of underlying shadowing field.

III. ESTIMATE THE CHANNEL USING MULTIPLE SENSORS

In this section, the following two substantial results will be shown:

- Multiple attackers can obtain more accurate sender-to-receiver channel estimate, i.e., the link signature authentication is more vulnerable under multiple attackers;
- Under certain conditions, multiple attackers can obtain perfect sender-to-receiver channel estimate, i.e., the mean-square-error (MSE) of the estimate is zero. This implies that, the current link signature authentication method cannot work at all in these situations.

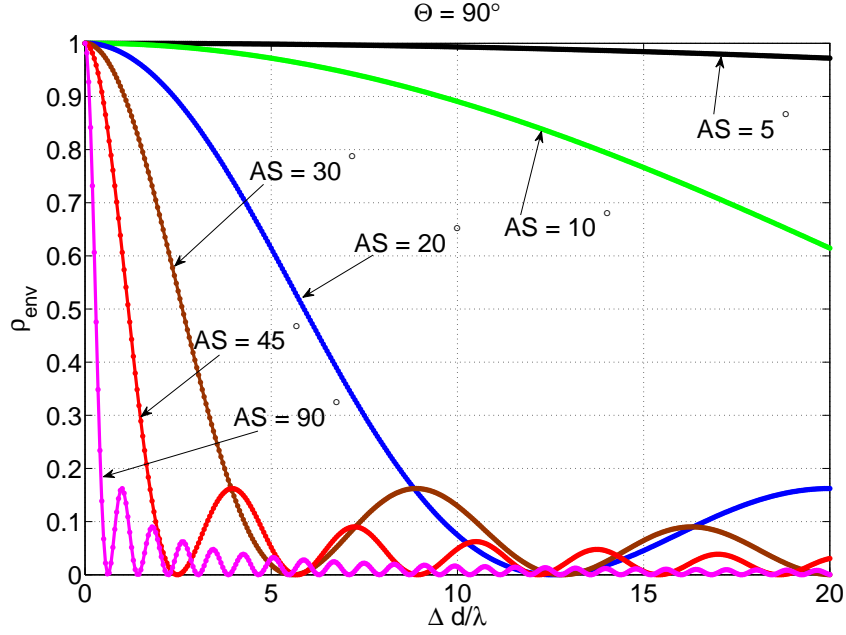


Fig. 4. Envelope correlation for AoD $\Theta = 90^\circ$ with different AS.

First, the fact that multiple attackers always have a more accurate sender-to-receiver channel estimate than single attacker is shown. Denote the sender-to-receiver channel at time t as a random variable X , and the sender-to-attacker $_i$ channel at time t as Y_i . In addition, assume that the covariance between any of these random variables are known because the covariance can be derived from the physical models that will be introduced in next section. The following proposition will show that the estimate of the sender-to-receiver channel $H_{s,r}$ based on n attackers' channel measurements H_{s,a_i} 's is always smaller than that based on single attacker's channel measurement H_{s,a_i} .

Proposition 1: The linear channel estimator $\hat{H}_{s,r}$ based on multiple channel measurements $H_{s,a} = [H_{s,a_1}, H_{s,a_2}, \dots, H_{s,a_n}]^T$ from $n(\geq 1)$ attackers is always no worse than the estimator based on single attacker channel measurement in terms of MSE. In particular, let $C_{n \times n} = Cov(H_{s,a}, H_{s,a})$ and $B_{n \times 1} = Cov(H_{s,r}, H_{s,a})$ be the covariance matrix of attacker measured channels and the covariance vector of the sender-to-receiver channel and attacker measured channels, respectively. Then, the linear minimum mean square error (LMMSE) estimator $\hat{H}_{s,r}$ is given by

$$\hat{H}_{s,r} = E[H_{s,r}] + \xi^T (H_{s,a} - E[H_{s,a}]) \quad (6)$$

where ξ is the coefficient vector of the estimator that satisfies

$$C\xi = B \quad (7)$$

Proof: According to the orthogonality principle, it is straightforward to show (7) holds. Now, it is going to be shown that the estimator based on multiple measurements is no worse than that based on a single measurement.

Without lose of generality, let $X = H_{s,r} - E[H_{s,r}]$, $Y_i = H_{s,a_i} - E[H_{s,a_i}]$ and $Y = [Y_1, Y_2, \dots, Y_n]^T$, and consequently $E(X) = 0$ and $E(X^2) = 1$, and $E(Y_i) = 0$ and $E(Y_i^2) = 1$ ($i = 1, \dots, n$).¹ It is clear that, the covariance matrices corresponding to $H_{s,r}$ and $H_{s,a}$ are identical to those corresponding to X and Y . That is, $Cov(Y, Y) = C_{n \times n}$ and $Cov(X, Y) = B_{n \times 1}$. As a consequence, the coefficient vector of the estimator of X is identical to ξ , the estimator coefficient of $H_{s,r}$, and accordingly, the estimator of X is given by

$$\hat{X}_m = \xi^T Y \quad (8)$$

Similarly, the linear estimator using single measurement is $\hat{X}_s = \varphi Y_1$ where

$$C_{1,1} \varphi = B_1 \quad (9)$$

and $C_{1,1}$ is the variance of Y_1 . From (7) and (9), it can be seen that

$$C_1^{(r)} \xi = C_{1,1} \varphi \quad (10)$$

where $C_1^{(r)}$ is the first row of C and B_1 is the first element of B .²

Since it can be verified that $MSE(\hat{X}) = MSE(\hat{H}_{s,r})$, the following proof will focus on the MSE of \hat{X} . According to (8), the MSE of channel estimator using multiple attackers \hat{X}_m is given as

$$\begin{aligned} MSE_m &= E[(\hat{X}_m - X)^2] \\ &= E[X^2] - Cov(X, Y)^T Cov^{-1}(Y, Y) Cov(X, Y) \\ &= A - B^T C^{-1} B \end{aligned} \quad (11)$$

where $A = 1$ denotes the variance of X . Similarly, the MSE of the channel estimator using single measurement \hat{X}_s is given as

$$\begin{aligned} MSE_s &= E[(\hat{X}_s - X)^2] \\ &= E[X^2] - Cov(X, Y_1) Cov^{-1}(Y_1, Y_1) Cov(X, Y_1) \\ &= A - \frac{B_1^2}{C_{1,1}} \end{aligned} \quad (12)$$

The goal is to prove $MSE_m \leq MSE_s$. This is equivalent to prove $\xi^T C \xi \geq \varphi C_{1,1} \varphi$ considering (7) and (9).

Partition matrix C as $C = \begin{bmatrix} d & E^T \\ E & F \end{bmatrix}$ where $d_{1 \times 1} = Cov(Y_1, Y_1)$, $E_{(n-1) \times 1} = Cov(Y_1, [Y_2, \dots, Y_n]^T)$ and $C_{(n-1) \times (n-1)} = Cov([Y_2, \dots, Y_n]^T)$. Thus, $C_{1,1} = d$ and $C_1^{(r)} = [d \ E^T]$. Considering (10), to prove $\xi^T C \xi \geq \varphi C_{1,1} \varphi$ is equivalent to prove $\xi^T \begin{bmatrix} d & E^T \\ E & F \end{bmatrix} \xi \geq \frac{1}{d} \xi^T \begin{bmatrix} d \\ E \end{bmatrix} \begin{bmatrix} d & E^T \end{bmatrix} \xi$. It can be seen that it is sufficient to prove

¹Here, it is assumed that all the channel powers are normalized.

²Without loss of generality, assume that the first measurement is used.

that $\begin{bmatrix} 0 & 0_{1 \times (n-1)} \\ 0_{(n-1) \times 1} & d \cdot F - EE^T \end{bmatrix}$ is positive semi-definite (PSD), which is equivalent to prove that $d \cdot F - EE^T$ is PSD.

To do so, the eigenvalue decomposition of C is found as $C = \begin{bmatrix} \tilde{u}_1 & \dots & \tilde{u}_n \end{bmatrix} \begin{bmatrix} \lambda_1 & & \\ & \dots & \\ & & \lambda_n \end{bmatrix} \begin{bmatrix} \tilde{u}_1^T \\ \dots \\ \tilde{u}_n^T \end{bmatrix}$ where $\tilde{u}_i = \begin{bmatrix} u_{1,i} \\ u_i \end{bmatrix}$ and $u_i = [u_{2,i}, \dots, u_{n,i}]^T$. Based on this notation, it can be verified that $d = \sum_i \lambda_i u_{1,i} u_{1,i}$, $E = \sum_i \lambda_i u_{1,i} u_i$ and $F = \sum_i \lambda_i u_i u_i^T$. In addition, all $\lambda_i > 0$ because C is PSD and full-rank.

For any vector α ,

$$\begin{aligned} \alpha^T (d \cdot F - EE^T) \alpha &= \alpha^T \left(\sum_i \sum_j \lambda_i \lambda_j u_{1,i} u_{1,i} u_j u_j^T - \sum_i \sum_j \lambda_i \lambda_j u_{1,i} u_{1,j} u_i u_j^T \right) \alpha \\ &= \alpha^T \left(\sum_i \sum_j \tilde{\lambda}_i \tilde{\lambda}_j v_j v_j^T - \sum_i \sum_j \tilde{\lambda}_i \tilde{\lambda}_j v_i v_j^T \right) \alpha \\ &= \sum_i \sum_j \tilde{\lambda}_i \tilde{\lambda}_j \beta_j \beta_j - \sum_i \sum_j \tilde{\lambda}_i \tilde{\lambda}_j \beta_i \beta_j \\ &= \left(\sum_i \tilde{\lambda}_i \right) \left(\sum_j \tilde{\lambda}_j \beta_j^2 \right) - \left(\sum_i \tilde{\lambda}_i \beta_i \right)^2 \\ &\geq 0 \end{aligned} \tag{13}$$

where $v_i = \frac{u_i}{u_{1,i}}$, $\tilde{\lambda}_i = \lambda_i u_{1,i}^2 > 0$ and $\beta_i = \alpha^T v_i$ and the last step in (13) is due to the Cauchy-Schwartz inequality.

Therefore, $MSE(\hat{X}_m) \leq MSE(\hat{X}_s)$ for \hat{X} and so is $\hat{H}_{s,r}$. \blacksquare

Proposition 2: The MSE of \hat{X} based on measurements Y , which is identical to the MSE of $\hat{H}_{s,r}$, is given by $\frac{\det(\Gamma)}{\det(C)}$ where $\Gamma = Cov\left(\begin{bmatrix} X \\ Y \end{bmatrix}, \begin{bmatrix} X \\ Y \end{bmatrix}\right) = \begin{bmatrix} A & B^T \\ B & C \end{bmatrix}$, where $A_{1 \times 1} = Cov(X) = 1$, $B_{n \times 1} = Cov(X, Y)$ and $C_{n \times n} = Cov(Y)$.

Proof: Let $\tilde{\Gamma} = \begin{bmatrix} C & B \\ B^T & A \end{bmatrix}$ and $S = A - B^T C^{-1} B$ be the Schur complement of $\tilde{\Gamma}$. Then,

$$\begin{aligned} MSE(\hat{X}) &= E \left[(\hat{X} - X)^2 \right] \\ &= A - B^T C^{-1} B \\ &= \det(A - B^T C^{-1} B) \\ &= \det(S) \\ &= \frac{\det(\tilde{\Gamma})}{\det(C)} \\ &= \frac{\det(\Gamma)}{\det(C)} \end{aligned} \tag{14}$$

Proposition 3: If the correlation between any two sensors (either attacker or receiver) with displacement vector d is $f(|d|)$, i.e., omnidirectional channel correlation model, and all the attackers are uniformly deployed around the receiver on a circle with radius r , then the MSE that can be achieved by deploying n attackers is given by

$$MSE_n = 1 - \frac{n \cdot f^2(r)}{\sum_{k=0}^{n-1} f(2r \cdot \sin(\frac{\pi k}{n}))} \quad (15)$$

Proof: In this setting, the channel correlation between the sender-to-receiver channel and sender-to-attacker channel is $f(r)$, and the correlation between the channels measured by the i th and j th attackers is $f(2r \cdot \sin(\frac{\pi|i-j|}{n}))$. Denote $f(r)$ by b and $f(2r \cdot \sin(\frac{\pi k}{n}))$ by $g(k)$, respectively, then the determinant of Γ is given by

$$\begin{aligned} \det(\Gamma) &= \left| \begin{array}{cccccc} 1 & b & b & \cdots & \cdots & b \\ b & 1 & g(1) & \cdots & \cdots & g(n-1) \\ b & g(n-1) & 1 & g(1) & \cdots & g(n-2) \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \cdots & \ddots & \vdots \\ b & g(1) & g(2) & \cdots & g(n-1) & 1 \end{array} \right|_{(n+1) \times (n+1)} \\ &= \left| \begin{array}{cccccc} 1 & b & b & \cdots & \cdots & b \\ 0 & 1-b^2 & g(1)-b^2 & \cdots & \cdots & g(n-1)-b^2 \\ 0 & g(n-1)-b^2 & 1-b^2 & g(1)-b^2 & \cdots & g(n-2)-b^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \cdots & \ddots & \vdots \\ 0 & g(1)-b^2 & g(2)-b^2 & \cdots & g(n-1)-b^2 & 1-b^2 \end{array} \right|_{(n+1) \times (n+1)} \\ &= \left| \begin{array}{cccccc} 1-b^2 & g(1)-b^2 & \cdots & \cdots & g(n-1)-b^2 \\ g(n-1)-b^2 & 1-b^2 & g(1)-b^2 & \cdots & g(n-2)-b^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \cdots & \ddots & \vdots \\ g(1)-b^2 & g(2)-b^2 & \cdots & g(n-1)-b^2 & 1-b^2 \end{array} \right|_{n \times n} \\ &= \prod_{i=0}^{n-1} (c_0 + c_1 \omega_i^1 + \cdots + c_{n-1} \omega_i^{n-1}) \quad (16) \end{aligned}$$

where $\omega_k = \exp(j\frac{2\pi k}{n})$, i.e., the n th roots of unity, and $c_0 = 1 - b^2$ and $c_i = g(n - i) - b^2$ for $i > 0$. The last step of (16) is due to the property of circulant matrix [5]. Similarly, the determinant of C is given by

$$\det(C) = \prod_{i=0}^{n-1} (c'_0 + c'_1 \omega_i^1 + \cdots + c'_{n-1} \omega_i^{n-1}) \quad (17)$$

where $c'_0 = 1$ and $c'_i = g(n - i)$ for $i > 0$. According to (14), the MSE of using n attackers is given by

$$\begin{aligned} MSE_n &= \frac{\det(\Gamma)}{\det(C)} \\ &= \prod_{i=0}^{n-1} \left[\frac{c_0 + c_1 \omega_i^1 + \cdots + c_{n-1} \omega_i^{n-1}}{c'_0 + c'_1 \omega_i^1 + \cdots + c'_{n-1} \omega_i^{n-1}} \right] \\ &= \prod_{i=0}^{n-1} \left[\frac{c'_0 + c'_1 \omega_i^1 + \cdots + c'_{n-1} \omega_i^{n-1} - b^2 \sum_{k=0}^{n-1} \omega_i^k}{c'_0 + c'_1 \omega_i^1 + \cdots + c'_{n-1} \omega_i^{n-1}} \right] \\ &= \frac{c'_0 + c'_1 + \cdots + c'_{n-1} - n \cdot b^2}{c'_0 + c'_1 + \cdots + c'_{n-1}} \\ &= 1 - \frac{n \cdot f^2(r)}{\sum_{k=0}^{n-1} f(2R \cdot \sin(\frac{\pi k}{n}))} \end{aligned} \quad (18)$$

where the second last equality is due to the fact that $\sum_{k=0}^{n-1} \omega_i^k = \delta(i)$. ■

Corollary 1: In order to show more insight about how the correlation between receiver and attacker and the correlation between any two attackers affects the MSE of multiple attacker channel estimation, a special theoretical model is considered. Assume that the correlation between any attacker to the receiver is b and the correlation between any two attackers is a . Then, the resulting MSE of using n attackers is given by $\frac{1+(n-1)a-nb^2}{1+(n-1)a}$.³

Proof: In this special case, the determinant of Γ is

$$\det(\Gamma) = \begin{vmatrix} 1 & b & b & \cdots & b \\ b & 1 & a & \cdots & a \\ b & a & 1 & \cdots & a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b & a & \cdots & a & 1 \end{vmatrix}_{(n+1) \times (n+1)} \quad (19)$$

Mathematically, this is a special case of (15) and thus the corresponding MSE of n attackers can be obtained by substituting $f(r) = b$ and $f(2r \sin(\frac{\pi k}{n})) = a$ ($k = 1, \dots, n - 1$) into (15). The resulting expression is $MSE = \frac{\det(\Gamma)}{\det(C)} = \frac{1+(n-1)a-nb^2}{1+(n-1)a}$. ■

Corollary 2: If $a \leq b^2$, then $\exists n = \frac{1-a}{b^2-a}$, s.t., the MSE of using n attackers is zero. If $a > b^2$, the limits of MSE is $\frac{a-b^2}{a}$ as $n \rightarrow \infty$.

³The covariance matrix Γ exists (or it is positive-definite) iff $1 + (n - 1)a - nb^2 > 0$. Therefore, the MSE is always no less than zero.

For example, when $a = 0.05$, and $b = 0.3$, the minimum number of attackers required for zero MSE is about 24. However, when $a = 0$, i.e., the measured channels from any two attackers are uncorrelated, and $b = 0.5$, only 4 attackers are able to achieve zero MSE. That is, from the attacker's perspective, small a , i.e., less correlation between attacker measured channels, and large b , i.e., strong correlation between attacker measured channel and receiver measured channel, are preferred.

IV. SIMULATION RESULTS

A. A Toy Example

Fig. 5–Fig. 7 show how the MSE is affected by the correlation between attacker and receiver b and that between any two attackers a based on Corollary 1. All the simulated values are based on 10000 Monte Carlo runs. In

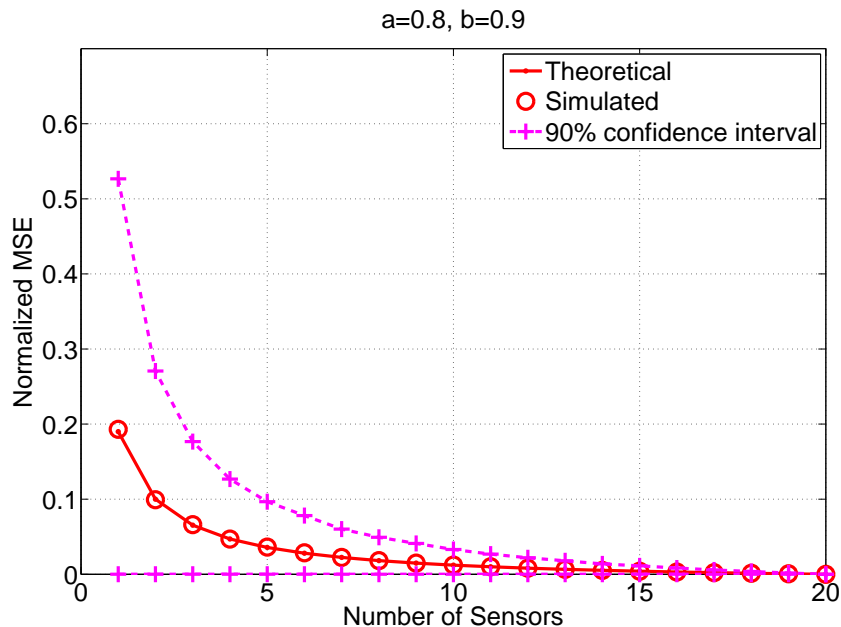


Fig. 5. MSE comparison of using single and multiple attackers.

Fig. 5, the condition $a < b^2$ is satisfied and thus by using multiple attackers the MSE can be reduced to nearly zero as the number of attackers increases.⁴ In Fig. 6, since $a = b^2$, more than 20 (infinite number of) attackers are required to reduce the MSE to zero. In Fig. 7, since a is larger than b^2 , then according to Corollary 1, no matter how many attackers are used, the MSE can never be reduced to zero, but instead a limit exist, which is about 0.05 in this case.

⁴Due to the roundoff problem, i.e., n can only take integer value, the MSE cannot be exactly zero.

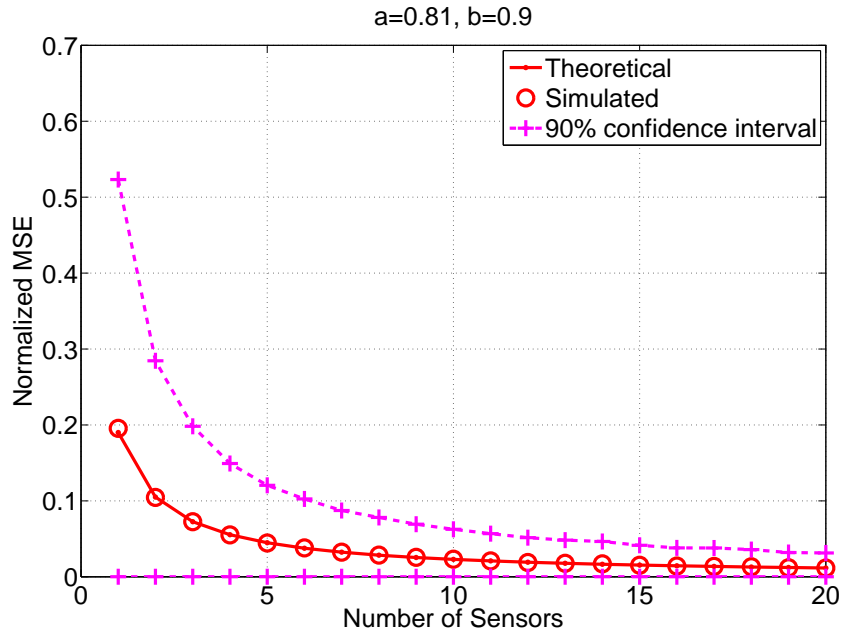


Fig. 6. MSE comparison of using single and multiple attackers.

B. One-ring Model & Attackers Along x -direction

In this section, the sender-to-receiver channel estimation results of single and multiple attackers will be shown. The one-ring model is used to characterize the channel correlation assuming that the scatters is on the sender side. In addition, the attackers are equal-spaced deployed along the x -axis, i.e., in the sender-to-receiver direction. Assume the distance between two adjacent attackers is Δd (wavelength), and the nearest attacker of the receiver is also with distance Δd as show in Fig. 8. The corresponding simulation result of sender-to-receiver channel estimation based on the sender-to-attacker channel measurements are shown in Fig. 9 and Fig. 10. Further, the variance of the sender-to-receiver channel is assumed to be unity.

As shown in Fig. 9 and Fig. 10, it can be seen that the MSE of channel estimation of single attacker is high (about 0.42 and 0.63). However, the MSE of multiple attackers is about 0 in Fig. 9 and 0.04 in Fig. 10. The MSE of the second case is a little bit higher is because the distance of the attackers to receivers are larger, but in both case, multiple attackers achieve much better MSE than single attacker. The low MSE implies that multiple attackers is able to launch effective attacker to link signature authentication. Fig. 11 and Fig. 12 show similar simulation but with smaller AS (5°) and larger Δd (60 wavelengths and 80 wavelengths). As the results show, a smaller AS allows larger Δd while achieves similar MSE performance. That is, smaller AS implies slower channel de-correlation between receiver and attacker and thus less secure.

Fig. 13 and Fig. 14 show the relation between the nearest attacker to receiver distance Δd and the MSE of channel estimation of multiple attackers. As shown in these figures, the further away the attacker is from the receiver, the

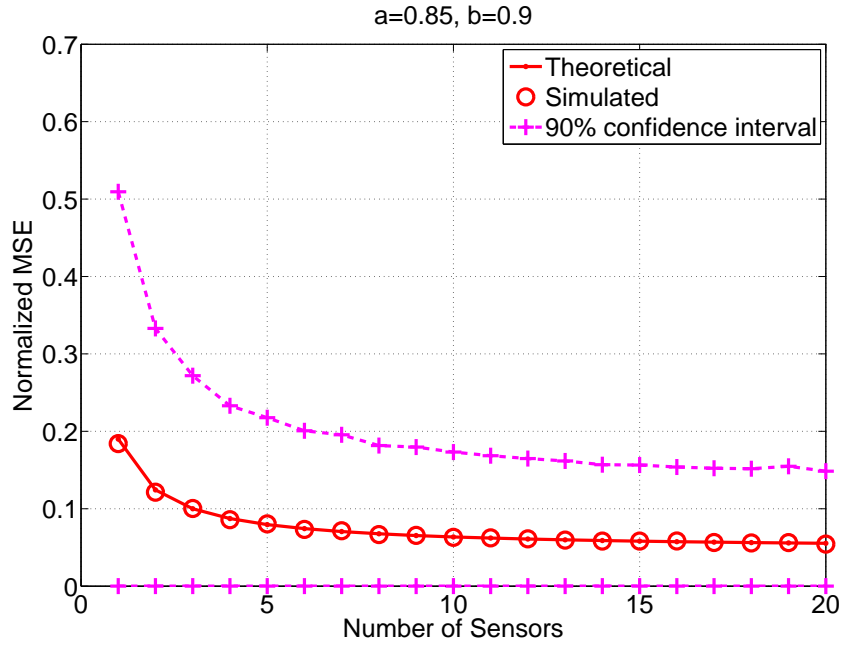


Fig. 7. MSE comparison of using single and multiple attackers.

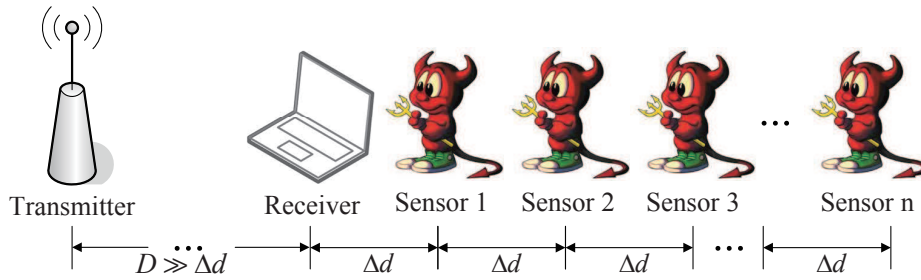


Fig. 8. Attackers along x-direction.

larger MSE is and thus more secure the system is. Therefore, from defense point of view, it is always better to put larger protection region around the receiver to prevent the attacker to be too close to the receiver. However, as shown in the figure, by using multiple attackers, it is always possible to achieve better MSE than single attacker. For example, assume a MSE larger than 0.05 is worse enough to have the link signature authentication being secure. As indicated in Fig. 13, if AS is 5° , to prevent single attacker, the receiver needs a protection region with radius about 20 wavelength, which is approximately 6.7(m) for 900MHz signal, however, to prevent multiple, e.g., 8 attackers, the protection region needs to be extended to about 80 wavelength, which is approximately 26.7(m) for 900MHz signal.

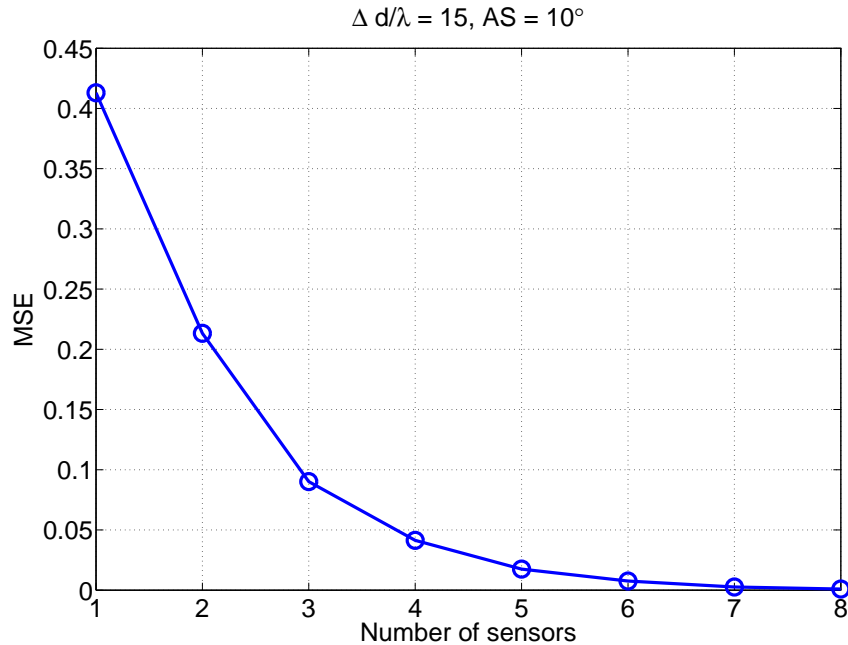


Fig. 9. MSE of channel estimation.

C. Isotropic Slow De-correlation Model

The one-ring model indicates that the slow de-correlation occurs in the sender-to-receiver direction. However, as shown in [6], the slow de-correlation occurs in all direction. Therefore, it is also to explore the MSE under isotropic slow de-correlation models. This is like to be occurred when the line-of-sight component exist. In particular, the correlation in x-direction obtained by the one-ring model is $J_0^2 \left(\left(\frac{\Delta}{2} \right)^2 \frac{2\pi}{\lambda} d_x(r, a) \right)$ according to (4) and (5). In isotropic case, it may be reasonable to conjecture that the correlation between two receivers with distance d is $J_0^2 \left(\left(\frac{\Delta}{2} \right)^2 \frac{2\pi}{\lambda} d \right)$. In addition, in this case (15) can be applied. Based on this assumption, the MSE of n circulant deployed attackers are shown in Fig. 15–Fig. 18. Fig. 19 and Fig. 20 show the relation between MSE and AS. Similar conclusion can be drawn as in previous subsection. *However, the difference is that in the isotropic circulant case, there would be no more MSE improvement when the number of attackers exceeds 5.*

V. CONCLUSIONS

In this technical report, two fundamental conclusions with respect to the existing link signature authentication are drawn: 1) Multiple attackers can obtain more accurate sender-to-receiver channel estimate, i.e., the link signature authentication is more vulnerable under multiple attackers; 2) Under certain conditions, multiple attackers can obtain perfect sender-to-receiver channel estimate, i.e., the mean-square-error (MSE) of the estimate is zero. This implies that, the current link signature authentication method cannot work at all in these situations. Simulation results justify the theoretical derivations. Future works include: 1) enrich and extend our channel modeling to include other important physical factors that are currently ignored; 2) explore the practical designs the adversary can take to

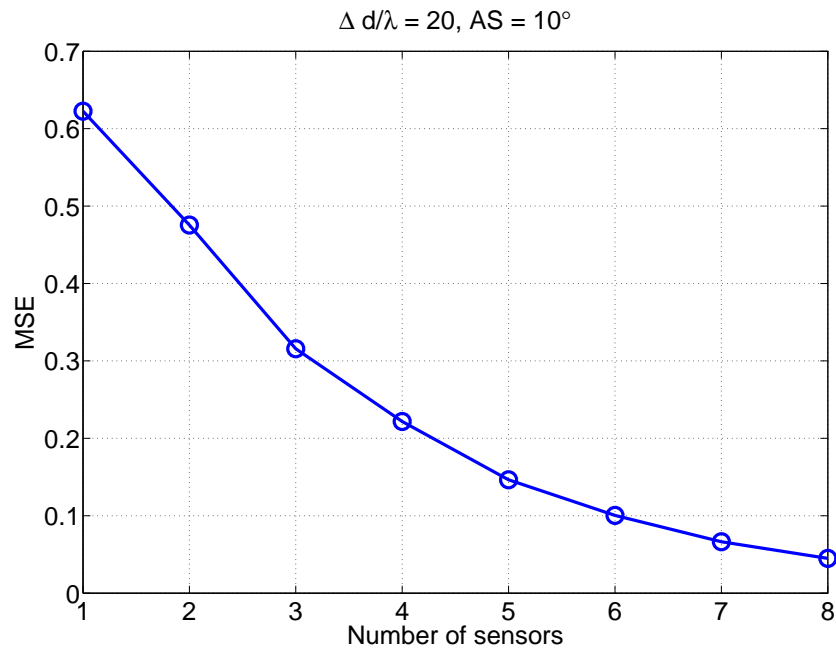


Fig. 10. MSE of channel estimation.

approximate the theoretical results; 3) explore how is the channel estimate related to the security of wireless link signatures used in different applications.

REFERENCES

- [1] A. Abdi and M. Kaveh. A space-time correlation model for multielement antenna systems in mobile fading channels. *Selected Areas in Communications, IEEE Journal on*, 20(3):550–560, August 2002.
- [2] 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. *Communications, Radar and Signal Processing, IEE Proceedings of*, 133(6):506–512, 1986.
- [3] G. Bakhshi, R. Saadat, and K. Shahtalebi. A modified two-ring reference model for MIMO mobile-to-mobile communication channels. In *Telecommunications, 2008. IST 2008. International Symposium on*, pages 409–413. IEEE, 2008.
- [4] D. Chizhik, J. Ling, P.W. Wolniansky, R.A. Valenzuela, N. Costa, and K. Huber. Multiple-input-multiple-output measurements and modeling in Manhattan. *Selected Areas in Communications, IEEE Journal on*, 21(3):321–331, April 2003.
- [5] P. J. Davis. *Circulant matrices*. Chelsea Pub Co, 1994.
- [6] M. Edman, A. Kiayias, and B. Yener. On passive inference attacks against physical-layer key extraction. In *Proceedings of the Fourth European Workshop on System Security*, pages 8–13. ACM, 2011.
- [7] J. Fuhl, A. F. Molisch, and E. Bonek. Unified channel model for mobile radio systems with smart antennas. In *Radar, Sonar and Navigation, IEE Proceedings of*, volume 145, pages 32–41. IET, August 1998.
- [8] D. Gesbert, H. Bolcskei, D. Gore, and A. Paulraj. MIMO wireless channels: Capacity and performance prediction. In *Global Telecommunications Conference, 2000. GLOBECOM'00. IEEE*, volume 2, pages 1083–1088. IEEE, 2000.
- [9] D. Gesbert, H. Bolcskei, D. A. Gore, and A. J. Paulraj. Outdoor MIMO wireless channels: Models and performance prediction. *Communications, IEEE Transactions on*, 50(12):1926–1934, 2002.
- [10] F. Graziosi, M. Pratesi, M. Ruggieri, and F. Santucci. A multicell model of handover initiation in mobile cellular networks. *Vehicular Technology, IEEE Transactions on*, 48(3):802–814, 1999.

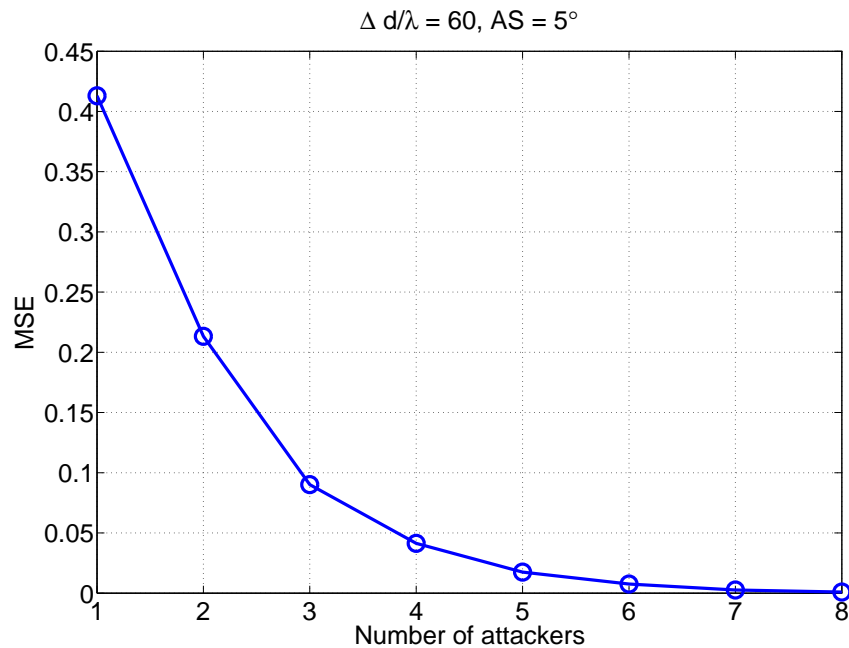


Fig. 11. MSE of channel estimation.

- [11] F. Graziosi and F. Santucci. A general correlation model for shadow fading in mobile radio systems. *Communications Letters, IEEE*, 6(3):102–104, 2002.
- [12] M. Gudmundson. Correlation model for shadow fading in mobile radio systems. *Electronics letters*, 27(23):2145–2146, 1991.
- [13] M. T. Ivrlac, W. Utschick, and J. A. Nossek. Fading correlations in wireless MIMO communication systems. *Selected Areas in Communications, IEEE Journal on*, 21(5):819–828, June 2003.
- [14] W. C. Jakes. *Microwave mobile communications*. New York: Wiley, 1974.
- [15] P. Kyritsi, D. C. Cox, R. A. Valenzuela, and P. W. Wolniansky. Correlation analysis based on MIMO channel measurements in an indoor environment. *Selected Areas in Communications, IEEE Journal on*, 21(5):713–720, June 2003.
- [16] R. O. LaMaire and M. Zorzi. Effect of correlation in diversity systems with Rayleigh fading, shadowing, and power capture. *Selected Areas in Communications, IEEE Journal on*, 14(3):449–460, August 1996.
- [17] W. Lee. Effects on correlation between two mobile radio base-station antennas. *Communications, IEEE Transactions on*, 21(11):1214–1224, November 1973.
- [18] Y. Liu, P. Ning, and H. Dai. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 286–301. IEEE, 2010.
- [19] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 128–139. ACM, 2008.
- [20] A. F. Molisch. *Wireless communications*. Wiley, 2011.
- [21] N. Patwari and P. Agrawal. Effects of correlated shadowing: Connectivity, localization, and RF tomography. In *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on*, pages 82–93. IEEE, 2008.
- [22] N. Patwari and P. Agrawal. Nesh: A joint shadowing model for links in a multi-hop network. In *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, pages 2873–2876. IEEE, 2008.
- [23] A. Saleh and R. Valenzuela. A statistical model for indoor multipath propagation. *Selected Areas in Communications, IEEE Journal on*, 5(2):128–137, 1987.
- [24] J. Salz and J. H. Winters. Effect of fading correlation on adaptive arrays in digital mobile radio. *Vehicular Technology, IEEE Transactions*

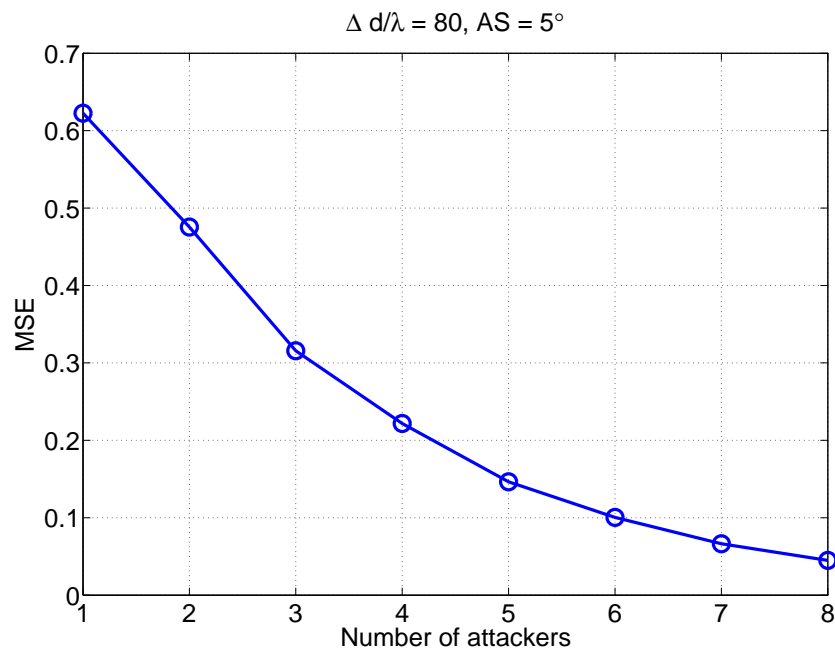


Fig. 12. MSE of channel estimation.

on, 43(4):1049–1057, November 1994.

- [25] L. Schumacher and B. Raghothaman. Closed-form expressions for the correlation coefficient of directive antennas impinged by a multimodal truncated Laplacian PAS. *Wireless Communications, IEEE Transactions on*, 4(4):1351–1359, July 2005.
- [26] 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. *Communications, IEEE Transactions on*, 48(3):502–513, August 2000.
- [27] M.A. Tope and J.C. McEachen. Unconditionally secure communications over fading channels. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE*, volume 1, pages 54–58. IEEE, 2001.
- [28] A.J. Viterbi, A.M. Viterbi, K.S. Gilhousen, and E. Zehavi. Soft handoff extends CDMA cell coverage and increases reverse link capacity. *Selected Areas in Communications, IEEE Journal on*, 12(8):1281–1288, 1994.
- [29] J.W. Wallace and M.A. Jensen. Statistical characteristics of measured MIMO wireless channel data and comparison to conventional models. In *Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th*, volume 2, pages 1078–1082. IEEE, 2001.
- [30] S. Wang, A. Abdi, J. Salo, H. M. El-Sallabi, J. W. Wallace, P. Vainikainen, and M. A. Jensen. Time-varying MIMO channels: parametric statistical modeling and experimental results. *Vehicular Technology, IEEE Transactions on*, 56(4):1949–1963, July 2007.
- [31] K. Yu, M. Bengtsson, B. Ottersten, D. McNamara, P. Karlsson, and M. Beach. Modeling of wide-band MIMO radio channels based on NLoS indoor measurements. *Vehicular Technology, IEEE Transactions on*, 53(3):655–665, May 2004.
- [32] K. Yu and B. Ottersten. Models for MIMO propagation channels: a review. *Wireless Communications and Mobile Computing*, 2(7):653–666, 2002.
- [33] K. Zayana and B. Guisnet. Measurements and modelisation of shadowing cross-correlations between two base-stations. In *Universal Personal Communications, 1998. ICUPC'98. IEEE 1998 International Conference on*, volume 1, pages 101–105. IEEE, 1998.
- [34] M. Zhang, P. J. Smith, and M. Shafi. An extended one-ring MIMO channel model. *Wireless Communications, IEEE Transactions on*, 6(8):2759–2764, August 2007.

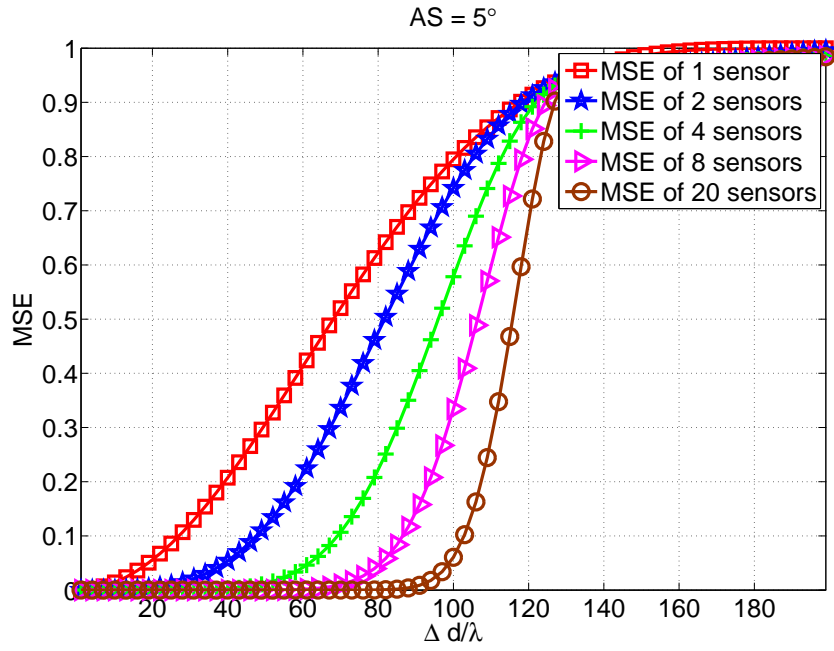


Fig. 13. MSE vs protection distance.

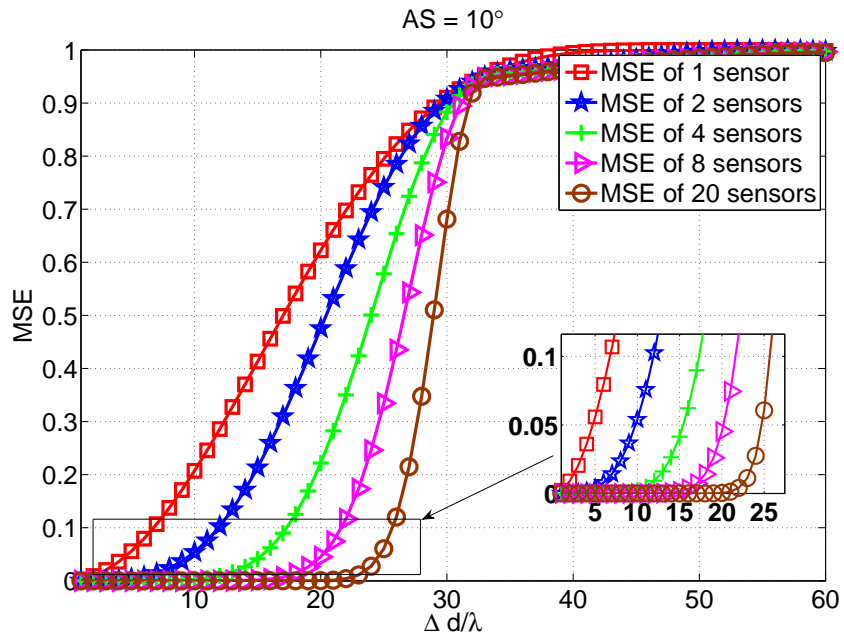


Fig. 14. MSE of protection distance.

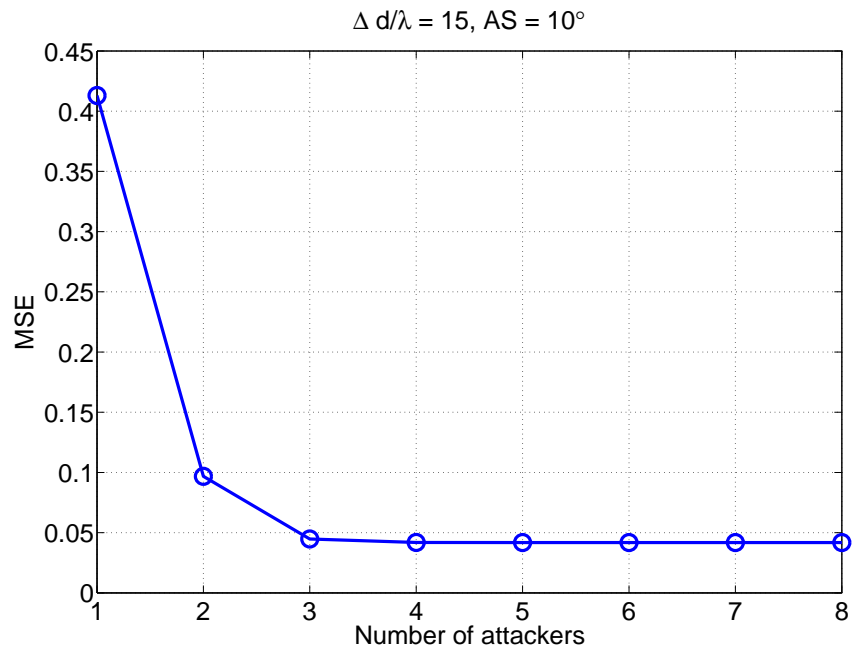


Fig. 15. MSE of channel estimation (isotropic).

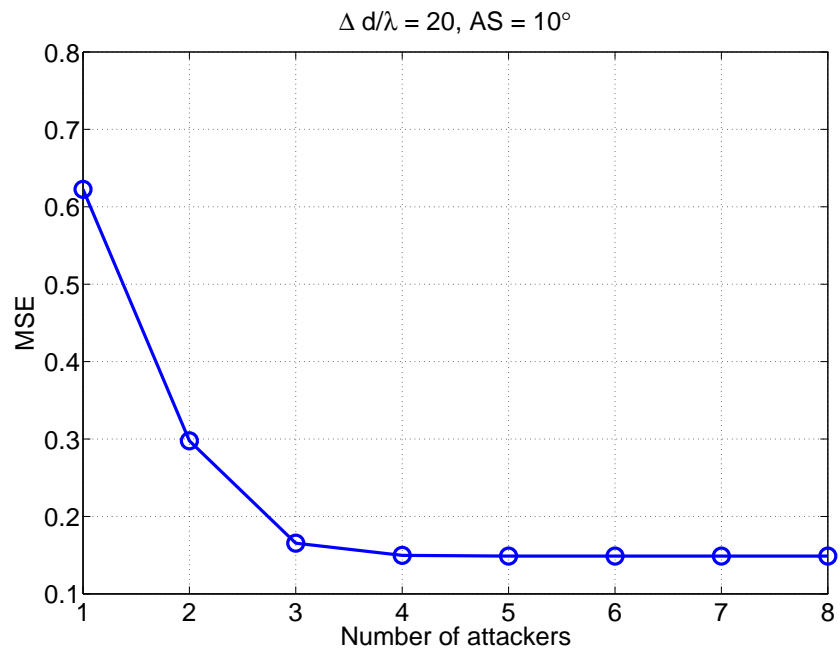


Fig. 16. MSE of channel estimation (isotropic).

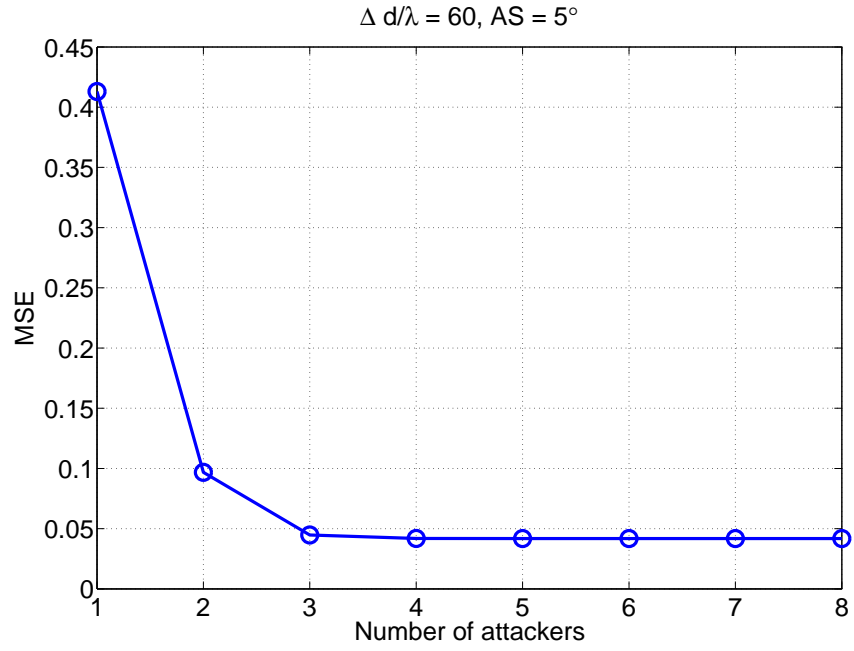


Fig. 17. MSE of channel estimation (isotropic).

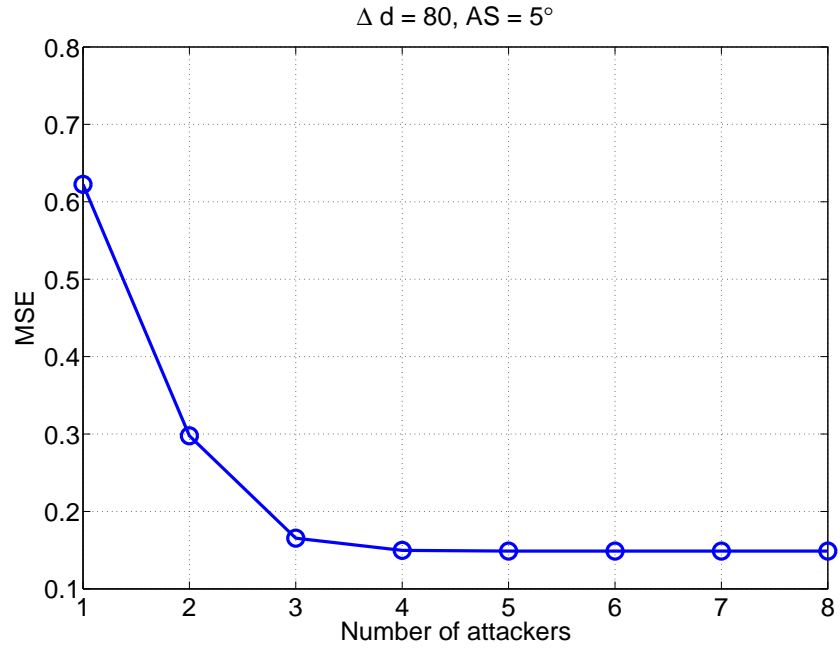


Fig. 18. MSE of channel estimation (isotropic).

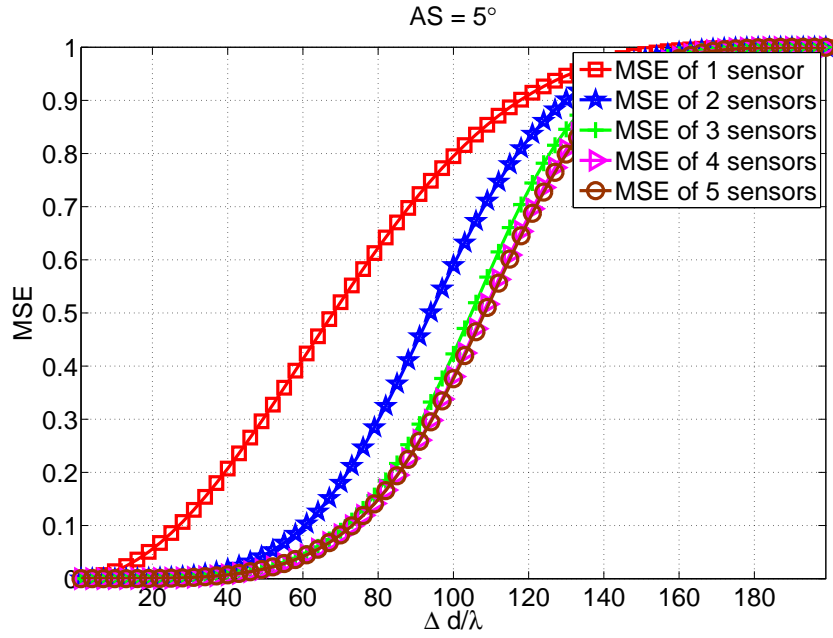


Fig. 19. MSE vs protection distance (isotropic).

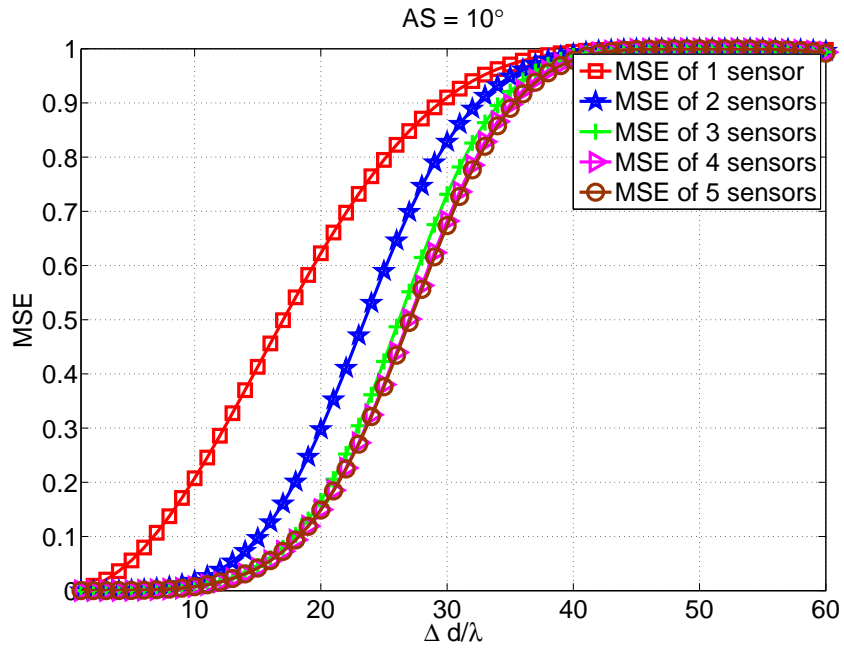


Fig. 20. MSE of protection distance (isotropic).