Towards Proper Guard Zones for Link Signature

Xiaofan He, Student Member, IEEE, Huaiyu Dai, Senior Member, IEEE, Wenbo Shen, Peng Ning, Senior Member, IEEE and Rudra Dutta, Member IEEE

Abstract—Motivated by information-theoretic security, link signature (LS) based security mechanisms exploit the ample channel characteristics between wireless devices for security establishment. Nevertheless, LS is originated from wireless environments and hence may exhibit potential vulnerabilities that can be exploited by adversary in the vicinity. As to this, it is widely believed in existing literature of LS that, a half-wavelength guard zone is sufficient to decorrelate the adversary channel from the legitimate one and thereby secures the legitimate LS. However, such an assumption may not hold universally—in some environments, high channel correlations have been observed for even much larger spatial separations. Considering this, a comprehensive understanding of channel correlation in different wireless environments is needed for more confident deployment of LS based security mechanisms. To this end, various well-established channel correlation models are investigated in this work. A set of important physical factors that have significant influence on LS security are identified, and with the obtained insights, extensive simulations are conducted to explore suitable guard zone sizes for LS in several typical indoor and outdoor environments. Experimental results based on Universal Software Radio Peripheral (USRP) platforms and GNURadio are also presented to further support the analysis.

Keywords: Link signature, channel correlation model, guard zone, physical-layer security.

I. INTRODUCTION

While conventional computational-complexity based cryptography has received great success, there is a haunting concern that building security on the hardness of computing problems is not worry-free, leaving the secrecy of systems vulnerable to the invention of super-power computers or efficient algorithms in the future. This concern has rekindled the interest on information-theoretic security originally considered in [3]. Building upon common randomness rather than the computational hardness, the security established through information-theoretic approaches (e.g., [4–8] and references therein) is free from the concerns about adversary’s computational power. Particularly, it has been shown theoretically that, when two wireless nodes observe a common random process, secret key generation is possible by reconciling errors of the observed sequence over a public channel and distilling information unobservable to the adversary [9, 10].

Motivated by the concepts in information-theoretic security, link signature (LS) based security protocols have been developed recently. The underlying idea is that LS, which refers to the ample channel characteristics between two wireless devices, is nearly reciprocal in many scenarios and hence can serve as the source of common randomness for secret key generation. In [11], a scheme for generating secret bits from correlated observations of deep fades is proposed, with the focus on the theoretical construction for randomness extraction through universal hash families. Later, a practical level-crossing algorithm that extracts secret bits from channel impulse response is developed in [12, 13]. Further extensions of this technique to wideband systems [14], environments with different variations [15] and multi-antenna systems [16] have also been explored in literature. A more comprehensive survey on LS based secret key extraction can be found in [17].

Another prominent application of LS is location distinction (a.k.a. physical layer authentication). Particularly, location distinction based on the received signal strength [18], the channel gains of multi-tonal probes [19] and the multipath characteristics [20] have been considered in literature, and a comparison of these different forms of LS is given in [21].

In [22], a generalized likelihood ratio test based spoofing detection is proposed to further improve location distinction accuracy. Another prominent application of LS is location distinction using MIMO channels has been examined in literature as well [23].

While providing a good complement at the physical layer to security establishment, LS originates from wireless environments and hence may exhibit vulnerabilities that also arise because of the wireless environment. Recently, several potential attacks that can severely impair the security established by LS based mechanisms have been revealed by researchers. For example, an active virtual multipath attack is proposed in [24] to defeat LS based location distinction, in which the attacker creates an “artificial channel” that can mimic a real multipath propagation to spoof the legitimate system. While in this work, we focus on passive attacks, in which, the adversary deploys sensors near the legitimate transceivers and aims at inferring the legitimate channel information and the corresponding LS through its own channel measurements [1, 25]. To defend against such attacks, guard zones with suitable sizes must be

1The secret key generation rate is limited by the channel secrecy capacity.

2According to [22], one may not be able to discriminate between two locations due to detection errors. Such a conclusion coincides with the main theme of this work.
deployed around the legitimate devices. As to this, existing LS based security schemes often assume that the legitimate and the adversary channels are essentially uncorrelated and hence the attacker can barely acquire any useful information about the legitimate LS, as long as the adversary receiver is separated from the legitimate one by more than half a wavelength; and such assumed fast channel decorrelation has been observed in [26]. However, high channel correlation has been observed in practice as well, even when the spatial separation is more than half-wavelength, though in the context of MIMO systems [27]. These seemingly contradictory facts indicate that channel correlation varies in different environments. Then, the following questions naturally arise: When does the half-wavelength assumption hold? What will be the suitable guard zone size to protect the LS? Answering these questions is crucial to a more efficient and confident deployment of LS based security mechanisms, since an unnecessarily large guard zone increases the deployment cost and restricts the application while a too small one will render the legitimate systems in danger.

To help dispel misconceptions and promote further advancement of LS techniques based on a more solid foundation, this work contributes in the following aspects. First, a novel correlation attack is designed to demonstrate the potential vulnerability of LS based security mechanisms when the commonly believed half-wavelength guard zone is blindly adopted, with both theoretical and numerical justifications; to the best of our knowledge, we are among the first to raise this concern.

In addition, as few existing literature has ever explored channel correlation and the impact of physical-layer parameters in the context of LS security, another contribution of this work is to comprehensively investigate well-established channel correlation models (e.g., [28–31]) and endeavor to identify some important physical factors at the wireless medium that have significant implications to LS security. Moreover, a generic channel correlation model that synthesizes the obtained understandings is presented to facilitate LS security assessment. With this model, suitable guard zone sizes are numerically explored for LS based security mechanisms in several typical indoor and outdoor communication scenarios. Finally, real-world experiments through Universal Software Radio Peripheral (USRP) platforms and GNURadio are conducted to further corroborate our findings.

The rest of this paper is organized as follows. Section II demonstrates the existence of high channel correlation and the potential vulnerability of LS. Important factors and models influencing channel correlations and LS security are explored in Section III. Numerical and experimental results are presented in Section IV and Section V, respectively. Section VI concludes this work.

II. POTENTIAL VULNERABILITY OF LS AND THE CORRELATION ATTACK

Wireless signal usually propagates along multiple paths depending on the specific scattering environment, and the resulting channel impulse response between a pair of nodes is referred to as the LS, which can be exploited for security provisioning. For example, based on the observation that a location change of the transmitter often results in a different LS measured at the receiver side, LS based location distinction/authentication has been developed [18–23]. Also, as the wireless channel between two nodes is usually reciprocal, LS can be used as the common secret to establish secured communication [11–17]. More detailed background on LS can be found in [11–23] and the references therein.

It is worth noticing that, since the security established by LS based mechanisms relies on the confidentiality of the channel information between the corresponding legitimate transmitter ($T_l$) and receiver ($R_l$), a widely adopted assumption is that, when the legitimate receiver and the adversary receiver ($R_a$) are separated by more than half a wavelength ($\lambda/2$), the corresponding complex channel coefficients $h_{T_l,R_l}$ and $h_{T_l,R_a}$ are essentially decorrelated such that the adversary can barely acquire any information about the legitimate channel [11–23]. Nevertheless, as will be illustrated in the rest of this work, the half-wavelength decorrelation assumption does not hold universally—two wireless channels can be highly correlated over a much larger spatial range in some situations, and in such cases, the adversary can undermine the promised security of LS based mechanisms through the correlation attack.\(^3\)

In the following, the correlation between the legitimate and the adversary channels is defined as\(^4\),

$$\rho \triangleq \frac{E[h_{T_l,R_l}h_{T_l,R_a}^*] - E[h_{T_l,R_l}]E[h_{T_l,R_a}^*]}{\sqrt{\text{Var}(h_{T_l,R_l})\text{Var}(h_{T_l,R_a}^*)}}. \quad (1)$$

Since most of the existing LS based applications (e.g., [12, 20]) utilize channel envelope information $|h|$, we will focus on channel envelope correlations, defined as

$$\rho^{env} \triangleq \frac{E[|h_{T_l,R_l}|^2|h_{T_l,R_a}|] - E[|h_{T_l,R_l}|^2]E[|h_{T_l,R_a}|]}{\sqrt{\text{Var}(|h_{T_l,R_l}|^2)\text{Var}(|h_{T_l,R_a}|)}}, \quad (2)$$

throughout this work, and $\rho^{env}$ is related to the complex channel correlation coefficient $\rho$ in (1) through $\rho^{env} \approx |\rho|^2$ [32].

A. Channel Correlation based on One-ring Model

We start our discussion from the one-ring model [28, 33, 34]. As well-supported by real-world evidence, the one-ring model is suitable to characterize the correlation between two wireless channels when one communication end is surrounded by rich scatterers while the other end experiences much less diffusion (Fig. 1). According to this model, the correlation between a pair of channels $h_{pq}$ and $h_{pq'}$ is given by [34]

$$\rho_{pq,pq'} = \int_{-\pi}^{\pi} \frac{2\pi j}{\sqrt{\lambda}} \exp\left(\frac{2\pi j}{\lambda}d_{pq'} \cos(\theta_T - \varphi)\right)$$

\(^3\)Although we focus on narrowband and single antenna cases in this work, our discussions can be extended to the more general wideband and multiple antenna scenarios.

\(^4\)In (1), $E[\cdot]$ and $\text{Var}(\cdot)$ denote the conjugate, the expectation and the variance operators, respectively.
correlation factors, including 1) the angle spread \( \Delta \), 2) the legitimate receiver position on channel envelope correlation between the legitimate and the adversary receivers. When the scatterer-ring is on the receiver side, the legitimate and the adversary receiver position on channel envelope correlation can be processed similarly by switching the roles of corresponding quantities.

Specifically, \( \rho(\theta_R) = 0 \) when \( \theta_R = 0^\circ \), and \( \rho(\theta_R) \) increases with \( \theta_R \). From (3) it can be noted that, in general, the channel correlation \( \rho_{pq, p'q'} \) depends on not only the transceiver spatial separations \( d_{pq} \) and \( d_{p'q'} \) but also several other important factors, including 1) the angle spread \( \Delta = \arcsin(R/D) \) with \( R \) and \( D \) determined by the geometry shown in Fig. 1, 2) the power azimuth spread (PAS) \( f(\theta) \), characterizing the scatterer density over the azimuth \( \theta \) on the scatterer-ring, and 3) \( \theta_T \) and \( \theta_R \), determined by the azimuth positions of the transceivers. Since all these factors are environment-dependent, it is not difficult to realize that channel correlation will change in different environments.

To apply the one-ring model to LS security analysis, one can modify it by setting \( p = p' = T_l \), \( q = R_l \) and \( q' = R_a \) when rich scattering resides at the receiver side (Fig. 2), and then employ (3) to compute the corresponding correlation between the legitimate and the adversary channels; the case of transmitter side scattering can be processed similarly by switching the roles of corresponding quantities.

With this modeling, the impacts of the angle spread \( \Delta \) and adversary receiver position on channel envelope correlation \( \rho_{env} \) are examined when the PAS is uniform (i.e., \( f(\theta) = 1/(2\pi) \)). The corresponding results are presented in Fig. 3. Several important observations can be made: 1) When the scatterer ring is on the receiver side, the legitimate and the adversary channels will be quickly decorrelated by these local scatterers (Fig. 3(a)–3(b)). In such rich scattering environments, the fast spatial decorrelation assumed by existing LS techniques is valid. 2) However, when the scatterer-ring is on the transmitter side while the receivers are free from local scattering, a small angle spread \( \Delta \) can induce fairly high channel correlations, as can be seen from Fig. 3(c)–3(d). 3) In addition, by comparing Fig. 3(c) and Fig. 3(d), it can be seen that the adversary can obtain even higher channel correlation by placing its sensor along the transmitter-to-receiver direction (corresponding to \( \theta_R = 0^\circ \)). For example, with a small angle spread \( \Delta = 2^\circ \), the adversary can increase the channel correlation from 0.05 (Fig. 3(c)) to 0.99 (Fig. 3(d)) by changing \( \theta_R \) from \( 90^\circ \) to \( 0^\circ \), even when the spatial separation \( \delta d \) between the legitimate and the adversary receivers is \( 10\lambda \), thus incurring security concerns.

### B. Correlation Attack to LS

In this subsection, the correlation attack is introduced to illustrate how the attacker can exploit the high channel correlation (when it exists) to impair the security of LS.

In the correlation attack, the adversary deploys \( n \) \((\geq 1)\) receivers, denoted by \( \{R_{a_1}, \ldots, R_{a_n}\} \), in the vicinity of the legitimate receiver; then based on the measured channels, denoted by \( h_{a} = [h_{T_l, R_{a_1}}, \ldots, h_{T_l, R_{a_n}}]^T \) (with \( T \) denoting the transpose operator) from these receivers, it constructs an estimate \( \hat{h}_{T_l, R_l} \) of the legitimate channel \( h_{T_l, R_l} \) through linear minimum mean square error (LMMSE) estimation. Specifically, \( \hat{h}_{T_l, R_l} \) is

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 [35]. It is used here to convey the basic idea while in practice other estimators can be used as well.

---

Fig. 1. One-ring model with receiver side scatterers (\( S_p \): scatterer at azimuth \( \theta \); \( p, p' \): transmitters; \( q, q' \): receivers).

Fig. 2. Scatterer-ring on receiver side (\( T_l \): legitimate transmitter; \( R_l \): legitimate receiver; \( R_a \): adversary receiver; \( \delta d \): spatial separation between the legitimate and the adversary receivers).

![Image](image1.png)

Fig. 3. Scatterer ring on receiver side (a) Scatterer ring on receiver side and \( \theta_R = 90^\circ \).

![Image](image2.png)

(c) Scatterer ring on transmitter side (d) Scatterer ring on transmitter side and \( \theta_R = 90^\circ \).

![Image](image3.png)
given by

$$\hat{h}_{T_1,R_i} = \mathbb{E}[h_{T_1,R_i}] + B^T C^{-1}(h_a - \mathbb{E}[h_a]),$$

(6)

where $B_{n \times 1} \triangleq \text{Cov}(h_{T_1,R_i}, h_a)$ is the correlation vector between the legitimate channel and the adversary channels, and $C_{n \times n} \triangleq \text{Cov}(h_a, h_a)$ is the correlation matrix of the adversary channels. Several related analytical results are in order.

**Proposition 1:** The MSE of the LMMSE estimate $\hat{h}_{T_1,R_i}$ is given by

$$\text{MSE} = \frac{\text{det}(A)}{\text{det}(C)},$$

where $A = [A \ B^T]$ and $A_{1 \times 1} \triangleq \text{Var}(h_{T_1,R_i})$ is the variance of the legitimate receiver channel.

**Proof:** Please see Appendix A.

**Remark:** In the special case of $n = 1$, it can be verified that the normalized (with respect to the variance $A$ of $h_{T_1,R_i}$) MSE of $\hat{h}_{T_1,R_i}$ is $1 - \rho^2$ (with $\rho$ denoting the correlation coefficient between the legitimate and the adversary channels), which indicates that higher channel correlation allows the attacker to obtain finer estimate and thereby causes more severe threats to the legitimate LS.

**Proposition 2:** The estimator $\hat{h}_{T_1,R_i}$ is always no worse than that based on any subset of $\{h_{T_1,R_i}^{k}\}_{i=1}^{n}$ with $k(< n)$ adversary sensors.

**Proof:** Please see Appendix B.

Actually, not only that $\hat{h}_{T_1,R_i}$ becomes more accurate with more adversary receivers deployed, it can be also shown that in some circumstances with the presence of sufficient high correlation between the legitimate and the adversary channels, the adversary is even capable of perfectly reconstructing the legitimate channel by increasing the number of adversary receivers, as given in the following corollary.

**Corollary 1:** Assume that the correlation between any adversary and the legitimate channels is $\rho$, and the correlation between any two adversary channels is $\rho'$. Then, if $\rho^2 > \rho'$, there exists an $n = \left\lceil \frac{1 - \rho^2}{\rho^2 - \rho'} \right\rceil$, such that the MSE of the attacker's estimate can be driven down to zero when employing $n$ adversary receivers.

**Proof:** Please see Appendix C.

To further illustrate Corollary 1, numerical results for $\rho = 0.9$ and $\rho' = 0.8$ is presented in Fig. 4. From Fig. 4, it can be seen that, 8 to 10 adversary receivers will result in satisfactory estimation quality to the attacker, and by further increasing to 20 adversary receivers, the adversary can even achieve perfect estimation.

Then we move one step further to consider a more practical example, where the channel correlations among all channels are assumed to be determined by the one-ring model with transmitter side scattering and the adversary receivers are deployed along the transmitter-to-receiver direction (i.e., $\theta_R = 0^\circ$ in (3)) as shown in Fig. 5. The corresponding normalized MSE’s of the attacker’s estimate for different numbers of adversary sensors are given by Proposition 1 and presented in Fig. 6. As shown in Fig. 6, when $\Delta$ is small ($\Delta = 6^\circ$) and the PAS is uniform, 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 spatial separation is 20 wavelengths.

These results clearly indicate that the commonly believed half-wavelength separation may not be sufficient to protect the LS itself in certain environments. For a more clear understanding on the suitable guard zones for LS in different environments, a more comprehensive studies on channel correlation will be conducted in the next section.

---

In (6), 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., the one-ring model) when these models are known to match the environment of interest well.
AS the modified Bessel function of the first kind,

\[
\text{AS} = \text{exp}(\Delta) - \text{confused with the angle spread}
\]

different P AS's with the same AS, based on the one-ring model

scatterer-ring size and transmitter-to-receiver distance.

\[
\text{defined as } [37]
\]

the concentrations of scatterers for different P AS's, which is

E CU RIT Y

A. Power Azimuth Spectrum and the Azimuth Spread

Besides the angle spread \(\Delta\) discussed in Section II-A, the PAS

\(f(\theta)\) (c.f. (3)), which describes the scatterer density over the

azimuth \(\theta\), is another important factor for channel correlation

and LS security. In addition to the uniform PAS assumed

previously, various other PAS’s are also proposed in literature

such as the cosine function PAS [36], the truncated uniform

PAS [37], the truncated Gaussian PAS [38, 39], the von-Mises

PAS [34] and the truncated Laplacian PAS [40]. These single-

mode scatterer distributions (i.e., scatterers mostly concentrate

around a mean azimuth \(\bar{\theta}\)) are compared in Fig. 7, and can be

easily extended to multi-mode ones when multiple clusters of

scatterers exist [40].

The azimuth spread (AS)\(^7\) is a generic metric to measure the

concentrations of scatterers for different PAS’s, which is

defined as [37]

\[
AS = \sqrt{1 - |F_n|^2/|F_0|^2},
\]

where \(F_n = \int_0^{2\pi} f(\theta) \exp(jn\theta)d\theta\) is the \(n\)th complex Fourier

coefficient of \(f(\theta)\). The AS ranges from 0 to 1 where \(AS = 0\)

corresponds to signal incidence from a single direction and

\(AS = 1\) corresponds to all-around arrivals.\(^8\)

Fig. 8 presents the spatial channel correlation functions for
different PAS’s with the same AS, based on the one-ring model

\(^7\)The azimuth spread is also called angular spread in [41], which

is determined by the angular domain scatterer distribution, and should not be

confused with the angle spread \(\Delta\) defined earlier, which is determined by the

scatterer-ring size and transmitter-to-receiver distance.

\(^8\)When the PAS follows the von-Mises distribution

\(f(\theta) = \exp(\kappa \cos(\theta - \bar{\theta}))/2\pi I_0(\kappa)\) with \(\theta \in (-\pi, \pi)\) and

\(I_0(\cdot)\) denoting the modified Bessel function of the first kind, \(AS = 0\) when \(\kappa \rightarrow \infty\) and

\(AS = 1\) when \(\kappa = 0\).

III. Key Channel Factors/Models for LS Security

In this section, various wireless channel correlation models

are investigated and several key factors that have substantial

impacts on channel correlation and LS security are identified.

A. Power Azimuth Spectrum and the Azimuth Spread

Besides the angle spread \(\Delta\) discussed in Section II-A, the PAS

\(f(\theta)\) (c.f. (3)), which describes the scatterer density over the

azimuth \(\theta\), is another important factor for channel correlation

and LS security. In addition to the uniform PAS assumed

previously, various other PAS’s are also proposed in literature

such as the cosine function PAS [36], the truncated uniform

PAS [37], the truncated Gaussian PAS [38, 39], the von-Mises

PAS [34] and the truncated Laplacian PAS [40]. These single-

mode scatterer distributions (i.e., scatterers mostly concentrate

around a mean azimuth \(\bar{\theta}\)) are compared in Fig. 7, and can be

easily extended to multi-mode ones when multiple clusters of

scatterers exist [40].

The azimuth spread (AS)\(^7\) is a generic metric to measure the

concentrations of scatterers for different PAS’s, which is

defined as [37]

\[
AS = \sqrt{1 - |F_n|^2/|F_0|^2},
\]

where \(F_n = \int_0^{2\pi} f(\theta) \exp(jn\theta)d\theta\) is the \(n\)th complex Fourier

coefficient of \(f(\theta)\). The AS ranges from 0 to 1 where \(AS = 0\)

corresponds to signal incidence from a single direction and

\(AS = 1\) corresponds to all-around arrivals.\(^8\)

Fig. 8 presents the spatial channel correlation functions for
different PAS’s with the same AS, based on the one-ring model

\(3\). It can be seen that 1) channel correlation is not very sen-

tive to the particular forms of PAS but is mainly determined

by the corresponding \(AS\), and that 2) a smaller \(AS\) always

leads to higher channel correlation. This implies that much

larger guard zones are needed to ensure sufficient decorrelation

between the legitimate and the adversary channels for better

LS protection, in the environments where scatterers are highly

concentrated. For example, when the scatterers follow the \(\cos^n\)

distribution with \(n = 8.5\), a guard zone with radius larger

than \(10\lambda\) is needed, instead of the commonly assumed half-

wavelength, to keep the correlation below 0.1.

B. Rician Factor

In addition to the (random) diffusion component induced by

the scattering effect (as considered in (3)), a wireless channel

may also contain a (deterministic) line-of-sight (LOS) component.

For such cases, the so-called Rician factor, denoted by \(K\),

is defined as the power ratio between these two components,

and correspondingly a space-time correlation \(\tilde{\rho}\) may be defined

as in [34], given by

\[
\tilde{\rho}_{pq,p'q'} \triangleq \frac{\mathbb{E}[h_{pq}^{*} h_{p'q'}^{*}]}{\sqrt{\mathbb{E}[|h_{pq}|^2] \mathbb{E}[|h_{p'q'}|^2]}} = \rho_{\text{TDF}}^{\text{LOS}} + \rho_{\text{TDF}}^{\text{LOS}},
\]

where the space-time correlation for the diffusion component

\(\rho_{\text{TDF}}^{\text{LOS}}\) can be computed by (3) with a scaling factor \(1/(1 + K)\),

and that for the LOS component is given by
wanted directions. The gain of a directive antenna in azimuth
following, only the diffusion part will be considered.
impact on the security of these LS based applications. In the
existence of the LOS component will not have a significant
two channel measurements to the standard deviation (instead
found that, in most LS based secret key generation algorithms,
are investigated as to how the LOS component is handled. It is
before the key generation process [12, 15, 16, 42, 43], and that,
the LOS component is removed from the channel measurement
A. Directive Antenna

\[
\rho_{p,q,p',q'}^{LOS} = \frac{K}{1+K} \exp \left\{ \frac{2\pi j}{\lambda} \left[ d_{pp'} \cos(\theta_T) - d_{qq'} \cos(\theta_R) \right] \right\}.
\]

Based on (8), it can be verified that a large Rician factor
induces high space-time correlation, which seemingly implies
a severe vulnerability of LS when a strong LOS component ex-

\[
\rho = \int_{-\pi}^{\pi} \exp \left\{ \frac{2\pi j}{\lambda} \delta \cos(\theta_R - \theta) \right\} f(\theta) G(\theta) d\theta,
\]

where receiver side scattering is assumed.\(^9\) It is worth noting
from (10) that, mathematically, the PAS \( f(\cdot) \) and the antenna
radiation pattern \( G(\cdot) \) have equivalent impacts on channel
correlation.

Based on (10), the spatial correlation functions with different
radiation patterns are compared in Fig. 9, where a truncated

\(^9\)In the cases of small angle spread \( \Delta \) assumed by the one-ring model, the
incident signal’s spread in angular domain will be smaller than the antenna’s
3dB beamwidth when the scatterers reside on the transmitter side, and hence,
using directive antenna may not change the channel correlation significantly.

uniform PAS with \( \theta_{max} = 10^\circ \) and \( \theta_{min} = -10^\circ \) is assumed.
It can be seen that highly directional antennas (with small
\( \theta_{3dB} \) ) can induce large channel correlations, and hence larger
guard zones will be required to protect the legitimate LS. For
example, when directive antennas with \( \theta_{3dB} = 5^\circ \) are adopted,
the guard zone size has to be increased substantially from \( 3\lambda \)
to \( 10\lambda \) to ensure the correlation between the adversary and
the legitimate channels below 0.05. (Similar trends are also observed
for other PAS’s as well.)

An intuitive explanation for the correlation boosting phe-
nomenon of directive antenna is as follows [2,46]: First notice
that channel decorrelation is essentially caused by that the
signal phase shifts due to different scatterers are independent;
the directive antenna will suppress the signals reflected by
those scatterers in unwanted direction (which equivalently
leads to a more concentrated PAS) and hence reduces the
randomness in scattering, inducing high channel correlation.
In general, channel correlation boosting effect appears only
when directive antenna reduces the angular domain spread
of effective scatterers, i.e., the scatterers illuminated by
the directive antenna, as shown in Fig. 10, which explains why
in Fig. 9, channel correlation is significantly enhanced only
when \( \theta_{3dB} < (\theta_{max} - \theta_{min}) \).

C. Directive Antenna

In practice, a directional antenna is often used to enhance
communication performance by suppressing signals from un-
wanted directions. The gain of a directive antenna in azimuth
is characterized by its radiation pattern \( G(\cdot) \), which is
parameterized by the main lobe direction \( \theta_G \) and the 3dB
antenna beamwidth \( \theta_{dB} \).

When the adversary employs the same directive antenna as
the legitimate receiver, the corresponding channel correlation
is given by [40]

D. Other Models for Different Scattering Environments

Different scattering environments other than that assumed by
the one-ring model exist in practice, and several other channel
models will be studied in this subsection to account for these
cases. For these models, previous conclusions as to angle
spread, PAS/AS, Rician factor and directive antenna in the
one-ring model carry over when applicable.

1) Two-Ring Models: In both indoor and outdoor environ-
ments, both communication ends may be enclosed by local
scatterers. In these cases, two-ring models [29,30,47–49]
can be employed to characterize the corresponding channel
correlation. With different assumptions on signal propagation,
both the single-bounce and the double-bounce two-ring models
are proposed in literature.

In the single-bounce two-ring model, it is assumed that
the received signals are reflected by either the transmitter
side or the receiver side scatterers, as depicted in Fig. 11.
With this assumption, the single-bounce model is in fact a
weighted superposition of two one-ring models with corre-
sponding scatterer-rings on the transmitter and the receiver
sides, respectively [30].
scatterers is given by \(^{10}\)

\[
\rho_{SBT}^{(SBR)} = \int_{-\pi}^{\pi} \exp\left\{ 2\pi j [\delta d \cos(\theta_R - \varphi) - \delta d] \right\} f_T^{(SBR)}(\theta') G_T(\theta') d\theta',
\]

where \(\theta'\) and \(\varphi\) admit similar relations in (4) and (5). The correlation due to receiver side scatterers is given by

\[
\rho_{SBR}^{(SBR)} = \int_{-\pi}^{\pi} \exp\left\{ 2\pi j [\delta d \cos(\theta_R - \theta)] \right\} f_R(\theta) G_B(\theta) d\theta.
\]

The overall correlation is given by

\[
\rho_{SB}^{(SBR)} = (\eta_{SBT} \cdot \rho_{SBT}^{(SBR)} + \eta_{SBR} \cdot \rho_{SBR}^{(SBR)}),
\]

where \(\eta_{SBT}\) and \(\eta_{SBR}\) represent the strengths of the reflected signals from the two scatterer-rings, respectively, and admit \(\eta_{SBT} + \eta_{SBR} = 1\).

In the double-bounce two-ring model \([29]\), wireless signals get reflected and scattered at both the transmitter side and receiver side scatterers; nevertheless, it can be verified that, for the purpose of LS security assessment where only one transmitter is considered, the double-bounce two-ring model reduces to the one-ring model.

2) Elliptical Ring Model: In the elliptical scatterer-ring model, an elliptical scatterer-ring encloses both the transmitter and the receivers, as depicted in Fig. 12. This model may be applied to office environments where the two communication ends are not far from each other and surrounded by common scatterers nearby. Denoting the major and minor radii of the ellipse by \(a\) and \(b\), respectively, the corresponding channel correlation is given by \([31]\)

\[
\rho_{EB}^{(E)} = \int_{-\pi}^{\pi} \exp\left\{ 2\pi j [\delta d \cos(\theta_R - \alpha_R)] \right\} f_E(\theta) G_T(\alpha_T) G_B(\alpha_R) d\theta,
\]

where \(f_E\) denotes the PAS of the elliptical scatterer-ring; \(\alpha_T\) and \(\alpha_R\) are functions of \(\theta\) determined by the geometry shown in Fig. 12, and they correspond to the angles of departure and arrival, respectively, with respect to the scatterer at angle \(\theta\).

Channel correlation under elliptical scatterer-ring modeling is shown in Fig. 13. It can be seen that a narrower elliptical scatterer-ring (i.e., smaller \(a\)) will induce higher channel correlation, which in turn indicates a requirement of larger guard zones for LS protection.

3) Far Scatterer-Ring Model: A far scatterer-ring model in which the scatterers that are distant from both communication ends, as depicted in Fig. 14, has been considered in \([50]\), and it is indicated that the correlation function due to far scatterers is mathematically the same as that due to local scatterers with the displacement of the ring center. Based on this principle, the correlation function due to far scatterers can be derived as

\[
\rho_{FB}^{(F)} = \int_{-\pi}^{\pi} \exp\left\{ 2\pi j [\delta d \cos(\theta_R - \alpha_R)] \right\} f_F(\theta) G_T(\alpha_T) G_B(\alpha_R) d\theta,
\]

where \(f_F\) denotes the PAS of the far scatterer-ring with corresponding angle spread defined as \(\Delta_F = \arcsin(R_F/D)\); \(\alpha_T\) and \(\alpha_R\), which correspond to the angles of departure and
in terms of LS security. Based on the obtained understanding and insights, a generic channel correlation model that includes the security implications of all these factors and models is given as follows:

\[
\rho = \eta_{SBT} \cdot \rho^{(SBT)} + \eta_{SBR} \cdot \rho^{(SBR)} + \eta_E \cdot \rho^{(E)} + \eta_F \cdot \rho^{(F)},
\]

where the sub-model coefficients admit \(\eta_{SBT} + \eta_{SBR} + \eta_E + \eta_F = 1\) and \(\rho^{(SBT)}\), \(\rho^{(SBR)}\), \(\rho^{(E)}\) and \(\rho^{(F)}\) are given by (11), (12), (14) and (15), respectively. Some explanations are in order. First, the LOS component is omitted, since it will not change the adversary’s attacking performance, as discussed in Section III-B. The one-ring model is a special case of the single-bounce two-ring model captured here, and so is the double-bounce two-ring model as far as LS security assessment is concerned. As will be seen in the next section, this weighted sum form provides flexibility in modeling channel correlations in various environments of interest with properly chosen weighting coefficients, either by selecting the most suitable model (as in Scenario I), or by an appropriate combination of roughly independent sub-models (as in Scenario II and III).

### IV. Simulation and Numerical Results

As can be noted from the above discussions, the correlation of wireless channels varies substantially depending on the scattering environment and hence, the commonly believed half-wavelength cannot ensure LS security universally. As will be shown in this section, in many scenarios, much larger guard zone may need to be deployed around legitimate devices for security assurance of LS-based mechanisms.

Specifically, the guard zone sizes for three typical wireless communication scenarios are numerically explored. The performance of two LS based security mechanisms, secret key generation [12] and location distinction [20], is investigated under the correlation attack discussed in Section II-B when guard zones of different sizes are deployed. To account for various physical environments, multiple combinations of parameters are chosen for each of the three scenarios. In all simulations, the legitimate and the adversary channels assume Rayleigh fading with correlation given by (16) based on the corresponding environment parameters. We mainly present the results for the one adversary receiver case to convey the basic idea; when multiple collaborative adversary receivers are deployed, even larger guard zones are needed, as indicated by Proposition 2.

Considering that in practice different cryptographic algorithms and detection thresholds may be used for LS based secret key extraction and location distinction, two security levels, Lv1 and Lv2, are considered in this work. For Lv1 (Lv2) security, it is assumed that the promised security by the

<table>
<thead>
<tr>
<th>Angle spread (\Delta F)</th>
<th>Applicable models</th>
<th>Favorable value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scatterer distribution (AS)</td>
<td>O, T, F</td>
<td>(AS = 1)</td>
</tr>
<tr>
<td>Rician factor (K)</td>
<td>O, T, E, F</td>
<td>no influence</td>
</tr>
<tr>
<td>Directive antenna (\theta_{dir})</td>
<td>O, T, E, F</td>
<td>omni-directional</td>
</tr>
<tr>
<td>Eccentricity (\sqrt{a^2 - b^2} / a)</td>
<td>E</td>
<td>(\sqrt{a^2 - b^2} / a \rightarrow 0)</td>
</tr>
<tr>
<td>Adversary’s angular position (\theta_R)</td>
<td>O, T, E, F</td>
<td>\pm \pi/2</td>
</tr>
</tbody>
</table>

### E. A Generic Channel Correlation Model for LS

Based on the previous discussions, the key channel factors and models for LS security assessment are summarized in Table I, together with the corresponding most favorable values
LS is thwarted if the normalized MSE\textsuperscript{11} of the adversary’s estimated channel in the location distinction application is below 0.1 (0.5) or more than 90\% (50\%) secret key bits are inferred by the adversary. For secret key extraction, the level-crossing algorithm in [12] is implemented where $1 \times 10^4$ samples are generated for each channel and an excursion of length 4 is used.\textsuperscript{12} Finally, the (empirical) outage probability $P_{\text{out}}(\delta d)$ for each scenario, defined as

$$P_{\text{out}}(\delta d) \triangleq N_{\text{insecure}}/N_{\text{total}},$$

is employed as the metric for LS security assessment, where $N_{\text{insecure}}$ and $N_{\text{total}}$ are the number of insecure and the number of total considered environments in each scenario, respectively. A non-zero $P_{\text{out}}(\delta d)$ implies the existence of environment(s) where the LS application is insecure when the guard zone size is $\delta d$. Clearly, Lv2 specification is easier for the adversary to achieve and thus indicates a higher outage probability for the same guard zone size, or demands a larger guard zone size for the same outage probability.

A typical indoor scenario (Scenario I) is considered first, where both the legitimate transceivers and the adversary receiver are in the same office. In such a scenario, both communication ends are surrounded by common scatterers, and hence the elliptical scatterer-ring model can be used to characterize the corresponding channel correlations (i.e., $\eta_F = 1$). To account for various physical environments in this scenario, 42 different parameter combinations are considered. Particularly, $(a:b) \in \{4 : 1, 4 : 2, 4 : 3\}$, $\text{PAS} \in \{\text{omni}, \text{von-Mises} (\kappa = 10, 50; \theta = 0, 90^\circ, 180^\circ)\}$, $\text{GT} \in \{\text{omni}\}$ and $\text{GR} \in \{\text{omni}, \theta_{3d} = 40^\circ\}$.

Fig. 16 and Fig. 17 show the outage probabilities for LS based location distinction and secret key extraction, respectively, in Scenario I. It can be seen that the commonly believed safe-distance $\lambda/2$ is not sufficient to secure the LS applications for all the cases. For example, as shown in Fig. 16, when $\delta d = \lambda/2$, in more than 50\% of the considered cases with omni-directional antennas, the adversary can obtain an estimate of the legitimate LS with normalized MSE less than 0.1 and thus defeats the Lv1 security requirement of location distinction; it becomes even worse (i.e., larger $P_{\text{out}}$) when both the legitimate and adversary receivers adopt directive antennas, or Lv2 security is considered. Similar observations can be made in Fig. 17 for LS based secret key extraction as well. In fact, the results in Fig. 16 and Fig. 17 suggest that a guard zone of size about $\delta d = 19\lambda$ is needed to achieve Lv1 security with zero outage probability for LS.\textsuperscript{13} For the more demanding Lv2 security, even larger guard zones are required.

\textsuperscript{11}Note that in the location distinction application [20], the channel difference $|h - \bar{h}|$ (with $\bar{h}$ the empirical average channel) is compared with channel standard deviation $\sigma_F$ for location change detection. When the adversary can obtain an estimate of the legitimate channel with small MSE, it can launch the mimicry attack [25] so as to spoof the detector that it is located at the same position as the legitimate transceiver.

\textsuperscripts{12}Although a more advanced version of the algorithm is available in [13] for more general channel state distributions, the basic version in [12] that is well-suited for the assumed Rayleigh fading is adopted here for simplicity.

\textsuperscripts{13}When the adversary can deploy two sensors, our simulation results indicate that $\delta d = 37\lambda$ is needed.

\begin{table}[h]
\centering
\caption{Elliptical-ring model ($\eta_F = 1$)}
\begin{tabular}{|l|l|}
\hline
Model & Elliptical-ring model ($\eta_F = 1$) \\
\hline
$a : b$ & $4 : 1, 4 : 2, 4 : 3$ \\
\hline
\text{PAS} & uniform, von-Mises ($\kappa = 10, 50; \theta = 0, 90^\circ, 180^\circ$) \\
\hline
\text{GT} & omni; \\
\hline
\text{GR} & omni, $\theta_{3d} = 40^\circ$; \\
\hline
\end{tabular}
\end{table}

\begin{table}[h]
\centering
\caption{Two-ring model (\text{\textit{SBR}} = 0.9, $\eta_{SBR} = 0.1$)}
\begin{tabular}{|l|l|}
\hline
Model & Two-ring model (\text{\textit{SBR}} = 0.9, $\eta_{SBR} = 0.1$) \\
\hline
$\Delta$ & $2^\circ, 5^\circ, 10^\circ, 20^\circ$ \\
\hline
$\text{PAS}_T$ & uniform, von-Mises ($\kappa = 10, 50; \theta = 0, 90^\circ, 180^\circ$) \\
\hline
$\text{PAS}_R$ & uniform, von-Mises ($\kappa = 10, 50; \theta = 0^\circ$) \\
\hline
$\text{GT}$ & omni, $\theta_{3d} = 40^\circ$; \\
\hline
$\text{GR}$ & omni, $\theta_{3d} = 40^\circ$; \\
\hline
\end{tabular}
\end{table}

---

Fig. 16. Location distinction in Scenario I. ("O-": Omni-directional; "D-": Directive)

Fig. 17. Secret key generation in Scenario I. ("O-": Omni-directional; "D-": Directive)

Fig. 18. Location distinction in Scenario II. ("O-": Omni-directional; "D-": Directive)

Fig. 19. Secret key generation in Scenario II. ("O-": Omni-directional; "D-": Directive)
Table IV
Scenario III

<table>
<thead>
<tr>
<th>Model</th>
<th>One-ring &amp; far scatterer-ring models ($\eta_{SBR} = 0.8, \eta_F = 0.2$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta$ and $\Delta_F$</td>
<td>$2^\circ, 5^\circ, 10^\circ, 20^\circ$</td>
</tr>
<tr>
<td>$PAS_R$</td>
<td>uniform, von-Mises ($\kappa = 10, 50; \theta = 0^\circ, 90^\circ, 180^\circ$)</td>
</tr>
<tr>
<td>$PAS_F$</td>
<td>uniform, von-Mises ($\kappa = 10, 50; \theta = 0^\circ, 90^\circ, 180^\circ$)</td>
</tr>
<tr>
<td>Far scatterers position</td>
<td>$\gamma_T = 45^\circ, \gamma_R = 90^\circ, 135^\circ$</td>
</tr>
<tr>
<td>$G_R$</td>
<td>omni, $\theta_{BR}^{(R)} = 40^\circ$</td>
</tr>
</tbody>
</table>

In the second scenario (Scenario II), it is assumed that the transmitter is inside the office (with rich scattering) while both the legitimate and the adversary receivers are in the hallway (with much less scattering). A single-bounce two ring model with weighting coefficients $\eta_{SBR} = 0.9$ and $\eta_{SBR} = 0.1$ is employed to characterize the channel correlation, and the corresponding parameter settings are given in Table IV with a total of 336 combinations. Again, a guard zone of size $\delta d = \lambda/2$ cannot ensure LS security, as shown in Fig. 18 and Fig. 19. Instead, a guard zone of size $\delta d = 12\lambda$ has to be deployed to achieve Lv1 security. Although a smaller guard zone is required in this scenario for Lv1 security, it can be seen by comparing Figs. 16–17 and Figs. 18–19 that Scenario II requires a larger guard zone for Lv2 security as compared to Scenario I.

The last scenario (Scenario III) assumes a base station-to-mobile user communication where the transmitter is assumed high raised (with less scattering) and the legitimate and adversary receivers are surrounded by scatterers, and far scatterers exist as well. A weighted combination of one-ring and far scatterer-ring models (with $\eta_{SBR} = 0.8$ and $\eta_F = 0.2$) is employed to characterize the channel correlation in such scenario, and the corresponding parameter settings are given in Table IV with a total of 3136 combinations. As it can be seen from Fig. 20 and Fig. 21 that $\delta d = 5\lambda$ is required for Lv1 security and Lv2 again requires a larger guard zone. In this outdoor scenario, the dense local scatterers ($\eta_{SBR} = 0.8$) around the receivers decorrelate the legitimate and the adversary channels fairly quickly and thus provide better security protection for LS (i.e., smaller guard zones are needed), as compared to the previous two indoor scenarios.

V. EXPERIMENTAL VERIFICATION

In this section, experiment results obtained from Universal Software Radio Peripheral (USRP) platforms and GNU Radio prototype implementation are presented. It is worth pointing out that high channel correlation has already been observed, even when the spatial separation is more than $\lambda/2$, in the context of MIMO systems [27]. The experiment results and discussions presented here focus on the LS context and aim at providing real-world justification to the previous study.

In our experiments, the carrier frequency is 2.4 GHz with the corresponding wavelength 12.5 cm and the channel sampling rate is 100 samples/sec. Both indoor and outdoor experiments are conducted. In each experiment, 40 pairs of legitimate and adversary channels are recorded for two different spatial separations $\delta d = 1.5\lambda$ and $\delta d = 3.3\lambda$, respectively. Based on these channel measurements, the normalized MSE between the legitimate and the adversary channels are computed to assess the LS based location distinction, while the match rates $\xi$ between the secret keys generated from the legitimate channel and the adversary channel are computed to assess the LS based secret key extraction.

The setting of the indoor experiment is depicted in Fig. 22(a). In this experiment, the transmitter is placed in an office room (Fig. 22(b)) with ample scatterers around, while the two receivers (with one of them serving the role of the

![Fig. 20](image_url) Location distinction in Scenario III. (“O-”: Omni-directional; “D-”: Directive)

![Fig. 21](image_url) Secret key generation in Scenario III. (“O-”: Omni-directional; “D-”: Directive)
adversary can recover the legitimate LS and the corresponding
where the transmitter is placed behind a building pillar while
the legitimate devices is significantly weakened. When the adversary further employs LMMSE estimation in (6), the corresponding average values of channel correlation ($\bar{\rho}$), normalized MSE ($\text{NMSE}$) and key match rate ($\bar{\xi}$) over the collection of all channel measurements are summarized in Table V, where the numbers in the parentheses are the corresponding sample standard deviations. It can be seen that even when the adversary receiver is separated from the legitimate one by more than half-wavelength, fairly high correlations around 0.8 are observed; in these cases, the attacker can construct an estimate of the legitimate LS with normalized MSE around 0.3 and can successfully infer around 75% legitimate secrecy bits.

The setting of the outdoor experiment is depicted in Fig. 24, where the transmitter is placed behind a building pillar while the two receivers are placed in a large open lawn (without much scatterers nearby). The corresponding experiment results are summarized in Table VI. Again, it can be observed that the adversary can recover the legitimate LS and the corresponding generated secret bits with substantial fidelity.

In the environments of these two experiments, if guard zones with size of only half-wavelength are deployed, a large portion of the secrecy of the legitimate LS will be inferred by the attacker and hence the promised security protection to the legitimate devices is significantly weakened. This observation is consistent with our previous analysis, and in fact, the one-ring model may be employed to provide an intuitive explanation: In both experiments, the transmitter is surrounded by relatively rich scatterers while the receivers experience much less scattering; in such cases, two wireless channels will be highly correlated given a small angle spread. In such environments, much larger guard zones are needed to protect the legitimate LS.

### VI. Conclusions

After illustrating potential vulnerabilities of LS through correlation attack when high channel correlation exists, several key factors that have important influence on LS security are identified through a comprehensive investigation of well-established channel models. With the obtained understanding and insights, a generic model characterizing the spatial correlation between the legitimate and the adversary channels is developed to explore proper guard zone sizes for LS based security schemes. Both our numerical and experimental results indicate that spatial channel correlation varies for different wireless environments. In particular, the commonly believed half-wavelength decorrelation assumption is valid mainly in environments with rich scattering; while in poor scattering environments, the legitimate and the adversary channels may decorrelate much slower over space than expected. These findings suggest that in practice, more careful investigation on channel correlation for the specific environment of interest must be conducted before a confident deployment of LS based security mechanisms.

### ACKNOWLEDGMENT

The authors would like to thank Mr. Dixuan Yang and Mr. Weikang Qiao for their help on conducting the experiments.

### APPENDIX A

**Proof of Proposition 1**

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

$$MSE(\hat{h}_{T_i,R_i}) = \mathbb{E} [(\hat{h}_{T_i,R_i} - h_{T_i,R_i})^2] = A - B^T C^{-1} B$$

$$\quad = \det(A - B^T C^{-1} B)$$

$$\quad = \det(S) = \frac{\det(\Gamma)}{\det(C)}.$$  \hspace{1cm} (18)

### APPENDIX B

**Proof of Proposition 2**

**Proof:** It is assumed without loss of generality that the first $k$ adversary channels $\{h_{T_i,R_{a1}}, \ldots, h_{T_i,R_{ak}}\}$ are used. For clarity, let $x = h_{T_i,R_i} - \mathbb{E}[h_{T_i,R_i}], y_i = h_{T_i,R_{ai}} - \mathbb{E}[h_{T_i,R_{ai}}].$

---

14 The exact amount of performance degradation to an LS based security scheme depends on the specific implementation and is beyond the scope of this work.

15 How to efficiently estimate the (dynamic) wireless environments while still perform LS based security mechanisms itself is a fundamental issue. But it is beyond the scope of this work and remains an interesting future direction.

---

**Table V:** Indoor Experiment

<table>
<thead>
<tr>
<th>$\delta d$</th>
<th>$\bar{\rho}$ ($\sigma_\rho$)</th>
<th>NMSE ($\sigma_{\text{NMSE}}$)</th>
<th>$\bar{\xi}$ ($\sigma_\xi$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6$\lambda$</td>
<td>0.86 (0.06)</td>
<td>0.24 (0.1)</td>
<td>77% (9%)</td>
</tr>
<tr>
<td>3.3$\lambda$</td>
<td>0.74 (0.06)</td>
<td>0.39 (0.1)</td>
<td>74% (10%)</td>
</tr>
</tbody>
</table>

**Table VI:** Outdoor Experiment

<table>
<thead>
<tr>
<th>$\delta d$</th>
<th>$\bar{\rho}$ ($\sigma_\rho$)</th>
<th>NMSE ($\sigma_{\text{NMSE}}$)</th>
<th>$\bar{\xi}$ ($\sigma_\xi$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6$\lambda$</td>
<td>0.91 (0.04)</td>
<td>0.18 (0.06)</td>
<td>86% (7%)</td>
</tr>
<tr>
<td>3.3$\lambda$</td>
<td>0.83 (0.06)</td>
<td>0.31 (0.09)</td>
<td>74% (9%)</td>
</tr>
</tbody>
</table>

---

Fig. 24. Outdoor experiment.
and \( y^{(m)} = [y_1, y_2, \ldots, y_m]^T \) \((m \leq n)\). Consequently, \( \mathbb{E}[x] = 0 \), and \( \mathbb{E}[y_i] = 0 \) \((i = 1, \ldots, n)\). It is clear that, the covariance matrices corresponding to \( h_{TI,R_1} \) and \( \{h_{TI,R_{a_i}}\}_{i=1}^m \) are identical to those corresponding to \( x \) and \( y^{(m)} \). Consequently, the coefficient vector in the estimator of \( x \) based on measurement \( y^{(m)} \) is also \( B^TC^{-1} \) (c.f. (6)) and will be denoted by \( \xi \) in the following. Define \( C_m \triangleq \text{Cov}(y^{(m)}, y^{(m)}) \) and \( B_m \triangleq \text{Cov}(x, y^{(m)}) \) for all \( m \leq n \). Then, \( \xi = \xi_n \), where \( \xi_m \triangleq C_m^{-1}B_m \) for all \( m \leq n \). Further, it can be verified that \( \text{MSE}(\hat{x}_m) \), the MSE of the estimate of \( x \) based on \( y^{(m)} \), is the same as the MSE of the legitimate channel estimate based on \( \{h_{TI,R_{a_1}}, \ldots, h_{TI,R_{a_m}}\} \).

Proposition 2 holds if \( \text{MSE}(\hat{x}_{m+1}) \leq \text{MSE}(\hat{x}_m) \) for all \( m \leq n - 1 \) by induction. Let \( D_{m+1} \triangleq \text{Cov}(y_{m+1}, y^{(m)}) \) and \( c_{m+1} \triangleq \text{Cov}(y_{m+1}, y_{m+1}) \). It is not difficult to see the following facts:

1) \( \text{MSE}(\hat{x}_m) = \mathbb{E}[x^2] - B_m^TC_m^{-1}B_m. \)
2) \( c_{m+1} \geq \beta^2D_{m+1}^TC_m^{-1}D_{m+1}. \)
3) \( [C_m \ D_{m+1}]\xi_{m+1} = B_m \) (due to \( C_{m+1}\xi_{m+1} = B_{m+1} \)).

Decomposing \( \xi_{m+1} \) as \( \xi_{m+1} = [\alpha_{m+1} \beta]^T \), the above facts lead to the following equivalence relations:

\[
\text{MSE}(\hat{x}_{m+1}) \leq \text{MSE}(\hat{x}_m) \\
\leq \beta^2c_{m+1} \geq \beta^2D_{m+1}^TC_m^{-1}D_{m+1}. \quad (19)
\]

If \( \beta = 0 \), the proof is completed. Otherwise, it remains to show that \( c_{m+1} - D_{m+1}^TC_m^{-1}D_{m+1} \geq 0 \). Note that the left hand side of this inequality is the Schur complement of \( C_m \) in \( C_{m+1} \), denoted as \( S(C_m) \). Further applying the facts that \( \text{det}(C_m) > 0 \) and \( \text{det}(C_{m+1}) > 0 \), it leads to \( c_{m+1} - D_{m+1}^TC_m^{-1}D_{m+1} = \text{det}(S(C_m)) = \frac{\text{det}(C_m)}{\text{det}(C_{m+1})} > 0. \)

\[\text{APPENDIX C}
\]

\[\text{PROOF OF COROLLARY 1}\]

\[\text{Proof:} \text{ With the given assumptions, } \Gamma \text{ (defined in Proposition 1) is of the form } \]

\[
\Gamma = \begin{bmatrix}
1 & \rho & \cdots & \rho \\
\rho & 1 & \cdots & \rho' \\
\rho' & \rho & \cdots & \rho'' \\
\vdots & \vdots & \ddots & \vdots \\
\rho' & \rho' & \cdots & 1
\end{bmatrix} \quad (n+1) \times (n+1)
\]

Due to the circulant structure of \( \Gamma \), it can be shown that

\[
\text{det}(\Gamma) = \prod_{i=0}^{n-1} \left( c_0 + c_1\omega_i^1 + \cdots + c_{n-1}\omega_i^{n-1} \right), \quad (20)
\]

where \( \omega_k = \exp(j \frac{2\pi k}{n}) \) is the \( n \)th roots of unity, and \( c_0 = 1 - \rho^2, \ c_i = \rho^i - \rho^{-i} \) for \( i > 0 \). Similarly, the determinant of \( C \) is given by

\[
\text{det}(C) = \prod_{i=0}^{n-1} \left( c'_0 + c'_1\omega_i^1 + \cdots + c'_{n-1}\omega_i^{n-1} \right), \quad (21)
\]

where \( c'_0 = 1 \) and \( c'_i = \rho^i \) for \( i > 0 \). Then, according to Proposition 1, the MSE of the estimator \( \hat{h}_{TI,R_1} \) based on the channel measurements from these \( n \) adversary receivers is given by

\[
\text{MSE}(\hat{h}_{TI,R_1}) = \text{det}(C) / \prod_{i=0}^{n-1} \left( c'_0 + c'_1\omega_i^1 + \cdots + c'_{n-1}\omega_i^{n-1} \right)
\]

\[
= \frac{c_0 + c_1 + \cdots + c_{n-1} - n \cdot \rho^2}{c_0' + c_1' + \cdots + c'_{n-1}}
\]

\[
= \frac{1 + (n-1) \cdot \rho \cdot \rho'}{1 + (n-1) \cdot \rho'}. \quad (22)
\]

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

Then, Corollary 1 follows readily by setting \( \text{MSE}(\hat{h}_{TI,R_1}) = 0 \) in (22).

\[\text{REFERENCES}\]


Huaiyu Dai (M’03, SM’09) received the B.E. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1996 and 1998, respectively, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ in 2002.

He was with Bell Labs, Lucent Technologies, Holmdel, NJ, in summer 2000, and with AT&T Labs-Research, Middletown, NJ, in summer 2001. Currently he is a Professor of Electrical and Computer Engineering at NC State University, Raleigh. His research interests are in the general areas of communication systems and networks, advanced signal processing for digital communications, and communication theory and information theory. His current research focuses on networked information processing and crosslayer design in wireless networks, cognitive radio networks, wireless security, and associated information-theoretic and computation-theoretic analysis.

He has served as an editor of IEEE Transactions on Communications, Signal Processing, and Wireless Communications. He co-edited two special issues of EURASIP journals on distributed signal processing techniques for wireless sensor networks, and on multiuser information theory and related applications, respectively. He co-chaired the Signal Processing for Communications Symposium of IEEE Globecom 2013, the Communications Theory Symposium of IEEE ICC 2014, and the Wireless Communications Symposium of IEEE Globecom 2014.

Peng Ning (M’01, SM’12) received the B.S. degree in information sciences from the University of Science and Technology of China (USTC), Hefei, China, in 1994, the M.E. degree in communications and electronics systems from USTC, Graduate School in Beijing, Beijing, China, in 1997, and the Ph.D. degree in information technology from George Mason University, Fairfax, VA, in 2001.

He is a Professor of Computer Science at NC State University, where he also serves as the Technical Director for Secure Open Systems Initiative (SOSI). He is a recipient of National Science Foundation (NSF) CAREER Award in 2005. He is currently the Secretary/Treasurer of the ACM Special Interest Group on Security, Auditing, and Control (SIGSAC), and is on the Executive Committee of ACM SIGSAC. He is an editor for Springer Briefs in Computer Science, responsible for Briefs on information security. He has served or is serving on the editorial boards of several international journals, including ACM Transactions on Sensor Networks, Journal of Computer Security, Ad-Hoc Networks, Ad-Hoc & Sensor Networks; an International Journal, International Journal of Security and Networks, and IET Proceedings Information Security. He also served as the Program Chair or Co-Chair for ACM SASN ’05, ICICS ’06 and ESORICS ’09, ICDCS-SPCC ’10, and NDSS ’13, the General Chair of ACM CCS ’07 & ’08, and Program Vice Chair for ICDCS ’09 & ’10 – Security and Privacy Track. He served on the Steering Committee of ACM CCS from 2007 to 2011, and is a founding Steering Committee member of ACM WiSec and ICDCS SPCC. His research has been supported by NSF, Army Research Office (ARO), the Advanced Research and Development Activity (ARDA), IBM Research, SRI International, and the NCSU/Duke Center for Advanced Computing and Communication (CACC). Peng Ning is a senior member of the ACM, the ACM SIGSAC, and a senior member of the IEEE. http://discovery.csc.ncsu.edu/~pning/

Rudra Dutta was born in Kolkata, India, in 1968. After completing elementary schooling in Kolkata, he received a B.E. in Electrical Engineering from Jadavpur University, Kolkata, India, in 1991, a M.E. in Systems Science and Automation from Indian Institute of Science, Bangalore, India in 1993, and a Ph.D. in Computer Science from North Carolina State University, Raleigh, USA, in 2001. From 1993 to 1997 he worked for IBM as a software developer and programmer in various networking related projects. He has been employed from 2001 - 2007 as Assistant Professor, from 2007 - 2013 as Associate Professor, and since 2013 as Professor, in the department of Computer Science at the North Carolina State University, Raleigh. During the summer of 2005, he was a visiting researcher at the IBM WebSphere Technology Institute in RTP, NC, USA. His current research interests focus on design and performance optimization of large networking systems, Internet architecture, wireless networks, and network analytics.

His research is supported currently by grants from the National Science Foundation, the National Security Agency, and industry, including a recent GENI grant and a FIA grant from NSF. He has served as a reviewer for many premium journals, on NSF, DoE, ARO, and NSERC (Canada) review panels, as part of the organizing committee of many premium conferences, including Program Co-chair for the Second International Workshop on Traffic Grooming. Most recently, he has served as Program Chair for the Optical Networking Symposium at IEEE Globecom 2008, General Chair of IEEE ANTS 2010, Steering Committee of IEEE ANTS 2011-13, and as guest editor of a special issue on Green Networking and Communications of the Elsevier Journal of Optical Switching and Networking. He currently serves on the editorial board of the Elsevier Journal of Optical Switching and Networking.

Wenbo Shen received his Ph.D. degree in computer science from North Carolina State University, Raleigh, in 2015, the B.S. degree from Harbin Institute of Technology, Harbin, China, in 2010. His research area is the wireless network and system security, mainly focusing on leveraging physical layer signal properties to preserve the wireless security.