The Security of Link Signature: A View from Channel Models

Xiaofan He†, Huaiyu Dai†, Yufan Huang† and Dong Wang†
†Department of ECE
North Carolina State University, USA
Email: {xhe6,hdai,yhuang20,dwang18}@ncsu.edu

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

Abstract—Link signature (LS) provides security to wireless devices by exploiting multipath characteristics, with an essential assumption that half-wavelength separation is sufficient to prevent nearby adversary sensors from effectively inferring the legitimate LS. However, such an assumption may be too optimistic; high channel correlation has been observed in real world experiments even when the spatial separation is much larger than half-wavelength. In fact, channel correlation varies for different wireless environments. Considering this, various well-established channel correlation models are investigated in this work and a set of physical factors that have significant influence on link signature security are identified. With the obtained insights, we build a generic channel correlation model for LS security assessment in various wireless environments of interest. Numerical experiments are conducted to explore corresponding guard zone designs.

I. INTRODUCTION

As compared to conventional cryptography methods that land their security assurances on pre-shared secret and/or computational-complexity, link signature (LS) exploits the physical layer multipath channel characteristics between two wireless devices to provide security protections. A fair amount of works have been done on LS based security mechanisms, with focus on two prominent ones – secret key generation [1] and location distinction (a.k.a physical layer authentication) [2].

Before celebrating these promising results, it is worth noting that all the secrecy established by LS is contained in the channel information, and a fundamental assumption for LS is that two wireless channels are essentially de-correlated when the spatial separation of the corresponding devices is greater than half-wavelength. In fact, as discussed in [3, 4], when the correlation between the legitimate channel and the channel of an adversary sensor deployed nearby is sufficiently high, the attacker can employ estimation technique to infer the legitimate channel with high accuracy so as to thwart the promised security by LS. In addition, high channel correlations have been observed in real world experiments [5] even when the spatial separation is much larger than half-wavelength. This suggests that the spatial channel correlation may vary in different environments and the half-wavelength de-correlation assumption may not always hold. To ensure the security protection promised by LS in such environments, guard zones can be deployed around the legitimate devices to create sufficient legitimate-to-adversary device separation. This in turn leads to the problem of how to determine a suitable guard zone size, as a too large guard zone increases deployment costs and reduces feasibility of LS in practice.

Considering these facts, a more clear understanding of how the channel correlation varies over space in different communication environments is necessary for a more confident LS security assessment. In literature, various channel models have been proposed to characterize the spatial channel correlations for conventional communications in indoor picocell and outdoor micro-/macro-cell communications. This work studies how these well-established models can be applied to characterize the correlation between the legitimate and the adversary channels in the LS context, through which, a set of physical factors that have significant influence on LS security are identified. Based on the obtained understandings, a generic channel correlation model is developed for LS security assessment. With this model, suitable guard zone sizes are numerically explored for LS based security mechanisms to defend against the correlation attack [4], in several typical indoor and outdoor communication scenarios.

The rest of this paper is organized as follows. Section II discusses the relation between channel correlation and LS security. Important factors and models influencing channel correlations are explored in Section III and Section IV, respectively. The security of LS and corresponding guard zone sizes are numerically investigated in Section V. Conclusions are given in Section VI.

II. CHANNEL CORRELATION AND LS SECURITY

Since all the secrecy created by LS is contained in the channel information between the legitimate transmitter (t) and receiver (r), the correlation between the legitimate channel \( h_{t,r} \) and the transmitter-to-adversary sensor channel \( h_{t,a} \), defined as

\[
\rho \triangleq \frac{\mathbb{E}[h_{t,r} h_{t,a}^*] - \mathbb{E}[h_{t,r}] \mathbb{E}[h_{t,a}^*]}{\sqrt{\text{Var}(h_{t,r}) \text{Var}(h_{t,a}^*)}},
\]

(1)

is of paramount importance for LS security. In particular, through the correlation attack proposed in [4], the attacker can obtain an estimate \( \hat{h}_{t,r} \) of the legitimate channel based on

\[
\hat{h}_{t,r} = \hat{\rho} \cdot \hat{h}_{t,a} = \rho \cdot h_{t,a} + \sqrt{1 - \rho^2} \cdot \hat{h}_{t,a}.
\]

In (1), \( \rho, \mathbb{E}[] \) and \( \text{Var}[] \) denote the conjugate, the expectation and the variance operators, respectively.
its own channel measurement $h_{t,a}$’s by deploying adversary sensors near the legitimate receiver. For a single adversary sensor, the normalized mean-square error (NMSE) of $h_{l,r}$ is $(1 - \rho^2)$ when linear minimum mean square error (MMSE) estimation is adopted, and the accuracy can be further enhanced by deploying multiple adversary sensors [4]. This implies that the LS itself may not be secure when the channel correlation coefficient $\rho$ is sufficiently high.

Considering that most of the existing LS based applications (e.g., [1, 2]) utilize channel envelope information $|h|$, in all simulations, we focus on channel envelope correlations $\rho^{|env}| \triangleq \frac{\mathbb{E}[|h_t|^2| |h_r|^2]}{\sqrt{\mathbb{E}[|h_t|^4] \mathbb{E}[|h_r|^4]}}$, which is related to the complex channel correlation coefficient $\rho$ through $\rho^{|env}} \approx |\rho|^2$ [6].

III. MODELS AND KEY FACTORS FOR CHANNEL SPATIAL CORRELATION

In this section, through investigating existing channel models, key factors to channel spatial correlations and LS security are identified.

A. One-Ring Model and Angle Spread

We start from the well-known one-ring model [7, 8], which is originally designed to characterize base station-to-mobile user communications in outdoor micro/macro-cell systems. In this model, one communication end is surrounded by rich scatterers while the other end experiences much less diffusion, as depicted in Fig. 1. In this model, the correlation between a pair of channels $h_{pq}$ and $h_{p'q'}$ is given by [7]

$$\rho_{pq,p'q'} = \int_{-\pi}^\pi \exp \left( \frac{2\pi j}{\lambda} \left[ d_{pp'} \cos(\theta_T - \varphi) + d_{qq'} \cos(\theta_R - \theta) \right] \right) f(\theta) d\theta,$$

where $\theta_T$ ($\theta_R$) is determined by the azimuth positions of the transmitters (receivers); $d_{pp'}$ ($d_{qq'}$) is the spatial separation between the transmitters (receivers); $\Delta \triangleq \arcsin(R/D)$ is termed the angle spread; $f(\theta)$ is the power azimuth spread (PAS) that characterizes the scatterer density at azimuth $\theta$ on the ring; and $\varphi$ admits

$$\sin(\varphi) = \Delta \sin(\theta)/\sqrt{1 + \Delta^2 + 2\Delta \cos(\theta)},$$

$$\cos(\varphi) = (1 + \Delta \cos(\theta))/\sqrt{1 + \Delta^2 + 2\Delta \cos(\theta)}.$$

The general correlation model above can be used to model the channel correlation $\rho^{|env}|$ between the legitimate and the adversary receivers in the LS security context. As an example, Fig. 2 depicts the transmitter side scatterer-ring case, and the corresponding $\rho^{|env}|$ can be computed using (2) by setting $q = q'$ and replacing $\theta_T$ and $d_{pp'}$ by $\theta_R$ and $\delta d$, respectively.

Fig. 3 shows the channel correlations $\rho^{|env} under different angle spread $\Delta$'s. Several important observations can be made. 1) A small angle spread $\Delta$ always induces high channel correlation, when the scatterer-ring is on the transmitter side (Fig. 3(a)–3(b)). 2) By comparing Fig. 3(a) and Fig. 3(b), it can be seen that the adversary can obtain 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(b)) to 0.99 (Fig. 3(a)) by changing $\theta_R$ from $90^\circ$ to $0^\circ$, even when the spatial separation $\delta d$ is 10\lambda. In this case, the adversary can obtain nearly perfect estimate of the legitimate channel, causing severe security concerns. 3) In contrast, when the scatterer ring is on the receiver side, angle spread has no influence on channel correlation, and fast spatial decorrelation is always observed (Fig. 3(c)–3(d)). In such cases, the half-wavelength decorrelation assumption is valid.

B. Power Azimuth Spectrum and the Azimuth Spread

In the above discussion, uniform PAS ($f(\theta) = 1/2\pi$) is assumed, while various other PAS’s are also proposed in literature such as the cosine function PAS, the truncated Gaussian PAS, the von-Mises PAS, and the truncated Laplacian PAS [7, 9].

The azimuth spread (AS) is a generic metric to measure the concentrations of scatterers for different PAS’s, which is defined as \( AS \triangleq \sqrt{1 - |F_1|^2/|F_0|^2} \) with \( F_n = \int_{0}^{2\pi} f(\theta) \exp(jn\theta) d\theta \) the $n$th complex Fourier coefficient of
In addition to the (random) diffusion component, denoted with highly concentrated scatterers are not suitable for LS applications. This implies that environments with highly concentrated scatterers are not suitable for LS applications.

C. Rician Factor

In addition to the (random) diffusion component, denoted by $h_{\text{DIF}}$ in this subsection, caused by the scattering effect discussed above, a wireless channel may also contain a (deterministic) LOS component $h_{\text{LOS}}$. The so-called Rician factor is defined as the ratio power between them $K = |h_{\text{LOS}}|^2/[|h_{\text{DIF}}|^2]$. In the presence of the LOS component, the space-time correlation $\rho$ between two channels $h_{pq} = h_{pq}^{\text{DIF}} + h_{pq}^{\text{LOS}}$ and $h_{p'q'} = h_{p'q'}^{\text{DIF}} + h_{p'q'}^{\text{LOS}}$ is defined as [7]

$$\rho_{pq,p'q'} = \frac{\mathbb{E}[h_{pq}h_{p'q'}]}{\sqrt{\mathbb{E}[|h_{pq}|^2]|h_{p'q'}|^2]} = \rho_{pq,p'q'}^{\text{DIF}} + \rho_{pq,p'q'}^{\text{LOS}}, \quad (5)$$

where the space-time correlation for the diffusion component $\rho_{pq,p'q'}^{\text{DIF}}$ can be computed by (2) with a scaling factor $1/(1+K)$, and that for the LOS component is given by

$$\rho_{pq,p'q'}^{\text{LOS}} = \frac{K}{1+K} \exp \left\{ \frac{2\pi}{\lambda} \left[ d_{pq'} \cos(\theta_T) - d_{q'p} \cos(\theta_R) \right] \right\}. \quad (6)$$

Based on (5), it can be verified that large Rician factor induces high space-time correlation, which seemingly implies a severe vulnerability of LS when a strong LOS component exists. Considering this, existing LS based security applications are investigated as to how the LOS component is handled. It is found that, in LS based secret key generation algorithms, the LOS component is removed from the channel measurement before the key generation process [1,11–14], and that, in the location distinction algorithms, the LOS effect is also removed implicitly by comparing the difference between two channel measurements to the standard deviation (instead of the channel magnitude) [2,3,15–17]. Therefore, the existence of the LOS component will not have a significant impact on the security of these LS based applications. In the following, only the diffusion part will be considered.

D. Directive Antenna

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

When the adversary employs the same directive antenna as the legitimate receiver, the corresponding channel correlation can be computed using [9]

$$\rho = \int_{-\pi}^{\pi} \exp \left\{ \frac{2\pi}{\lambda} \delta d \cos(\theta_R - \theta) \right\} f(\theta) G(\theta) d\theta, \quad (7)$$

where receiver side scattering is assumed. It is worth noting that mathematically the PAS $f$ and the antenna radiation pattern $G(\theta)$ have equivalent impacts on channel correlation as can be seen from (7). In addition, it can be observed from Fig. 5 that highly directional antennas (with small $\theta_{\text{dB}}$) can induce large channel correlations. The reason is that directive antenna reduces the angle range of the incoming signals reflected from scatterers and equivalently leads to a more concentrated PAS.

Fig. 4. Spatial correlation function for different PAS’s using one-ring model with $\Delta = 5^\circ$, $\theta_T = 0$ and $\theta_R = 0$ (‘Tr’: truncated).

Fig. 5. Comparison of $\rho_{\text{env}}$ with different directive antenna patterns ($\theta_R = 90^\circ$, $\theta_G = 0^\circ$, $\theta_{\text{max}} - \theta_{\text{min}} = 20^\circ$).

IV. OTHER MODELS FOR DIFFERENT SCATTERING ENVIRONMENTS

To characterize channel correlation in other different scattering environments, several other models are discussed in this section.

A. Single-bounce Two-ring Model

In a 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. 6. With this assumption, the single-bounce model is in fact a weighted superposition of two one-ring models with corresponding scatterer-rings on the transmitter (Fig. 2) and receiver sides, respectively [19]. The correlation due to transmitter side scatterers is given by

\[ \rho^{(SBT)} = \int_{-\pi}^{\pi} \exp\left(\frac{2\pi j}{\lambda}[\delta d \cos(\theta_T - \varphi)]\right)f_T(\theta')G_T(\theta')d\theta', \quad (8) \]

where \( \theta' \) and \( \varphi \) admit similar relations in (3) and (4). The correlation due to receiver side scatterers is given by

\[ \rho^{(SBR)} = \int_{-\pi}^{\pi} \exp\left(\frac{2\pi j}{\lambda}[\delta d \cos(\theta_R - \theta)]\right)f_R(\theta)G_R(\theta)d\theta. \quad (9) \]

The overall correlation is given by

\[ \rho^{(SB)} = \left(\eta_{SBT} \cdot \rho^{(SBT)} + \eta_{SBR} \cdot \rho^{(SBR)}\right), \quad (10) \]

where \( \eta_{SBT} \) and \( \eta_{SBR} \) represent the strengths of the reflected signals from the two scatterer-rings, respectively, and admit \( \eta_{SBT} + \eta_{SBR} = 1 \). (For the purpose of LS security assessment where only one transmitter is considered, it can be verified that the double-bounce two-ring model in [20] reduces to one-ring model and hence is omitted in the interest of space.)

**B. Elliptical Ring Model**

In the elliptical scatterer-ring model, an elliptical scatterer-ring encloses both the transmitter and the receivers, as depicted in Fig. 7. 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, and the center-to-focus distance of the ellipse by \( a, b \) and \( \xi = \sqrt{a^2 - b^2} \), respectively, the corresponding channel correlation is given by [21] (and the discussions in Section III-D)

\[ \rho^{(E)} = \int_{-\pi}^{\pi} \exp\left(\frac{2\pi j}{\lambda}[\delta d \cos(\theta_R - \alpha_R)]\right)f_E(\theta)G_T(\alpha_T)G_R(\alpha_R)d\theta, \quad (11) \]

where the expression of \( \alpha_R \) as a function of \( \theta \) is determined by the geometry shown in Fig. 7.

The channel correlation behaviors under elliptical scatterer-ring modeling are shown in Fig. 8. It can be seen that a narrower elliptical scatterer-ring (i.e., smaller \( a \) with fixed \( \xi = 1 \)) will induce higher channel correlation.

\[ \text{TABLE I} \]

**IMPORTANT FACTORS FOR LS SECURITY. (O: ONE-RING, T: TWO-RING, E: ELLIPTICAL SCATTERER-RING, F: FAR SCATTERER-RING)**

<table>
<thead>
<tr>
<th>Factor</th>
<th>Applicable models</th>
<th>Favorable value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angle spread ( \Delta(\Delta_F) )</td>
<td>O, T (F)</td>
<td>maximum possible value</td>
</tr>
<tr>
<td>Scatterer distribution AS</td>
<td>O, T, E, 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_{d_B} )</td>
<td>O, T, E, F</td>
<td>omni-directional</td>
</tr>
<tr>
<td>Eccentricity ( \xi/a )</td>
<td>E, F</td>
<td>( \xi/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>

**C. Far Scatterer Ring Model**

Far scatterer ring model considers the scatterers that are distant from both communication ends, as depicted in Fig. 9. The corresponding channel correlation is given by

\[ \rho^{(F)} = \int_{-\pi}^{\pi} \exp\left(\frac{2\pi j}{\lambda}[\delta d \cos(\theta_R - \alpha_R)]\right)\cdot f_F(\theta)G_T(\alpha_T)G_R(\alpha_R)d\theta, \quad (12) \]

where the angle spread for the far scatterer-ring is defined as \( \Delta_F \triangleq \arcsin(R_F/D) \), and relevant parameters can be found in Fig. 9. As in the near-scatterer case, small angle spread, highly concentrated PAS and directive antenna pattern will induce high channel correlation.

**D. A Generic Model**

The key factors and models investigated previously are summarized in Table I, together with the corresponding most favorable values 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 developed as follows:

\[ \rho = \eta_{SBT} \cdot \rho^{(SBT)} + \eta_{SBR} \cdot \rho^{(SBR)} + \eta_E \cdot \rho^{(E)} + \eta_F \cdot \rho^{(F)} \quad (13) \]

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 (8), (9), (11) and (12), 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-C. The one-ring model is a special case of the

\[ \text{Fig. 6. Single-bounce two-ring model.} \]

\[ \text{Fig. 7. Elliptical scatterer-ring model.} \]

\[ \text{Fig. 8. Correlation comparisons in elliptical scatterer-ring model.} \]

\[ \text{Fig. 9. Far scatterer ring model.} \]
single-bounce two-ring model captured here. 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).

V. SECURITY OF LS IN TYPICAL INDOOR/OUTDOOR ENVIRONMENTS

Suitable guard zone sizes for LS security assurance are explored in this section in three different typical wireless communication scenarios. In particular, the performances of two LS based security mechanisms, secret key generation [1] and location distinction [2], are investigated under the correlation attack [4] 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 (13) based on the corresponding environment parameters. We focus on presenting the results for one adversary receiver case in the interest of space; when multiple collaborative adversary receivers are deployed, even larger guard zones are needed.

Note that in the location distinction application [2], when the adversary can obtain an estimate of the legitimate channel with small NMSE, it can launch the mimicry attack [3] so as to spoof the detector that it is located at the same position as the legitimate transceiver. Further considering that, in practice different encryption/decryption 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 LS is thwarted if the NMSE 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 algorithm in [1] is implemented where $1 \times 10^4$ samples are generated for each channel and an excursion of length 4 is used. Finally, the (empirical) outage probability $P_{out}$, defined as

$$P_{out} \equiv \frac{\text{number of insecure environments}}{\text{total number of considered environments}}, \quad (14)$$

is employed as the metric for LS security assessment, and a non-zero $P_{out}$ implies the existence of environment(s) where the LS application is insecure.

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., $\eta_E = 1$). To account for various physical environments in this scenario, 42 different parameter combinations are considered. Particularly, $(a : b) \in \{(4 : 1), (4 : 2), (4 : 3)\}$, $PAS \in \{\text{uniform,von-Mises ($\kappa = 10, 50$; $\hat{\theta} = 0^\circ, 90^\circ, 180^\circ$)}\}$, $G_T \in \{\text{omni,} \theta_{SDT}^{(T)} = 40^\circ\}$ and $G_R \in \{\text{omni,} \theta_{SDR}^{(R)} = 40^\circ\}$.

Fig. 10 and Fig. 11 show the outage probabilities for LS based location distinction and secret key extraction, respectively. 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. 10, when $\delta d = \lambda/2$, in more than 50% of the 21 considered cases, the adversary can obtain an estimate of the legitimate LS with NMSE less than 0.1 and thus defeats the Lv1 security requirement of location distinction; it becomes even worse (i.e., larger $P_{out}$) when both the legitimate and adversary receivers adopt directive antennas (in the rest 21 cases). Similar observations can be made in Fig. 11 for LS based secret key extraction as well. In fact, the results in Fig. 10 and Fig. 11 suggest that a guard zone of size about $\delta d = 19\lambda$ is needed to achieve Lv1 security with zero outage probability for LS. In addition, our simulation results indicate that $\delta d = 37\lambda$ is needed when the adversary deploys two sensors (not shown here in the interest of space). For the more demanding Lv2 security, even larger guard zones are required.

In the second scenario (Scenario II), 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 $\eta_{SBT} = 0.9$ and $\eta_{SBR} = 0.1$ is employed to characterize the channel correlations, and 336 combinations of different parameter settings are examined. In particular, $\Delta \in \{2^\circ, 5^\circ, 10^\circ, 20^\circ\}$, $PAS_T \in \{\text{uniform,von-Mises ($\kappa = 10, 50$; $\hat{\theta} = 0^\circ, 90^\circ, 180^\circ$)}\}$, $PAS_R \in \{\text{uniform,von-Mises ($\kappa = 10, 50$; $\hat{\theta} = 0^\circ$)}\}$.
Better security protection for LS (i.e., smaller guard zones are needed), as compared to the previous two indoor scenarios. In this outdoor scenario, the dense local scatterers environments, and instead of assuming the commonly believed that the spatial channel correlation varies for different physical presence of a correlation attacker, so as to shed lights on the performances of LS based security mechanisms are needed. Based on this model, spatial correlation between the legitimate and the adversary channels for LS security assessment. Based on this model, addition, a generic model is developed to characterize the \[ \eta \]

Particularly, \[ \Delta \] and \[ \Delta_F \] \in \{ \text{uniform, von-Mises} (\kappa = 10, 50; \theta = 0^\circ, 90^\circ, 180^\circ) \}, PAS_R \in \{ \text{uniform, von-Mises} (\kappa = 10, 50; \theta = 0^\circ, 90^\circ, 180^\circ) \}, \gamma_T = 45^\circ, \gamma_R \in \{ 90^\circ, 135^\circ \} \) (for far scatterer-ring positions), \[ G_R \in \{ \text{omni, } \theta_3dB = 40^\circ \} \]. As it can be seen from Fig. 14 and Fig. 15 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.

VI. CONCLUSIONS

Through investigating channel correlation models and applying them in the LS context, several key factors that have important influence on LS security are identified in this work. In addition, a generic model is developed to characterize the spatial correlation between the legitimate and the adversary channels for LS security assessment. Based on this model, the performances of LS based security mechanisms are numerically explored for different wireless environments, in the presence of a correlation attacker, so as to shed lights on the corresponding guard zone designs. Simulation results indicate that the spatial channel correlation varies for different physical environments, and instead of assuming the commonly believed half-wavelength universally, more investigations on channel correlation for the specific environment of interest must be conducted before deploying the LS based security mechanisms confidently.

REFERENCES