On the half-wave assumption

# 1. From: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7120011> (2015)

“The literature is filled from with references to the wide-sense stationary” with uncorrelated scatterers channel assumption and Jake’s well uniform scattering model to declare that a received signal rapidly decorrelated over a distance of roughly half a wavelength, and concequently that spatial separation of one to two wavelengths is sufficient for assuming independent fading paths. This decorrelative property is used as the basis to conclude that it is hard for an adversary to estimate the channel that Alice and Bob experience. First is quantifying when we are in a sufficiently rich scattering environment. Alice and Bob need to verifiably assess that they are in a richly scattering environment before commencing with physical layer key establishment (or authentication). It must be realised that simple environments are the bane of physical layer security. Two examples bring the severity of this problem to light: freespace and a simple rectangular room (Fig. 1). In freespace, if Bob and Eve are the same distance from Alice, they will experience the same propagation phenomena (notably, just path loss). While in a rectangular room, it is possible to construct benign scenarios where the Alice-Bob channel is the same as the Alice-Eve channel. The community is already examining questions related to the security of the propagation assumption, such as [9], and I expect that the community will continue to find cases where poor environmental scattering undermines the security of key extraction and physical layer authentication.

A slightly more sophisticated adversary might be able to employ ray-tracing methods to predict the channel, and an important question to explore is how much the secret key rate is affected by an adversary’s ability to perform ray-tracing. Related to this is the interesting question of how complex the descriptive model for the environment must be in order to undermine physical layer security. I would note that ray-tracing has been used to validate physical layer authentication methods, and there is an amusing paradox here. The very tool used to validate physical layer authentication could also be employed by the adversary to undermine physical layer authentication: Eve could use the same ray-tracing to identify promising locations within a building to conduct spoofing attacks against Alice-Bob. Certainly, this is a matter of concern since many building blueprints are in the public domain, thereby facilitating ray-tracing analysis by an adversary. Developing tools that can estimate an environment’s “propagation” complexity in real time will be an important practical tool for supporting physical layer security. Of course, this begs the fundamental question of what the right notion of environmental channel complexity is for physical layer security. It is quite unlikely that the notions of delay spread and the K-factor will carry the appropriate properties needed for physical layer security.”

# 2. From: <https://dl.acm.org/doi/10.1145/1972551.1972559>

(On passive inference attacks against physical-layer key extraction?) That’s relevant to what you are doing.

Diagram

Description automatically generated

*“A key security assumption made in previous literature is that the signal envelope observed by an adversary located greater than a half-wavelength away is uncorrelated with that shared between the two communicating devices; however, this assumption has yet to be rigorously evaluated in previous work on physical-layer key extraction. In this paper, we present an experimental analysis that examines the relationship between the channel measurements used to extract a symmetric key between two devices and those observed by one or more distantly located passive adversaries. We find that, contrary to previous assumptions, there does exist a strong correlation in measurements observed by adversaries located significantly greater than a half-wavelength away from two communicating wireless devices. Further, we provide initial results that show the extent to which the adversary is able to leverage such correlations to infer portions of the key extracted between two devices using previously published physical-layer key extraction techniques”*

I need to compare my results with those (?) Ok. They do LoS scenarios only. It is expected to experience strong correlation XD My environments are trying to be non LoS with many scatterers. I use ray tracing. I use complex correlation instead of the envelope correlation.

# 3. Points that I need to make:

Using the phase information as well as the amplitude information result in smaller correlation, rather than using the envelope correlation.