Educated Eavesdropping

Quantifying the Security of Fading-Based Key Generation

***Abstract:*** The inherent variability of wireless fading channels, also known as the link signature, has recently attracted attention as a potential source of random numbers for symmetric key generation. The technique is attractive because

* No requirement to physically meet for key distribution because of reciprocity
* Key agreement like Diffie-Helman is computationally intensive and runs down mobile batteries
* Could potentially be information theoretically secure (ok against high-performance & quantum computing) because it depends on something that is actually random rather than the computational difficulty of an inverse problem

Encryption keying based on wireless link signatures cannot be adopted unless its level of security is quantifiable. Because of the structure of the problem, this takes the form of a minimum secure distance beyond which eavesdroppers cannot estimate the link signature between legitimate nodes. This is typically accomplished by examination of the channel correlation function’s spatial variation. We argue that the channel correlation function is not an appropriate metric because the mutual information between channel samples can vary much more slowly than the (typically oscillatory) correlation function.

The widespread assumption that the channel is secure beyond a half wavelength has been shown to be inapplicable for certain channels with low angular spread (He 2013). However, that analysis depends on the channel correlation function and does not capture situations where the correlation function is highly oscillatory but the environmental parameters of the channel do not change.

Toward that end, this work undertakes a more general analysis that includes all spatially non-ergodic channels and is based on the mutual information rather than the correlation function. The first objective of this work is to quantify eavesdropper capabilities in general using estimation theory and direction finding techniques. Second, the project will identify possible strategies for improving security based on eavesdropper estimation capability results.

***Intellectual Merit:*** The applicability of link signature keying depends on quantitative security analysis. The mutual information based approach proposed here is a fundamentally new technique for evaluating the security of link signature security.