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 channel’s reciprocity allows the nodes to agree on a key without physically meeting. It is particularly attractive in cases where two parties cannot pre-arrange or securely exchange keys.

Despite its unique features, 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 environmental parameters, and thus the mutual information between channel samples, can vary much more slowly than the correlation function.

It is already clear that the widespread assumption that the channel is secure beyond a half wavelength is inapplicable for certain channels with low angular spread (He *et al*., 2013). However, our preliminary results have shown that eavesdroppers may also estimate channels with wide angular spread and highly oscillatory correlation functions if the environmental parameters do not change rapidly.

The proposed analysis includes all spatially non-ergodic channels and is based on mutual information and estimation theory rather than the correlation function. The first objective of this work is to quantify eavesdropper capabilities in general through both analysis and experimentation. Second, the project will identify possible strategies for improving security based on eavesdropper estimation capability results.

***Intellectual Merit:*** The hybrid estimation theory and mutual information based approach proposed here is a fundamentally new technique for evaluating the security of link signature security.

***Broader Impact:*** This work will result in a significant advance toward practical applicability of link signature keying. It will provide interdisciplinary mentorship and training opportunities to graduate and undergraduate students in the most diverse student body in New England.