Educated Eavesdropping

Quantifying the Security of Wireless Fading-Based Key Generation

***Abstract:*** The link signature of wireless fading channels 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. Since key exchange protocols such as Diffie-Helman are computationally demanding, link signature keying is attractive if the communicating parties’ computational ability or power is low. It is also considered to have potential application as a security option against eavesdroppers with high computing power or quantum computing, since it ultimately depends on a random natural quantity.

Despite its unique features, link signature keying cannot be adopted unless its level of security is quantifiable. Such quantification takes the form of a minimum secure distance beyond which eavesdroppers cannot estimate the link signature of the channel between the legitimate nodes. We argue that the present method of estimating the minimum secure distance is dangerously optimistic. In the present literature, the correlation length is assumed to be a good estimate of the minimum secure distance. 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.

The first objective of this work is to quantify eavesdropper capabilities in general through both analysis and experimentation. Eavesdropper capabilities in spatially non-ergodic channels will be examined using spectral estimation. The approach may be extended to spatially ergodic channels using time difference of arrival techniques. The project will also 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 establishing the 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.