WINLAB Focus Project: Fingerprints in the Ether - Exploiting the Radio Channel to Enhance Wireless Security

Project Objectives:

The "Fingerprints in the Ether" project sought to address security problems in wireless systems by turning the nature of the wireless medium from a security disadvantage into a security advantage. In essence, rather than rely solely upon generic, higher-layer cryptographic mechanisms, as has been the norm, the investigating team has shown that it is possible to achieve a lower-layer approach that supports important security objectives, such as authentication and confidentiality. The enabling factor in "Fingerprints" is the fact that, in the rich multipath environment typical of wireless scenarios, the response of the medium along any transmit-receive path is *frequency-selective* (or in the time domain, *dispersive*) in a way that is *location-specific*. In particular, channel characterizations (e.g. a set of complex gains at different frequencies, or the impulse response at different time delays) decorrelate from one transmit-receive path to another if the paths are separated by the order of an RF wavelength or more.

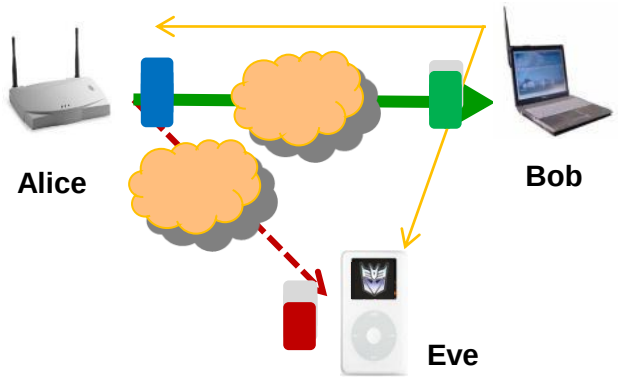
Technology Rationale:

The multipath wireless environment can be a powerful source of secret information that can enhance traditional approaches to securing wireless networks.

Two lower-layer security services are possible:

- **Authentication/Identification:** The wireless channel, with its unique space, time and frequency decorrelation properties can be used to verify the authenticity of a claimed transmitter compared to that transmitter's prior channel history.
- **Confidentiality:** The channel may be used as a source of common-randomness to extract secret key information, or as a means to opportunistically convey keying bits in a secret manner.

The feasibility of such lower-layer security services is motivated by other notable historical paradigm shifts in wireless communication, such as code division multiple access (CDMA) systems, where the use of Rake processing transforms multipath into a diversity enhancing benefit.

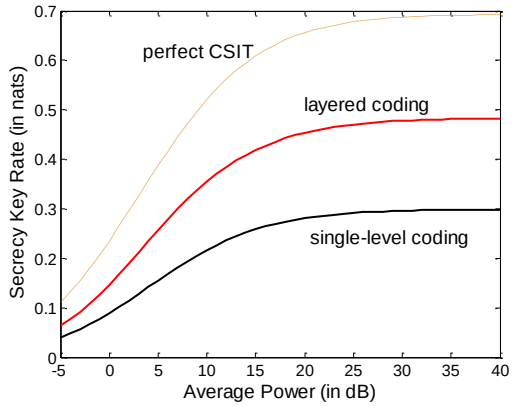


Technical Approach:

The research activities during the project involved several complimentary tracks: develop physical layer authentication protocols, develop physical layer secrecy protocols, and work to better understand the underlying propagation theory underpinning the proposed physical layer security work.

We have proposed an enhanced physical-layer authentication scheme for multi-carrier wireless systems, exploiting the spatial variability property of the radio channel in a rich scattering environment, as is typical of indoor environments. Simulation results show that it is efficient to discriminate legal transmitters from potential intruders, and is relatively robust against channel time variation due to environments and terminal mobility. We have built a significance test that exploits the spatial variability of propagation to enhance the authentication in a time-invariant channel [1]. Then we explored its performance in a time-variant channel, caused by environment changes [2]. We also proposed a scheme

to solve the terminal mobility problems, by introducing the concept of inter-burst keys [3]. Additionally, we have investigated the application of physical layer security for defending against Sybil attacks [5].



The Fingerprints project also uses the properties of the wireless channel to support confidential communications. There are two different strategies to achieve secret communication: (1) exploit the fact that the wireless channel may itself be considered a source of shared, secret information; and (2) code communications in a manner to ensure that an adversary can't successfully decode information. For the first strategy, the team has developed algorithms that exploit the reciprocal and decorrelative nature of the wireless channel to generate a cryptographic key between legitimate parties that is guaranteed to be concealed from any number of eavesdropping adversaries. The team evaluated the secret key generation rate using channel impulse responses collected from quasi-static indoor wireless environments, and have developed a key generation scheme that is capable of generating secret bits at roughly 0.5 - 1.0 bits/second at a 20dB SNR-a result that is approximately 0.2 - 0.5 bits/second less than theoretical limits. These results were empirically shown using indoor channel sounding measurements and through system implementations using a custom 802.11a platform [7][8]. For the second approach to confidential wireless communication, the investigating team has shown that the variations in wireless medium can significantly facilitate secret communication in the presence of a passive eavesdropper[9].

References and Published Papers:

[1] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in Proceedings of the IEEE Int.. Conf. on Comm., 2007, pp. 4646 – 4651.

[2] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "Channel-based Spoofing Detection in Frequency-Selective Rayleigh Channels," in IEEE Transactions on Wireless Communications, vol. 8, Issue 12, pg. 5948-5956, Dec. 2009.

[3] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals," in Proceedings of the 2008 IEEE International Conference on Communications, pg. 1520-1524, May 2008.

[4] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "MIMO-assisted Channel-based Authentication in Wireless Networks," in Proceedings of the 42nd Annual Conference on Information Sciences and Systems, pg. 642-646, 2008.

[5] L. Xiao, L. Greenstein, N. Mandayam, W. Trappe, "Channel-Based Detection of Sybil Attacks in Wireless Networks," in IEEE Transactions on Information Forensics and Security, vol. 4, Issue 3, pg. 492-503, Sept. 2009.

[6] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in WiSe '06: Proceedings of the 5th ACM workshop on Wireless security, 2006, pp.33–42.

[7] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in Proc. of the 14th annual conference on mobile computing and systems (MobiCom 2008), San Francisco, CA, Sept 2008.

[8] C. Ye, S. Mathur, A. Reznik, W. Trappe and N. Mandayam, "Information-theoretically Secret Key Generation for Fading Wireless Channels", in IEEE Transactions on Information Forensics and

Contact:

Prof. Wade Trappe (trappe at winlab.rutgers.edu)