Alice and Bob Get Physical: Insights into Physical Layer Security

by Wade Trappe, Rutgers University

Date: November 10, 2008 (Monday)
Time: 6:00 pm (refreshment starts at 5:45 pm)
Place: 202 ECEC, NJIT

About the Speaker

Wade Trappe received his B.A. degree in Mathematics from The University of Texas at Austin in 1994, and the Ph.D. in Applied Mathematics and Scientific Computing from the University of Maryland in 2002. He is currently an associate professor in the Electrical and Computer Engineering Department at Rutgers University, and is Associate Director of the Wireless Information Network Laboratory (WINLAB). His research interests include wireless security, wireless networking, multimedia security, and network security. While at the University of Maryland, Dr. Trappe received the George Harhalakis Outstanding Systems Engineering Graduate Student award. Dr. Trappe is a co-author of the textbook Introduction to Cryptography with Coding Theory, Prentice Hall, 2001. He is the recipient of the 2005 Best Paper Award from the IEEE Signal Processing Society. He is a member of the IEEE Signal Processing and Communications societies, and a member of the ACM.

About the Talk

Although conventional cryptographic security mechanisms are essential to the overall problem of securing wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats. The properties of the wireless medium are a powerful source of domain-specifc information that can complement and enhance traditional security mechanisms. Recently, the fact that the radio channel decorrelates rapidly in space, time and frequency has led to a growth of new security research "at the physical layer". In this talk, we present an overview of authentication and confidentiality services that operate at the physical layer and can be used to facilitate cross-layer security paradigms. Specifcally, for authentication services, we show how channel probing techniques can verify the authenticity of a transmitter (thus thwarting spoofing attacks), as well as provide a means to ensure that a transmitter claims a single identity (thus thwarting Sybil attacks). Similarly, for confidentiality, we examine several strategies for establishing shared secrets/keys between two communicators using the wireless medium. These strategies range from extracting keys from channel state information, to utilizing the channel variability to secretly disseminate keys. We present the results of validation efforts to support these techniques, including real system implementations involving a customized 802.11a platform, which uses channel impulse responses estimated from preambles to establish secret bits at a rate of 1b/sec in a typical indoor office environment. Lastly, in the spirit of good security research, we identify potential "security pitfalls" with physical layer security-- problems that suggest that the physical layer security field has a lively future ahead of it.

Sponsors: **IEEE Communications Society North Jersey Chapter**
NJIT Department of Electrical and Computer Engineering

For more information contact Nirwan Ansari (973)596-3670 or Yanchao Zhang (973)642-7817. Check **http://web.njit.edu/~ieeenj/comm.html** for latest updates. Directions to NJIT can be found at: **http://www.njit.edu/University/Directions.html**.