Title: Wireless Information Assurance Going Forward

Speaker: Prof. Srikanth Krishnamurthy,
Department of Computer Science and Engineering, University of California, Riverside

There has been a rapid and extensive proliferation of wireless networks in the last decade. The anytime, anywhere connectivity has made these networks attractive in every sense. However, research in wireless networking and security have followed seemingly disjoint paths. Wireless network protocol design has focused on performance ignoring to some extent, security implications. While wireless security has recently taken off, the hit in terms of performance has not been adequately studied. To secure today's wireless networks, some of the vulnerabilities that exist will have to be addressed, possibly with patchwork solutions. More importantly, going forward needed is a holistic view of security and performance and a new paradigm of thinking in designing protocols and architectures. I will first highlight some new directions that are being pursued in this context under a newly funded academic research center by the Army Research Laboratories.

Following, I will describe some of the more focused research problems in security that our group is addressing. First, I will focus on a specific attack related to the manipulation of the carrier sense or Clear Channel Assessment (CCA) threshold in 802.11 networks. Tuning the CCA has been proposed for improving spatial reuse in 802.11 networks. A malicious or selfish user can however, exploit this functionality to obtain an unfair share of the available bandwidth. I will then describe the design and implementation of a system to detect such an exploitation in 802.11 WLANs.

Next, I will describe some of our more recent work, relating to trustworthy routing in multi-hop wireless networks. Trust, in the social context, depends on the success of transactions between human users. However, unlike in wireline settings, trust depends on wireless channel induced factors, interference, and the trustworthiness of intermediary relays to a destination. One of the challenges that we seek to address is to model and understand the establishment and time evolution of trust while accounting for these factors. Choosing a trustworthy path could have implications on performance; on the other hand, choosing a high performance path may limit the extent to which a source can trust the path. We examine these trade-offs by jointly considering the above factors. We seek to design an intelligent routing framework that yields the desired trade-offs.

==========

Short Biography:

Srikanth V. Krishnamurthy received his Ph.D. degree in electrical and computer engineering from the University of California at San Diego in 1997. From 1998 to 2000, he was a Research Staff Scientist at the Information Sciences Laboratory, HRL Laboratories, LLC, Malibu, CA. Currently he is a professor of Computer Science at the University of California, Riverside.

His research interests are primarily in wireless networks and security. Dr. Krishnamurthy is the recipient of the NSF CAREER Award from ANI in 2003. He was the editor-in-chief for ACM MC2R from 2007 to 2009.