NJIT New Jersey's Science & Technology University

IEEE COMMUNICATIONS SOCIETY North Jersey Chapter

IEEE Signal Processing Society North Jersey Chapter

A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environment

by Ming Yu, Florida State University

Date: March 10, 2009 (Tuesday)
Time: 6:00 pm (refreshment starts at 5:45 pm)
Place: 202 ECEC, NJIT

About the Speaker

Ming Yu received his Ph.D. from Rutgers University, New Brunswick, NJ, in 2002, and a Doctor of Engineering from Tsinghua University, Beijing, in 1994, both in Electrical and Computer Engineering. He is an assistant professor in the Dept. of Electrical and Computer Engineering, Florida State University, Tallahassee, FL. Before 2006, he was with the Dept. of Electrical and Computer Engineering, State University of New York at Binghamton for three years and with AT&T Labs, Middletown, NJ and other companies for six years. His research interests are MAC and routing protocols for wireless networks, radio resource management, network traffic modeling, and network fault management.

Ming Yu has served as NSF IT Research Panelist and NSF Cyber Trust Panelist. He has been a reviewer for many journals and TPC member, session chair and reviewer for many conferences including IEEE GLOBECOM, ICWMC, and WCNC. He was the financial chair of the 2006 IEEE IWAT and a guest editor for a special issue of the Int. Journal of Wireless and Mobile Computing. He was a winner of the IEEE Millennium Medal awarded by the IEEE USA on May 2000.

About the Talk

To secure a mobile ad hoc network (MANET) in adversarial environments, a particularly challenging problem is how to feasibly detect and defend possible attacks on routing protocols, especially the internal attacks, such as Byzantine attack. In this talk, we present a novel algorithm that detects internal attacks by using both message and route redundancy during route discovery. The route discovery messages are protected by pair-wise secret keys between a source and destination and some intermediate nodes along a route established by using public-key cryptographic mechanisms. We also propose an optimal routing algorithm with routing metric combining both requirements on a node's trustworthiness and performance. A node builds up the trustworthiness on its neighboring nodes based on its observations on the behaviors of the neighbor nodes. Both of the proposed algorithms can be integrated into existing routing protocols for MANETs, such as AODV and DSR. The simulation results have demonstrated the significant advantages of the proposed attack detection and routing algorithm over some known protocols.

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

For more information contact Nirwan Ansari (973)596-3670 or Yun-Qing Shi (973)596-3501. 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**.