NJIT
New Jersey's Science & Technology University

IEEE
COMMUNICATION
SOCIETY
North Jersey Chapter

Timing Covert Communications: A Method for Keyless Security

by Shamik Sengupta, Stevens Institute of Technology

Date: December 11, 2008 (Thursday)
Time: 6:00 pm (refreshment starts at 5:45 pm)
Place: 202 ECEC, NJIT

About the Speaker

Shamik Sengupta is presently appointed as a Post-Doctoral researcher in Department of Electrical and Computer Engineering at Stevens Institute of Technology, NJ with Prof. R. Chandramouli. Prior to that, Shamik Sengupta received his Ph.D. from the School of Electrical Engineering and Computer Science at the University of Central Florida in 2007 under the guidance of Prof. Mainak Chatterjee. His research interests include keyless security in wireless networking, dynamic spectrum access, cognitive radio, network economics, auction and game theories, and WRAN technologies. Currently, Shamik Sengupta serves on the organizing and technical program committee of several IEEE international conferences.
Email: Shamik.Sengupta@stevens.edu

About the Talk

Covert channels primarily refer to the concept of stealth channel and hidden information. For example, timing covert channels are secret operations existing in a normal communication channel where the output alphabet is constructed from different inter-arrival timing of the packets. Thus timing covert channels does not use header or payload embedded information to encode covert messages. Due to its special capability of key-less security and camouflaging, covert channels are gaining popularity recently in wireless networking to secure information. However, currently, there is little understanding on how such a timing covert networking with multiple timing covert communications simultaneously would operate so as to make the system secure from defense and security perspectives amidst foreign adversaries in dynamic spectrum access systems.

In this research, we present a game-theoretic framework to model an attack-defense scenario in tactical network dynamic spectrum access system with multiple timing covert channels based on cognitive radio nodes. An attacker (eavesdropper), which might possibly be another cognitive radio node from a competitor network or a competitor agent (e.g., terrorist organization), wants to sense the real time secret messaging by sensing/snooping into the spectrum bands and upon successful detection, tries to destroy (jam) the ongoing timing covert operations. To defend the attack successfully, DSA system, on the other hand, can potentially enable multiple auxiliary cognitive radio node communications in the spectrum bands dynamically that help the timing covert communications in each of the spectrum bands to camouflage. We analyze the scenario with two-tier game model: i) sensing game (with passive eavesdropper) and ii) jamming game (with active destroyer). With regard to the aforementioned secrecy model, we propose a dynamic minimax camouflaging strategy for DSA system and sensing and jamming strategies for attacker to capture the conflict of interest between attacker and the DSA system, both of whom try to maximize their respective net utilities. We show that even in such a greedy and non-cooperative behavioral game model, it is in the best interest of the attacker and DSA system to adhere to the proposed strategies to achieve equilibrium point. Through numerical analysis and simulation results, we show that how game strategies can be used as an effective tool for developing secure timing covert networking based on DSA.

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**.