Power Systems Engineering Research Center

False Data Injection Attacks: Feasibility of Limited Knowledge Attacks and Scalability of Attacks on Large Power Systems

Lalitha Sankar

Electrical, Computer and Energy Engineering Department
Arizona State University
lsankar@asu.edu

PSERC Public Webinar
September 5, 2017
2:00-3:00 p.m. Eastern Time (11:00-12:00 p.m. Pacific)

Description: The electric power system is vulnerable to false data injection (FDI) attacks wherein the attacker can change SCADA measurements within a small sub-network. It has been shown that FDI attacks can be designed to be unobservable to the bad data detection module of the electric power energy management system (EMS). More recently, we have shown that FDI attacks can also be designed to cause physical damage, specifically line overflows, that are unobservable to the EMS. In this talk using a synthetic network model for the Washington state, we will first demonstrate the ability of such an unobservable attack to cause post-contingency violations.

We will then address two questions about such FDI attacks: (i) how much knowledge does an attacker need? In other words, can an attacker with knowledge of only a small sub-network and limited knowledge of the rest of the network be successful in causing line overflow FDI attacks?; and (ii) are line-overflow-causing FDI attacks scalable, i.e., are large power systems vulnerable to FDI attacks wherein the attacker only affects a small sub-network? We address both questions by introducing a bi-level optimization problem to model the attacker's strategy to determine the attack vector; the first level of such a bi-level problem maximizes the target line chosen by the attacker to cause an overflow under constraints on limited attack resources, while the second level formulates system responses to such attacks via DC optimal power flow (OPF). Our results demonstrate the vulnerability of EMS to limited information FDI attacks and show that even large systems are vulnerable to such attacks. This is joint work with Jiazi Zhang, Zhigang Chu, and Oliver Kosut.

Biography: Lalitha Sankar received a B.Tech degree from the Indian Institute of Technology, Bombay, an M.S. degree from the University of Maryland, and a Ph.D degree from Rutgers University. She is presently an Assistant Professor in the ECEE department at Arizona State University. Prior to this, she was an Associate Research Scholar at Princeton University. Following her doctorate, Dr. Sankar was a recipient of a three year Science and Technology teaching postdoctoral fellowship from the Council on Science and Technology at Princeton University. Her research interests include information privacy and security in distributed and cyber-physical systems. For her doctoral work, she received the 2007-2008 Electrical Engineering Academic Achievement Award from Rutgers University. She received the IEEE Globecom 2011 Best Paper award for her work on side-information privacy. She received the NSF CAREER award in 2014.