Abstract:
Smart Grid, a typical energy-based Cyber-Physical System (CPS), uses modern advanced communication technologies to make the power grid more efficient, reliable, secure and resilient. It supplies electric power from various generators through power transmission and distribution networks to large geographical areas. Nevertheless, the Smart Grid may operate in hostile environments and lacking tamper-resistance hardware for sensor and meters increases the chance to be compromised by cyber-attackers. Through the compromised nodes, the attackers may inject false measurement reports and disrupt the operation of smart grid. In this talk, I will begin with the introduction of smart grid and its security challenges. I will then present the study of two representative false data injection attacks against the state estimation and the distributed energy transmission and distribution, respectively. Lastly, I will discuss countermeasures against the afore-mentioned attacks.

Bio:
Dr. Wei Yu is currently an Assistant Professor in the Department of Computer and Information Sciences at Towson University. Before joining Towson University, he worked as a networking software developer for Cisco Systems, Inc. for nine years. His work at Cisco involves developing the world’s leading enterprise unified communication system. He received his Ph.D. degree in Computer Engineering from the Department of Computer Science and Engineering at Texas A&M University in May 2008. His research interests are in the areas of cyber space security, computer networks, and cyber physical systems. His research work has been published in premier security and system conferences such as IEEE S&P, ACM CCS, INFOCOM, ICDCS and journals such as ToN, TDCS, TC, TPDS, TMC, and TVT. He was invited to give research talks at National Reconnaissance Office (NRO), National Security Agency (NSA), and Army Research Laboratory (ARL). His research is currently supported by NSF, ARL, NIST, and AFRL.