Network Security in Smart Grid Communication Systems

Shengjie Xu, *University of Nebraska-Lincoln*

In smart grid, network security issues are more important than those in traditional power grid since it have adopted advanced communication technology to establish the two-way communication networks. Nowadays smart grid will be relied on sufficient network communications, with messages digitally secured through encryption and authentication. However, most current security schemes and protocols do not satisfy requirement of real-time communications in the smart grid, such as low latency, multicast, low key distribution overhead, etc. Because of this need for authenticating time critical multicast data in smart grid, one of our future work will study and explore appropriate time-critical multicast data authentication schemes for potential use in smart grid networks, especially vastly used in distributed networks. We will provide a detailed theoretical and practical analysis of security in terms of low latency, security against brute force attacks, massive distributed key management, flexibility and scalability of authentication scheme being deployed, and performance evaluation. After we provide through security analysis, future efforts will be considered on practical aspects of implementing this secure scheme. In our future study on AMI and neighborhood area networks, we will study and explore two topics: secure AMI networks and secure data aggregation protocols. Because of the highly-distributed nature of the AMI network, it is expected that wireless technologies are to be used for efficient and low-cost deployment. The openness of the wireless communication medium can further expose information exchange to attackers targeting data integrity and confidentiality. In the AMI network, message delivery becomes non-time critical and availability is less important than integrity and confidentiality. Thus, we will focus primarily on providing integrity and confidentiality for the AMI network, and can also leverage existing solutions for the Internet and sensor networks. According to previous study in our group, it is evident that DoS attacks are crucial security threats to communication networks in the Smart Grid. Toward this challenge, we will study and perform some quantitative approaches of risk management analysis for AMI network, including probabilistic, graph based, attack-countermeasure tree based and security metric based methods. We will also study secure data aggregation protocols. Data aggregation can be an efficient and effective alternative for metering reading in the AMI network. We will examine on the pitfalls associated with current approaches, and improve them to provide better confidentiality, data integrity, and also be resilient to malicious attacks.