Prof. dr. J.L. Hurink (UT), ISoLATE

English scientific summary

The integration of renewable energy resources, controllable devices and energy storage into electricity distribution grids requires Decentralized Energy Management to ensure a stable distribution process. This demands the full integration of information and communication technology into the control of distribution grids. Supervisory Control and Data Acquisition (SCADA) is used to communicate measurements and commands between individual components and the control server. In the future this control is especially needed at medium voltage and probably also at the low voltage. This leads to an increased connectivity and thereby makes the system more vulnerable to cyber-attacks. According to the research agenda NCSRA III, the energy domain is becoming a prime target for cyber-attacks, e.g., abusing control protocol vulnerabilities. Detection of such attacks in SCADA networks is challenging when only relying on existing network Intrusion Detection Systems (IDSs). Although these systems were designed specifically for SCADA, they do not necessarily detect malicious control commands sent in legitimate format. However, analyzing each command in the context of the physical system has the potential to reveal certain inconsistencies.

We propose to use dedicated intrusion detection mechanisms, which are fundamentally different from existing techniques used in the Internet. Up to now distribution grids are monitored and controlled centrally, whereby measurements are taken at field stations and send to the control room, which then issues commands back to actuators. In future smart grids, communication with and remote control of field stations is required. Attackers, who gain access to the corresponding communication links to substations can intercept and even exchange commands, which would not be detected by central security mechanisms. We argue that centralized SCADA systems should be enhanced by a distributed intrusion-detection approach to meet the new security challenges. Recently, as a first step a process-aware monitoring approach has been proposed as an additional layer that can be applied directly at Remote Terminal Units (RTUs). However, this allows purely local consistency checks. Instead, we propose a distributed and integrated approach for process-aware monitoring, which includes knowledge about the grid topology and measurements from neighboring RTUs to detect malicious incoming commands. The proposed approach requires a near real-time model of the relevant physical process, direct and secure communication between adjacent RTUs, and synchronized sensor measurements in trustable real-time, labeled with accurate global time-stamps.

We investigate, to which extend the grid topology can be integrated into the IDS, while maintaining near real-time performance. Based on topology information and efficient solving of power flow equation we aim to detect e.g. non-consistent voltage drops or the occurrence of over/under-voltage and -current. By this, centrally requested switching commands and transformer tap change commands can be checked on consistency and safety based on the current state of the physical system. The developed concepts are not only relevant to increase the security of the distribution grids but are also crucial to deal with future developments like e.g. the safe integration of microgrids in the distribution networks or the operation of decentralized heat or biogas networks.

English public summary

Renewable energy requires advanced control networks. To ensure safe and secure energy distribution in complex networks, we build an additional security layer: Using the grid topology and real-time measurements from neighbouring stations, a model of the state of substations is maintained, which allows to identify malicious commands and false measurements.

Dutch public summary

Energie uit duurzame bronnen vraagt om geavanceerde aansturing. Voor dit complexere distributienetwerk ontwikkelen wij een extra beveiligingslaag om de beschikbaarheid te waarborgen. Met de opbouw van het verdeelnetwerk, real-time metingen bij aangrenzende verdeelstations en ons beveiligingsmodel zijn wij in staat om illegale commando's en foute metingen live te identificeren.