Cyber Security-Oriented EPS State Estimation Based on Test Equation Method

Irina Kolosok, Liudmila Gurina

Energy Systems Institute,
Lermontov St., 130, 664033 Irkutsk, Russia

The electric power systems (EPS) in the most advanced countries are developing towards the creation and large-scale adoption of smart grid which got the name of intelligent energy system in Russia. An attribute of the smart grid is cyber-physical intrusion tolerance of the network. Developing the conceptual smart grid models and projects, researchers nowadays, pay great attention to the issue of cyber security. In this connection it is necessary to note the elevated vulnerability of EPS information-communication infrastructure. Thus, it becomes essential to upgrade the existing mathematical tools and develop new ones to furnish the data of required quality to the tasks of EPS control and monitoring under internal and external impacts.

We consider the state estimation tool as a link between physical and information - communication infrastructures of EPS. It acts as a barrier to the corruption of data on current operating conditions of the electric power system in the control problem, including the data corruption caused by cyber attacks on data collection and processing systems of the EPS.

State estimation is a mathematical data processing method which is widely used for calculation of power system state variables on the basis of measurements. The most vulnerable facilities in terms of cyber attack consequences for state estimation are the information-communication control subsystems (SCADA and WAMS). Since the input data for the state estimation are represented by the SCADA measurements and PMU data. Due to cyber attacks on the SCADA and WAMS, measurement data coming to the state estimation problem are distorted. If no special measures are taken to identify these distortions and suppress their impact on the state estimation results, serious errors can appear in decisions made by dispatchers using the state estimation results. Therefore, to obtain quality state estimation results, the used measurements should be tested for the presence of bad data.

Researchers from Energy Systems Institute SB RAS have developed the method of test equations to detect bad data in traditional SCADA measurements and make state estimation. The main advantages of the test equation method are the opportunity to reduce the dimensionality of the problem and to use the obtained test equations for a priori detection of bad data in measurements.

The paper is concerned with the problem of identification and mitigation of the malicious cyber attacks in the EPS state estimation. To this end, we consider SCADA and WAMS structures, reveal vulnerable points, and analyze

potential cyber attacks. Special attention is paid to hidden cyber attacks, aimed at distorting the state estimation results.

In this connection, we propose an algorithm for detection and mitigation of cyber intrusions. The algorithm is based on test equations as an additional stage in state estimation. The SCADA data were used to implement the algorithm under simulated cyber attacks. The obtained results showed effectiveness of the algorithm in state estimation.