On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures

ABSTRACT:

It is critical for a power system to estimate its operation state based on meter measurements in the field and the configuration of power grid networks. Recent studies show that the adversary can bypass the existing bad data detection schemes, posing dangerous threats to the operation of power grid systems. Nevertheless, two critical issues remain open: 1) how can an adversary choose the meters to compromise to cause the most significant deviation of the system state estimation, and 2) how can a system operator defend against such attacks? To address these issues, we first study the problem of finding the optimal attack strategy—i.e., a data-injection attacking strategy that selects a set of meters to manipulate so as to cause the maximum damage. We formalize the problem and develop efficient algorithms to identify the optimal meter set. We implement and test our attack strategy on various IEEE standard bus systems, and demonstrate its superiority over a baseline strategy of random selections. To defend against false data-injection attacks, we propose a protection-based defense and a detection-based defense, respectively. For the protection-based defense, we identify and protect critical sensors and make the system more resilient to attacks. For the
detection-based defense, we develop the spatial-based and temporal-based detection schemes to accurately identify data-injection attacks.

EXISTING SYSTEM:

State estimation has been widely used by Energy Management Systems (EMS) at the control center to ensure that the power grid is running in desired states. It provides the estimation of system states in real time based on meter measurements in the field. The meter measurements are collected by the Supervisory Control and Data Acquisition (SCADA) Systems and processed by a state estimator to filter the measurement noise and to detect gross errors. The results of state estimation are then used by applications at the control center, for purposes such as contingency analysis, optimal power flow, economic dispatch, and others.

One can see that state estimation plays a critical role in the stability of power grid systems. Meter measurements collected via the SCADA system contain not only measurement noise due to the finite accuracy of meters and communication media, but also errors caused by various issues for example, meters with faulty connection and calibration.

To reduce the impact of noise and errors, power system researchers have developed numerous methods to process meter measurements after the state estimation process. The essential goal of these methods is to leverage the
redundancy of multiple measurements to identify and remove anomalies. While most existing techniques for protecting power grid systems were designed to ensure system reliability (i.e., against random failures), recently there have been growing concerns in smart grid initiatives on the protection against malicious cyber attacks. There are growing concerns in the smart grid on protection against malicious cyber threats and the operation and control of smart grid depend on a complex cyberspace of computers, software, and communication technologies. Because the measurement component supported by smart equipment (e.g., smart meters and sensors) plays an important role, it can be a target for attacks. As those measuring devices may be connected through open network interfaces and lacking tamper-resistance hardware increases the possibility of being compromised by the adversary.

**PROBLEM DEFINITION:**

1. The adversary can inject false measurement reports to the controller. This causes the controller to estimate wrong system states, posing dangerous threats to the operation of the power grid system.

2. If the controller to estimates wrong system states, posing dangerous threats to the operation of the power grid system.
PROPOSED SYSTEM:

In this paper, we study a novel problem of defending against false data-injection attacks from the system operator’s point of view. Because most adversaries are limited in the amount of resources they possess, we first consider a least-effort attack model—i.e., the objective of the adversary is to identify the minimum number of meters that one has to manipulate to change a predetermined number of state variables (so as to launch a false data-injection attack accordingly).

We prove the NP-hardness of this problem by reduction from the minimum subadditive join problem. To address this problem in a practical setting, we develop a linear transformation-based approach, which finds the optimal solution through the matrix transformation. Nevertheless, the computation complexity of the matrix transformation grows exponentially with the size of the power network. To address this issue, we develop a heuristic yet extremely efficient approach. Specifically, through the analysis of the H matrix, for a set of bus state variables, the adversary needs to compromise less meters when the buses are connected to one another with the largest degrees and connected to the least number of buses beyond its area. Based on this insight, we divide the network into a number of overlapping areas. The linear transformation or brute-force search (BF) can be used to identify the optimal set of meters for individual small areas and then derive the set of meters for the whole network.
We have implemented our proposed heuristic-based approach on power system state manipulation on various IEEE standard buses. Our extensive experimental data validate the feasibility and effectiveness of the developed approach.

ADVANTAGES OF PROPOSED SYSTEM:

1. The spatial-based detection algorithm is able to recognize at least 95 percent of the false data-injection attacks once the attack changes more than 6 percent of the state variable values.

2. The temporal-based detection algorithm can identify the compromised meters that send manipulated measurements quickly.

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.
SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7.
- Coding Language : JAVA/J2EE
- IDE : Netbeans 7.4
- Database : MYSQL