EEE – 5924 Smart Grid Communications

Summary of Chapter – 17

Power-System state-estimation security: attacks and protection Schemes

Presented by:

Tom DesRosiers

INSTRUCTOR:

Dr. Nabhi Jaber,

Dept. of Electrical and Computer Engineering

Lawrence Technological University

INTRODUCTION:

Supervisory control and data acquisition (SCADA) systems are implemented in most modern power transmission grids to assist with power control and management. The importance of SCADA systems makes them prime target for attacks. This paper will discuss features of a modern SCADA system with a focus on security vulnerabilities and protection.

SCADA systems must have accurate and timely data measurements such as voltage magnitude and power flow. Measurements are collected by meters in substations and then forwarded to a control center. Delivering the measurements from the substations to the control center is usually implemented by using wide area networks (WAN's). Since SCADA systems cover such a large geographic area WAN's are a practical choice when it comes to transporting data to the control center. Using WAN's for this purpose does present new security concerns.

The volume of measurements to process in a SCADA system is immense. It is not realistic for the SCADA system to be able to handle all these measurements when creating a state estimate of the entire system. Most SCADA systems use a model-based state estimator (SE) to create the estimate of the complete physical state of the system. The SE provides a model from which many important functions can be performed including detection of faulty equipment, identification of corrupted measurement data, optimal flow analysis, and contingency analysis. The importance of the state estimator (SE) is increasing as Smart Grids become less predictable with the inclusion of elements such as non-renewable power generation. Since the SE is such a pivotal part of the SCADA EMS (energy management system) it is a tempting target for attacks. Investigation into this vulnerability and potential protection methods is a primary focus of this discussion.

MEASUREMENT MODEL:

To simulate a transmission power network a steady state transmission model is considered. The model assumes the transmission power network has a total of *n* buses in a steady state. Each bus can be attached to either a power supply or power load. For this discussion of transmission power networks, the power supply is generally a power plant and the power load a distribution power grid (I.e. supplying power to a community). Each bus contains two possible states: phase angle δ_i and Voltage V_i. Since each bus can have two states the total number of states required to describe the system is $2n$. For most of this discussion a simpler model called *decoupled estimate* is used where only the *n* phase angles are considered the unknown. The basic measurement model is given by the equation:

$$z = h(x) + e \in \mathbb{R}^M \quad (equation\ 1)$$

M represents the total number of measurements available in the state estimator (SE) algorithm. The variable$e \in \mathbb{R}^M$ is a vector of independent random variables modelling measurement noise. The variable $h(x) \in \mathbb{R}^M$ represents the measurements' dependence on the state. Three types of measurements are considered in this model: power-flow, power-injection and PMU (phasor measurement unit) measurements (least common).

Power-flow measurements are the most common of the three types. A measurement of a power flow from bus *i* to bus *j* is modelled by the following:

$$z_k = h_k(x) = P_{ij} + e_k \quad (equation\ 2)$$

An active power-injection measurement such as a power plant at bus *i* is represented by:

$$z_k = h_k(x) = P_i + e_k \quad (equation\ 3)$$

A measurement of the phase angle in bus *i* is represented by:

$$z_k = h_k(x) = \delta_i + \delta_{GPS} + e_k \quad (equation\ 4)$$

The term δ_{GPS} from above represents a constant phase angle offset setting the frame of reference used by all PMU measurements in the system. The equations above give the basic framework of the measurement model.

STATE ESTIMATION AND BAD-DATA DETECTION (BDD):

The measurement model allows for the development of a state estimate for the system. This state estimate is derived using the weighted least squares estimate of the state and is represented by $\hat{x}$. The Bad Data Detection (BDD) system depend on $\hat{x}$ for predictions of the true power, injections, flows and angles. These predictions are compared to the measured data and the difference between the predicted and actual measurements is called the measurement residual *r*. If *r* is larger than expected the BDD flags an alarm triggering an algorithm which attempts to identify the bad measurements.

An attack on a SCADA system can potentially corrupt some of the measurement data without triggering an alarm in the BDD. This type of undetected attack is called a stealth attack. If we let a specific measurement be represented by *z* then an attack *a* on measurement z is represented by:

$$z_a := z + a \in \mathbb{R}^M \quad (equation\ 5)$$

The original measurement *z* is offset by the attack *a* resulting in the corrupted measurement z_a. A stealth attack occurs If the attack *a* does not trigger an alarm in the BDD. The BDD system only triggers when measurements deviate a set amount from a valid physical state. A stealth attack goes undetected when the corrupted value is too close to an acceptable state. If many corrupted stealth measurements are accepted as valid the measured state of the SCADA system will be off.

An attacker on the SCADA system would logically pursue the easiest (least costly) attack on the system. The cost of an attack is the difficulty or measurement of required effort to successfully implement the attack. While the attackers try to minimize the cost the system defenders try to maximize it.

The underlying communication infrastructure plays an important role on attack costs. Two SCADA network infrastructures are considered in this discussion Point-to-Point and routed. In Point-to-

Point SCADA systems are measurements from meters are sent to the control center over independent communication channels. Measurements in routed networks can travel through several substations on the way to the control center.

STEALTH ATTACKS OVER A POINT-TO-POINT SCADA NETWORK

Two types of attacks are considered with point-to-point SCADA networks. Stealth meter attacks require the attackers to gain access to each individual meter in order to perform a stealth attack against a specific measurement. The cost to the attacker is equal to the number of meters required to compromise the measurement. The protection cost for the operators is equal to the number of meters required to protect the system. The amount of investment required to tamper-proof meters is an example of a possible cost to the protectors.

Remote Terminal Units (RTU) multiplex measurement data from sensors to the control centers. RTU's present tempting targets for attackers. The cost to the attacker of an RTU attack is equal to the number of RTU's required to compromise the measurement.

The cost to the protectors or operators is equal to the number of RTU's to be defended. RTU protection can be accomplished by various methods including physically tamper proofing RTU units and utilizing cryptography for data authentication.

A mathematical model is created to quantify attack and protection costs. The set of measurements $\{1, \dots, M\}$ is partitioned forming $M = \{M_1, \dots, M_{|M|}\}$. An attack on any of the measurements contained in a specific partition M_j will result in an attack cost of one. The operators (protectors) can protect any measurements in partition $M_j$at a cost of one. There is also a set of protected measurements defined as $P \subseteq \{1, \dots, M\}$. The protected measurements in P cannot be attacked. This notation describes the basic model for performing analysis of several attack and protection cost models.

Stealth meter attacks result in the partition $M = \{\{1\}, \dots, \{M\}\}$. Since the attacker must attack each meter individually every element in partition M is a single measurement. When considering stealth RTU attacks each element in the partition represents a bus. For example, if you have n buses the number of partitions is $|M| = n$.

Attackers are interested in finding the minimum stealth attack cost. For this cost model this is equivalent to finding the minimum number of partition blocks required to complete the attack. Attackers cannot compromise any measurement belonging to the protected set P.

Two algorithms are presented to generate the minimum-cost stealth attack problem for a point-to-point SCADA system. A mixed integer linear (MILP) algorithm is used to find the minimum number of partitions to attack. The MILP algorithm requires a fair amount of computing power and is often solved using tools such as CPLEX and Gurobi.

The second algorithm used to solve the minimum-cost stealth attack problem is the Graph augmentation algorithm. This algorithm relies on iteration checking all possible attacks.

The MILP and Graph augmentation algorithms calculate exact solutions to the minimum cost stealth attack problem. Finding a solution using these algorithms can be resource demanding and time-consuming. Sometimes an approximation to the solution is sufficient. Two efficient algorithms are presented which approximate the solution to the minimum cost stealth attack problem. The first algorithm can rather quickly generate an upper bound for the minimum stealth attack cost. The second

algorithm uses a process called convex relaxation to generate the upper bound for the minimum stealth attack cost.

The protector (operator) is interested in finding the best possible protection against stealth attacks. Calculating the best protection scenarios can help if a model is used such that π is the budget or number of measurement-partition blocks which can be protected. The model defines a set of P protected measurements and $C_M(P)$ is the cost of protecting P considering the partition M. Perfect protection occurs when the set of protected measurements P is such that no stealth attacks are possible. In order to achieve perfect protection for a meter attack with no *PMU* measurements the required budget is $\pi = n - 1$ where n equals the number of buses in the network. For an RTU attack the required budget for perfect protection is calculated using a Dominating-set augmentation algorithm (DSA).

Situations occur where the operator's budget π is limited and cannot supply perfect protection. For these non-perfect protection situations, the protector is interested in finding the set of measurements P which maximize the system's protection level corresponding to a specific metric. Two commonly used metrics are the minimum attack cost and the average attack cost. The MSM (most shortest minimal-attack) algorithm is often used to find an optimal set of protected measurement P for the given budget π .

STEALTH ATTACKS OVER A ROUTED SCADA NETWORK

The routed network is the most common type of SCADA network infrastructure. Messages are delivered to the control center not through a routed network. When attacking a routed network infrastructure, the attacker would try to gain access to the switching equipment in substations. If the attacker successfully gained access to a substation, they would be able to manipulate the RTU and switching equipment. An attacker could manipulate data measured in the substation in addition to any data routed through that substation. Performing a stealth attack on a specific measurement may require that the attacker target several substations simultaneously.

One approach to protecting a routed SCADA network would be to install a secret key in the substation. A device called a bump-in-the-wire (BITW) is one option and it protects the data between it and the control center. The only drawback of the BITW is that it does not protect the data if an attacker gains physical access to the substation. Installing RTU's with message authentication support is another approach to protecting SCADA networks. To protect substation from outside and inside (physical) attacks the protector can install RTU's with tamper proof and authentication features built in.

The attack scenario for routed network infrastructures is modeled with n buses spread over a set of S substations. Two security metrics are considered when analyzing the vulnerability of the system. The first metric focuses on evaluating the vulnerability of individual measurements. The second metric focuses on quantifying the importance of individual substations.

The first metric is similar to the attack cost used for the meter and RTU attack models. This metric expresses the attack cost in terms of the number of attacked substations. The vulnerability of measurement k is defined as the minimum number of substations that must be attacked in order to perform a successful stealth attack against that measurement. This approach depends on the routing in set R, the encrypted substations in set $\mathcal{E}$ and the set of protected substations P.

The second metric quantifies the importance of a specific substation based on its attack impact I_s. The impact is the number of measurements an attacker can corrupt when performing a stealth attack on a single substation s. The attack impact relies on the power system topology and the routing set R, the encrypted substations $\mathcal{E}$, protected substations P.

The protector in a routed SCADA network has several options for protection including changing single-path routes, using multi-path routing, incorporating data authentication, or installing physical protection.

When deciding on alternate routes for a system the protector would want to find routes which minimize the attack impact I_s. The attack impact Is measures the amount of potential damage if an attack is successful.

Maximizing the attack cost is also a goal of the protector. Maximizing the attack cost makes it more difficult for an attacker to make a successful attack. A method called Critical First Algorithm can be used to test alternate protection schemes.

Modifying routes is less complex than deploying authentication or protection. One approach is to modify the routing to avoid vulnerable substations. Multi-path routing introduces another layer of complexity in the management of the communication system. The advantage of multi-path routing is that it can decrease the maximum attack impact by as much as 50%.

CONCLUSION

Supervisory Control and Data Acquisition Systems (SCADA) in transmission line systems play an important role in modern smart grid systems. The importance of SCADA systems makes them tempting targets for attacks. Computation and testing methods to recognize vulnerabilities and increase security require the creation of power system modeling state estimates, and bad data detection. Point-to-point and routing network infrastructures are considered. The defenders of these systems have several options to decrease the chances of a successful attack. Careful planning of the structure and components of the system is key to creating a secure SCADA system.

References:

Based on course textbook for EEE 5924 Smart Grid Communications Chapter 17 “Power-system state-estimation security: attacks and protection schemes”

- E.H., Z.H. & H.P., “Smart Grid Communications and Networking,” Cambridge University Press, 2012