Final Project

Professor Deepa Kundur

Objective

The objective of the final project in this course is to provide an opportunity to go in-depth on a research topic in smart grid cyber security. In this project you will be studying the topic of false data injection attacks in DC state estimation. Specifically, you will be constructing attack vectors as detailed in the following paper:

> Y. Liu, P. Ning and M.K. Reiter, "False Data Injection Attacks against State Estimation in Electric Power Grids," *Proc. 15th ACM Conference on Computer and Communications Security*, Chicago, IL, pp. 21-32, November 2009.

Please note that this is an *individual* project and each person can talk to others, but must ultimately do their own work, conduct their own simulations and write their own final report. You cannot copy or share code. You must submit your code along with your report and I will be passing them through a code similarity analysis package.

The deadline is posted on the course webpage.

Background

As discussed during the lectures, the paper by Liu, Ning and Reiter (2009) addresses the problem of false data injection attacks that bypass bad data detection algorithms employing the L_2-norm of the measurement residual vector to detect corrupt measurements. In such situations, it is found that the attack vector **a** that biases the meter measurements must be a linear combination of the column-vectors of the associated power system **H**-matrix; that is, **a** = **H c** where **c** is the bias introduced on the state estimation vector.

The attacker is assumed to be restricted in resources in one of two possible ways: 1) limited access to meters where a specific subset of *k* meters are considered to be corrupted and hence it is possible for an opponent to add a bias to the associated meter measurements, and 2) limited resources to meters where any subset of the *k* meters may be corrupted. Within each class, three different attack objectives are considered: 1) a random attack which aims to find any attack vector as long as it results in an incorrect estimation of the state, 2) a targeted constrained attack in which an attack vector must result in injecting a specific error into certain select state variables and no error in the remaining state variables, and 3) a targeted unconstrained attack in which an attack vector must result in injecting a specific error into certain select state variables and any possible error in the remaining state variables.

Some conditions for guaranteeing the existence or lack of attack vector are provided. In addition, heuristic approaches to constructing attack vectors are presented.

Simulation Instructions

In this project you must simulate (using any software package you like, but I recommend MATLAB) the attack constructions of the Liu, Ning and Reiter (2009) paper. Specifically, you must address the first three types of attacks discussed in the paper related to limited access to meters; these are random false data injection attack, targeted false data injection attack – constrained case and targeted false data injection attack – unconstrained case.

You are given (in a *.mat file available on the course webpage) the **H** matrices for the 9-bus, 14-bus, 30-bus, 118-bus and 300-bus IEEE test systems and a **z** vector for each system that you can use for verification purposes to determine whether the L_2-norm of the measurement residual vector stays the same under the attack. Ms. Yao Liu, the first author of the paper, has graciously given us this file for use in this project.

For each of the five IEEE test systems, and for each of the three attacks (under the limited access to meters constraint), you will verify two graphs and a table generated in the paper. Specifically, the graphs present the probability that an opponent can construct an attack vector (number of successful trials/number of trials) versus the percentage of meters under the attacker's control (k/m). You should also test for execution time.

Your simulations should attempt to reproduce the results of Figures 2 and 3 and Table 1 of the Liu, Ning and Reiter (2009) paper. You should present your versions of Figures 2 and 3 and Table 1 in your report.

Questions

1. How, if at all, do your results deviate from the results generated in the paper corresponding to Figures 2 and 3 and Table 1? Please provide an explanation for why you think there may be deviations.

2. For the case of limited access to meters and the random false data injection attack, the attack vectors are constructed using a given algorithm that you are to code for simulations. For this algorithm, it is stated that the "number of arithmetic operations in the elementary transformations is at most $m(n-1) + m(n-2) + \ldots + 1 = (mn(n\text{-}1))/2$." Please show why this is the case referring to relevant parts of the algorithm.

3. When false data injection attacks exist, does the algorithm you implemented from the paper provide an exhaustive list of attack vectors that are possible? Please explain why or why not.

4. The false data injection attack overcomes bad data detection methods that employ the L_2-norm of the measurement residual vector to detect corrupt measurements. Essentially, it ensures that $\| \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{bad} \|$ is below a threshold τ and passes bad data detection if $\| \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \| \leq \tau$ because the attack vector $\mathbf{a} = \mathbf{Hc}$ guarantees that $\| \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{bad} \| = \| \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \|$. However, this tight restriction can make it difficult to generate attacks; for example, in the case of targeted false data injection attacks in the constrained case. One approach to improve the possibility of obtain attack vectors for the targeted false data injection attacks case is to loosen the strict restriction that

$\mathbf{a} = \mathbf{Hc}$. Please discuss one way in which this can be done. For this approach, explain what the implications would be for bad data detection statistics of $\| \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \|$ versus $\| \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{bad} \|$?

Tips

1. Please note that the only information you need to construct attack vectors for each IEEE system is the associated **H** matrix. The **z** vector is needed for verification that $\| \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_{bad} \| = \| \mathbf{z} - \mathbf{H}\hat{\mathbf{x}} \|$ when a false data injection attack is applied.
2. If you use MATLAB, the `randperm` function could be your friend.
3. A cautionary note. The simulations for the 118- and 300-bus test systems may take a considerable amount of time even for 100 trials. Hence, it is recommended that you test and correct any errors in the code using the 9-, 14- and 30-bus systems initially and then execute the simulations on the larger systems.