Final Project

Instructor: Professor Deepa Kundur
Teaching Assistant: Alex Cybulski
Semester: Fall 2015
DEADLINE: Monday, December 21, 2015, 11:59 pm ET.

Objective

The objective of the final project in this course is to:

- provide an opportunity to go in-depth on a topic of interest to you in cyber security; and
- encourage collaboration amongst members of the class; exchange of complex ideas and opinions is an important life skill that this project hopes to develop in some way.

Because of the diverse backgrounds of the members of this class and possible varying interests, you have the option to select between a few different projects. In each case, students should work in groups of **two or three** individuals. If there is a significant problem finding partners, please contact me and I'll try to help find you a group or partner.

Please note that ONLY one member of the group needs to submit the final project and the group member names and student numbers should be listed in two places: 1) on the first page of the report, and 2) in the comments section of the Blackboard assignment submission system.

Research Report

In this project, you must select a topic (see below) related to cyber or cyber-physical security, conduct research on the topic and write a report on the subject. The purpose of the report is to have you investigate a topic of interest providing, in part, your personal group insights on the topic. There are two different types of topics you could select as discussed below.

Topic Possibility 1: Privacy Analysis

Identify a technology or software platform that you believe has a significant impact on privacy. Please write your group report to address the following. How does this technology/software impact privacy? Are there any incidents of this technology or software leaking private information? How could this technology or software be improved to have a less significant privacy impact? Please choose an interesting/novel technology/software platform and provide a solution that respects risk management practices, is plausible using existing solutions (or a solution you can create yourself). This solution should be robust, providing not only a technological fix, but addressing any social or political factors (policy & law).

The following is an example of the organization your report could have (of course, this could deviate depending on how you decide to convey your ideas):

- Title
- Executive summary
- Description of your selected technology or platform
- Privacy implications (assessment and critique) of technology
- Description of proposed improvements of technology

- Analysis of proposed improvements
- General conclusions and future avenues of work to improve the technology
- References

Topic Possibility 2: Incident or Vulnerability Analysis

Research and identify a cyber security incident or vulnerability that has caused a disruption or damage to the power grid. Please write a report explaining the cause of this problem, what its effects were, and whether any proposed resolutions were proposed by parties impacted by the damage/disruption. Please provide a critique of any proposed solutions. Finally, provide your own solution to prevent or remediate the problem. Make sure that your solution will not only fix or prevent future problems, but will be governed by reasoning that respects risk management practices, is plausible using existing solutions (or solutions that you can create) and respects the freedom and privacy of citizens living in a democratic society.

The following is an example of the organization your report could have (of course, this could deviate depending on how you decide to convey your ideas):

- Title
- Executive summary
- Description of incident or vulnerability
- Impact of the incident or potential impact of the vulnerability on the power grid
- Description and critique of any proposed improvements of technology
- Description of your own proposed solution
- General conclusions and future avenues of work to improve the technology
- References

Topic Possibility 3: Comparative Study

You must survey a specific topic related to the course and compare different solutions, ideas or frameworks (e.g., you can compare two definitions of privacy in the context of smart grid systems). In your research you will need to find at least two papers that have proposals/ideas that you intend to compare and then use related papers to help you enhance your assessment. The comparative report should be written *in your own words*. The following is an example of the organization your report could have (of course, this is highly dependent on the topic(s)/papers you select):

- Title
- Executive summary highlighting what you are comparing and your general conclusions
- Introduction and motivation for the general area (include the metrics you will use for assessing the different ideas)
- Introduction of first idea/solution/proposal/framework
- Introduction of second idea/solution/proposal/framework …
- Introduction of last idea/solution/proposal/framework
- Comparison of different approaches
- Discussion with your personal critical assessment
- General conclusions
- References

Report Tips

Each report should include a personal group-based evaluation or personal assessment as highlighted above as well as a list of references. Please note that assessment should have both positive and negative aspects. This is your report, so all diagrams, tables and other content must be original and your work. Text should be in your own words. For example, you must draw your own diagrams even though similar ones may exist the paper (although you should probably improve them by making them more accessible to the general reader). It is okay to present results from the paper such as simulation plots, but credit and a reference has to be clearly given.

Simulation Assignment

Possibility 1: Propose Your Own Simulation

If you would like to conduct a group-based simulation-based project, please make a proposal to me via email *before* December 4, 2015 providing:

1. a reference for what you intend to simulate;
2. a statement in your own words of what you will simulate and why you think it is appropriate for the course theme of smart grid cyber-physical security.

I'll send an approval message and/or some comments to help you define the scope/topic.

Possibility 2: False Data Injection Attacks

If you would like me to propose a simulation project for you, here is one. 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.

Background

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 $\mathbf{a}$ that biases the meter measurements must be a linear combination of the column-vectors of the associated power system $\mathbf{H}$-matrix; that is, $\mathbf{a} = \mathbf{H}\,\mathbf{c}$ where $\mathbf{c}$ 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 or directly from http://www.comm.utoronto.ca/~dkundur/course_info/1518/2015F/project/Hmatrix.mat) 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.

Report Format

Your report should be written in complete sentences and should present the simulations results along with a discussion of the questions above. Please list your name and student on the top of the report. You will be graded on the correctness, preciseness and comprehensiveness of your answers and quality of your presentation. 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.