Poster: False Data Injection Attacks against Contingency Analysis in Power Grids

M. Ashiqur Rahman
marahman@fiu.edu
Florida International University
Miami, Florida, USA

Md Hasan Shahriar
mshah068@fiu.edu
Florida International University
Miami, Florida, USA

Rahat Masum
rmasum42@students.tntech.edu
Tennessee Tech University
Cookeville, Tennessee, USA

ABSTRACT

Smart grid provides efficient and cost-effective management of the electric energy grid by allowing real-time monitoring, coordinating, and controlling of the system using communication networks between physical components. This inherent complexity significantly increases the vulnerabilities and attack surface in smart grid due to misconfigurations or the lack of security hardening. Therefore, it is important to ensure secure and resilient operation of smart grid by proactive identification of potential threats, impact assessment, and cost-efficient mitigation planning. This paper aims to achieve these goals through the development of an efficient security framework for the Energy Management System (EMS), a core smart grid component. In this paper, we present a framework that combines formal analytic with PowerWorld simulator which verifies the solution model to investigate the feasibility of false data injection attacks against contingency analysis in power grid. We evaluate the impact of such attacks by running experiments using synthetic data on the standard IEEE test cases .

KEYWORDS

smart grid, false data injection, formal analysis, SCOPF, PowerWorld Simulator

1 INTRODUCTION

In power system, contingency refers to outage of an electric element, e.g. generator, transmission/distribution line, transformer, circuit breaker, etc. To secure the power system, utility companies usually simulate the virtual model of the power system to see the impact of the post-contingency scenarios by tripping each element one by one, called contingency analysis. A system is said to be n-1 contingent if it sustains and retrieve stability instead of losing any of its elements accidentally [3].

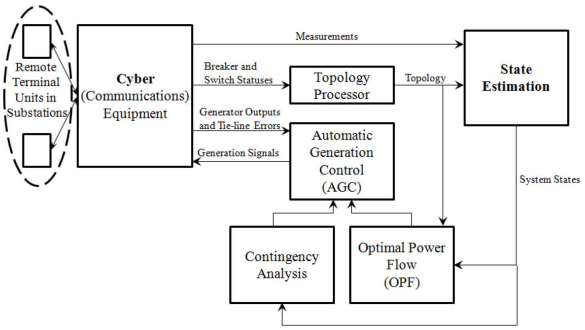

Figure 1: A schematic diagram of an Energy Management System (EMS)

The Optimal Power Flow (OPF) calculation determines the best set of dispatches for the power plants to satisfy the demands considering transmission line constraints, minimizing the operating cost. Although OPF ensures the lowest generation cost, it does not consider the contingency conditions. Thus, to increase the reliability of the system, contingency analysis should also be carried out with OPF calculation, which is called Security Constrained Optimal Power Flow (SCOPF). If a system is running under SCOPF and one of the lines trips, the amount of power flowing through that line will be distributed to the other lines by a certain factor without overloading them but fulfilling the existing load and generation dispatches. This factor is called the Line Outage Distribution Factor (LODF) [1].

In smart grid different communication networks exist for sensing measurements from the remote field devices (e.g., IEDs, PLCs, and RTUs), sending the sensor data to the control center(s), and transmiting control commands from the control center(s) to the remote devices [2]. EMS runs at the control center, analyzes the received data, and generates necessary control commands that ensure secure and optimal operation of the grid. Fig. 1 shows a schematic diagram of EMS modules [3]. The increasing use of IT in smart grids escalates the possibility of cybersecurity vulnerabilities and incidents. The inherent complexity associated with smart grid increases

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05…$15.00
https://doi.org/10.1145/3317549.3326323

the potential of security threats such as data unavailability and false data injection. Intelligently altered data can corrupt the EMS functionality without being detected by existing Bad Data Detection (BDD) algorithm known as Undetected False Data Injection (UFDI) attack. The rest of this article is organized as follows: in Section II, we provide the problem statement. We present our formal solution model in Section III and conclude our work in Section IV.

2 PROBLEM STATEMENT

In this paper, two levels of attack are considered from the attacker's perspective. Firstly, the attacker can alter the load data of some specific buses in the SCADA system by injecting false load value. Thus, based on the new (attacked) load scenario, EMS will run the SCOPF again and calculate the new dispatches for the generators. As this calculation is based on modified load data, it may overload some specific lines as the real loads are still the same as before. Thus, in this case, the attacker's goal is to overload the original power flows of some transmission lines instantly.

The second level shows an extended and more complex attack scenario where UFDI attack will be done in a similar way as stated above. However, in this case, after the attack, all the line flows are now within the rated capacity in normal condition. Thus, with the new set of dispatches, the system will run without kind of overloading or alarm. However, when any contingency (i.e., line outage) happens, although the system operator expects that the system will sustain as it is running under SCOPF, it will collapse as it is running SCOPF with attacked load scenario. Thus, depending on the attacker goals, some lines will be overloaded which were completely fine for a non-contingent situation.

3 PROPOSED SOLUTION APPROACH

In this work, the DC power flow model is used to describe the power balance equations in a loss-less power system. We model our physical system with parameters and constraints using SMT (Satisfiability Modulo Theories), which is a powerful tool for solving constraint satisfaction problems. A program is written using the Microsoft Z3.Net API encoding the formalization of our proposed UFDI attack. We test our model on IEEE standard bus systems. The system configurations and the constraints are given in a text file (input file) as an input for the proposed model.

In our solution model, firstly, the optimum generation cost is calculated by running the SCOPF for the original load scenario. As the attacker's goal is not to increase the generation cost, this cost is taken as a constraint for the attack scenario. Then the attacker calculates and injects the false load data which asks for a new set of generation dispatches with a generation cost not higher than the optimal cost. One of the goals of the attack is to inject data in such a way that the new generation set does not overload any of the lines in the real scenario under normal condition. However, as the new set of generation is calculated by running SCOPF based on the attacked load, contingency analysis will not report any overloading for both normal and n-1 contingency conditions. However, the attacked load is calculated in such a way that, for the real load, although there is no overloading in normal condition, some lines will be overloaded when some contingencies occur in the system.

By executing the model, we obtain the verification result as either satisfiable (*sat*) or unsatisfiable (*unsat*). If the result is *unsat*, it means that there is no attack vector that satisfies the constraints. In the case of *sat* result, we get the attack vector from the assignments of the variables, which represent the amount of load changes that are required to be altered for the attack. Our attack model is also verified by PowerWorld simulator. We also use a loss-less DC simulation option in the PowerWorld simulator; which is similar to our approximation.

4 CONCLUSION

Cyber technologies are increasingly used in smart power grids with the promise of providing more capacity, efficiency, and reliability. Cyber intrusion and false data injection can cause improper controls and lead to serious damages in smart grid, including power outages and destruction of critical equipment. In this work, we applied formal method to calculate the false data that can be injected after SCOPF operation and undetected unless there is a contingency. During any contingency, based on the attacker's goal, some lines are overloaded which initiates cascading failing impact. We have successfully generated attack scenarios for the standard IEEE 5 & IEEE 14 bus systems and working on larger bus models. As a future direction, we would like to consider this UFDI attack for AC power system and build a defense mechanism to make the smart grid more robust to any kind of cyber attacks.

ACKNOWLEDGEMENT

This work is supported by National Science Foundation [grant number 165730].

REFERENCES

[1] Rashid H AL-Rubayi, Afaneen A Abood, and Mohammed R Saeed Alhendawi. 2016. Simulation of Line Outage Distribution Factors (LODF) Calculation for N-Buses System. *International Journal of Computer Applications* 156, 3 (2016).

[2] Mohammad Ashiqur Rahman, Ehab Al-Shaer, and Rajesh Kavasseri. 2014. Impact analysis of topology poisoning attacks on economic operation of the smart power grid. In *2014 IEEE 34th International Conference on Distributed Computing Systems*. IEEE, 649–659.

[3] Allen J Wood, Bruce F Wollenberg, and Gerald B Sheblé. 2013. *Power generation, operation, and control*. John Wiley & Sons.