Cyber-Security of SCADA Systems

Göran Andersson, Peyman Mohajerin Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, André Teixeira, György Dán, Henrik Sandberg, and Karl H. Johansson

***Abstract*—After a general introduction of the VIKING EU FP7 project two specific cyber-attack mechanisms, which have been analyzed in the VIKING project, will be discussed in more detail. Firstly an attack and its consequences on the Automatic Generation Control (AGC) in a power system are investigated, and secondly the cyber security of State Estimators in SCADA systems is scrutinized.**

***Index Terms*—Cyber-Security, SCADA Systems, AGC, State Estimators.**

I. Introduction

THE electric power transmission system is probably the most vital infrastructure in our society [1]. Large power systems are nowadays very complex and tightly coupled with the SCADA system, which supervises them in terms of collecting data from remote facilities and sending back control commands. The resilience of power system on this infrastructure, makes it more susceptible not only to operational errors but also to external attacks.

The SCADA system measures data through remote devices and transmits them to control centers through communication channels. There computer processing takes place and control commands are sent back to the system. The vulnerabilities that are introduced could be exploited by malicious attackers. In [2], [3], [4],[5] real examples of cyber attacks were reported. The authors of [6] proposed a framework in order to clarify the interaction between the power system and the IT infrastructure and identify the vulnerabilities and the malfunctions of both that could lead to an abnormal operation of the power network. From another perspective the authors of [7] attempted to quantify the impact of a cyber attack in the power market.

The work in this presentation is motivated by the framework proposed by the VIKING research project [8]. This project proposes a novel concept to address the challenges introduced by the interaction between the IT systems and the power transmission and distribution systems. Main objective is to identify the vulnerabilities of these safety critical infrastructures, determine the impact that possible failures or attacks might have and develop strategies to mitigate these effects.

Peyman Mohajerin Esfahani, Kostas Margellos and John Lygeros are with the Automatic Control Laboratory, Department of Electrical Engineering, Swiss Federal Institute of Technology (ETH), Physikstrasse 3, ETL I22, 8092, Zürich, Switzerland. email: {mohajerin, margellos, lygeros}@control.ee.ethz.ch

Maria Vrakopoulou and Göran Andersson are with the Power Systems Laboratory, Department of Electrical Engineering, Swiss Federal Institute of Technology (ETH), Physikstrasse 3, ETL G26, 8092, Zürich, Switzerland. email: {vrakopoulou, andersson}@eeh.ee.ethz.ch

Henrik Sandberg, André Teixeira, and Karl H. Johansson are with the Automatic Control Lab, School of Electrical Engineering, Royal Institute of Technology, 100 44 Stockholm, Sweden. email: {hsan,andretei,kallej}@ee.kth.se

György Dán is with the Laboratory for Communication Networks, School of Electrical Engineering, Royal Institute of Technology, 100 44 Stockholm, Sweden. email: {gyuri}@ee.kth.se

In this presentation attacks and their consequences on the Automatic Generation Control (AGC) in a power system are investigated, and the cyber security of State Estimators in SCADA systems is scrutinized. These presented results are all from the VIKING project.

II. Cyber Attacks on the AGC

Here we investigate the impact of a cyber attack on the Automatic Generation Control (AGC) in a power system. The primary objective of the AGC is to regulate frequency to the specified nominal value and maintain the power exchanged between the controlled areas to the scheduled values by adjusting the generated power of specific generators in the area. AGC actions are usually determined for each control area at a central dispatch center. Measured system frequency and tie line flows are sent to this center and then a feedback signal that regulates the generated power is sent back to the generators, participating in the AGC, through the SCADA system.

AGC is one of the few control loops that are closed over the SCADA system without human operator intervention. To reveal its vulnerabilities, we consider a two-area power system and analyze the safety of the system in the case where an attacker has gained access to the AGC signal of one area and is able to inject any undesirable input to it. For this purpose, a dynamic nonlinear frequency model, which is suitable for load-frequency studies for the two interconnected areas, was developed.

In this paper, two approaches on designing an optimal control strategy to destabilize a power system in the case of a cyber attack in AGC are developed. The first approach, is an open loop policy based on Markov Chain Monte Carlo optimization. However, via simulations it was demonstrated that this policy is extremely sensitive to parameter uncertainty. Motivated by this a systematic algorithm based on feedback linearization was developed so as to construct an attack signal. The proposed scheme was tested numerically and its robustness to parameter mismatching were verified from the obtained simulation results. Current work concentrates on the implementation of the proposed scheme on a realistic, IEEE benchmark network. Methods to identify these attacks will also be presented.

III. Cyber Security Analysis of State Estimators

We have analyzed the cyber security of state estimators in Supervisory Control and Data Acquisition (SCADA) systems operating in power grids. Safe and reliable operation of these critical infrastructure systems is a major concern in our society. In current state estimation algorithms there are bad data detection (BDD) schemes to detect random outliers in the

978-1-4577-2159-5/12/$31.00 ©2011 IEEE

measurement data. Such schemes are based on high measurement redundancy. Although such methods may detect a set of very basic cyber attacks, they may fail in the presence of a more intelligent attacker, as first pointed out in [9]. We have explored the latter by considering scenarios where deception attacks are performed, sending false information to the control center. As discussed in, for example, [10], there are several vulnerabilities in the SCADA system architecture that could be exploited to perform such attacks. These include the direct tampering of remote terminal units (RTUs), communication links from RTUs to the control center, and the IT software and databases in the control center.

In [11], we have introduced a security metric tailored to quantify how difficult it would be to perform these deception attacks. The metric depends on the physical topology of the power network as well as the available measurements. How the SCADA communication system topology can be taken into account is shown in [12], where the metric is also used to deploy a small number of protected RTUs, in order to make the described deception attacks as difficult as possible. By a protected RTU we mean its communication with the control center is encrypted, or that the substation where it is located is physically protected.

Most studies of these attacks have assumed that the attacker has perfect model knowledge. In [13], we instead assume the attacker only possess a perturbed model. Such a model may correspond to a partial model of the true system, or even an out-dated model. Specifically, we quantify trade-offs between model accuracy and possible attack impact for different BDD schemes. Finally, in [14] we have studied how an actual SCADA system responds to deception attacks constructed using an approximate linear model. The study indicates that they indeed can be made significant: In the example considered in [14], a power flow measurement was corrupted by 150 MW (57% of the nominal power flow) without triggering BDD alarms.

ACKNOWLEDGMENT

This research work is supported by the European Commission under the project VIKING, FP7-ICT-SEC-2007-1.

REFERENCES

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1922–1928, 2005.

[2] *Forbes, Congress Alarmed at Cyber-Vulnerability of Power Grid, available at http://www.forbes.com/2008/05/22/cyberwar-breach-government-tech-security_cx_ag_0521cyber.html*.

[3] *CNN, Sources: Staged cyber attack reveals vulnerability in power grid, available at http://www.cnn.com/2007//US/09/26/power.at.risk/index.html*.

[4] *Comptuterworld, DHS to review report on vulnerability in West Coast power grid, available at http://www.computerworld.com/s/article/9138017*.

[5] J.-W. Wang and L.-L. Ronga, "Cascade-based attack vulnerability on the US power grid," *Elsevier, Safety science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[6] D. Kirschen and F. Bouffard, "Keep the Lights On and the Information Flowing," *Power and Energy Magazine, IEEE*, vol. 7, no. 1, pp. 50–60.

[7] M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment," *IEEE Power Tech Conference*, 2009.

[8] *VIKING Project, http://www.vikingproject.eu*.

[9] Y. Liu, M. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *16th ACM Conference on Computer and Communication Security*, New York, NY, USA, 2009, pp. 21–32.

[10] A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg, "The VIKING project: an initiative on resilient control of power networks," in *Proc. 2nd Int. Symp. on Resilient Control Systems*, Idaho Falls, ID, USA, Aug. 2009, pp. 31–35.

[11] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010*, 2010.

[12] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Proc. of IEEE SmartGridComm*, Oct. 2010.

[13] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proceedings IEEE Conference on Decision and Control*, Dec. 2010.

[14] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," http://arxiv.org/abs/1011.1828, 2011, to appear in Proc. IFAC World Congress, 2011.