Co-simulation for Cyber Security Analysis: Data Attacks against Energy Management System

Kaikai Pan*, André Teixeira†, Claudio David López* and Peter Palensky*
*Intelligent Electrical Power Grids
Faculty of EEMCS, Delft University of Technology, Delft, The Netherlands
†Engineering Systems and Services
Faculty of TPM, Delft University of Technology, Delft, The Netherlands

***Abstract*—It is challenging to assess the vulnerability of a cyber-physical power system to data attacks from an integral perspective. In order to support vulnerability assessment, with the exception of analytic methods, a suitable platform for security tests needs to be developed. In this paper we analyze the cyber security of energy management system (EMS) against data attacks. First we extend our analytic framework that characterizes data attacks as optimization problems with the objectives specified as security metrics and constraints corresponding to the communication network properties. Second, we build a platform in the form of co-simulation - coupling the power system simulator DIgSILENT PowerFactory with communication network simulator OMNeT++, and Matlab for EMS applications (state estimation, optimal power flow). Then the framework is used to conduct attack simulations on the co-simulation based platform for a power grid test case. The results indicate how vulnerable of EMS to data attacks and how co-simulation can help assess vulnerability.**

I. Introduction

Cyber security vulnerabilities within the information and communication technology (ICT) infrastructure may allow attackers to manipulate the physical system, communication network or software applications in the cyber-physical power system. As a real example of cyber attack reported recently, highly destructive malware corrupted automation systems in substations resulting in a large scale blackout in the Ukrainian power grid [1]. Modern energy management systems (EMS) combined with Supervisory Control and Data Acquisition (SCADA) networks provide support for the monitoring and control of power grids. However, this critical infrastructure is vulnerable to cyber attacks and several attack events have been reported, see [2], [3]. In order to increase the security of these systems, one needs analytic methods to first understand the vulnerabilities and then to validate or explore them with appropriate tools. Some of the literature has already tackled these problems. Vulnerability assessment methods mainly using analytic expressions have been proposed in [4], [5], [6]. Some tools based on co-simulation techniques to integrate simulated power systems, communication network and controls have been developed to analyze the behavior of cyber-physical power systems including cyber security issues [7], [8], [9].

However, these two parts of the work are usually conducted independently even though they are related. Analytic methods may have to ignore some details when modeling the heterogeneous cyber-physical system, but could be used to guide the cyber security tests on co-simulation tools, while the tools can support the security analysis with empirical results. This could contribute to develop more robust algorithms/methods that combine system-theoretic and ICT-specific measures to protect EMS against data attacks [10]. In this paper, we aim to contribute in closing this gap by extending the typical vulnerability assessment framework to incorporate communication network properties and developing a co-simulation platform to conduct simulations on data attacks against EMS. In order to achieve this, some communication network properties are modeled in the analytic vulnerability assessment framework. Additionally, experiments are conducted on the developed co-simulation platform and the simulation results are analyzed.

The outline of the paper is as follows. Section II details the problem statement and our motivations on developing the methods and tools. In Section III, the analytic vulnerability assessment framework is illustrated. We further analyze what communication network properties should be considered in order to extend the framework. The co-simulation platform is presented in detail in Section IV, including how the power system and communication network are modeled, how the tools are integrated and how the attacks are implemented in OMNeT++. Section V shows the empirical results from co-simulation. We also provide a discussion on combining system-theoretic and ICT-specific measures to protect EMS. The conclusion remarks are in Section VI.

II. Problem Statement and Motivation

A. Data Attacks Against Energy Management System

The SCADA system supports the EMS of the information delivery as indicated in Figure 1. As a core part of EMS, State Estimation (SE) provides the operator an estimate of the state of the electric power system. SE uses measurements collected by the Remote Terminal Units (RTUs) in substations and transmitted through the SCADA communication network to the Master Terminal Units (MTUs) in the control center. The estimated state information is then processed by other applications in EMS such as optimal power flow (OPF) and Contingency Analysis (CA) to compute optimal control action while ensuring reliability and safety. The critical nature of EMS highlights the importance of making it accurate and secure for power grid operations.

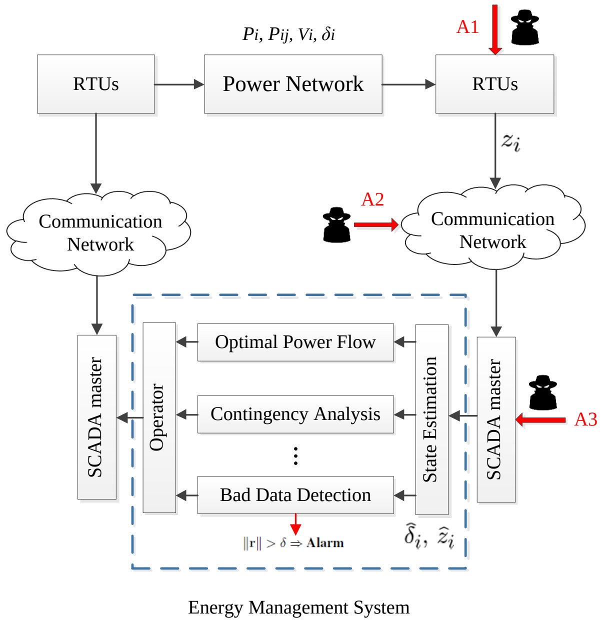

Figure 1. A schematic block diagram of the power network, SCADA system and EMS. The SE uses power flow (P_i, P_{ij}) measurements (z_i) collected by RTUs and transmitted by the SCADA system to estimate the current state (δ_i) of the power network. An alarm is triggered by the Bad Data Detection (BDD) when the norm of the measurement residual r exceeds a given threshold. The cyber attack can manipulate the measurements by directly tampering the RTUs (A1), the SCADA communication network (A2) and even the SCADA master (A3). Figure adapted from [11].

However, as SCADA systems become more connected to the Internet and corporate networks, they are potentially vulnerable to a large number of security threats. This is one motivation of our work. Substations need remote access connection for monitoring and maintenance, which may expose them to cyber attacks. Besides, for most industrial communication protocols, e.g., DNP 3.0, IEC 61850, adequate cyber security features were not always included at the time of publishing [12]. As shown in Figure 1, the manipulation of measurements can arise from various levels (A1, A2, A3). The attacks can corrupt measurement data by attacking the RTUs, by tampering with the communication network, or even by breaking into the SCADA master.

B. Towards Cyber-Secure and Resilient State Estimation

Assuming that the power system has $N+1$ buses, the typical state estimation technique solves the following problem under AC power flow model,

$$z = h(x) + e, \tag{1}$$

where the vector z denotes the m power flow measurements, $h(x)$ is the nonlinear power flow model with the state vector $x \in \mathbb{R}^N$ of N bus phase angles except the reference one, e is the measurement noise vector which is always assumed to have a Gaussian distribution of zero mean and covariance matrix $R = \text{diag}(\sigma_1^2, \ldots, \sigma_m^2)$. For such a large-scale SCADA system, lost data, inaccurate measurements and failing RTUs or other infrastructures in communication network are common [11]. Thus there is a built-in Bad Data Detection (BDD) scheme to deal with that. In BDD, the residual signal r is evaluated to detect and locate existing anomalies of data, as depicted in Figure 1. However, such kind of system-theoretic measure is not adequate to protect the EMS against potential data attacks. The data can be corrupted in a coordinated way that still fulfills the power flow laws and would not be detected by BDD [13].

A considerable amount of work has been done on vulnerability assessment of data attacks against EMS [4], [5], [6], [14]. Usually these are system-theoretic measures that are based on analytic methods. Another group of measures from ICT-specific security includes firewalls, network intrusion detection systems and authentication, etc. Recently some organizations (e.g. NIST, NERC) have proposed security standards that combine the measures from ICT-specific and system-theoretic ones [10]. Regarding these issues, we have the following recommendations:

- The system-theoretic measures based on analytic methods need empirical results for validation and analysis;
- The vulnerability assessment of data attacks should take the attack impact/consequences into account;
- To improve the security of EMS, there is a necessity to explore the interactions between system-theoretic and ICT-specific measures and try to combine them.

To support the security analysis above, an integrated platfrom using various tools including simulators for power network, SCADA communication network and EMS applications could offer these capabilities. Co-simulation is currently one of the most popular methods to analyze such a large, heterogeneous cyber-physical system [15]. Therefore in this paper we propose to extend our current analytic vulnerability assessment methods to incorporate communication network properties and enable them with support from a co-simulation platform.

III. Analytic Framework Incorporating Communication Network Properties

A. Data Attacks and Typical Vulnerability Assessment Problem

With the goal of perturbing the SE and further corrupting the applications in EMS, the attacker would gain access to the measurement data through various levels (A1, A2, A3) as shown in Figure 1. The measurements under different attack scenarios from the view of SE can be presented as follows:

- Data integrity attack - also known as false data injection (FDI) attack, is able to change measurements values from z to $z+a$ where a is the *FDI attack vector*.
- Data availability attack - includes DoS or jamming attack which would make specific measurements unavailable to SE, i.e., $z_0 = (I - \text{diag}(d))z$ where $d \in \{0,1\}^m$ is the *availability attack vector* and I is an identity vector.
- Combined attack - combines the FDI and availability attack that makes the measurements from z to $(I - \text{diag}(d))z + a$ corrupted by a and d.

The typical vulnerability assessment considers the problem of how many measurements need to be manipulated by the attacker to avoid triggering alarms in BDD of EMS. This index can quantify the attack resources and consequently the vulnerabilities of EMS to attacks. Taking the attack scenarios under DC power flow model as an example, if the attacker corrupts certain measurements using FDI attack vector $a = Hc$ where H represents the network model that depends on topology and parameters of transmission lines and placement of RTUs, it can remain hidden from the BDD but perturb the current state to a degree of c [13]. It's also shown in our recent work [6] that combined attacks can achieve the same target with the attack vector $a = (I - \mathrm{diag}(d))Hc$. It should be noted that these data attacks are assumed not to make the system unobservable and lead to non-convergence of the SE algorithm. In sight of this, it is natural to consider the following problem:

$$
\begin{aligned}
\alpha_j := \min_{c,d} \quad & \|a\|_0 + \|d\|_0 \\
\text{s.t.} \quad & a = H_0 c, && \text{(2a)}\\
& H_0 = (I - \mathrm{diag}(d))H, && \text{(2b)}\\
& a(j) = \mu, && \text{(2c)}\\
& d(i) \in \{0,1\} \quad \text{for all } i,
\end{aligned}
$$

where $\|a\|_0$ and $\|d\|_0$ denote the number of non-zero element in the vectors. Here μ is a non-zero value denoting the attack magnitude on measurement j, and α_j is the so-called *security metric* that can illustrate how many measurements or RTUs needed by the attacker to corrupt EMS and keep stealthy.

B. Analytic Vulnerability Assessment Incorporating Communication Network Properties

The vulnerability assessment problem in (2) suits for the cases that attacks arise from the level of A1 in Figure 1. This security metric directly shows that manipulation on several RTUs is needed for the attacker. However in practice, tampering with RTUs directly becomes much harder as more RTUs are authenticated and secured. A more interesting scenario is to look into attacks from the level of A2 since usually attacks would explore vulnerabilities in communication networks, e.g., compromising remote access points, obtaining access to corporate networks. The vulnerability assessment should consider the communication network. However, modeling the communication network in an analytic framework is challenging due to its complexity and heterogeneity. Here, the communication network properties of interest for security analysis are as follows:

- Communication topology;
- Routing schemes - the routing paths of packets/data;
- Communication latency - how the packets/data would be delayed in each communication infrastructure;
- Packet loss/data missing - the possibility of packet drop in each communication infrastructure.

Here we introduce a method to deal with the first two properties that can be employed in the analytic vulnerability assessment. Another two properties of communication networks, latency and packet loss, could also be incorporated into analytic framework, not for vulnerability assessment but for combining ICT-specific measures and system-theoretic measures. We show such potentials and have a discussion in Section V. Let us consider a simple communication network as shown in Figure 2. We can describe it as an undirected graph $\mathsf{G} = (\mathsf{V}, \mathsf{E})$ where V is the set of nodes and E is the set of communication links. Assuming that a measurement i would be transmitted through a routing path $P1$, we establish a binary vector called *routing vector*,

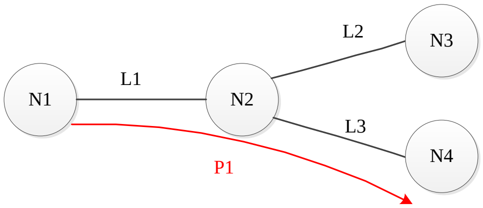

Figure 2. A simple communication network for illustration of routing path. $N1, N2, N3, N4$ represent communication nodes and $L1, L2, L3$ represent communication links. The routing path $P1$ follows $N1 - L1 - N2 - L3 - N4$.

$$
r_{i,P1} = [r_{vi,P1}^T, r_{ei,P1}^T], \tag{3}
$$

where in routing vector $r_{vi,P1} \in \{0,1\}^N$ denotes the part corresponding to nodes and the entries are equal to 1 if the route traverses the node. $r_{ei,P1} \in \{0,1\}^E$ denotes the part corresponding to communication links and the entries are equal to 1 if the route traverses the link. N and E denote the whole number of nodes and edges in the graph. Thus for the path $P1$, we can obtain

$$
r_{vi,P1} = [1,1,0,1]^T, r_{ei,P1} = [1,0,1]^T. \tag{4}
$$

Using the graph of the communication network and routing schemes for all the measurements, we can build a *routing matrix* and each row of the matrix is a *routing vector*. The *routing matrix* and *routing vectors* contain the information of communication topology and routing schemes. In our recent work [6], we extend the typical vulnerability assessment problem (2) to the following one,

$$
\begin{aligned}
\beta_j := \min_{c,d,x,y} \quad & \|x\|_0 + \|y\|_0 \\
\text{s.t.} \quad & a = H_0 c, && \text{(5a)}\\
& H_0 = (I - \mathrm{diag}(d))H, && \text{(5b)}\\
& a(j) = \mu, && \text{(5c)}\\
& a(i) = 0 \text{ if } r_{vi,P} = 0, \text{ for all } i \neq j, P, && \text{(5d)}\\
& d(i) \leq r_{vi,P}x + r_{ei,P}y \quad \text{for all } i \neq j, P, && \text{(5e)}\\
& d, x, y \quad \text{are all binary vectors,}
\end{aligned}
$$

where $x \in \{0,1\}^N$ and $y \in \{0,1\}^E$ are vectors whose entries are 1 if certain nodes/links are attacked. The constraints (5d) and (5e) use the *routing vectors* to map the data attacks on measurements to attacks on communication network. They also indicate that for FDI attack on measurement j, at least one node should be attacked and included on all of its routing paths and for availability attack on measurement j, at least one node or communication link should be attacked and included

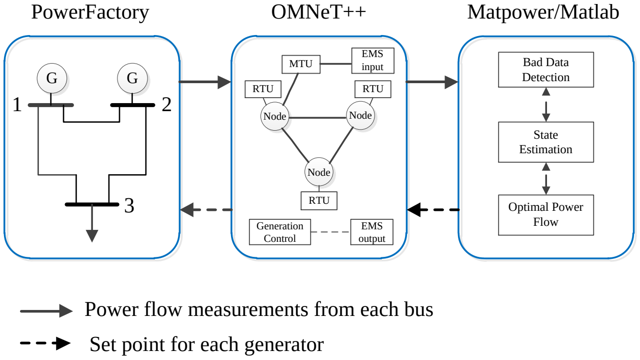

Figure 3. Co-simulation diagram.

on all of its routing paths. This is the worst-case scenario that the attacker is assumed to have the knowledge of both communication network (topology and routing schemes) and power system network (the network model H). The metric β_j can illustrate the vulnerability of EMS to data attacks on the communication network. It should be noted that some ICT-specific security measures can be modeled in (5). For instance, multi-path routing schemes can be described using *routing vectors* in constraints (5d) and (5e). Data authentication can also be implemented by adding constraints to indicate which measurement originates from the node with authentication is protected.

These two analytic vulnerability assessment problems (2) and (5) can be formulated as mixed integer linear programming (MILP) problems. Further details on formulations and solutions can be found in [6]. However, these security metrics do not consider the attack impact on the physical system operation. In fact, data attacks with the same security metrics could have considerable different impact. Co-simulation could offer the capabilities to look into the attack impact and provide empirical results to validate and contribute in developing mitigation measures, as discussed in Section II-B.

IV. Co-simulation Supporting Vulnerability Assessment and Security Analysis

A. Co-simulation Tools

An integrated environment including simulators of power system, communication network and EMS applications is needed for security analysis. In order to allow for real-time analysis of cyber attacks, the co-simulation platform is implemented with three tools: DIgSILENT PowerFactory for the power system, OMNeT++ for the communication network, and Matlab/Matpower for the EMS algorithms. They are coupled as shown in Figure 3. Here, measurements of the power flow going in and out of each bus of the power system simulated in PowerFactory are sent to the EMS applications in Matlab through a communication network simulated in OMNeT++. The co-simulation runs in real time.

1) Power system simulator: DIgSILENT PowerFactory is used to conduct a quasi-static power flow simulation. PowerFactory's Python API is used to create a script that controls the execution of the simulation. The same script implements the interface with OMNeT++. Real time execution is achieved by synchronizing the power flow calculations with the system clock. The script sends power flow measurements to OMNeT++ every fixed time (set to be 5 seconds), but it can expect generator set points at any time. Thus, a dedicated thread that received set points and sets them in the power system model is required. This thread sets the generators according to the set points as soon as they arrive, unless a power flow calculation is being executed, in which case it waits for the calculation to finish.

2) Communication Network Simulator: OMNeT++ is used for discrete-event based communication network simulation. The communication model in OMNeT++ is shown in Figure 4. A custom OMNeT++ *scheduler* is built to enable data exchange with PowerFactory and Matlab over TCP/IP sockets and run the OMNeT in real-time. In Figure 4, *RTU* is a module served by the scheduler and acts as a RTU proxy. The second module developed called *MTU* works as master unit and data concentrator that receives packets and has a FIFO queue. There is a *Modem* module that acts as a communication bridge and a *Router* module with routing table for the packets. Thus, the RTU, Modem and Router represent the LAN (local area network) of a substation. Besides, the module *EMSInput* and *EMSInout* provide measurements to EMS and receive set points from EMS in Matlab respectively. For the message implementation, a new packet class *MeasurePacket* is derived to contain the measurement data and be used by all the modules and scheduler. There are two kinds of communication channels: channel of the LAN and channel of the WAN (wide area network) between routers. Different latency and packet loss probability parameters are set in these two channels. It should be noted that implementation of a real SCADA system with protocols (e.g., IEC61850, DNP3.0) and hierarchical network structure that is close to reality in OMNeT++ is not our focus in this paper. Instead we try to explore how co-simulation can support the analytic vulnerability assessment.

3) EMS algorithm: Matpower has been used to simulate the EMS applications in Matlab, including state estimation (with bad data detection) and optimal power flow algorithms. A script is implemented to exchange data with OMNeT++ scheduler over TCP/IP sockets and store measurements into a data pool. The State Estimation module uses the latest measurements from data pool to create a snapshot of estimated power flow. For every fixed time (set to be 30 seconds), the Optimal Power Flow module uses load estimates from State Estimation to perform optimal power flow calculation (also see Figure 1) and sends commands of generator set points to PowerFactory through OMNeT++.

B. Simulation Integration

Data is exchanged between PowerFactory, OMNeT++ and Matlab via TCP/IP sockets using the ASN.1 protocol. On the PowerFactory side, this is implemented directly in the Python script that controls the simulator execution, while on the OMNeT++ side, this is implemented through a custom

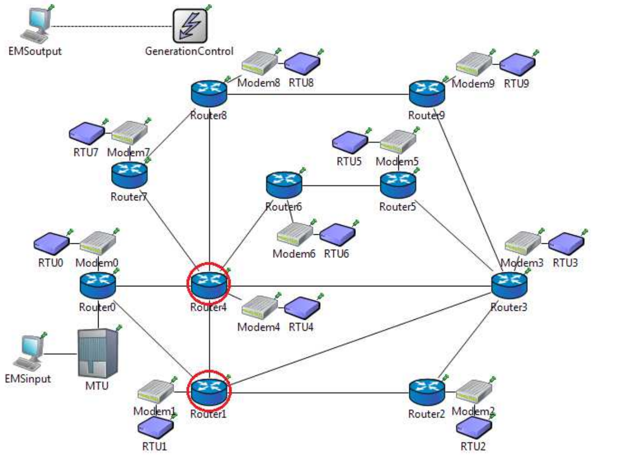

Figure 4. Test communication network of IEEE 14 bus system modeled in OMNeT++.

scheduler which adapted part of the work from [7]. This scheduler act as the "master" to coordinate the co-simulation, handle the data exchanges with PowerFactory and Matlab, and also run the OMNeT++ in a real-time mode. For the synchronization, all simulators would be started from a command after initialization and tagged with time stamps with the system clock.

C. Modeling attacks in OMNeT++

As discussed in Section III, an attacker can manipulate the measurements by injecting false data, making it unavailable or both. After accessing a router, the attacker can launch a data integrity and availability attack on all the data travelling through it by executing a *man-in-the-middle attack*. By jamming, DoS or physical attack, the attacker can also cut the communication links between devices. In this paper, we consider the worst case scenario that the attacker is intelligent enough with full knowledge of both the power system and communication network. The attack would use the combined attack policy in the analytic vulnerability assessment framework in Section III, i.e., try to remain hidden from the BDD and manipulate the minimum number of routers. Then the corrupted measurement vector become

$$z_a = (I - \mathrm{diag}(d))z + a, \tag{6}$$

where $a = (I - \mathrm{diag}(d))Hc$ and d denote the FDI attack and availability attack respectively. The results from the analytic work in (5) is used to choose the routers to be attacked. These attacks is implemented in OMNeT++ by changing the behavior of the router in case it is accessed by the attacker.

V. Simulation Results and Discussion

We consider the IEEE 14 bus system in Figure 5 to perform the security analysis. Mapping with Figure 5, the communication network as depicted in Figure 4 is used. The modeling of the communication network of IEEE 14 bus system is adapted from [16]. There are ten substations (each circle represents a substation in Figure 5) and the control center with MTU and EMS is located at the reference/slack bus (i.e., Bus 1). Correspondingly, in Figure 4 there is an RTU, a modem and a router in each substation. The packets containing the measurement data would be routed through multiple routers before reaching MTU. We use the single-path routing scheme for each measurement, which is common in real SCADA networks. Besides, we assume that the control center is protected and cannot be compromised.

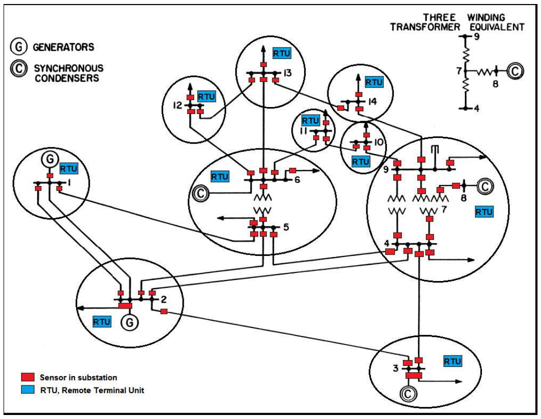

Figure 5. IEEE 14 bus system. There are 2 generators. Bus 1 with Generator 1 is the reference/slack bus. Generator 2 is in Bus 2. The power flow measurements are collected in each bus and both sides of the branch. Each circle represents a substation.

The case of combined integrity and availability attack in Section IV-C has been implemented. The analytic results of (5) can be found in [6]. It shows the minimum number of routers and links to be attacked in order to corrupt specific measurements and keep stealthy. According to the analytic results, Router 4 (the backbone router) and Router 1 (marked with a red circle) are the most vulnerable network components. Thus we change the behavior of Router 4 and Router 1 independently to simulate the attack scenarios once an attacker gains access to their internals and the packets traveling through it. Figure 6 shows the attack impact on the generation profile of generators in Bus 1 and Bus 2.

As shown in Figure 6, when Router 1 is attacked, the system "fakes" that the generation profile changes according to the set points. The generation of Generator 2 has decreased and Generator 1 should compensate. The "latency" between the attack occurrence and the change of generation profile is due to that the EMS sends out set points every 30 seconds. After the attack occurs, the generation profiles remain almost the same although the attack continues, which means the attack impact mainly depends on the initial attack magnitudes and measurements that are corrupted. When Router 4 is attacked, however, it seems that there is no attack impact on the generation profile, though Router 4 is the backbone router with the most number of packets traveling through. This is mainly because of the packets in or traveling through these

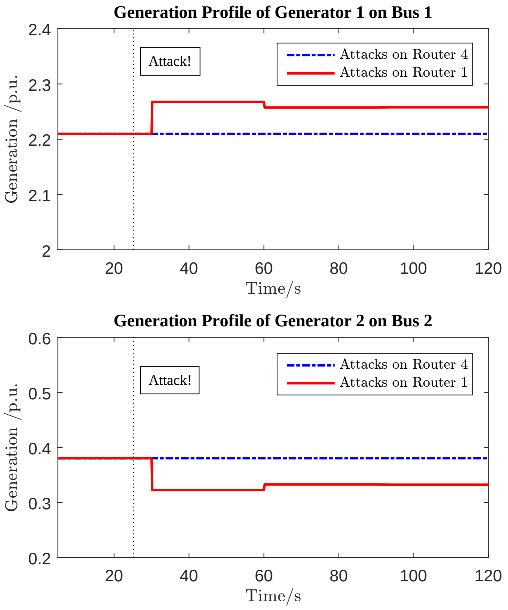

Figure 6. Attack impact of stealthy attacks on generation profile of Generator 1 and 2. The per-unit system is used and the power base is $100MW$. The true power flow measurements are generated by DC power flow model with Gaussian noise ($\sigma_i = 0.005$ for all the measurements). Before the attack occurrence, the system is operating under the optimal power flow status giving the loads. The loads on each bus keep the same before and after the attack. In these two cases, the same number of measurements are corrupted.

two routers containing different measurements. According to our single path routing scheme, in Router 1, the attacker can gain access to the power flow and injection measurements on bus 2, 3 and 4, which has the major impact on the generation profiles of these two generators.

Discussion on Combining Theoretic and ICT-specific Measures

The proposed analytic vulnerability assessment method can be used to narrow down the attack scenarios. Using the co-simulation platform, the attack impact can be explored by directly simulating attacks. New security metrics could be formulated taking into account the impact of the data attack.

As discussed in Section II-B, co-simulation could support security analysis in combining the system-theoretic and ICT-specific measures. In the case of data attacks against EMS, the BDD scheme acts as a theoretic measure to detect bad data. However, it fails to trigger alarms when we simulate attacks on Router 1 and Router 4 since the measurements still fulfill the physical laws and thus there is no increase on residual errors. To make it robust against data attacks, the communication network properties supported by co-simulation show the potential for developing a new BDD algorithm. For instance, the latency parameters in the communication channel can be modeled to have a Gaussian distribution. When FDI attacks take place, the latency of attacked packets changes due to the attack process. When availability attacks occur, the latency of attacked packets can be treated as an extreme case. Thus a robust BDD algorithm could be developed to trigger alarms when combined attacks take place, incorporating network properties with the latency of packets measured in the co-simulation platform. We leave this for future work.

VI. Conclusion

In this paper, we contribute to extend analytic methods incorporating communication network properties and develop a co-simulation platform to analyze data attacks against EMS. The results shows the need to consider the vulnerability and attack impact in an integrated assessment framework and combine the system theoretic and ICT-specific measures to protect EMS. Our future work includes more security analysis on AC power flow model and other EMS applications using the co-simulation platform, developing robust algorithms for detection and mitigation measures, etc.

References

[1] D. Goodin, "First known hacker-caused power outage signals troubling escalation," *Ars technica*, 2016. [Online]. Available: http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/

[2] S. Gorman, "Electricity grid in us penetrated by spies," *The Wall Street Journal*, vol. 8, 2009.

[3] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[4] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[5] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[6] K. Pan, A. M. H. Teixeira, M. Cvetkovic, and P. Palensky, "Combined data integrity and availability attacks on state estimation in cyber-physical power grids," in *Proc. IEEE Int. Conf. Smart Grid Communications (SmartGridComm)*, Nov. 2016, pp. 271–277.

[7] M. Stifter, J. H. Kazmi, F. Andrén, and T. Strasser, "Co-simulation of power systems, communication and controls," in *Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2014 Workshop on*, 2014, pp. 1–6.

[8] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *INFOCOM, 2014 Proceedings IEEE*, 2014, pp. 2625–2633.

[9] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A testbed for analyzing security of scada control systems (tasscs)," in *Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES*, 2011, pp. 1–7.

[10] M. Findrik, P. Smith, J. H. Kazmi, M. Faschang, and F. Kupzog, "Towards secure and resilient networked power distribution grids: Process and tool adoption," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*, 2016, pp. 435–440.

[11] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS), Stockholm*, 2010.

[12] J. Hong, Y. Chen, C.-C. Liu, and M. Govindarasu, "Cyber-physical security testbed for substations in a power grid," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 261–301.

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

[14] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, 2012.

[15] P. Palensky, A. A. V. D. Meer, C. D. López, A. Joseph, and K. Pan, "Cosimulation of intelligent power systems: Fundamentals, software architecture, numerics, and coupling," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 34–50, mar 2017.

[16] C. B. Vellaithurai, S. S. Biswas, R. Liu, and A. Srivastava, "Real time modeling and simulation of cyber-power system," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 43–74.