21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

CIGRE US National Committee
2015 Grid of the Future Symposium

Development of Cyber-Aware Energy Management System Applications

Y. SUN, S. SRIDHAR, M.J. RICE, M. VALLEM
Pacific Northwest National Laboratory (PNNL)
USA

SUMMARY

Supervisory Control and Data Acquisition (SCADA) systems play an integral role in the efficiency and reliability of power system operation. These systems provide system operators with feedback on critical power system variables, thus facilitating appropriate control. This control action, in most cases, is obtained from applications running within the Energy Management System (EMS). An adversary can cause severe consequences by compromising the computation and communication layer facilitating these applications. There is a growing need for cyber-attack-resilient control applications to detect highly skilled attacks. In this paper, we discuss the steps involved in the development of future EMS applications that are required to be cyber-threat aware. The traditional contingency analysis and state estimation procedures are enhanced by incorporating cyber information in the process. A sample SCADA network is designed for the IEC TC 57 test power system model for future test cases. The proposed algorithms provide a method to protect the electric power grid from cyber threats.

KEYWORDS

cyber-physical systems, cyber security, state estimation, contingency analysis

yannan.sun@pnnl.gov
The Pacific Northwest National Laboratory is operated by Battelle for the U.S. Department of Energy under Contract DE-AC06-76RL01830.

I. INTRODUCTION

The operation of modern electric power grids is performed by system operators through a suite of control applications available in the Energy Management System (EMS). The applications within the EMS arrive at control decisions by processing field measurements that are delivered through a network of computers and embedded devices called the Supervisory Control and Data Acquisition (SCADA) system. The applications enabled by the SCADA backbone can be automated or human-in-the-loop, local or area-wide, proactive (once-in-an-hour unit commitment) or reactive (protection). They are prevalent in all domains of power system operations – generation, transmission and distribution.

The vulnerabilities in SCADA are well documented. More critically, the number of cyberattack on critical infrastructure is rapidly increasing. Inherent redundancy and current operational practices are sufficient to defend the grid against threats from less-knowledgeable attackers. However, recently discovered cases in industrial control systems have revealed highly sophisticated attacks and extremely knowledgeable attackers.

The focus of this paper is on the state estimation (SE) and contingency analysis (CA) applications in the EMS. SE is used by system operators to calculate the voltage at various buses in the power system. Measurements supplied by field devices are expected to be inaccurate due to transducer errors and calibration errors, so they are "curated" by SE. The output SE is used as an input to other applications within the EMS that perform computations based on the current system state. CA is one such application that makes use of the estimated state to perform "what if" studies. CA identifies events that could lead to violations given the current state of the power system. SE and CE enable system operators mitigate violations.

As identified earlier, knowledgeable threat actors have the capability to attack EMS applications to i) directly enforce a change to the power system, or ii) trick the system operators into making an incorrect decision by providing them with malicious information. Future EMS applications must operate accurately in the presence of malicious data and be aware of cyber-events that could impact the system. Toward this end, we propose an algorithm that enhances SE in the presence of malicious data. Specifically, we show that de-weighting measurements from vulnerable substations can achieve accurate state estimates. We also enhance CA by considering contingencies that could arise from cyber threats. Specifically, we rank contingencies based on the vulnerability of substations to cyber-attacks.

There is prior work combining cyber-information with SE and CA. For SE, cyber-security of supervisory control and data acquisition (SCADA) was examined in [1] with an analysis of attack detectability (via bad data detection (BDD)) contingent upon the attacker's knowledge of the power grid topology. SCADA SE security was also examined in [2]. The authors of [3] analyzed the robustness of all-PMU SE during network failures and false-data injection. A compressive-sensing based approach to false-data attack detection was developed in [4]. In [5], it was shown that an attack can be made undetectable with knowledge of the power system topology. A "security-oriented cyber-physical SE system" was developed in [6] with improved intrusion detection capabilities and the ability to identify compromised resources.

Metrics for evaluating the impact of physical- and cyber-contingencies in cyber-physical systems require further development. In [5], metrics were proposed based on financial loss due to undetected cyber-attacks, and [7] used reliability as a risk metric. In [8], vulnerability metrics were developed in terms of the whole system, various scenarios, and different access points. In [9], $(N-x)$ contingencies were analyzed using graph theory, and contingency rankings were developed for coordinated cyber-attacks. Security benchmarks were proposed in [10], focusing on both faults and attacks with explicit cyber-physical defense models.

In this paper, new algorithms of SE and CA are proposed for cyber-physical systems. The SCADA network model is designed for the IEEE 57 bus system. A Petri net model for the entire SCADA model is created using individual substation Petri nets to estimate the network vulnerability, which is needed in the SE and CA. We show how SE results can be used to confirm cyber events in order to guide the CA procedure. The rest of this paper is organized as follows. Section II introduces an SE algorithm that uses the cyber vulnerability estimates to adjust the weights in the iterative state estimation process. Section III proposes a contingency analysis framework to examine $(N-x)$ contingencies partially for cyber events. Section IV presents a simulation study using the proposed algorithms. Section V concludes the paper.

II. SITUATION-AWARE EMS APPLICATIONS

A. State Estimation

In this section, a generic algorithm is introduced to perform SE with information from the communication network. The existing BDD algorithm is improved to identify possible compromised measurements (PCMs) from grid based cyber events. We assume that probability of each measurement being compromised can be estimated by certain methodologies such as security information and event management (SIEM) solutions online. Offline vulnerability evaluation models such as Petri net models can be used to estimate the vulnerability level of each substation and identify the trust level for each measurement, which is used to compute the measurement's weight used in the weighted least squares (WLS) algorithm for estimating states.

In the process of BDD, the PCMs are treated as normal measurements with normal weights, since cyber-events may not necessarily affect SE. If any of the PCMs is detected as bad data, its weight used in the WLS algorithm is reduced unless the weight is already smaller than the preselected threshold. The weights for the measurements corresponding to the same physical node will be reduced if one of the measurements is detected as bad data. These measurements are not removed as normal bad data immediately. Therefore, this approach will prevent the SE process from having observability issues. The flowchart in Fig. 1 gives the details of the developed SE algorithm.

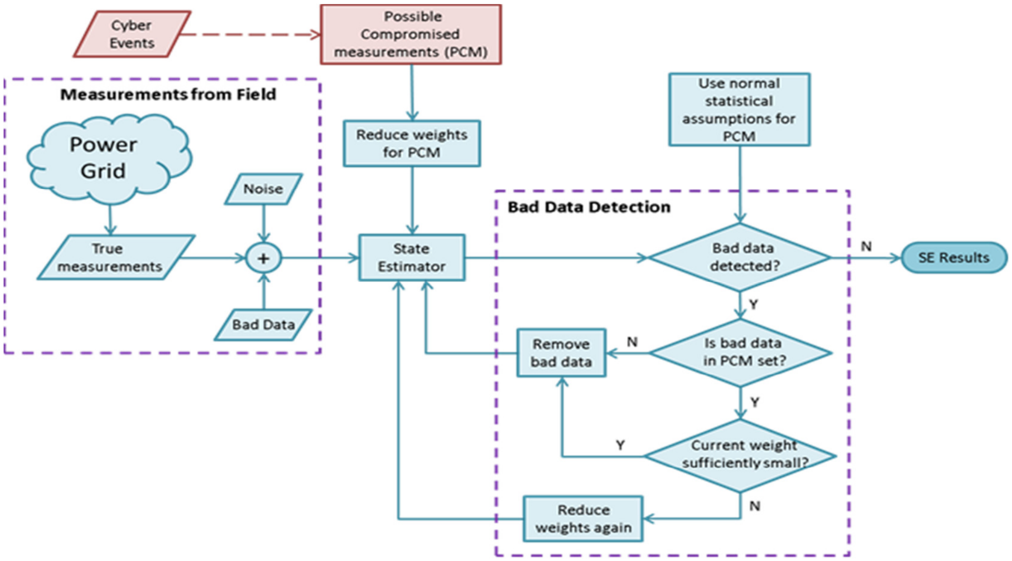

Fig. 1 Algorithm for State Estimation with Cyber Information, the 'Possible Compromised Measurements' block is implemented online

B. Contingency Analysis

Contingency analysis is an offline procedure typically performed to observe system response to an $(N-1)$ condition, that is, the loss of a single component (generator or transmission line). Based on this "what if" analysis, operators adjust system operating points such that the actual occurrence of a contingency will not affect system reliability. The events considered within the scope of CA, e.g., open-circuit faults due to inadvertent tripping of breakers, originate from natural causes uninfluenced by human action. However, the possibility of attackers being able to inject malicious "trip commands" to breakers could result in an $(N-k)$ contingency, where the loss of 'k' system components could severely affect reliability. It is not computationally feasible to evaluate the impact of and recompute operating points for all $(N-k)$ scenarios for changing system conditions.

Our framework for cyber CA will drastically reduce the number of $(N-k)$ contingencies to be analyzed in two steps. First, an offline vulnerability analysis of the cyber (SCADA) infrastructure helps understand the "strength" of installed cyber-defense mechanisms, and thereby provides an estimate of the most vulnerable substation networks in the system. Second, real-time monitoring of the cyber network during online operation reveals active targets in the system. A high-level view of the proposed cyber CA is given in Fig. 2.

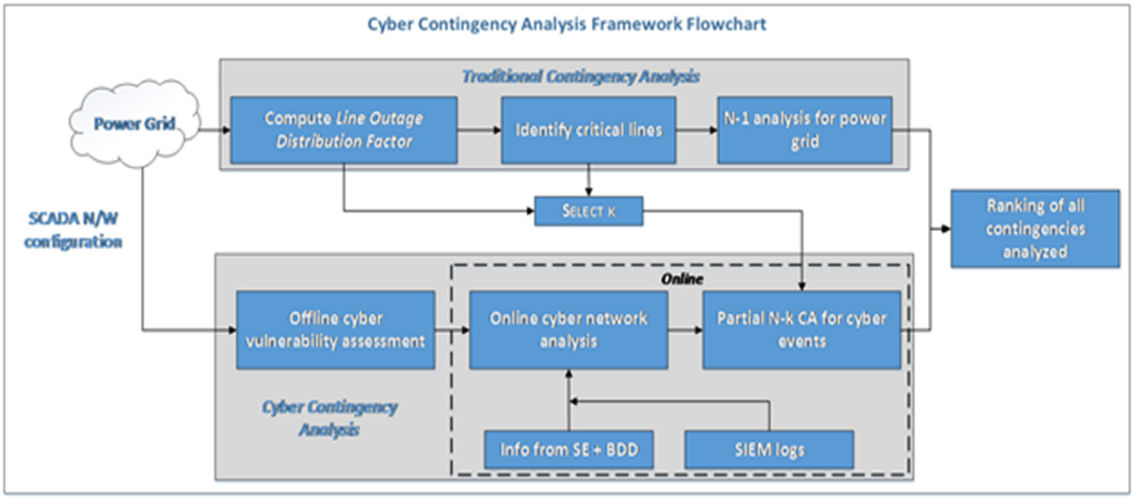
Cyber Contingency Analysis Framework Flowchart
Traditional Contingency Analysis
Power Grid
Compute Line Outage Distribution Factor
Identify critical lines
N-1 analysis for power grid
SELECT K
SCADA N/W configuration
Ranking of all contingencies analyzed
Online
Offline cyber vulnerability assessment
Online cyber network analysis
Partial N-k CA for cyber events
Cyber Contingency Analysis
Info from SE + BDD
SIEM logs

Fig. 2 Cyber Contingency Analysis Framework

The power grid block, which includes the associated SCADA network, provides input to both the traditional CA and cyber CA. The SCADA network information should include the following: network architecture/configuration, existing network security mechanisms/devices and available access points. This information is used by the offline cyber vulnerability assessment block to model the cyber network and evaluate the strength of existing security measures. Mathematical modelling tools such as stochastic Petri nets could be used for this purpose [11]. The output of vulnerability assessment is provided as input to the online analysis section. The objective of online analysis is to estimate the probability of network compromise based on input from offline vulnerability analysis, and online "cyber health" information from SIEM logs and information from SE/BDD. A substation with a compromised cyber network is one in which an attacker could inject malicious control commands, such as opening breakers. Hence, with information on potentially compromised substations, an

$(N-k)$ CA becomes computationally inexpensive. This is because the size of N is significantly reduced to include the components in the compromised substations only.

The computations maybe further reduced by using input from traditional $(N-1)$ CA. The $(N-1)$ CA uses Line Outage Distribution Factors (LODFs) to calculate the change in line flows for the loss of a single transmission line. Therefore, the traditional CA will help identify critical lines that, when tripped, can cause significant change to the flow in other lines of the system. Critical lines are most likely to cause a severe impact when tripped in combination with other transmission lines. Hence, the partial $(N-k)$ CA will be performed according to a priority list generated based on the critical line information. This will help accommodate the CA procedure to any time constraints. Finally, the framework will provide a ranking of contingencies that include both $(N-1)$ contingencies from traditional CA and partial $(N-k)$ contingencies from cyber CA. With this ranking, the system operator will be able to perform appropriate control actions to prepare the system for contingencies.

III. CYBER-PHYSICAL DATA CREATION

In order to test the proposed algorithms, an example cyber-physical system is needed for creating data. In this section, the IEEE 57 bus system, which contains 57 buses, 80 transmission lines, and 5 active generators, is used to demonstrate how the cyber network can be modelled. In addition, a Petri Net model is given to analyze the vulnerability of the SCADA network offline.

A. *Modelling the SCADA Network*

A SCADA network typically has multiple substations communicating with a control center using technologies such as fiber optics, microwave and twisted-pair. Measurement signals originating from substations are relayed to the control center by network routers and similarly, control commands from the control center are relayed back to the substations. This wide-area communication typically uses communication protocols such as DNP and IEC 61850. Inside a substation, remote terminal units are used to communicate the control commands to IEDs which implement the actual control action. Some control actions are also initiated locally by operators at the substation level. This may include operations such as transmission line switching and voltage control. Protocols such as MODBUS are typically used for this communication.

A pictorial representation of the modeled SCADA network for the IEEE 57 bus system is given in Fig. 3. Each square (green or yellow) represents a substation LAN, where the yellow squares represent transmission substations and the green squares represent generation stations. Each substation consists of a substation network and they are connected to one another and the control center via a wide-area network (WAN). The WAN is designed such that each network router has more than one path to every other router in the network. Consistent with real-world design, this ensures there aren't any single points of failure in the network. In total, there are 22 substations (15 transmission and 7 generation) that are interconnected by six network routers. The control center is not shown in this figure.

B. *Modelling Cyber Vulnerability Using Petri Nets*

The objective of modeling the cyber network is to estimate the vulnerability of the substation network to intrusion attacks, i.e., attack scenarios where the attacker attempts to gain access to the HMI/workstation in order to control the IEDs. If successful, in the assumed substation configuration, the attacker would be able to perform malicious switching operations that will affect grid reliability by causing transmission line overloads. In this study, stochastic Petri Nets are used to model the substation and SCADA networks in order to identify a metric called probability of compromise. The probability of compromise, identifies the probability of an attacker being able to gain access to the

HMI/Workstation when a penetration attempt is made. In order to identify the probability of compromise of a substation, it is important for the cyber model to capture the security technologies installed in the network. In our case, two cyber security features are considered; a firewall to prevent unauthorized network access and a password protection mechanism for the HMI/workstation. The Petri Net modeling of the substation network used in this work was first developed in [8]. In the interest of space, we omit the details in this paper and point readers to the original work in [8].

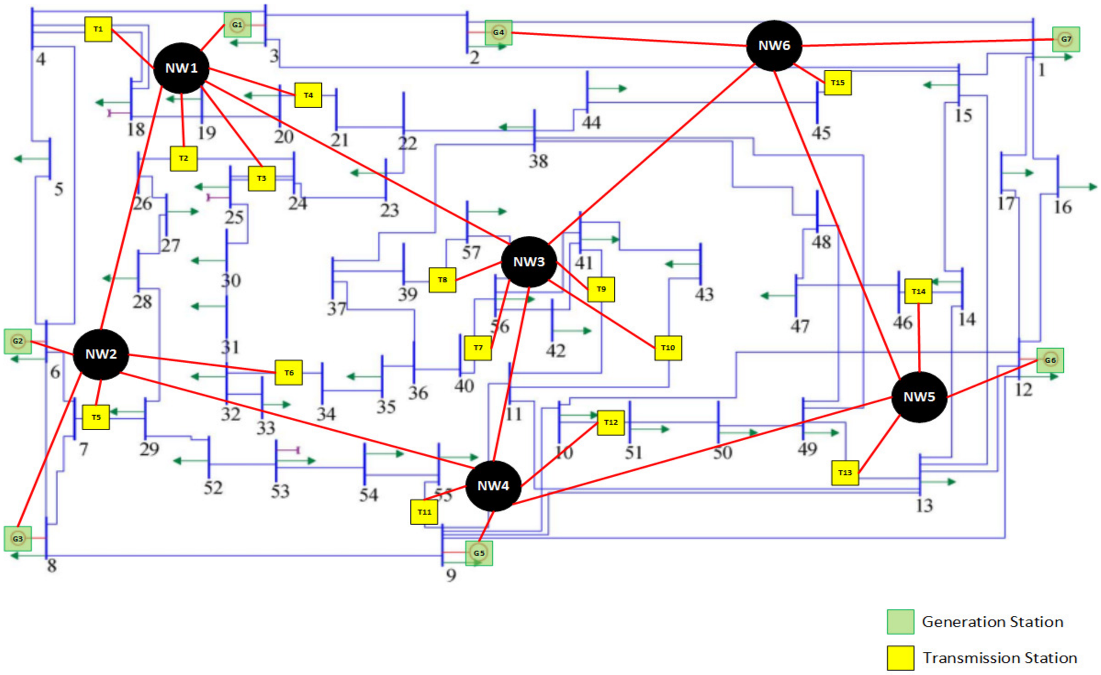

Fig. 3 IEEE 57 bus-system SCADA network configuration.

To summarize, Fig. 4 represents a Petri net model for a substation consisting of one firewall and two password protected computers. The model consists of "places" (the circles), "transitions" (rectangular bars) and "tokens" (the solid circle/dot in place T5_cmpB). The probabilities associated with the model were obtained by analyzing firewall and computer logs from real-world systems. The probability of successful compromise is obtained from the probability of a "token" in either "place" T5_cmpB (1st computer) or T5_cmpC (second computer). This probability is obtained from Petri Net solvers that accept the Petri Net model and probabilities as input. A Petri net model for the entire SCADA network model for the IEEE 57-bus model was created using individual substation Petri nets. Table I gives the analysis results for the SCADA network designed previously. The risk is a function of the probability of compromise of a substation and the corresponding impact of compromise.

The data collected for firewall and password probabilities was collected from real-world IT network of a university. These values will be different for an operations environment. Even more, these values will also change with time as more vulnerabilities are discovered and as patches are installed. The intent of this paper was to show how probability of compromise values calculated by processing network traffic logs could be used to identify high-risk attack vectors. In real-world operations environment, the probability of compromise should be calculated by applying the same methodology. These values should also be updated on a regular basis to reflect the true state of infrastructure security.

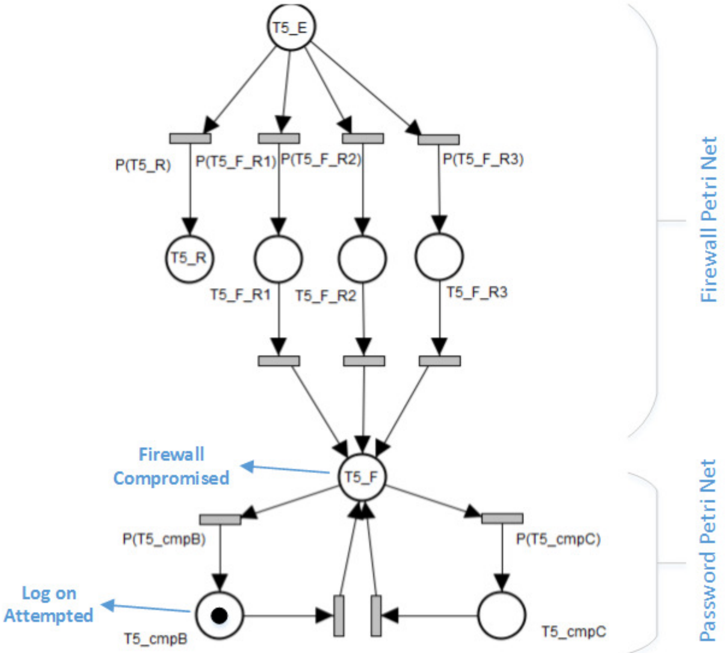

Fig. 4 Firewall and password Petri net model for a substation

Table I. Vulnerability Analysis Results using Petri Net Model

Substation #	Risk	Substation #	Risk	Substation #	Risk
1	0.154	6	0.032	11	0.011
2	0.098	7	0.019	12	0.012
3	0.110	8	0.020	13	0.010
4	0.096	9	0.022	14	0.012
5	0.037	10	0.019	15	0.010

IV. CONCLUSIONS

In this paper, we proposed new algorithms for SE and CA in cyber-physical systems. The SCADA network model is designed for the IEEE 57 bus system to test the algorithms. A Petri net model for the entire SCADA model is created using individual substation Petri nets to estimate the network vulnerability, which is necessary for testing the proposed algorithms. Due to the limited space of this paper, we are not able to present the test results for the algorithms using the IEEE 57 bus test system. As future work, we will compare our results to a baseline case where the cyber information is not considered to show the effectiveness of the proposed algorithms.

BIBLIOGRAPHY

[1] A. Teixeira, S. Amin, H. Sandberg, K. Johansson, and S. Sastry, “Cyber security analysis of state estimators in electric power systems,” in *Decision and Control (CDC), 2010 49th IEEE Conference on*, 2010, pp. 5991–5998.

[2] G. Andersson, P. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, A. Teixeira, G. Dan, H. Sandberg, and K. Johansson, “Cyber-security of SCADA systems,” in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1–2.

[3] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, “Cyber security impacts on all-PMU state estimator - a case study on co-simulation platform GECO,” in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*, 2012, pp. 587–592.

[4] K. C. Sou, H. Sandberg, and K. Johansson, “On the exact solution to a smart grid cyber-security analysis problem,” *Smart Grid, IEEE Transactions on*, vol. 4, no. 2, pp. 856–865, 2013.

[5] L. Xie, Y. Mo, and B. Sinopoli, “Integrity data attacks in power market operations,” *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 659–666, 2011.

[6] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, “SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures,” *Smart Grid, IEEE Transactions on*, vol. 3, no. 4, pp. 1790–1799, 2012.

[7] J. Stamp, A. McIntyre, and B. Ricardson, “Reliability impacts from cyber attack on electric power systems,” in *Power Systems Conference and Exposition, 2009. PSCE ’09. IEEE/PES*, 2009, pp. 1–8.

[8] C.-W. Ten, C.-C. Liu, and G. Manimaran, “Vulnerability assessment of cybersecurity for SCADA systems,” *Power Systems, IEEE Transactions on*, vol. 23, no. 4, pp. 1836–1846, 2008.

[9] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information,” *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 235–244, 2013.

[10] S. Amin, G. Schwartz, and A. Hussain, “In quest of benchmarking security risks to cyber-physical systems,” *Network, IEEE*, vol. 27, no. 1, pp. 19–24, 2013.

[11] G. Ciardo, J. Muppala, and K. Trivedi, “Spnp: stochastic petri net package,” in *Petri Nets and Performance Models, 1989. PNPM89., Proceedings of the Third International Workshop on*. IEEE, 1989, pp. 142–151.