Cyber Vulnerabilities on Agent-based Smart Grid Protection System

Md Shihanur Rahman and Hemanshu R. Pota
School of Engineering and Information Technology
University of New South Wales
PO Box 7916, Canberra BC 2610, Australia

Md Jahangir Hossain
Griffith School of Engineering
Griffith University
Gold Coast, QLD 4215, Australia

***Abstract*—This paper presents an innovative approach to identify potential impacts of cyber attacks on agent-based smart grid protection relays. An agent-based protection framework is developed, where an attacker may injects a malicious breaker trip command to the relay settings. This could cause unintentional tripping of CBs, even if there is no physical disturbance on the system. It results a healthy line of smart grids to be out-of-service that leads cascading failures. An algorithm is proposed to identify such kind of attack generated latency caused by unexpected malicious trip command. Using this algorithm agents can check the breaker statuses to ensure which line is out-of-service due to unintentional tripping. Furthermore, the proposed technique will be able to distinguish cyber attacks from faults on the system.**

***Index Terms*—smart grid, agent, cyber attack, protection relay, security, phasor measurement**

I. Introduction

A smart power grid usually depends on a complex network of computers, software, and communication technologies for its operation and control. It deploys many new technologies including intelligent electronic devices (IEDs), smart meters, sensors, actuators, phasor measurement units (PMUs) which require a communication infrastructure superimposed on physical grid components. The implementation of synchrophasors enhance the best situational awareness on smart grid protection systems. Besides physical failures, smart grids are also prone to various cyber threats. Every communication path that supports monitoring and control of smart grids is a two-way communication path which can be a potential attack path for an attacker [1]. This paper considers an unexpected malicious operation of protection relays. An agent-based smart grid framework is developed in this paper, where each agent is assumed to be equipped with a protection relay. These agent-based relays are considered as IEDs, since they are capable of taking autonomous decision for relay coordination using the breaker status signals provided by PMUs. An innovative algorithm is proposed which assists these relay agents to identify potential impacts of attacks on the protection systems. Subsequently, the agents are also able to distinguish attacks from faults.

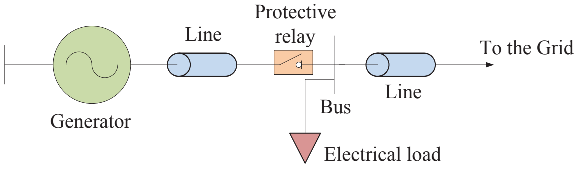

Fig. 1. A node in a smart grid

A large smart grid is a distributed critical infrastructure which includes an interconnection of a large number of autonomous nodes. A node of a typical physical smart grid architecture is shown in Fig 1. Each node may consist of a generator with necessary control equipments, an electrical load and a protection relay conncted to a main grid through transmission lines. Being a large cyber-physical system (CPS), smart grids are vulnerable to several cyber security threats [2]. The U.S. Department of Homeland Security concerns about the coordinated cyber attacks that result prolonged outages in large portions of electricity grids [3]. A very few works related to cyber vulnerabilities on protection systems have been discussed in [3]–[6]. A potential cyber threat may modify the settings of the protection relays. The intention of this attack is to open and close CBs at undesirable time. This unintentional opening and closing of CBs may cause a risk to the rotating machinery. Consequently, an undesired disconnection of healthy portion of a line may damage the equipments connected to the main grid.

In this paper, the impacts malicious breaker trip command in the from of integrity attack is considered. An integrity attack is assumed that PMU-based relays are hacked by an attacker by altering the relay settings. As a result, the breaker status signals have changed and consequently, unintentional tripping of CBs occur. This may cause a healthy line to be out-of-service, even if there is no physical disturbance. An innovative algorithm along with three key indices namely, fault current measurement, breaker status look up table and line current flow look up table, is proposed in this paper. Using this algorithm intelligent relay agents are capable of detecting an attack and hence further distinguish it from fault on the system. An illustrative example of a well known WSCC three-machine nine-bus power system is provided to validate the effectiveness of the proposed approach. Both scenarios of physical and cyber disturbances are considered for simulations.

II. Agent-based Protection Framework

Smart grid is a modern electric power grid infrastructure, where information and communication technologies (ICT) provide a fundamental element on its growth and performance [7]. It uses specific protocols and diverse transmission

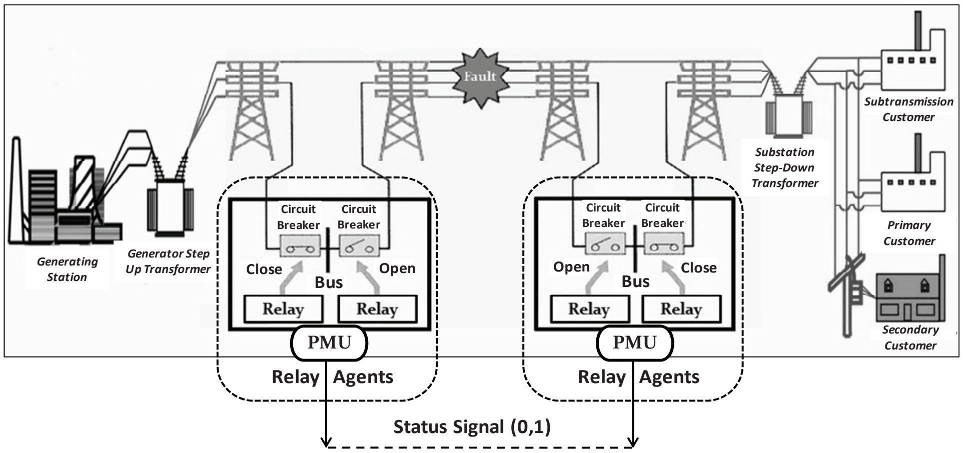

Fig. 2. Agent-based smart grid protection infrastructure

media for monitoring and controlling its critical infrastructure [8]. In smart grids, communication networking and intelligent ICT functions are embedded from power generation, transmission and distribution to the consumer appliances. This kind of infrastructure is open to several cyber threats. In large-scale power systems, coordination of protection relay operation is a critical task. One of the effective solution is to implement multi-agent systems (MASs) on protection relays for proper relay coordination. An agent-based protection relay infrastructure is presented in the following section.

A. Agent-based relay infrastructure

Modern relays are Internet Protocol (IP) ready and support communication protocols such as IEC 61850 [9]. Using global positioning system (GPS) technology, PMU-based protection systems are currently used in smart grids. With the advent of PMU-based digital relays [10] the concept of agent-based protection relay brings a new dimension to the smart grid protection and security. An agent-based protection relay framework is shown in Fig. 2, where intelligent agents are embedded with protection relays through softwares. In addition, PMUs are used to provide a set of breaker status signals among the relay agents to assist in decision making for proper relay coordination. These relay agents are placed in different geographical locations along with the nodes. The functions of these relay agents are determined through software and they use breaker status signals to implement their control actions by opening and closing CBs during disturbances.

For CB operation, each agent uses the breaker status signal $c_{\mathrm{i}}(t)$ for breaker i, where $i = 1, 2, 3, ...n$, where n is the number of circuit breakers (CBs) in a smart grid. The status signal for opening and closing of CB can be initiated as,

$$C_i(t) = \begin{cases} 0, & \text{for opening of CB at time } t \\ 1, & \text{for closing of CB at time } t \end{cases}$$

Initially the status signal is set to 1 for normal operation of the system. In addition, agents use these signals to communicate with each other via high speed communication network for relay coordination. In this paper, it is assumed that the smart grid infrastructure already has a necessary communication network.

B. Cyber vulnerabilities on smart grid protection system

Phasor measurements are very effective since reliable measurements from PMUs substantially improve the protection functions possible. As the protection relay agents use binary status signals (0,1) provided by PMUs for CB operation, therefore, an adversary may take an advantage of using these signals to manipulate the relay settings which could cause an unintentional tripping of CBs. A false tripping is likely to cause cascading failures that consequences transient instability and system collapse, even if there is no physical disturbances. From cyber security perspective, it can be recognized that a relay agent may trip when it should not be or it may fail to trip when it should be.

A successful cyber attack may results an unintentional opening of CBs which will remove the healthy line from service without any fault. Subsequently, it may cause unintentional closing of breakers, even before critical fault clearing time. Recent research studies have focused on interactions between the cyber and physical aspects of a smart grid to aid in impact analyses of various cyber attacks [11]. One of the major cyber security requirements is the integrity of data, commands, and knowledge of a smart grid. An integrity attack is crucial that can alter the relay settings during normal operation, i.e., inject a malicious breaker trip command to alter the behavior of relays. This could cause a relay agent to make wrong decision that results a significant loss to the utility grid. The cyber vulnerability analysis for smart grids is described in the following sections.

III. Cyber vulnerability analysis

An agent-based framework is proposed in this paper for cyber vulnerability analysis. An algorithm is developed through which agents can detect cyber threats and distinguish it from physical failures. In fact, the algorithm is responsible for determining the present network topology by simultaneously monitor the present system status. Agents can coordinate the protection relays during fault by measuring the fault current flows from across the relays. In addition, they use the line current flows to identify an out-of-service line and consequently, breaker status signals to confirm an outage after experiencing a cyber attack.

A. Algorithm

The algorithm developed in this research is used to assists agents for detecting both fault and cyber attack in addition with distinguishing between them. This algorithm uses fault current measurement for fault analysis. Subsequently, it includes a full network model of smart grid for load flow analysis. For attack detection, this algorithm uses breaker status and line current measurement look up tables. Breaker status look up table consists of number of breakers for each line and status signals are used from across the network for cyber threat detection. In addition, the line current measurement look up table is used for identifying an out-of-service line. The current measurement look up table consists of current measurements of each line which indicating flow and no flow statuses as "1" and "0", respectively.

The algorithm can update the measured system information at each iteration of the program to reflect any changes in the system. It first monitors and measures the present system status from the full network topology. If the system behaves normally, agents decide for normal operation. If abnormal condition happens, algorithm first checks the fault current. If fault current flows from across the relays then it will go for fault analysis. On the other hand, if there is no fault current flows across the relays, it will go for cyber vulnerability analysis. If line current flows as normal perhaps due to problems resolved automatically, it takes the decision for normal operation. If there is no current flows, it will refer to the breaker status look up table to check CB operation. Once the agents can properly recognize a cyber threat, they alert the system operator via alarm systems to take preventive counter measures. The flowchart of the proposed mechanism is shown is shown in Fig. 3.

B. Fault detection

For fault detection, a threshold value of current, I_{th}, is set for each relay agent. Therefore, during a fault in a particular branch, agents can detect it by measuring the fault current. That means when a fault current flows above its rated or predefined threshold value, i.e., $I_{\text{f}} > I_{\text{th}}$ across the relays, agents can recognize a fault on the system. Once a fault is identified, corresponding agents coordinate the protection relays using the breaker status signal. They initiate the status signal $c_{\text{i}}(t) = 0$ to open the corresponding CBs to disconnect the faulted line from the rest of the system. When the fault is cleared they initiate $c_{\text{i}}(t) = 1$ for reclose the CBs to reconnect the line. It should be noted that, a high-speed fault clearing within the critical clearing time (CCT) is highly desirable for avoiding instabilities which is not discussed in this paper.

C. Cyber attack detection

To identify a cyber attack, the algorithm looks at the current measurement look up table for each iteration. It can determine whether current flows in the lines or not, even if no fault current flows across the relays. The algorithm stores a set of data in a vector for first iteration. For next iteration, it compares to the same vector from the previous iteration. If the subtraction of two vectors in all branches is zero then there is no change in the line currents since last iteration. If there is a non-zero vector found in a particular branch, it can detect a change in the line current, i.e., no current flows. Hence, the algorithm can indicate which branch of the network is affected without any fault occurring on it and thereby, identify out-of-service line as well. The agents can recognize this could happen due to the latency of breaker status signals. A possible reason for this latency may assume to be a cyber attack.

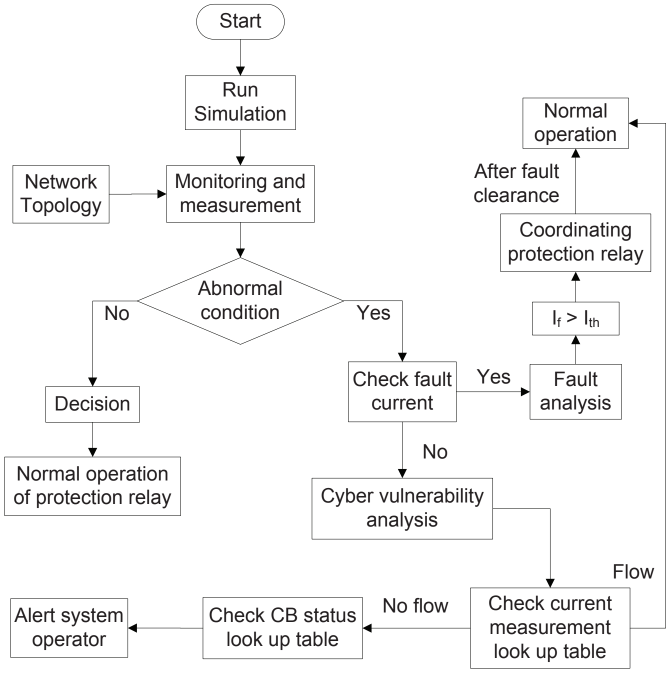
Start
Run Simulation
Network Topology
Monitoring and measurement
Abnormal condition
No
Yes
Decision
Normal operation of protection relay
Check fault current
Yes
Fault analysis
$I_f > I_{th}$
Coordinating protection relay
After fault clearance
Normal operation
No
Cyber vulnerability analysis
Flow
Check current measurement look up table
No flow
Check CB status look up table
Alert system operator

Fig. 3. Flowchart of the proposed mechanism

For more robust detection of cyber threat, the algorithm refers to the breaker status look up table. Using this table agents can identify which breaker is "open", even if there is no fault current flows across the relay. The algorithm checks the inconsistencies in the breaker status data by comparing the recent set of it with the previous one. Subsequently, it updates the present system information and output the result. If an adversary injects a malicious trip command in relay settings, there is a mismatch in the breaker status signal. That means an integrity attack alters the behavior of the relays using status signal "1" for normal operation to "0". This will cause an unintentional opening of CBs at undesired time. In fact, if an attacker knows about the full network topology, he can manipulate the relay settings by corrupting their status from "open" to "close" and vice-versa. This will lead the system to an unstable condition that results widespread blackouts.

The agents can distinguish a fault and an attack by using the three key indices mentioned above. To recognize a fault in a line, agents use fault current measurement across the relays.

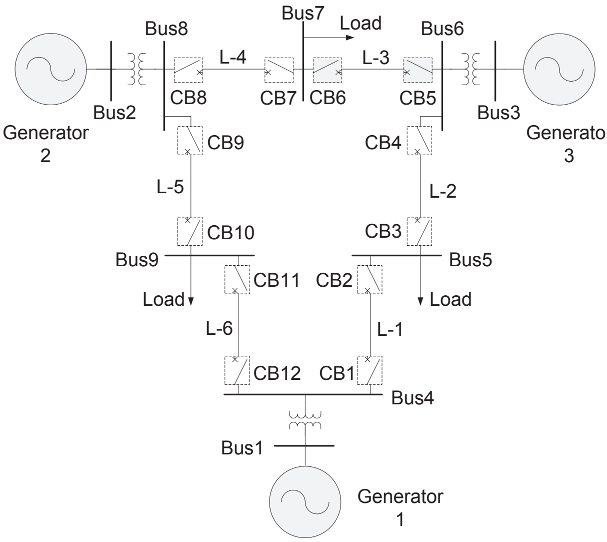

Fig. 4. Single-line diagram of WSCC 3-machine 9-bus power system

As a matter of fact, they refer to the current measurement and breaker status look up tables for attack detection. If agents find that breakers in a particular branch read "open" without any fault or read "close" before fault clearing, they recognize it due to cyber attacks.

IV. Illustrative example and results

As cyber vulnerability is now accounts for a great security threat for smart grids, more attention has been directed to the impact analysis of cyber attacks. To evaluate the potential of the proposed approach a WSCC three-machine nine-bus system [12] is used in this paper considering generator 1 as slack bus. A single line diagram of the test system is shown in Fig. 4, where the relays with corresponding breakers are represented as relay agents. It is considered that the system is running normally at steady state and all the branches are in service. A short-circuit fault is applied at t = 2.0 s in line 3 between bus 6 and 7. When fault current flows above the predefined threshold value set across the relays 5 and 6, the corresponding relay agents detect it. Once fault is identified, they initiate the status signal "0" to open the corresponding CBs to remove the faulted line. After a certain duration, when fault is cleared, agents initiate "1" to reclose the CBs to reconnect the line. From Fig. 5 it can be seen that, the generator rotor angles are transiently stable over the period of 8 s after successful relay coordination by agents.

Now to analyze the impacts of cyber attack, an integrity attack is initiated at t = 0.85 s. This attack template is generated by injecting a set of malicious signals "0" and "1" that follows like "AND" logic to the original breaker status signals used by agents. The malicious signals are responsible for altering the CB status signal and their intention is to hamper the normal operation of the CBs. This can be assumed an integrity attack executed by an adversary who has knowledge about the protocol of protection relay settings.

When the system behaves abnormally due to other than faults, the agents start to investigate for cyber vulnerability analysis. It is assumed that the attacker may take a chance to corrupt the relay settings at any instances. Using the proposed algorithm, the agents first check the line current measurement look up table. If there is an inconsistencies between last and previous iteration, agents are able to identify the out-of-service line. Subsequently, they check the breaker status look up table to confirm which CB is open without any fault occurring on the corresponding line. The look up tables for current measurement and breaker status at normal operation are shown in Table I and Table II, respectively. If the algorithm finds inconsistencies in current measurement and breaker status, it updates the full network model for each integration step. The output results are summarized in Table III and Table IV.

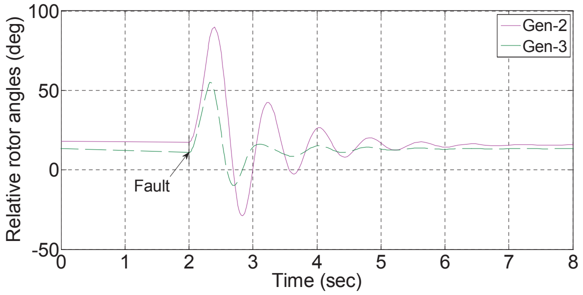

Fig. 5. Generator relative rotor angles due to fault

TABLE I
Current measurement look up table

Current measurement	Line	Status	Current measurement	Line	Status
1	1	1	7	4	1
2	1	1	8	4	1
3	2	1	9	5	1
4	2	1	10	5	1
5	3	1	11	6	1
6	3	1	12	6	1

TABLE II
Circuit breaker status look up table

Circuit breaker no	Breaker status	Circuit breaker no	Breaker status
1	1	7	1
2	1	8	1
3	1	9	1
4	1	10	1
5	1	11	1
6	1	12	1

TABLE III
Full network line flows after experiencing a cyber attack

Line number	From bus	To bus	Line status
1	4	5	1
2	6	5	1
3	6	7	0
4	8	7	1
5	8	9	1
6	4	9	1

Table III summarizes the full network model. It indicates the line number in first column, from and to bus in second and

TABLE IV
CIRCUIT BREAKER STATUS AFTER EXPERIENCING A CYBER ATTACK

Breaker number	Present status	Breaker number	Present status
Breaker 1	close	Breaker 7	close
Breaker 2	close	Breaker 8	close
Breaker 3	close	Breaker 9	close
Breaker 4	close	Breaker 10	close
Breaker 5	close	Breaker 11	close
Breaker 6	**open**	Breaker 12	close

third column, respectively, and the current flow status in fourth column. From Table III it can be seen that, the line current flows from bus 6 to 7 is zero without any fault between them. On the other hand, Table IV summarizes the output of the breaker statuses. This table shows that CB 6 is "open" without any fault current flows across the corresponding protection relay agent. This is due to cyber attack on CB 6. As CB 6 is used in line 3 for its protection, therefore, its unintentional tripping results current flow from bus 6 to 7 becomes zero and thereby, causes line 3 to be out-of-service. From Fig. 6 it can be seen that, the generator rotor angles are in steady state till 0.85 s without any cyber attack. The angles after 0.85 s, when an integrity attack is initiated, suddenly increases and continues that plotted over the period of 2 s. Proper counter measuring can be useful to mitigate the risk of cyber attacks for preserving the system stability. The CB status provided by PMUs for pre-fault, during fault, post-fault, during attack and normal operation is shown in Fig. 7 over the period of 5 s. A few counter measuring techniques can be available to mitigate the attacks, such as breaker closing supervision with a time delay, CB command supervision, a reclosing supervision by a backup protective relay, high-level communication and IT security for wide-area synchronized phasor measurements [3], and also a few more can be found in [13], etc,.

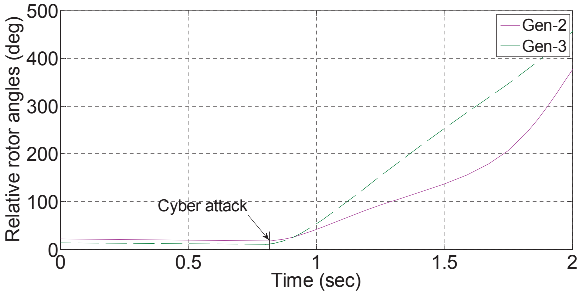

Fig. 6. Generator relative rotor angles due to cyber attack

V. CONCLUSION

In this paper, an agent-based framework for smart grid protection and security is developed. Become a large CPS, smart grid protection system is vulnerable to several cyber threats. An integrity attack impact on smart grid relay operation is discussed in this paper. A potential cyber attack may cause an unintentional tripping of CBs that leads to an outage. An algorithm is proposed through which agents are able to detect an attack rather than fault using three key indices. The algorithm uses line flows along with breaker statuses to provide a more robust identification of cyber attacks. The preliminary results give a hope that implementation of such kind of mechanism can be an effective tool for identifying cyber threats which affect the protection relay operation. Furthermore, this can be also useful for designing a counter measure for protection relay security.

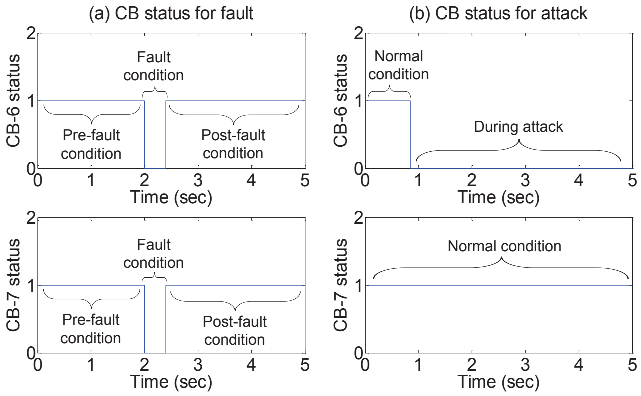

Fig. 7. CB status provided by PMUs for (a) fault and (b) attack

REFERENCES

[1] *Study of Security Attributes of Smat Grid Systems- Current Cyber Security Issues*, National SCADA test bed report 2009 Std.

[2] Y. Deng and S. Shukla, “Vulnerabilities and countermeasures- A survey on the cyber security issues in the transmission subsystem of a smart grid,” *Journal of Cyber Security and Mobility*, vol. 1, pp. 251–276, 2012.

[3] D. Salmon, M. Zeller, A. Guzman, V. Mynam, and M. Donolo, “Mitigating the aurora vulnerability with existing technology,” in *36th Annual western protection relay conference*, 2009.

[4] J. Fadul, K. Hopkinson, C. Sheffield, J. Moore, and T. Andel, “Trust management and security in the future communication-based "smart" electric power grid,” in *44th Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1–10.

[5] K. Ross, K. Hopkinson, and M. Pachter, “Using a distributed agent-based communication enabled special protection system to enhance smart grid security,” *IEEE Trans. on Smart Grid*, vol. 4, no. 2, pp. 1216–1224, 2013.

[6] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid,” *IEEE Trans. on Smart Grid*, vol. 4, no. 2, pp. 847–855, 2013.

[7] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, “A survey on smart grid potential applications and communication requirements,” *IEEE Trans. on Industrial Informatics*, vol. 9, no. 1, pp. 28–42, 2013.

[8] C. Queiroz, A. Mahmood, and Z. Tari, “A probabilistic model to predict the survivability of scada systems,” *IEEE Trans. on Industrial Informatics*, vol. 9, no. 4, pp. 1975–1985, 2013.

[9] M. Govindarasu, A. Hann, and P. Sauer, “Cyber-physical systems security for smart grid,” Power Systems Engineering Research Center, Tech. Rep., 2012.

[10] A. Phadke and J. Thorp, *Synchronized Phasor Measurements and their Applications*. Springer, 2008, ch. 9, pp. 197–221.

[11] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, “Towards modelling the impact of cyber attacks on a smart grid,” *International Journal of Security Network*, vol. 6, no. 1, pp. 2–13, 2011.

[12] P. M. Anderson and A. A. Foud, *Power System Control and Stability*. The Iowa State University Press, 1977.

[13] S. Ward, J. O’Brien, B. Beresh, G. Benmouyal, D. Holstein, J. Tengdin, K. Fodero, M. Simon, M. Carden, M. V. V. S. Yalla, T. Tibbals, V. Skendzic, S. Mix, R. Young, T. Sidhu, S. Klein, J. Weiss, A. Apostolov, D.-P. Bui, S. Sciacca, C. Preuss, S. Hodder, and G. Seifert, “Cyber security issues for protective relays,” in *IEEE Power and Energy Society General Meeting (PESGM)*, June 2007, pp. 1–8.