An Artificially Intelligent Physical Model-Checking Approach to Detect Switching-Related Attacks on Power Systems

Mohamad El Hariri, Samy Faddel, Osama Mohammed
Department of Electrical and Computer Engineering
Florida International University
Miami, Fl., USA
e-mail: mohammed@fiu.edu

***Abstract*—Decentralized and hierarchical microgrid control strategies have lain the groundwork for shaping the future smart grid. Such control approaches require the cooperation between microgrid operators in control centers, intelligent microcontrollers, and remote terminal units via secure and reliable communication networks. In order to enhance the security and complement the work of network intrusion detection systems, this paper presents an artificially intelligent physical model-checking that detects tampered-with circuit breaker switching control commands whether, due to a cyber-attack or human error. In this technique, distributed agents, which are monitoring sectionalized areas of a given microgrid, will be trained and continuously adapted to verify that incoming control commands do not violate the physical system operational standards and do not put the microgrid in an insecure state. The potential of this approach has been tested by deploying agents that monitor circuit breakers status commands on a 14-bus IEEE benchmark system. The results showed the accuracy of the proposed framework in characterizing the power system and successfully detecting malicious and/or erroneous control commands.**

Keywords-agent systems; cyber-physical security; decentralized control; intelligent systems; microgrid reliability

I. INTRODUCTION

Decentralized and hierarchical microgrid control requires judicious cooperation between several cyber and physical entities in which communication signals could be regarded as feedback signals from sensory devices or control commands to actuators, forming a closed loop.

The recent history has repeatedly shown the ability of attackers to exploit vulnerabilities in power system communication networks and maliciously tamper with exchanged signals, especially those targeting control fields[1], [2]. This class of attacks pose a serious threat to power systems as they can lead to catastrophic consequences, such as overloading of transmission lines and/or generators [1]. The study conducted in [3] showed that the sequential removal of substation or transmission lines by attackers can cause large blackouts. Similarly, authors in [4] studied and proposed several attack scenarios that could cause cascaded failures in power systems. Also, recent public disclosures have emphasized the disastrous consequences of control-related attacks on critical processes such as the Stuxnet malware, the Crash Override malware targeting the Ukraine power grid, and several other incidents present in the media. Aside from targeting critical infrastructure, the gravity of these attacks is emphasized by their ability to remain undetectable by conventional network Intrusion Detection Systems (IDSs). This is due to the fact that the modified control fields are re-encoded in the proper packet format before being transmitted [1], [5]. In light of that, several efforts have been placed to detect control-related attacks in the energy sector using cyber and physical rules. In [1], a semantic analyses framework which integrates network IDS with power flow analyses was proposed to detect malicious control commands. This technique targets only DNP3 packets and requires a complex mathematical representation of the power system, which increases in complexity as the system grows. The framework also requires adapting the power flow analyses leading to a tradeoff between accuracy and latency. The authors in [6] proposed an anomaly detection algorithm for detecting and mitigating attacks on automatic generation control. The control signal in [6] is processed only if it is regarded as legitimate by an anomaly detection engine, otherwise, a signal from a model-based automatic generation control is utilized. This work assumes that the feedback frequency and tie-line measurements are trusted and do not discuss their security requirements. In [7], a multi-agent system that utilizes cyber and physical rules was introduced to detectcyber-attacks and distinguish them from physical faults. Similarly, [8] introduced an algorithm to detect tripping cyber-attacks on protection systems using physical properties. Both [7] and [8] rely solely on static physical rules.

The work in this paper proposes an Artificially Intelligent Physical Model-Checking (AI-PMC) multi-agent microgrid security framework that detects malicious and/or erroneous circuit breaker switching control commands. Unlike the work presented in the literature, the proposed approach does not need online load flow analyses, instead it uses a coupled Artificially Intelligent - Expert System (AI-ES) to characterize the power system and benefits from their fast responses to produce accurate power flow solutions. Moreover, the ES has the ability to decide on whether an incoming control command contains malicious/bad content or not. The performance of the proposed framework was tested in simulation on a 14-bus IEEE benchmark system.

The rest of the paper is organized as follows: Section II describes the details of the proposed model-checking

approach. Section III presents and discusses the results. Section IV concludes the paper and proposes future work.

II. THE AI-PMC APPROACH

A. Physical System Description

The proposed AI-PMC framework was applied on the 14-bus IEEE benchmark system shown in Fig. 1. The minimum and maximum limits of voltage magnitude are considered to be 0.95 p.u. and 1.05 p.u., respectively. This follows the ANSI C84.1-2006 standard [9]. Details of all system parameters and ratings can be found in [10]. The system is divided into three areas such that each area has at least one synchronous machine and one load point, as shown in Fig. 1. An agent is assigned to each of the three areas. Each agent is responsible for the security and control actions within its area. The three agents have a communication link with the main system operator for the hierarchal control of the microgrid.

B. Cyber Threats and the AI-PMC Security Algorithm

Two of the most commonly used protocols for microgrid operation and control are the Distributed Network Protocol (DNP3) in case of Supervisory Control and Data Acquisition (SCADA) systems and IEC 61850 Manufacturing Message Service (MMS), Generic Object Oriented Substation Event (GOOSE), and Sampled Measured Values (SMV) messages in more recent systems [1], [11]. Each of these protocol suits has its own vulnerabilities that have been exploited to launch successful attacks on power grids. The work in [1] presents a successful data manipulation attack on a DNP3 packet which has 4 control relay objects to operate 4 circuit breakers in a substation. A Man-in-the-middle attack was also presented in [5] to generate malicious circuit breaker control commands as GOOSE messages. Again, these attacks were established as legitimate network packets with malicious content. It is important to mention here that such networks are required to operate in real-time. This imposes strict time delay requirements on the transfer of control commands especially when current microcontrollers and IEDs have low processing powers. This leaves such industrial control networks unencrypted. In fact, a study conducted in [12] shows that even the latest processors cannot meet the 4 ms time delay requirement set by IEC 61850 on GOOSE messages.

To complement the work of network IDSs, this paper proposes a multi-agent framework based on a physical model-checking approach to detect cyber-attacks targeting circuit breakers in a microgrid or a distribution system. The objective of this framework is to add an intelligent layer which assesses the consequences of incoming circuit breaker control commands on a model of the power system and decide whether these commands are malicious or not. The System Operating Limits Methodology for the Operations Horizon Standard (FAC-011-2) indicates that power systems operating limits should be designed such that single or multiple contingencies do not result in cascading outages [13]. In this work, the classical N-1 contingency criterion is adopted. The power system shown in Fig. 1 is divided into three areas and an agent is assigned to each area. When a control command is issued from the control center, each agent checks whether this command will actuate a breaker within its area. If this is the case, then this agent's security feature will be activated and the remaining agents will stay idle.

The security module in the agents consists of two layers. The first layer takes in the control command as input, solves the power flow problem, and produces the bus number with the minimum voltage, the value of that minimum voltage, and the maximum transmission line loading as outputs. Since topology changes due to circuit breaker activities in one area might affect other locations, each agent is trained to assess the consequences of the control commands within its area and their effect on the neighboring areas. The second layer, which consists of an expert fuzzy module, processes the results of the first layer and produces a decision on whether the newly arrived control command is malicious or not. The security module in the agents is described in the flowchart of Fig. 2 and explained below.

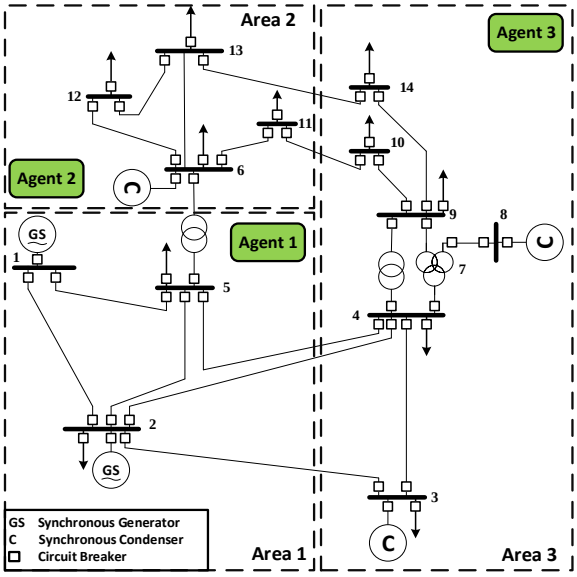


Figure 1. 14-bus IEEE benchmark system.

The power system characterization process occurs in the first layer utilizing the AI module. The power flow problem of the 14-bus IEEE benchmark system shown in Fig. 1 is solved offline using the Newton-Raphson method. PowerWorld software was used to calculate the power flow problem solutions for the different N-1 contingency cases. For the system under study, 36 contingency cases were populated along with 1 control case corresponding to the normal case. The generated database of power flow solutions was then used to train a feed-forward neural network. The input to the neural network is a binary coding corresponding to the contingency case number. For example, the code 000010 will be utilized to represent a control signal to actuate circuit breakers connecting bus 1 to bus 2. The output of the neural network is the load flow solution. This output will then be passed into an algorithm which will produce a 3-

element vector containing the minimum voltage in per unit, the bus number which has the minimum voltage, and the transmission line loading in percent. The minimum voltage is selected here since the voltage value will heavily reflect the system status. Maximum voltage was not considered as an input to the second layer because the severe over-voltage case will occur only if multiple loads were disconnected from the system and this will be detected and stopped by the proposed technique. This vector will then be passed into the expert fuzzy system for decision making.

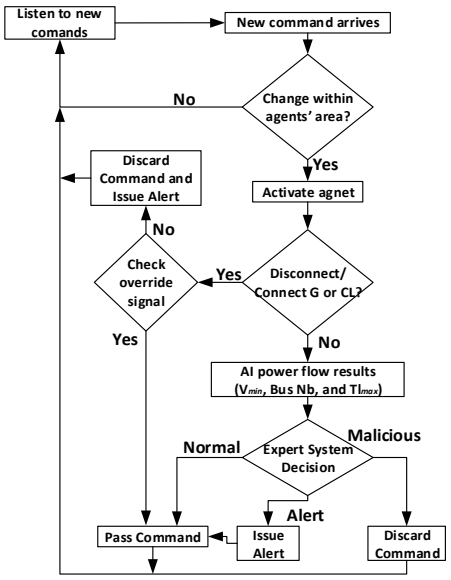


Figure 2. AI-PMC algorithm.

The first input to the expert fuzzy system is the minimum voltage obtained from the previous layer. This input voltage will have membership functions in the fuzzy controller. The membership functions are designed to reflect the system's behavior from the voltage point of view and according to the ANSI C84.1-2006 standard [9]. They are divided into four statuses: the two extreme cases are Very Low (VL) and Very High (VH) to represent a severe under or over voltage problem, respectively. The other two membership functions are High (H) and Low (L) to represent a normal operating condition or a mild under voltage problem that requires a corrective action (i.e reactive power support from the synchronous condenser or from the online tap changing transformer). The second input to the fuzzy system is the bus number. We assume that the system operator assigns different priority to each bus depending on the nature of the generation or the load connected to it. For example, buses that have main generator units or critical loads will have higher priorities while other buses that have small generation units or normal loads, that can be shed, will have a lower priority. In this paper, we assume that all buses with generation units are critical buses (buses 1, 2, 3, 6, and 8). We also assume that loads at buses 2, 3, 4, and 9 are critical loads. This priority will play a role in the decision-making process. The last input to the fuzzy system is the maximum transmission loading (TLL_{max}). It is divided according to the standard rating procedures in [12] to normal condition (N), allowable overloading (LTE), and unallowable overloading (STE).

The fuzzy output is defuzzified based on the Sugeno technique. The output of the controller is a crisp value corresponding to one of three cases: a normal condition status in which the decision is to pass the command, an alert to the system operator and passing the command, or a malicious status activity which discards the command. Table I summarizes ranges set for each membership function.

The fuzzy rules that dictate the controller decision are as follows:

1. If there is severe over-voltage (VH), sever under-voltage (VL) or severe overloading (STE), the fuzzy module will consider this command a malicious one since it is not expected that the system operator will perform a switching action that put the system in a critical condition or cause cascaded blackouts.

TABLE I. RANGES OF MEMBERSHIP FUNCTIONS

Variable	**Membership Function**			
V_{min} (p.u.)	**VL**	**L**	**H**	**VH**
	≤ 0.92	0.9 – 0.95	0.94-1.05	≥ 1.03
Bus Nb.	**Critical Bus**		**Non-critical Bus**	
	1, 2, 3, 4, 6, 8, and 9		5, 7, 10, 11, 12, 13, 14	
TLL_{max} (%)	**N**	**LTE**	**STE**	
	≤ 105	103-130	≥ 128	

2. If the voltage is low (L) on one of the main generator buses or on a critical load bus, the command will be considered as a malicious one since the voltage on these buses is expected to be maintained in a good condition.
3. If the voltage is low (L) on one of the other buses, that is not included in Rule 2, or the loading condition is LTE, the command will be considered as an alert and will be passed. However, an alert signal will be sent to the operator to double check if an action needs to be done.
4. Other cases, which do not put the power system in a contingency or disturbance state, will be considered as normal conditions and the command will be passed.

In some cases, the operator will need to temporary power off some transmission lines or other power equipment for maintenance or other critical reasons. In order to allow that, each agent will have an additional network interface through which it will be communicating with the operator over an isolated network. Through this isolated tunnel, the operator can send an encrypted override signal to bypass the operation of the agent and perform necessary changes.

III. RESULTS AND DISCUSSION

The performance of the developed neural network to model the power system under study was investigated in terms of the maximum mean squared error of its three output categories spanning all contingency cases. Fig. 3 (a) shows the maximum error in the active (P) and reactive (Q) power at the buses with generation units. The maximum error

produced by the neural network for this category was 2.6% corresponding to the reactive power of bus 1. Fig. 3 (b) shows maximum error of the voltages on each bus. The maximum error in bus voltages was 2.22×10^{-4} which was at bus 8. Since the voltages are dealt with in p.u., the small error range (of order 10^{-4}) indicates the good performance of the neural network. Finally, Fig. 3(c) shows the maximum error in the transmission line loading. It indicates that the maximum transmission line loading error was 0.614% at transmission line 19 connecting busses 12 and 13.

Next, the multi-agent system was simulated on Matlab in two scenarios. The first scenario is to perform a switching command while the initial status is the normal operation condition where all CBs are on. In the second scenario, the control commands were sent in a sequential manner one after the other

without getting back to the normal case. The results of both cases are presented in Table II. In the first case, i.e. comparing to the normal case after every new control command is received, it is noticed that every command to disconnect a generator or a critical load is automatically considered malicious without invoking the AI module. This is because the override signal from the operator was set to zero in these cases. Table II also shows that for every simulated case, the proper corresponding agent was activated. For example, in case 1, the control command is intended to actuate the circuit breakers on the transmission line connecting bus 1 to bus 2. In this case, the change is in Area 1 only. Thus, only Agent 1 was activated. On the other hand, in case 7, the control command is intended to actuate the circuit breakers on the transmission line connecting bus 4 to bus 5. This line connects Areas 1 and 3. Therefore, Agent 1 and Agent 3 were activated.

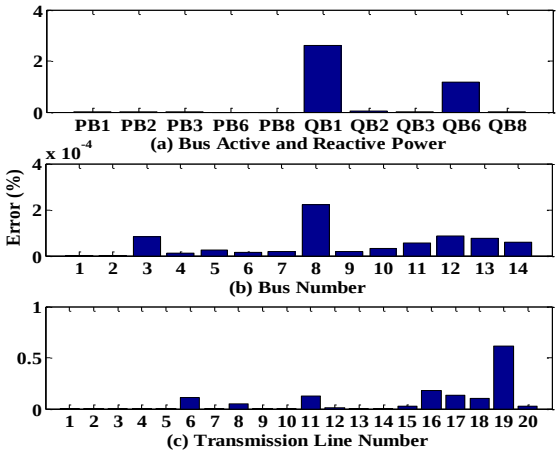


Figure 3. Goodness of fit of ai module in terms of mean squared error: (a) Generators active and reactive power; (b) Bus voltages; (c) Transmission line loading.

As mentioned earlier, the decision of the agents is based on the allowable operating limits of bus voltages, transmission line loading, and criticality of the affected buses. It can be noticed from the results in Table II that in all situations that passed the control commands but resulted in an alert to the system operator, the system did not violate its standard operational limits and the microgrid did not enter into an insecure operation state. Here, in the event of an alert situation, the final decision on overriding or reversing the current control actions is left to the system operator. It is noteworthy to highlight the cases where the agents regarded the disconnection of certain transmission lines or uncritical loads as normal. In cases 5, 6, 13, 16, and 17, the received control command resulted in the disconnection of transmission lines that connect buses within the same area.

In all the cases mentioned, the minimum voltage and the maximum transmission line loading did not violate the system standards. In fact, within the aforementioned cases, the minimum voltage recorded was 0.9989 p.u. and the maximum transmission line loading was 117%. It is also noticed that there was no generation overloading or power loss on any of the loads. Although these commands might be malicious or erroneous, they were passed by the multi-agent system since they did not put the microgrid in a contingency state and the microgrid's resiliency was maintained. Therefore, the multi-agent system was successful in satisfying its purpose by ensuring that only signals that do not violate the secure operational limits of the microgrids will be passed. In cases 32 and 33, non-critical loads were disconnected form the system. The changes in the minimum bus voltage and maximum transmission line loading from the normal case were negligible compared to other contingencies. Again, the multi-agent system passed these commands since they did not incur critical consequences on the system. Therefore, out of the 36 tested cases, the multi-agent system allowed the passage of a command that lead to disconnection of a non-critical load 2 times, equivalent to 5.56% of tested cases. To compensate for this, each agent generates and periodically sends a log report to the system operator over the isolated and encrypted network interface. By that, the system operator could get feedback on the state of the circuit breakers and can take corrective actions when deemed necessary.

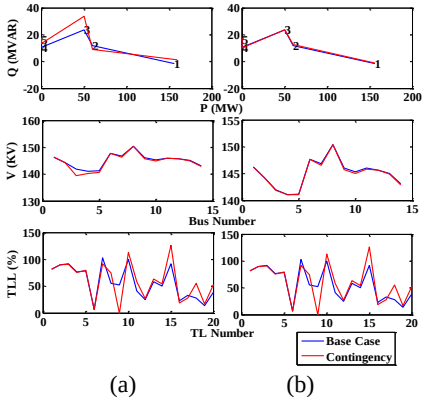
For the second scenario, the results showed similar responses to the previous cases. When not accompanied by an override signal from the isolated network interface, the commands which will result in the disconnection of a generator unit or a critical load are automatically regarded as malicious and are discarded. Also, cases 5, 6, 13, 16, 17, 32, and 33 had the same responses as previously discussed. The major difference in this case is the number of agents being activated. For instance, after executing case 4 in Table II, returning to the normal case, then executing case 5, only Agent 1 was activated and gave normal. However, when executing case 4 then directly executing case 5, Agent 1 and Agent 3 were activated and gave normal condition. This is because Agent 1 sensed a change in the status of the CB connecting bus 2 to bus 4 (from 0 back 1) and Agent 2 sensed a status change in the CB connecting bus 2 to bus 5 (from 1 to 0).

Fig. 4 shows a sample of the post processing done by the system operator based on the log reported by the agents. Fig. 4 (a) shows a comparison between the real and reactive power of generation units, bus voltages, and transmission

line loading of the base case and case 3, which is a malicious situation. Fig. 4 (b) shows the same for case 9, which is an alert situation. The reported data for case 3 shows that if the agent were to process that control command, the system would significantly deviate from its normal case. The graphs corresponding to the alert state shows that the processing of the control command would not result in a significant deviation from the normal case in terms of generators power and bus voltage. However, the transmission line loading would change but will not exceed the allowable limits. These graphs are useful visualization tools for system operators and designers that will assist in future plans and lessons learned.

TABLE II. PERFORMANCE EVALUATION OF MULTI-AGENT SYSTEM IN COMPARISON WITH NORMAL CASE AND DURING SEQUENTIAL CONTROL COMMAND EXECUTION

					Compare w. NC			Sequential								Compare w. NC			Sequential		
	Case	V_{min} (pu)	Bus Nb.	TLL_{max} (%)	A1	A2	A3	A1	A2	A3		Case	V_{min} (pu)	Bus Nb.	TLL_{max} (%)	A1	A2	A3	A1	A2	A3
	NC	1.0224	4	103	A	A	A	A	A	A		NC	1.0224	4	103	A	A	A	A	A	A
1	B1-B2	1.0152	5	252	M			M			19	12-13	1.0224	4	103		A			A	A
2	B1-B5	1.0106	5	134	M			M			20	13-14	1.0216	4	106		A	A		A	A
3	B2-B3	1.0099	3	156	M		M	M		M	21	GB1	---	---	---	M			M		
4	B2-B4	1.0127	4	180	M		M	M		M	22	G B2	---	---	---	M			M		
5	B2-B5	1.0146	5	113	N			N		N	23	G B3	---	---	---			M	M		M
6	B3-B4	1.0210	5	102			N	N		N	24	G B6	---	---	---		M			M	M
7	B4-B5	1.0207	4	131	M		M	M		M	25	G B8	---	---	---			M		M	M
8	B4-B7	1.0178	4	130			M	M		M	26	CL B9						M			M
9	B4-B9	1.0221	4	123			A			A	27	L B6	1.0240	4	103		A			M	M
10	B5-B6	0.9989	12	198	M	M		M	M	M	28	L B5	1.0240	4	102	A				M	
11	B6-11	1.0210	4	108		A		A	A		29	CL B4	---	---	---			M			M
12	B6-12	1.0221	4	103		A			A		30	CL B3	---	---	---			M			M
13	B6-13	0.9990	13	108		N			N		31	CL B2	---	---	---	M			M		M
14	B7-B8	0.0237	8	100		M	M		M	M	32	L B14	1.0259	4	98			N	M		
15	B7-B9	1.0206	14	129			A			A	33	L B13	1.0249	4	103		A			A	A
16	B9-10	1.0237	5	108			N			N	34	L B12	1.0232	4	102		N			A	
17	B9-14	0.9989	14	117			N			N	35	L B11	1.0232	4	102		A			A	
18	10-11	1.0220	4	107		A	A		A	A	36	L B10	1.0254	4	102			A		A	A



(a) (b)

Figure 4. (a) Comparison of real and reactive power, V, and TLL of malicious case to base case; (b) Comparison of real and reactive power, V, and TLL of alert case to base case.

IV. CONCLUSIONS AND FUTURE WORK

The work in this paper proposes an artificially intelligent physical model-checking approach to detect malicious and erroneous control commands controlling the state of circuit breakers in microgrids or distribution systems. The solution is presented as a multi-agent system, in which a given microgrid is sectionalized into separate areas and an agent is assigned to each area. The purpose of the work is to push enough intelli gence into the agents controlling the microgrid to enable them to assess the consequences of control commands before taking actions on the physical system. The proposed multi-agent control and security framework was tested on a 14-bus IEEE benchmark system. The results showed the accuracy of the AI module in characterizing the system under study and its effectiveness in not allowing the

system to go into an insecure state. As future work, the work presented will be extended to include a defense mechanism that will deal with the cases related to the disconnection of non-critical loads. A higher level agent will also be added to the proposed framework that will continuously adapt the neural network parameters to reflect changes in the system topology, such as the addition of the new buses or power equipment. Finally, since recent incidents have shown that attackers are simultaneously tampering with more than one system component, the training database will be expanded to include a large set of N-k contingency situations.

ACKNOWLEDGMENTS

The work in this paper is supported by grants from the United States Department of Energy (DoE).

REFERENCE

[1] [H. Lin, A. Slagell, Z. Kalbarczyk, P. Sauer, and R. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids," IEEE Trans. Smart Grid, vol. PP, no. 99, pp. 1–1, 2017.

[2] M. El Hariri, T. A. Youssef, H. Habib, and O. A. Mohammed, "Online False Data Detection and Lost Packet Forecasting System Using Time Series Neural Networks for IEC 61850 Sampled Measured Values," in IEEE PES Innovative Smart Grid Technologies North America, Wishington DC, USA, 2017.

[3] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience Analysis of Power Grids Under the Sequential Attack," IEEE Trans. Inf. Forensics Secur., vol. 9, no. 12, pp. 2340–2354, Dec. 2014.

[4] Y. Zhu, J. Yan, Y. (Sun, and H. He, "Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 12, pp. 3274–3284, Dec. 2014.

[5] M. El Hariri, T. A. Youssef, and O. A. Mohammed, "On the Implementation of the IEC 61850 Standard: Will Different Manufacturer Devices Behave Similarly under Identical Conditions?," Electronics, vol. 5, no. 4, p. 85, Dec. 2016.

[6] S. Sridhar and M. Govindarasu, "Model-Based Attack Detection and Mitigation for Automatic Generation Control," IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[7] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, "Multi-Agent Approach for Enhancing Security of Protection Schemes in Cyber-Physical Energy Systems," IEEE Trans. Ind. Inform., vol. 13, no. 2, pp. 436–447, Apr. 2017.

[8] M. S. Rahman, H. R. Pota, and M. J. Hossain, "Cyber vulnerabilities on agent-based smart grid protection system," in 2014 IEEE PES General Meeting | Conference Exposition, 2014, pp. 1–5.

[9] American National Standard for Electrical Power Systems and Equipment, "ANSI C84.1-2006, Voltage Ratings (60 Hertz)," 2006.

[10] Data Sheet for IEEE 14 Bus System. Available Online: http://shodhganga.inflibnet.ac.in/bitstream/10603/5247/18/19_appendix.pdf. Accessed on: 07/28/2017.

[11] A. Ruiz-Alvarez, A. Colet-Subirachs, F. A.-C. Figuerola, O. Gomis-Bellmunt, and A. Sudria-Andreu, "Operation of a Utility Connected Microgrid Using an IEC 61850-Based Multi-Level Management System," IEEE Trans. Smart Grid, vol. 3, no. 2, pp. 858–865, Jun. 2012.

[12] S. Fuloria and R. Anderson, "The Protection of Substation Communications," In the Proceedings of SCADA Security Symposium, Miami, FL, USA, 18-19 January 2010.

[13] Y. Jia, Z. Xu, L. L. Lai, and K. P. Wong, "Risk-Based Power System Security Analysis Considering Cascading Outages," IEEE Trans. Ind. Inform., vol. 12, no. 2, pp. 872–882, Apr. 2016.