An Advanced Optimization Based Simulation Model to Study the Impact of Cyber-Physical Attacks on Power Systems

Jiawei Zhu and Bhuvana Ramachandran
University of West Florida, Pensacola, FL 32514, USA
Email: zj4@students.uwf.edu, bramachandran@uwf.edu

***Abstract*—The promotion of energy internet causes external information to directly or indirectly affect power system control decisions through various business approaches. The interaction mechanism between power network and information network becomes increasingly complex. Modern power systems become more prone to cyber-attacks and physical attacks because of the high integration of information layer and physical layer. This paper provides an insight into the impacts of cyber and physical attacks on power systems, where the attacks are modeled in the form of mathematical (optimization) equations representing the attacks. Moreover, the cyber and physical attacks are modeled in the form of Mixed Integer Linear Programming (MILP) problem. The authors have simulated cyber-attack on transmission lines and cyber-physical attack on both transmission lines and loads. The MILP problem is solved by commercial solver, CPLEX. A case study on a modified IEEE 14 bus test system is considered to demonstrate the results of this research. Simulation results on the test system show that the cyber and physical attacks on power systems could cause undesirable load curtailment and mitigation of such attacks becomes essential for secure operation of the electric grid. This research would enable the power system operators to understand the potentially damaging effects of cyber-physical attack and advance their knowledge about such attacks so that prevention and mitigation of attacks on the power systems is possible.**

***Index Terms*—CPLEX, cyber-physical attack, load bus, MATLAB simulation, optimization model, security of power systems, transmission lines**

I. Introduction

Cyber Physical Systems (CPS) integrate computing system, communication network and physical environment through 3C (computation, communication and control) technology, forming a multi-dimensional and heterogeneous complex system integrating real-time perception, dynamic control and information services [1], [2]. In recent years, with the continuous development and deployment of smart grid technology, the extent to which a power system is automated has rapidly improved, and the number of power grid sensors, information network scale and decision making units has greatly increased [3]. In addition, the promotion of energy internet causes external information to directly or indirectly affect power system control decisions through various business approaches, and the interaction mechanism between power network and information network becomes increasingly complex [4]. Modern power system is no longer the traditional power equipment network, but has developed to have a variety of typical characteristics of CPS.

In the context of power systems, a CPS can obtain comprehensive and detailed information of the power grid in real time by means of a larger scale sensor measurement system and a more complex information and communication network [5]-[7]. Therefore, the power system based CPS depends more and more on the information system and network security plays an increasingly important role in the operation of the whole power system [6]. Attacks on power systems have strong concealment, long incubation period, small attack cost, and although it cannot directly damage electrical equipment at a time, the power system itself can be weakened. The attack can even completely destroy the normal function of the secondary system, achieve results that are similar to physical attacks, including weakening of system stability, economic operation, social stability and have more severe impact [2]. When the power grid is in normal operation, secondary equipment failure will cause measurement loss or error, which will affect the operator's accurate perception of the primary system of the power grid [8]. If the secondary systems in a communication network are attacked maliciously, like the relay protection device, Supervisory Control and Data Acquisition (SCADA), Energy Management System (EMS) or the Wide Area Measurement System (WAMS), the information will be dropped, delayed or tampered. As a result, it is likely that the control center will receive error instructions, or result in mal-operation of decision-making unit or withdrawal from synchronized operation of a power system, due to which system oscillation and large scope blackout accidents may occur [9]. The Ukraine blackout is a classic example of a secondary power system that suffered a network attack and triggered a system failure.

Malicious code attacked some substation monitoring systems, resulting in the failure of power generation equipment, triggering widespread blackouts in Ukraine.

Manuscript received July 16, 2020; revised November 22, 2020.

doi: 10.18178/ijeee.8.4.74-81

After this incident, governments of all countries began to pay attention to the impact of network attacks on their own power systems, and conduct self-examination of network security through simulated attacks [9]-[11].

NOMENCLATURE

$\boldsymbol{m}$	Measured values.
$\boldsymbol{T}$	Matrix of topology.
$\boldsymbol{x}$	State variables which will be estimated.
$\boldsymbol{e}$	The error during the process of the measurement.
$\boldsymbol{W}$	Diagonal matrix related to the system error.
$\boldsymbol{EVA(x)}$	Least square
$\boldsymbol{C}$	The criterion for identifying bad data.
$\boldsymbol{a}$	Injected false data.
$\boldsymbol{e_x}$	Deviation of the calculated state quantity.
$\boldsymbol{d}$	Load index.
$\boldsymbol{g}$	Generator index.
$\boldsymbol{l}$	Transmission line index.
$\boldsymbol{ND}$	Number of load buses.
$\boldsymbol{NG}$	Number of generators.
$\boldsymbol{NL}$	Number of lines.
$\boldsymbol{\varepsilon}$	Sufficiently small positive number.
M	Sufficiently big positive number.
$\boldsymbol{\tau}$	Given maximum percentage of change for load
$\boldsymbol{D_d}$	Load at bus $\boldsymbol{d}$.
$\Delta\boldsymbol{D_d}$	Injected false data into load measurement at bus
$\boldsymbol{PL_l}$	Flow of line $\boldsymbol{l}$.
$\boldsymbol{\delta_d}$	$\boldsymbol{\delta_d = 1}$ indicating $\boldsymbol{\Delta D_d \neq 0}$.
$\boldsymbol{\delta_{D,d}}$, $\boldsymbol{\delta_{D+,d}}$, $\boldsymbol{\delta_{D-,d}}$	Indicators. $\boldsymbol{\delta_{D,d} = 1}$ if the measurement of load $\boldsymbol{d}$ is attacked, i.e., $\boldsymbol{\Delta D_d \neq 0}$; $\boldsymbol{\delta_{D+,d} = 1}$ indicating $\boldsymbol{\Delta D_d > 0}$; $\boldsymbol{\delta_{D-,d} = 1}$ indicating $\boldsymbol{\Delta D_d < 0}$. $\boldsymbol{\delta_{D,d} = 0}$ if $\boldsymbol{\Delta D_d = 0}$.
$\boldsymbol{\delta_{PL}}$	$\boldsymbol{\delta_{PL} = 1}$ indicating $\boldsymbol{\Delta PL \neq 0}$.
$\boldsymbol{\delta_{PL,l}}$, $\boldsymbol{\delta_{PL+,l}}$, $\boldsymbol{\delta_{PL-,l}}$	Indicators. $\boldsymbol{\delta_{PL,l} = 1}$ if the measurement of line $\boldsymbol{l}$ is attacked, i.e., $\boldsymbol{\Delta PL_l \neq 0}$; $\boldsymbol{\delta_{PL+,l} = 1}$ indicating $\boldsymbol{\Delta PL_l > 0}$; $\boldsymbol{\delta_{PL-,l} = 1}$ indicating $\boldsymbol{\Delta PL_l < 0}$. $\boldsymbol{\delta_{PL,l} = 0}$ if $\boldsymbol{\Delta PL_l = 0}$.
$\boldsymbol{D}$	Bus load vector.
$\Delta\boldsymbol{D}$	False data injection vector into load
$\boldsymbol{PL}$	Line flow vector.
$\boldsymbol{PL_{max}}$	Line flow limit vector.
$\Delta\boldsymbol{PL}$	Incremental line flow vector.
$\boldsymbol{P_g}$	Generator power output vector.
$\boldsymbol{P_{max}}$	Generator maximum output power vector.
$\boldsymbol{P_{min}}$	Generator minimum output power vector.
$\boldsymbol{SF}$	Shift factor matrix of the power grid.
$\boldsymbol{KP}$	Bus-generator incidence matrix.
$\boldsymbol{KD}$	Bus-load incidence matrix.

Note that Δ represents an incremental change and symbols in bold represent vectors or matrices.

In this paper, a novel mathematical and simulation model is developed to mimic potential cyber and physical attacks targeted at power systems to study the impact of such attacks. The main contributions of this paper are two-fold.

1) A cyber and physical attack model of power systems is formulated as a Mixed Integer Linear Programming (MILP) problem.

2) The proposed attack model is built and simulated using a modified IEEE 14-bus system as a test system. A mathematical programming solver CPLEX is used to solve the optimization problem. Simulation results on the modified IEEE 14-bus system verify the accuracy and effectiveness of the proposed model.

The rest of this paper is organized as follows. Section II explains the academic literature review about research that has been carried out in the past. Section III reviews the principle of False Data Injection Attacks (FDIA). Section IV proposes an MILP problem to model the attacking strategy aimed at power systems. Section V and VI demonstrate simulation of the proposed model with a modified IEEE 14-bus system, and discusses the results. Section VII concludes this paper.

II. Literature Review—Cyber-Physical Attacks on Power Systems

Pasqualetti, *et al.* proposed a unified framework and novel detecting process to search for potential attacks [12], they focus on attack detection, but do not give solutions to overcome the attack. Chen, *et al.* introduced Petri nets to establish cyber-physical attacks on the smart grids [13], the communication protocol proposed can help to understand security vulnerabilities, but this reference doesn't build a mathematical model for the attack. Deng, *et al.* investigated two potential attacks, and analyzed how attackers can construct these two attacks [14]. Arghandeh, *et al.* proposed some new concepts of power system resilience and introduced a new way of thinking about power system operation [15]. Zhang and Sankar investigated the physical results of cyber-physical attacks [16], but attack detection is ignored in this paper.

Zonouz built a security-oriented cyber-physical state estimation system which can detect malicious data sets instantly [17], Zonousz does not solve how to minimize the serious effects of attack, since detection is just the first step of protection. Liu, *et al.* studied a way to establish a model for cyber-physical attacks and applied their models in the simulation of extensive system disturbances [18]. Xin built a cyber-physical equivalent model of Hierarchical Control Systems (HCS), and formulated the general information flow in an HCS by mathematical equations [19]. Vellaithural, *et al.* proposed an index that is able to measure the security level of the power systems [20]. This cyber-physical index called CPINDEX is calculated from a security-oriented stochastic risk management [20], it can indicate the malicious attack quickly and efficiently, but lack of solutions.

He and Yan conducted a survey to provide a comprehensive and systematic review of cyber-physical

attacks on the smart grid [21]. Sridhar, *et al.* highlighted the importance of cyber security in power systems, then introduced a method to evaluate the risks based on two parts: cyber layer and physical layer [22]. Xiang, *et al.* studied two possible attack scenarios. One is the coordination between load redistribution attack and attacking generators, the other is coordination between attacking transmission lines and loads [23]. Li, *et al.* built a bilevel model to determine the severest damage and undetectable physical attacks. The authors turned the model to a MILP problem, and used a two-stage solution method to solve the MILP problem [24].

Pasqualetti, *et al.* investigated a mathematical model for cyber-physical systems, attacks and monitors. In addition, the authors also designed centralized and distributed attack detection and identification monitors [25]. Davis, *et al.* built an online model for evaluating the operational reliability influence due to cyber-attacks [26]. Poudel and Malla presented the development of a real-time cyber-physical system testbed for cyber security and stability control [27]. Adhikari, *et al.* developed a WAMS cyber-physical test bed using a real time digital simulator with hardware-in-the-loop simulation [28]. Liang, *et al.* summarized the theoretical basis of FDIAs, and then discussed serious impacts of FDIA. Then the authors presented some defense strategies against FDIAs and potential future research directions in this field [29]. Chen, *et al.* proposed a real time cyber-physical framework or test bed [13]. Cardenas, *et al.* studied key challenges for securing cyber-physical systems [30].

Several of the references above proposed how to detect malicious attack, some researchers coming up with how to build a model of cyber-physical attack. However, they all have some disadvantages. In [12], [20] and [31], the authors mainly focused on detection, but did not work on how to solve the serious effects of attack. In [32], the authors did not investigate attack detection. At this juncture where cyber and physical attacks are on the rise and may have the potential to cause cyber-physical mayhem, a more systematic research about the impacts of cyber-physical attack and ways to prevent the attack from damaging/interfering with the operation of the power grid is the need of the hour.

In this paper, the principle of cyber-attack is investigated and a mathematical optimization model is developed for cyber and physical attack on power systems. The optimization model is formulated as a MILP problem. The proposed attack model is solved using MATLAB CPLEX. The simulation results provide the power systems operators with suggestions about how to minimize the results of attacks which then can be translated into control/corrective actions that have practical meanings.

III. Principle of False Data Injection Attacks

Control centers of power grids collects, monitors and controls the operation status of the entire power system through the SCADA system. The SCADA system transmits the collected data to advanced monitoring centers, including analysis of topology, state estimation, bad data identification, correction, and anticipated accident analysis, etc. The results can be used as references for scheduling decisions by operators.

With the deepening of the integration of information layer and physical layer, researchers pay more attention to the vulnerability of SCADA systems. Attacks on SCADA systems, known as SCADA hacking, is often the starting point of cyber-attacks. There are many types of network attack methods that can be used to attack SCADA system [33]-[35]. Here the authors focus on False Data Injection Attack (FDIA) on power systems. Attackers usually inject false data into vector devices. This behavior will cause a difference between quantities that are monitored through state estimation and the measured value of the quantity. If the false measurements are not detected by bad data detection, there will be severe consequences on normal operation and control of power grids. There are two hypotheses in the existing literature on FDIA:

1) Subject who carries out the attack has a certain knowledge of the power system, that is, to a certain extent, attacker understands the configuration information, topology structure, how to estimate the state and detect bad data.

2) Subject who carries out the attack has the ability to tamper with the measured values of all or part of the measuring devices. The model of state estimation could be briefly described as

$$\boldsymbol{m} = \boldsymbol{T}\boldsymbol{x} + \boldsymbol{e} \tag{1}$$

The evaluation of the state estimation results can be obtained by using the least square method

$$EVA(\boldsymbol{x}) = (\boldsymbol{m} - \boldsymbol{T}\boldsymbol{x})^T \boldsymbol{W} (\boldsymbol{m} - \boldsymbol{T}\boldsymbol{x}) \tag{2}$$

Its analytic solution is

$$\boldsymbol{x} = (\boldsymbol{T}^T \boldsymbol{W} \boldsymbol{T})^{-1} \boldsymbol{T}^T \boldsymbol{W} \boldsymbol{m} \tag{3}$$

Since state estimation is based on redundant measurements and there may be bad data in the measurements, if the operators want to make sure that measurement results are reliable, they need to detect and analyze the bad data. The criterion for identifying bad data is

$$EVA(\boldsymbol{x}) < C \tag{4}$$

Otherwise, the corresponding bad data will be removed and the state estimation will be redone until the bad data is detected. FDIA takes advantage of this principle. False data can be injected into the original measured value m, resulting in deviation of the input data

$$\boldsymbol{m_a} = \boldsymbol{m} + \boldsymbol{a} \tag{5}$$

Deviation of the calculated state quantity $\boldsymbol{x}$, i.e.

$$\boldsymbol{x_{bad}} = \boldsymbol{x} + \boldsymbol{e_x} \tag{6}$$

$\boldsymbol{e_x}$ represents difference in state variable before and after injecting false data (also known as "attack"). If the injected set of malicious data satisfies

$$\boldsymbol{a} = \boldsymbol{T}\boldsymbol{e_x} \tag{7}$$

It is not difficult to find that its target function

$$EVA(\boldsymbol{x_{bad}}) = EVA(\boldsymbol{x}) \quad (8)$$

In other words, although the original measurement data was tampered with, bad data was added maliciously, and the result of state estimation was offset, the target function value of bad data detection remained unchanged, so the operators cannot find bad data.

To overcome the disadvantages of the general false data injection attacking model, Yuan, *et al.* [36] proposed a load redistribution attack model which set some practical constraints on the general attack model.

1) The output reading of a generator cannot be altered.

2) The readings of the measurement at a load bus can only be attacked within certain ranges.

The mathematical model considering those constraints can be formulated as

$$\boldsymbol{1^T \Delta D = 0} \quad (9)$$

$$-\tau D_d \le \Delta D_d \le \tau D_d \quad (10)$$

$$\boldsymbol{\Delta PL = -SF \cdot KD \cdot \Delta D} \quad (11)$$

Constraint (9) ensures that the summation of changing load is equal to zero since the attacker wishes and plans the attack in such a way that it remains undetectable by the operator. Note that the changing load could be positive or negative. Constraint (10) indicates that the amount of attack on loads (change in loads) is limited within a certain range. Constraint (11) constructs the corresponding attacking vector of line measurements.

IV. Formulation of an Optimization Model to Depict Cyber and Physical Attacks on Power Systems

An attacker can inject false data into the measurements at load buses or damage transmission lines to change the meter readings (measurements) and induce the operator to perform a false Security Constrained Economic Dispatch (SCED) that leads to the insecurity of power systems. In this research, the mathematical model is developed from the defenders' perspective and involves solving an optimization problem which is formulated as a multi-objective MILP problem.

$$\min \sum_{d=1}^{ND} \Delta D_d + 2 \sum_{l=1}^{NL} \Delta PL_l \quad (12)$$

$$\text{subject to } \Delta D_d \neq 0 \leftrightarrow \delta_d = 1 \quad (13)$$

$$\Delta PL \neq 0 \leftrightarrow \delta_{PL} = 1 \quad (14)$$

Constraints (13) and (14) can be modeled as follows [36]:

$$\begin{cases} \Delta D_d + \tau D_d \delta_{D,d} \ge 0 \\ \Delta D_d - \tau D_d \delta_{D,d} \le 0 \\ \delta_{D+,d} + \delta_{D-,d} - 2\delta_{D,d} \le 0 \\ \Delta D_d + (-\tau D_d - \varepsilon)\delta_{D+,d} \ge -\tau D_d \\ \Delta D_d + (\tau D_d + \varepsilon)\delta_{D-,d} \le \tau D_d \\ \delta_{D+,d} + \delta_{D-,d} + \delta_{D,d} \le 2 \\ \delta_{D+,d} + \delta_{D-,d} - \delta_{D,d} \ge 0 \\ \delta_{D+,d}, \delta_{D-,d}, \delta_{D,d} \in \{0,1\} \end{cases} \quad (13\text{-a})$$

$$\begin{cases} \Delta PL_l + M\delta_{PL,l} \ge 0 \\ \Delta PL_l - M\delta_{PL,l} \le 0 \\ \delta_{PL+,l} + \delta_{PL-,l} - 2\delta_{PL,l} \le 0 \\ \Delta PL_l + (-M - \varepsilon)\delta_{PL+,l} \ge -M \\ \Delta PL_l + (M + \varepsilon)\delta_{PL-,l} \le M \\ \delta_{PL+,l} + \delta_{PL-,l} + \delta_{PL,l} \le 2 \\ \delta_{PL+,l} + \delta_{PL-,l} - \delta_{PL,l} \ge 0 \\ \delta_{PL+,l}, \delta_{PL-,l}, \delta_{PL,l} \in \{0,1\} \end{cases} \quad (14\text{-a})$$

$$\boldsymbol{-\tau D \le \Delta D \le \tau D} \quad (15)$$

$$\boldsymbol{1^T \Delta D = 0} \quad (16)$$

$$\boldsymbol{\Delta PL = -SF \cdot KD \cdot \Delta D} \quad (17)$$

$$\boldsymbol{1^T P_g = 1^T (D + \Delta D)} \quad (18)$$

$$\boldsymbol{PL = SF \cdot KP \cdot P_g - SF \cdot KD \cdot (D + \Delta D)} \quad (19)$$

$$\boldsymbol{P_{min} \le P_g \le P_{max}} \quad (20)$$

$$\boldsymbol{-PL_{max} \le PL \le PL_{max}} \quad (21)$$

Equation (12) is the objective function. It includes 2 parts, one is total change of loads, and another is total change in power flow through the transmission lines. From the perspective of power system operators (defenders of power systems), the total change to load demands and line flows must be minimized. Constraints (13) and (14) model the logical relationships between the attack vector and the resource it uses for each attackable device. Constraints (13) and (14) can be modeled in mixed integer linear forms viz., (13-a) and (14-a) by introducing binary variables. Constraints (15) and (16) indicate that the attacking amount is limited within a certain range and summed to zero, so that it is hard for power systems operators to detect the attack. Constraint (17) and (19) constructs the false data for the measurements on transmission lines. Constraint (18) matches the power generation output with the loads ensuring that sum of power generation equals power demand. Constraints (20) and (21) indicate the limits of generator power output and transmission line flow.

V. Case Study and Results

In this section, the proposed mathematical optimization model is tested using the IEEE 14-bus system [37]. The load, generator, and the line data of the system are given in Appendix: Appendix A, Appendix B, Appendix C respectively. The configuration of IEEE 14-bus system is shown in Fig. 1. For the purpose of illustration, all the loads are set to 50% of the levels in the base case. It is assumed that the attacker has the full topology, line parameters, and bus load information of the test system. It is also assumed that an attacker can attack all the loads and line flow measurements in the system. Without loss of generality, the maximum allowable attacking amount at a bus is set to 50% of its load [38].

A. Scenario 1

In this scenario, it is assumed that the attacker only attacks the transmission lines, and does not attack the loads. This scenario is called a physical attack. From the

defenders' perspective, the goal is to minimize the change in power flow through transmission lines and to prevent major changes in power system operation. The objective function will be

$$\min 2\sum_{l=1}^{NL} \Delta PL_l \quad (22)$$

The results from simulating power flow on the IEEE 14-bus system is provided below in Table I.

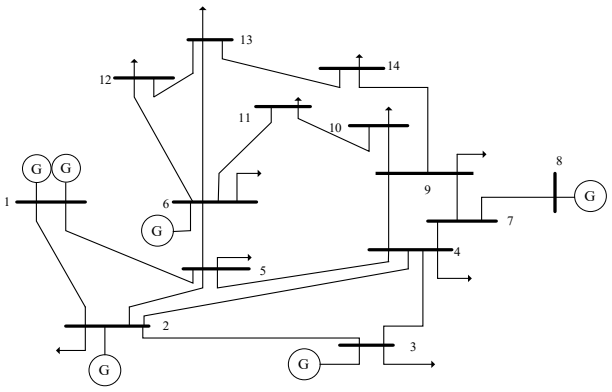

Figure 1. Configuration of IEEE 14-bus system.

TABLE I. RESULTS OF SCENARIO 1

Index	Change of Line Flow (MW)	Line Flow (MW)	Limit (MW)
1	-3.1810	10	10
2	3.1810	10.4417	25
3	-7.8117	1.0978	7
4	4.8928	14.6292	15
5	5.1629	9.9910	10
6	14.0862	13.8111	60
7	0.8316	-20.0000	20
8	3.9379	8.0000	25
9	2.2595	4.5903	25
10	7.2755	-5.2674	35
11	-0.3781	12.6592	30
12	1.5993	6.8236	15
13	3.2544	16.8498	30
14	0	7.7984×10^{-15}	25
15	3.9379	8.0000	8
16	3.5031	-3.2842	25
17	3.7714	2.2015	30
18	1.2531	-10.0342	20
19	0.0743	2.2486	10
20	-0.0464	8.9735	20

B. Scenario 2

In this scenario, the attacker is allowed to attack the loads (cyber) and inflict damage to the transmission lines (physical). This kind of attack is called cyber-physical attack. The objective function will become

$$\min\sum_{\mathrm{d}=1}^{ND} \Delta \mathrm{D}_d + 2\sum_{l=1}^{NL} \Delta PL_l \quad (23)$$

The result of attacking loads and transmission lines (changing power flow) are given in Table II and Table III.

TABLE II. RESULT OF SCENARIO 2 (LOAD ATTACK)

Index	Bus	Change of Load (MW)	Original Load (MW)
1	2	-5.4250	10.85
2	3	-21.8979	47.1
3	4	11.9500	23.9
4	5	1.9000	3.8
5	6	2.8000	5.6
6	9	-1.0771	14.75
7	10	2.2500	4.5
8	11	0.8750	1.75
9	12	1.5250	3.05
10	13	3.3750	6.75
11	14	3.7250	7.45

TABLE III. RESULT OF SCENARIO 2 (LINE ATTACK)

Index	Change of Line Flow (MW)	Line Flow (MW)	Limit (MW)
1	-3.1810	10	10
2	3.1810	10.4417	25
3	-7.8117	1.0978	7
4	4.8928	14.6292	15
5	5.1629	9.9910	10
6	14.0862	13.8111	60
7	0.8316	-20.0000	20
8	3.9379	8.0000	25
9	2.2595	4.5903	25
10	7.2755	-5.2674	35
11	-0.3781	12.6592	30
12	1.5993	6.8236	15
13	3.2544	16.8498	30
14	0	7.7984×10^{-15}	25
15	3.9379	8.0000	8
16	3.5031	-3.2842	25
17	3.7714	2.2015	30
18	1.2531	-10.0342	20
19	0.0743	2.2486	10
20	-0.0464	8.9735	20

VI. DISCUSSION

A. Scenario 1

In this scenario, the attacker will attempt to change the power flow through transmission lines, by physically attacking the transmission lines to inflict maximum damage to the power systems. The mathematical optimization model developed is used to minimize the impact of such attacks on the power system. When the attacker attacks the transmission lines, he poses a physical threat to the electric grid. However, if the power system operators can rearrange the power flow in such a way that the power flow through the transmission lines does not violate their respective limits, then the defender/operator can still maintain the security of the power system. Following this strategy, the optimization model was implemented using MATLAB CPLEX optimization model and the results are shown in Table I.

The results show that by following the proposed approach and by adjusting the power through line based on the schedule shown, the damage to the power system will be minimized.

The first column of Table I is the index of transmission lines. In the IEEE 14-bus system, there are 20 lines in total. The second column gives the change of line flow, which refers to ΔPL_l. The third column gives the line flow, which refers to PL_l. The last column gives the limit of line flow.

From Table I, almost all the line flow has changed, except for line 14. But for line 14, the original line flow is close to 0. According to the result, when an attacker is waging a physical attack on the transmission lines connected in the power system, from the perspective of defenders (power system operators), if they reduce the power flow in line 1 by 3.1810 MW, increase the power flow in line 2 by 3.1810 MW, decrease the power flow in line 3 by 7.8117 MW, and so on, they will cause least serious damage to the power systems. In other words, if the power system operators can change the line flow according to Table I, they can protect the power system against a physical attack by the attacker.

In addition, the total change in line flow and total line flow are 70.4381 MW and 168.9031 MW respectively, it means the total change in line flow has reached about 41.7032% of total line flow.

B. Scenario 2

In this scenario, the attackers are modeled to attack the loads and transmission line power flow simultaneously to damage the power systems. However, if the power system operators can configure the loads and power flows based on the results in Table II and Table III, the damage to the power systems will be minimized.

From Table II and Table III, it is observed that all the loads and line flow have changed. According to the results, when the attacker is targeting both the loads and transmission lines, from the perspective of defender, if they reduce the load at bus 2 by 5.4250 MW, decrease the load at bus 3 by 21.8979 MW, increase the load at bus 4 by 11.9500 MW, and so on, as for the line flow, if they reduce the power flow in line 1 by 3.1810 MW, increase the flow in line 2 by 3.1810 MW, decrease the flow of line 3 in 7.8117 MW, and so on, they will cause least damage to the power systems. It also means if the power system operators can change the loads and line flow based on results shown in Table II and Table III, they can protect the power systems well and defend against any cyber + physical attack on the power systems. In addition, as for the loads, the total change of loads and total original loads are 56.8 MW and 129.5 MW respectively. This means that this change has reached about 43.861% of total loads. As for the line flow, the total change of line flow and total line flow are 70.4381 MW and 168.9031 MW respectively. This means the change has arrived about 41.7032% of total power flow.

VII. Conclusion

The more complicated international environment and rising terrorist attacks raise a great concern about the security issue of power systems, including physical and cyber security. In this paper, cyber and physical attacks are formulated as a MILP problem. The MILP problem is solved by commercial solver, CPLEX. There are two scenarios in this paper, one being physical attack, and the other a cyber + physical attack. The simulation results on the modified IEEE 14-bus system verifies the efficacy, accuracy and feasibility of the proposed model.

In this paper, the primary focus was on the perspective of power system defenders and attempting to minimize the changes in load and power flow. However, the prospective of attackers must also be considered since their way of thinking about attacks and their objectives are not known. Then, the model formulation will change to a multi-level problem. In the next stage of research, the authors propose to include both the defender and attacker version of the attack model to study how each of their perspectives can coordinate/collaborate/counter with/against each other. This research will provide a comprehensive knowledge base about which attacks are the most severe and how to defend against those attacks and protect the power system better.

Appendix

Appendix A. Load Data of IEEE 14-Bus System

Index	Bus	Load (MW)
1	2	10.85
2	3	47.1
3	4	23.9
4	5	3.8
5	6	5.6
6	9	14.75
7	10	4.5
8	11	1.75
9	12	3.05
10	13	6.75
11	14	7.45

Appendix B. Generator Data of IEEE 14-Bus System

Index	Bus	P_{min} (MW)	P_{max} (MW)	Incremental Cost ($/MWh)
1	1	0	50	20
2	2	0	50	40
3	3	0	50	20
4	6	0	50	20
5	8	0	50	40
6	13	0	100	20

APPENDIX C. LINE DATA OF IEEE 14-BUS SYSTEM

Index	From Bus	To Bus	Reactance (p.u.)	Limit (MW)
1	1	2	0.05917	10
2	1	5	0.22034	25
3	2	3	0.19797	7
4	2	4	0.17632	15
5	2	5	0.17388	10
6	3	4	0.17103	60
7	4	5	0.04211	20
8	4	7	0.20912	25
9	4	9	0.55618	25
10	5	6	0.25202	35
11	6	11	0.1989	30
12	6	12	0.25581	15
13	6	13	0.13027	30
14	7	8	0.17615	25
15	7	9	0.11001	8
16	9	10	0.0845	25
17	9	14	0.27038	30
18	10	11	0.19207	20
19	12	13	0.19988	10
20	13	14	0.34802	20

CONFLICT OF INTEREST

The authors declare no conflict of interest

ACKNOWLEDGMENT

The authors thank the Department of Electrical and Computer Engineering, Hal Marcus College of Science and Engineering, University of West Florida, Pensacola, USA for supporting this research.

REFERENCES

[1] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-State operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12-19, 2010.

[2] N. Liu, X. Yu, and J. Zhang, "Coordinated cyber-attack: Inference and thinking of incident on Ukrainian power grid," *Automation of Electric Power Systems*, vol. 40, no. 6, pp. 144-147, 2016.

[3] Q. Guo, S. Xin, H. Sun, and J. H. Wang, "Power system cyber-physical modelling and security assessment: Motivation and ideas," *Proceedings of the CSEE*, vol. 36, no. 6, pp. 1481-1489, 2016.

[4] P. Yang, H. Cai, and H. B. Qiu, "Research on key technologies of big data for energy interconnection," *Electric Power Information and Communication Technology*, vol. 14, no. 4, pp. 9-12, 2016.

[5] W. Dexzng, "Study of CPS standards in East China power grid," *Automation of Electric Power Systems*, no. 8, 2000.

[6] Y. Tang, Q. Chen, M. Li, Q. Wang, M. Ni, and Y. Liang, "Overview on cyber-attacks against cyber physical power system," *Automation of Electric Power Systems*, no. 40, no. 17, pp. 59-69, 2016.

[7] X. Xingwei, L. Wei, and W. Jiahong, "Analysis of CPS performance of applying the AGC control model based on a standard in northeast power system," *Automation of Electric Power Systems*, no. 21, 2003.

[8] C. Guo, H. Lu, B. Yu, and T. Ma, "A survey of research on security risk assessment of secondary system," *Power System Technology*, vol. 37, no. 1, pp. 112-118, 2013.

[9] Q. Guo, S. Xin, J. Wang, and H. B. Sun, "Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine's blackout," *Automation of Electric Power Systems*, vol. 40, no. 5, pp. 145-147, 2016.

[10] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2016.

[11] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30-35, 2017.

[12] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715-2729, 2013.

[13] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed," in *Proc. IEEE International Workshop Technical Committee on Communications Quality and Reliability*, 2015, pp. 1-6.

[14] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420-2430, 2017.

[15] R. Arghandeh, A. V. Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060-1069, 2016.

[16] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, 2016.

[17] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-Oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790-1799, 2012.

[18] S. Liu, X. Feng, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "Switched system models for coordinated cyber-physical attack construction and simulation," in *Proc. the IEEE First International Workshop on Smart Grid Modeling and Simulation*, 2011, pp. 49-54.

[19] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-Physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2375-2385, 2015.

[20] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-Physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566-575, 2014.

[21] H. He and J. Yan, "Cyber-Physical attacks and defences in the smart grid: A survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13-27, 2016.

[22] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–Physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210-224, 2011.

[23] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156-168, 2017.

[24] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260-2272, 2015.

[25] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proc. 50th IEEE Conference on Decision and Control and European Control Conference*, 2011, pp. 2195-2201.

[26] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2464-2475, 2015.

[27] S. Poudel, Z. Ni, and N. Malla, "Real-Time cyber physical system testbed for power system security and control," *International Journal of Electrical Power & Energy Systems*, vol. 90, pp. 124-133, 2017.

[28] U. Adhikari, T. Morris, and S. Pan, "WAMS cyber-physical test bed for power system, cybersecurity study, and data mining," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2744-2753, 2016.
[29] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, 2016.
[30] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Proc. the Workshop on Future Directions in Cyber-Physical Systems Security*, 2009, pp. 1-4.
[31] S. Zonouz, K. M. Rogers, R. Berthier, R. B. Bobba, W. H. Sanders, and T. J. Overbye, "SCPSE: Security-Oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790-1799, 2012.
[32] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, 2016.
[33] J. Figueiredo and J. S. D. Costa, "A SCADA system for energy management in intelligent buildings," *Energy and Buildings*, vol. 49, pp. 85-98, 2012.
[34] Y. Zhang, L. Wang, Y. Xiang, and C. T. Ten, "Power system reliability evaluation with SCADA cybersecurity considerations," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1707-1721, 2015.
[35] N. Cai, J. Wang, and X. Yu, "SCADA system security: Complexity, history and new developments," in *Proc. the 6th IEEE International Conference on Industrial Informatics*, 2008, pp. 569-574.
[36] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382-390, 2011.
[37] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-State operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12-19, 2010.
[38] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720-729, 2015.

Jiawei Zhu was born in 1995 in China. He completed his Bachelor's Degree in Electrical Engineering in China and came to University of West Florida in 2019. He is currently a graduate student at the University of West Florida. His research interests are in the areas of electric power generation and control, cyber security of power systems, energy management of smart buildings.

Bhuvana Ramachandran is an Associate Professor in the Department of Electrical and Computer Engineering at the University of West Florida. She was born in India and came to the US to pursue her Post Doctoral Studies at Florida State University in 2009. She joined UWF in 2012 and has been teaching and researching in the area of Power Systems Operation and Control. Specifically her areas of interest include integration of renewable energy sources into the grid, Computational analysis for power system operation and control, Phasor Measurement Based Analysis, Real Time Cyber-Power System Modeling and Simulation and Smart Grid and Micro Grid.