MODELLING THE DYNAMIC ELECTRICAL SYSTEM IN THE CONTEXT OF CYBER ATTACKS

Delia Ioana DOGARU[1], Ioan DUMITRACHE[2]

Smart grid is a cyber-physical system described by the integration of information and communication technologies into the power system which is a key enabler for future technology developments through which the power grid can expand technically and geographically, creating a complex interconnected distributed system with additional cyber risks. In this article, we focus on the impact of cyber risks through this integration by modelling the dynamic power grid based on the IEEE-9bus benchmark and we conduct a behavior analysis when the grid is subjected to cyber-attacks.

Keywords: power grid; mathematical model; cyber-attacks; ICT; CPS; CPES

1. Introduction

The integration between the power grid and information and communication technologies (ICT) introduces a new flow of communication allowing data to be transmitted in real time to better monitor the grid's status over a wide area, diagnose errors, optimize control, improve energy efficiency, reduce power consumption, etc., leading to the emerging concept of cyber physical systems (CPS) in the context of power systems. Moreover, we can use the new paradigm of cyber-physical energy system (CPES) [15, 17], which better defines the relation between the cyber and the energy system components.

CPS is a collection of distributed cyber systems that monitors and controls, based on established rules, the interconnected physical systems in feedback loops [1]. CPS plays an important role in the Smart Grid which is an emerging technology in the power domain that uses information and bidirectional communication technologies for collecting data and using it in the control centers and utilities. This determines a better situational awareness of the grid's state helping to transmit and distribute electricity efficiently and guaranteeing power quality from suppliers to consumers [2].

[1] Faculty of Automatic Control and Computer Science, University POLITEHNICA Bucharest, Romania, e-mail: di.dogaru@gmail.com
[2] Faculty of Automatic Control and Computer Science, University POLITEHNICA Bucharest, Romania, e-mail: ioan.dumitrache@acse.pub.ro

It is paramount to stress the fact that the new power grid must be considered from two separate points of view, one physical or technical and the other one cybernetical or functional having control loops and informational loops interconnected through a communication network to enable possibilities to elevate the power grid to a new operational level. Cyber-attacks known in the ICT and introduced in the power grid cyber network can cause serious damage to it because they are capable of mimicking disturbances which in a normal execution occur randomly.

This article is concerned with the aspects of modelling the dynamic interconnected electrical system and behavior analysis when the grid is subjected to cyber-attacks modelled as disturbances/faults.

The most important aspect of a power grid is its ability to provide reliable and high standard continuous service to the consumers without interruptions. In order for the consumer's equipment to operate within satisfactory parameters it must be fed, within acceptable tolerance, with constant frequency and voltage, thus, the quality of power provided must be kept in check. To manage a reliable service of operation the grid requires to have its synchronous generators to run in parallel with a certain capacity for meeting the demand. If at some point, due to abnormal operation conditions (disturbance), the generators lose synchronism current and voltage fluctuations occur determining the circuit breakers at the end of the transmission line to trip and shift the power flow to a neighboring circuit.

The second aspect is to keep integrity of the power grid. This means that the infrastructure of the power grid must be protected against abnormal system conditions or faults that may disrupt the voltage and current anywhere along the flow from the generating stations through the high-voltage transmission lines to the loads [16].

A third aspect we consider is the degree to which the power grid can withstand an unexpected perturbation without damaging the overall performance, or robustness. It is possible to state that when random changes occur on the grid, like faults, equipment failure or power sources disconnecting from the grid, it will be capable of maintaining the balance of demand-supply energy despite these disturbances. But, the transition to an acceptable state of equilibrium after subjected to the events of disturbance is best to be studied as a stability issue of the power system. The robustness of a power grid is not sufficient to make it resilient, but it is necessary nonetheless.

A fourth aspect which we bring forth is the resilience of the power system that measures how fast the system is able to recover quickly after an unexpected event in contrast to robustness which measures how much damage the system took [3].

In Section 1, we discuss the power system nonlinear dynamics and underline the interdependencies of its physical components which in case of a

cyber disruption can have cascading effects. The paper also presents the relation between system parameters like rotor angle, power generation, voltage, etc. and how the alteration of one can lead to certain effects of another.

The power system is a high-order multivariable process described by various interacting control loops between physical and cyber components of nonlinear nature due to its dynamic behavior operating on multiple time scales considered in Section 2. We described this system with a mathematical representation from a stability perspective using the benchmark model [4, 6] of the synchronous machine connected to an infinite bus and extending it to the multimachine system connected to an infinite bus from which we obtain the desired linearized network equation between the currents in a 3-generator model network. The equation obtained is used in Section 3, where we analyze the case scenario of the IEEE 9 bus to present the continuous-time state-space model of the system in the nine-linear first order differential algebraic equations form.

Upon this linearized time-invariant representation of the network we model cyber-attacks in Section 4 targeting two important properties of the power system: controllability and stability to better understand their impact.

In the final section, we simulate some scenarios of cyber-attacks on the power system using the model from Section 4 and analyze the system response.

2. Dynamics of the power system

The power system is a nonlinear system that integrates multiple elements which influence its dynamic performance. Every characteristic of each element impacts the overall system stability and that is why it is important to have a good grasp of what are the points of focus that determine instability because these elements of the power system, like devices, control units, can be easily exploited by cyber-attacks to determine behaviors for disrupting the dynamic stability of the system.

In [5], it is presented the possible outcomes of instability in the power grid by different types of cyber-attacks that can target any level of the grid and any major device that plays a key role in the normal execution of the grid. The cyber-attack can take the form of a software error and can move anywhere in the system to map its vulnerabilities, so it can exploit them later.

Attackers can infiltrate through the communication channels of the substation or control centers to get control of transformers, switches, compensators and possibly inject false commands to disrupt the normal power flow or modify data from the sensor measurements to estimate the operational state of the grid based on which operators make informed decisions. An attacker can easily find out the state of the power grid by eavesdropping on the data gathered in real time (RT) from the field sensors. These field sensors, like

Intelligent Electronic Devices (IED), communicate through a serial communication channel (RS232, RS422 or Ethernet) with the Remote Terminal Units (RTU) that gathers information from digital relays, circuit breakers to transmit it to the control station through the Master Terminal Unit (MTU) using TCP/IP based protocols (like, DNP3.0, IEC 61850 etc.) susceptible to cyber-attacks due to their vulnerabilities.

The consequences of wrong estimation of the power grid's state can result in cascading failures and overall performance issues because some important devices maintaining the stability of operating conditions depend on the State Estimation (SE), like the Automatic Generator Control (AGC), Optimal Power flow (OPF) and Contingency Analysis (CA). For example, the AGC is used to maintain a balance between the power outputs versus demand from all power plants in the grid [14, 18]. It adjusts the set-point of power based on the information from remote sensors used by SCADA in the control centers and fed to the SE for gaining insights of the system variables: phase angles, voltage magnitudes, to integrate load frequency control within certain limits, power control and system optimization operations.

The AGC communicates with the control center for its reference points through standards and protocols such as Ethernet and Modbus, HART, PROFIBUS, DeviceNet and IEC61850. Each of these has exposed vulnerabilities that can be exploited by cyber-attacks. For example, the PROFIBUS has no encryption of messages, this making any message delivered vulnerable to interception and eavesdropping by a third party. Modbus is another protocol which due to its simplicity and efficiency is vastly used in the industrial environment, but its simplicity like having no authentication or lack of confidentiality of the messages transmitted and many more can lead to ways a cyber-attack can benefit from them [7, 8].

In the following section, we will be focusing on the mathematical model representation of a power system which is a **high-order multivariable process** considered from a stability point of view.

3. System description

The dynamics of a power network model having a synchronous generator connected to an infinite bus can be expressed in the form of the nonlinear differential equation, without disturbances, where f is a nonlinear vector function:

$$\dot{x}(t) = f(x, u, t) \tag{1}$$

The generator model of this benchmark [6] is considered transient having the rotor angle δ expressed in rad, ω as the rotor speed (rad/s), the transient voltages along the q and d axis e'_q and e'_d, and $x \epsilon R^4$ defining the state of the system:

$$x = [x_1\ x_2\ x_3\ x_4]^T = [\delta\ \omega\ e'_q\ e'_d]^T \tag{2}$$

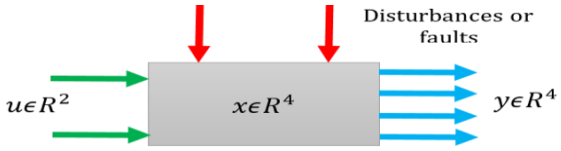

Fig. 1. The SMIB model under disturbances

And the input, $u \epsilon R^2$, of the SMIB having T_m as the mechanical torque (p.u) and E_{fd} as the internal field voltage (p.u):

$$u = [u_1\ u_2]^T = [T_m\ E_{fd}]^T \tag{3}$$

The output, $y \epsilon R^4$, represents the measurements given by the PMU at the terminal bus voltage of the generator having imaginary and real parts:

$$y = [y_1\ y_2\ y_3\ y_4]^T = [e_R\ e_I\ i_R\ i_I]^T \tag{4}$$

The generator model is expressed by the 4-th order DAE in the d-q reference frame [9]:

$$\begin{cases} \dot{x}_1 = x_2 - \omega_0 \\ \dot{x}_2 = \frac{\omega_0}{2H}\left(u_1 - T_e - \frac{K_D}{\omega_0}(x_2 - \omega_0)\right) \\ \dot{x}_3 = \frac{1}{\tau'_{d0}}(u_2 - x_3 - i_d(x_d - x'_d)) \\ \dot{x}_4 = \frac{1}{\tau'_{q0}}\left(-x_4 + i_q(x_q - x'_q)\right) \end{cases} \tag{5}$$

In the absence of disturbances of the system the nominal state dynamic can be expressed by the following equation:

$$\dot{x}(t) = f(x,u) = Ax(t) + Bu(t) + \varphi(x,u) \tag{6}$$

Where:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -\frac{K_D}{2H} & 0 & 0 \\ 0 & 0 & -\frac{1}{\tau'_{q0}} & 0 \\ 0 & 0 & 0 & -\frac{1}{\tau'_{q0}} \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 0 \\ \frac{\omega_0}{2H} & 0 \\ 0 & \frac{1}{\tau'_{d0}} \\ 0 & 0 \end{bmatrix}, \quad \varphi(x,u) = \begin{bmatrix} -\omega_0 \\ \frac{\omega_0}{2H}(-T_e(x,u) + K_D \\ -\frac{x_d - x'_d}{\tau'_{d0}} i_d(x,u) \\ \frac{x_q - x'_q}{\tau'_{q0}} i_q(x,u) \end{bmatrix} \tag{7}$$

Usually a single machine is connected to the infinite bus together with other machines separated by the transmission lines of low reactance forming a group on a designated geographical area.

According to [6, 8], the desired linearized network equation between the currents in a 3-generator model network is:

$$
\begin{bmatrix} I_{q1} & I_{d1} & I_{q2} & I_{d2} & I_{q3} & I_{d3} \end{bmatrix}^T =
$$

$$
\begin{bmatrix}
Y_{12}\cos(\theta_{12}-\delta_{120}) & -Y_{12}\sin(\theta_{12}-\delta_{120}) & Y_{13}\cos(\theta_{13}-\delta_{130}) & -Y_{13}\sin(\theta_{13}-\delta_{130}) & Y_{12}[E'_{d20}\cos(\theta_{12}-\delta_{120}) + E'_{q20}\sin(\theta_{12}-\delta_{120})] & Y_{13}[E'_{d30}\cos(\theta_{13}- + E'_{q30}\sin(\theta_{13}- \\
Y_{12}\sin(\theta_{12}-\delta_{120}) & Y_{12}\cos(\theta_{12}-\delta_{120}) & Y_{13}\sin(\theta_{13}-\delta_{130}) & Y_{13}\cos(\theta_{13}-\delta_{130}) & Y_{12}[E'_{d20}\sin(\theta_{12}-\delta_{120}) + E'_{q20}\cos(\theta_{12}-\delta_{120})] & Y_{13}[E'_{d30}\sin(\theta_{13}- + E'_{q30}\cos(\theta_{13}- \\
G_{22} & -B_{22} & Y_{23}\cos(\theta_{23}-\delta_{230}) & -Y_{23}\sin(\theta_{23}-\delta_{230}) & -E_1\,Y_{12}\sin(\theta_{12}-\delta_{120}) - E'_{d30}Y_{23}\cos(\theta_{23}-\delta_{230}) - E'_{q30}Y_{23}\sin(\theta_{23}-\delta_{230}) & Y_{23}[E'_{d30}\cos(\theta_{23}- + E'_{q30}\sin(\theta_{23}- \\
B_{22} & G_{22} & Y_{23}\sin(\theta_{23}-\delta_{230}) & Y_{23}\cos(\theta_{23}-\delta_{230}) & E_1\,Y_{12}\cos(\theta_{12}-\delta_{120}) - E'_{d30}Y_{23}\sin(\theta_{23}-\delta_{230}) + E'_{q30}Y_{23}\sin(\theta_{23}-\delta_{230}) & Y_{23}[E'_{d30}\sin(\theta_{23}- - E'_{q30}\cos(\theta_{23}- \\
Y_{23}\cos(\theta_{23}-\delta_{230}) & -Y_{23}\sin(\theta_{23}-\delta_{230}) & G_{33} & -B_{33} & Y_{23}[E'_{d20}\cos(\theta_{23}-\delta_{230}) + E'_{q20}\sin(\theta_{23}-\delta_{230})] & -E_1\,Y_{13}\sin(\theta_{13}- - E'_{d20}Y_{23}\cos(\theta_{23}- \\
Y_{23}\sin(\theta_{23}-\delta_{230}) & Y_{23}\cos(\theta_{23}-\delta_{230}) & B_{33} & G_{33} & Y_{23}[E'_{d20}\sin(\theta_{23}-\delta_{230}) + E'_{q20}\cos(\theta_{23}-\delta_{230})] & -E'_{q20}Y_{23}\sin(\theta_{23}- \\
 & & & & & E_1\,Y_{13}\cos(\theta_{13}- \\
 & & & & & -E'_{d20}Y_{23}\sin(\theta_{23}- \\
 & & & & & +E'_{q20}Y_{23}\cos(\theta_{23}-
\end{bmatrix}
\tag{8}
$$

4. Case Study

Considering the following example of a IEEE 9-bus system having 3 generators (one classical model and the other 2 are a two-axis model) and three active loads which is to be analyzed in the linearized equations [6].

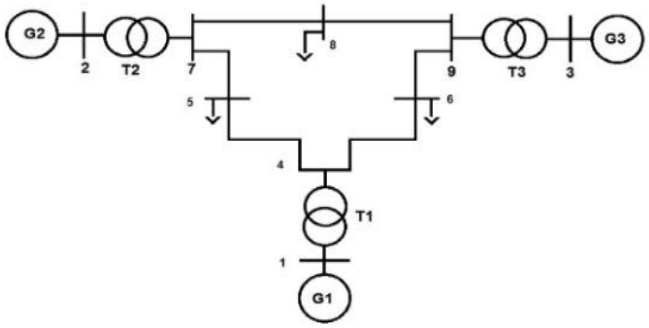

Fig. 2. IEEE 9-bus

The values for the 3 generators are, as in [6]:

Table 1

System data of a 3-generator system

Quantity	Unit	Generator 1 (classical)	Generator 2 (two-axis)	Generator 3 (two-axis)
H(MW*s/100MVA)	s	23.6	6.4	3.01
$r_j = 2H\,\omega_s$	pu	17824.14	4825.4863	2269.4865
$x_d - x'_d$	pu	0.0852	0.776	1.1312
$x_q - x'_q$	pu	0.0361	0.7447	1.0765
τ'_{q0}	s	0	0.535	0.6
τ'_{q0}	pu	0	201.69	226.19

τ'_{d0}	s	8.96	6	5.89
τ'_{d0}	pu	3377.8404	2261.9467	2220.4777
E'_{q0}	pu	1.0558	0.7882	0.7679
E'_{d0}	pu	-0.0419	-0.694	-0.6668
I_{q0}	pu	0.678	0.932	0.6194
I_{d0}	pu	-0.2872	-1.2902	-0.5615
V_{q0}	pu	1.0392	0.6336	0.6661
V_{d0}	pu	-0.0419	-0.8057	-0.7791
δ_0	Elec deg	2.2717°	61.0975°	54.1431°
E'	pu	1.0566	-	-

The generator internal nodes have the voltages $\overline{E'_1}$, $\overline{E'_2}$ and $\overline{E'_3}$ and using $\delta_{12} = -\delta_{21}$, $\delta_{13} = -\delta_{31}$, [6]:

Table 2

Preliminary Calculations

Nodes	1-2	1-3	2-3
Y_{ij}	1.5399	1.2434	1.1086
θ_{ij}	79.2544	80.2952	78.9084
δ_{ij0}	-58.8259	-51.8714	6.9545
$\theta_{ij} - \delta_{ij0}$	138.0802	132.1666	71.9540
$Y_{ij}\cos(\theta_{ij} - \delta_{ij0})$	-1.1458	-0.8347	0.3434
$Y_{ij}\sin(\theta_{ij} - \delta_{ij0})$	1.0288	0.9216	1.0541
$\theta_{ij} + \delta_{ij0}$	20.4285	28.4238	85.8629
$Y_{ij}\cos(\theta_{ij} + \delta_{ij0})$	1.4431	1.0935	0.0800
$Y_{ij}\sin(\theta_{ij} + \delta_{ij0})$	0.5375	0.5919	1.1058

Classical generator 1 is described by the following differential algebraic equation:

$$\begin{cases} \tau'_{j1}\dot{\omega}_1 = T_{m1} - E_1 I_{q1} - D_1\omega_1 \\ \dot{\delta}_1 = \omega_1 \end{cases} \tag{9}$$

Two-axis generator 2 and 3 equations:

$$\begin{cases} \tau'_{q0i}\dot{E'}_{di} = -E'_{di} - (x_{qi} - x'_i)I_{qi} \\ \tau'_{q0i}\dot{E'}_{di} = E_{FDi} - E'_{qi} - (x_{di} - x'_i)I_{di} \\ \tau_{ji}\dot{\omega}_i = T_{mi} - D_i\omega_i - E'_{di}I_{di0} - E_{iqi}I_{qi0} - E'_{di0}I_{di} - E'_{qi0}I_{qi} \\ \dot{\delta}_i = \omega_i, i = 2,3 \end{cases} \tag{10}$$

The linearized differential equation for the 3-machine system is in the form of:

$$\dot{x} = Ax + Bu \tag{11}$$

Where the state vector is:

$$x^T = [\omega_1 \quad E'_{q2} \quad E'_{d2} \quad \omega_2 \quad E'_{q3} \quad E'_{d3} \quad \omega_3 \quad \delta_{12} \quad \delta_{13}] \tag{12}$$

And the input of the system:

$$u^T = [T_{m1} \quad E_{FD2} \quad T_{m2} \quad E_{FD3} \quad T_{m3}] \tag{13}$$

By replacing with the numerical values from table 1 in equations (9), (10) and using them along with equation (9) - (13) and after simple algebraic manipulations, the continuous-time state-space model of the system is in the following form being comprised of nine-linear first order differential algebraic equations (14):

$$[\omega_1 \quad E'_{q2} \quad E'_{d2} \quad \omega_2 \quad E'_{q3} \quad E'_{d3} \quad \omega_3 \quad \delta_{12} \quad \delta_{13}]^T$$

$$= 10^{-4} \begin{bmatrix} -0.561D_1 & 0.6793 & 0.6099 & 0 & 0.4948 & 0.5463 & 0 & -0.952 & -0.7494 \\ 0 & -13.7658 & 1.4409 & 0 & 3.6163 & 1.1781 & 0 & 8.5472 & -3.3161 \\ 0 & -15.5076 & -150.1554 & 0 & -12.6793 & 38.9205 & 0 & 42.4023 & -21.4333 \\ 0 & -6.5352 & -1.1714 & -2.0723D_2 & 0.9552 & 2.2156 & 0 & 5.4592 & -2.3385 \\ 0 & 5.6334 & 0.4076 & 0 & -16.5675 & 1.4111 & 0 & -4.2309 & 10.1170 \\ 0 & -3.8073 & 52.627 & 0 & -13.1829 & -156.9117 & 0 & -38.8349 & 68.5987 \\ 0 & 2.9781 & 3.9766 & 0 & -10.6238 & -4.7247 & -4.4063D_3 & -5.2010 & 10.7116 \\ 10000 & 0 & 0 & -10000 & 0 & 0 & 0 & 0 & 0 \\ 10000 & 0 & 0 & 0 & 0 & 0 & -10000 & 0 & 0 \end{bmatrix} \begin{bmatrix} \omega_1 \\ E'_{q2} \\ E'_{d2} \\ \omega_2 \\ E'_{q3} \\ E'_{d3} \\ \omega_3 \\ \delta_{12} \\ \delta_{13} \end{bmatrix}$$

$$+ [0.561T_{m1} \quad 4.421E_{FD2} \quad 0 \quad 2.0723T_{m2} \quad 4.5035E_{FD3} \quad 0 \quad 4.4063T_{m3} \quad 0 \quad 0]^T \tag{14}$$

5. Attack model

The power grid is a non-linear system that can be approximated by a linear one to better study its properties near a region of operation. The state dynamics of the power system is described as a LTI (Linear Time Invariant) system of $u \epsilon R^n$ input control signals and $y \epsilon R^m$ output signals captured as measurements in continuous time by sensors (or PMUs) and subjected to cyber-attacks, disturbances and faults. The DAE equations are:

$$\begin{cases} \dot{\boldsymbol{x}}(\boldsymbol{t}) = \boldsymbol{Ax}(\boldsymbol{t}) + \boldsymbol{Bu}(\boldsymbol{t}) + P(t)\,d(t) + c \\ y_q(t) = C_q x(t) + v_q(t) \\ d(t) = [u_d(t)\ f_f(t)] \end{cases} \tag{15}$$

Where $A \in R^{3n_g x 3n_g}$, $B \in R^{3n_g x 3n_g}$, $C_q \in R^{qx3n_g}$, $P \in R^{3n_g x m_2}$ (the disturbances and faults against the actuator matrix), $u_d(t)$ is the input disturbance, $f_f(t)$ is the actuators fault and both are considered unknown inputs. C denotes the output matrix, q is the number of buses where PMUs are installed, $3n_g$ represent the states of the generators (rotor angles, rotor speeds, voltages), m_1 known grid inputs (mechanical input power and field voltage), m_2 unknown grid inputs and q output measurements. $v_q(t)$ is the potential vector against the output of the system measured by the PMUs or sensors and sent to the control centers.

Attacks on power grid are varied, all targeting one or multiple security objectives and can be launched either individually or distributed. The impact by a single or multiple attack of system's operations is described in the next section both quantitatively (numerical) and qualitatively (graphical).

6. Results

If an attacker wants to manipulate the system's operating conditions he can target the SCADA directly by denial-of-service (DoS) attacks and false data injection attacks (e.g. Load Redistribution attacks). A power grid is reliable if measurement information (bus voltage, reactive power, real power, etc.) sent to the control centers or command signals sent from the control center to the actuators are unaltered by a third party.

Below we simulated 2 types of cyber-attacks with the following scenarios each regarding the power grid's operational state:

1. False data injection attack
   a) Normal state of the power grid under normal operating conditions;
   b) The state of the power grid when only one cyber-attack is introduced;
   c) The state of the power grid when multiple cyber-attacks are introduced.
2. Replay attack
   a) Normal state of the power grid under normal operating conditions;
   b) The state of the power grid when the cyber-attack is introduced.

1. False data injection (bad measurement) is a type of attack that requires the attacker to know the target system configuration and manipulate several sensors to create the desired outcome, such as wrong estimation of system status which can lead to wrong actions, cascading failures and performance issues.

a) Normal state of the power grid under normal operating conditions:

The simulated output of the continuous-time state-space model of the IEEE 9-bus system described by equation (14) **under no cyber-attack** is:

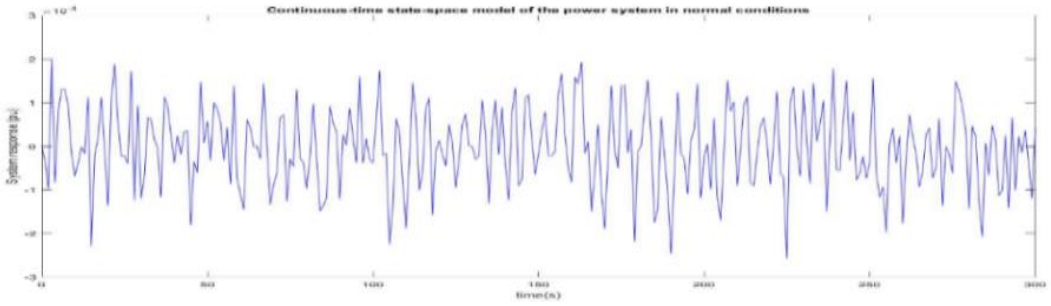

Fig. 3. Simulated system operation in normal state

b) The state of the power grid when only one cyber-attack is introduced:

In Figure 4, when T=259s the value of the system's state has been altered from 5.49991270526205e-05pu to 0.00020499127052621pu due to a cyber-attack causing an erroneous operating action.

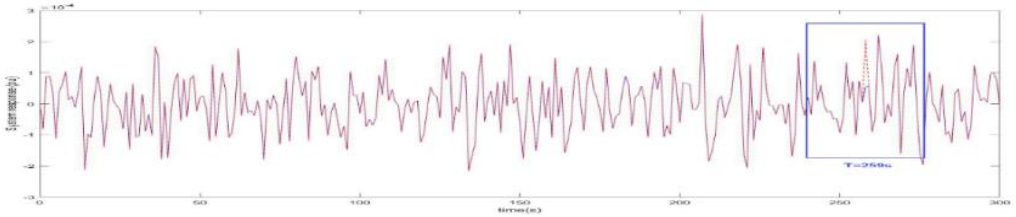

Fig. 4. Simulated system operation subjected to one cyber attack

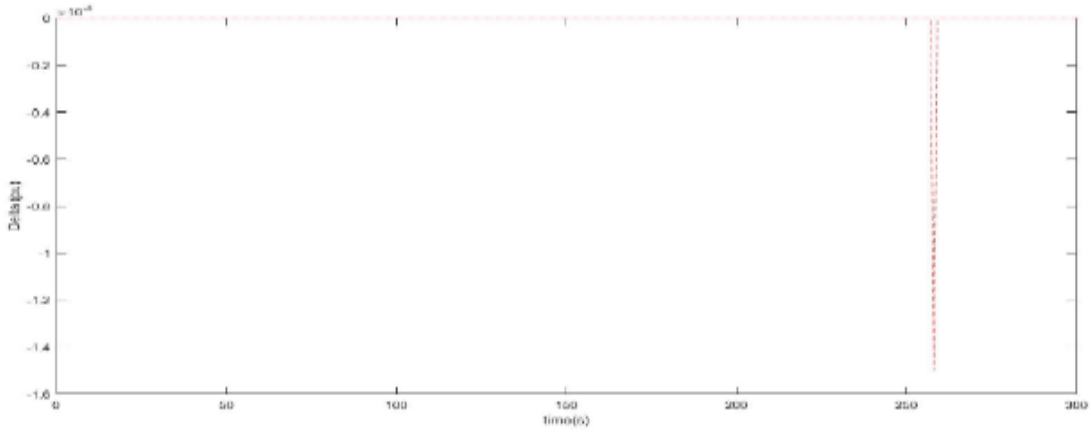

Fig. 5. Delta value of system response in normal state against a single attack

c) The state of the power grid when multiple cyber-attacks are introduced at different time periods:

Table 3

Altered system response by multiple cyber-attacks

Time (s)	Actual value (pu)	Modified value (pu)
71	-0.000179108208113039	-0.000279108208113000
135	-0.000214870352229724	-4.87035222972400e-05
200	4.68174108132947e-05	-1.68174108132947e-05

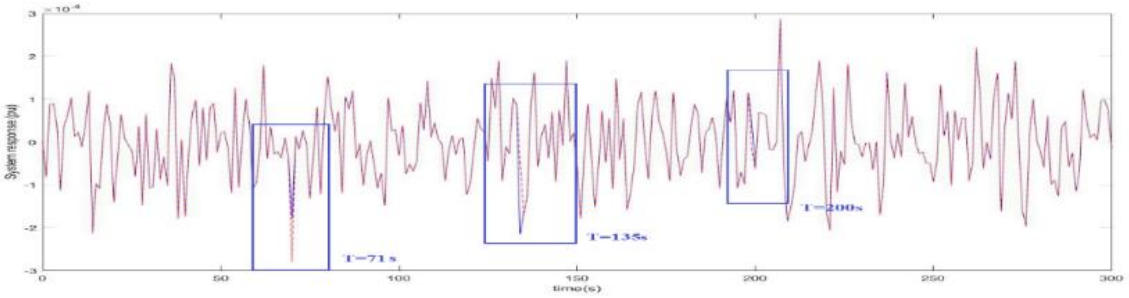

Fig. 6. Simulated system operation subjected to multiple cyber attacks

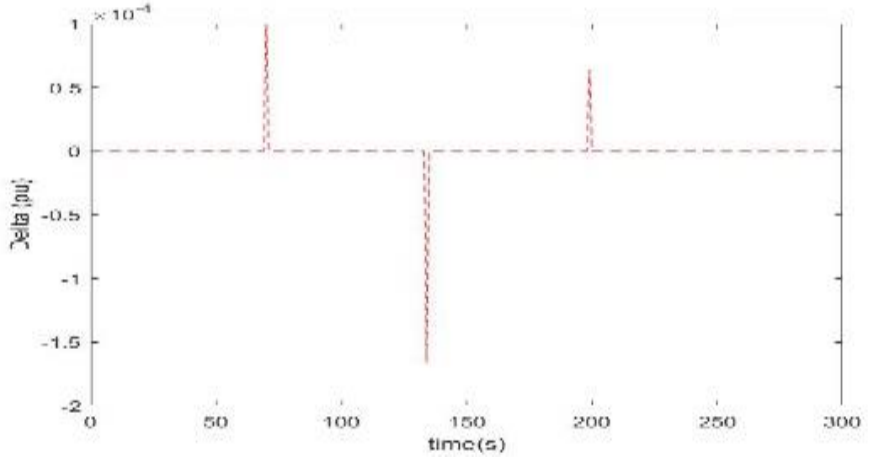

Fig. 7. Delta values of system response in normal state against multiple attacks

These deviations are either small or large depending on the effect that the cyber-attack causes, as shown in Figure 7. False commands sent to the AGC or AVR by exploiting the communication protocols or by infiltrating in the control center through the corporate network impact the dynamics of the power grid, as seen in Figure 4 and 6. Modifying the reference point of power of the AGC or the voltage reference of the AVR leads to increased output power that exceeds the mechanical power resulting in an imbalance between the electromagnetic and mechanical torque. This determines frequency instability and overload of the system resulting eventually in blackouts and financial loss.

2. Replay attacks. In the Common Weakness Enumeration, a community-based project of creating a catalog of most common cyber weaknesses and vulnerabilities of software, considers the replay attacks as a "*flaw that exists when the design of the software makes it possible for a malicious user to sniff network traffic and bypass authentication by replaying it to the server in question to the same effect as the original message*" [10, 13].

This class of attacks has the advantage of not being detected by normal anomaly detection mechanisms because of the valid data used.

a) Normal state of the power grid under normal operating conditions;

In Figure 8. a) the normal and actual state of the system is simulated while Figure 8. b) represents also the actual system state but from a later point in time. The window frame of 300 sec of the actual true state of the system is replaced through the replay attack with the historical one which is valid. The control center receives valid measurement/command data without questioning if that is the current state of the system.

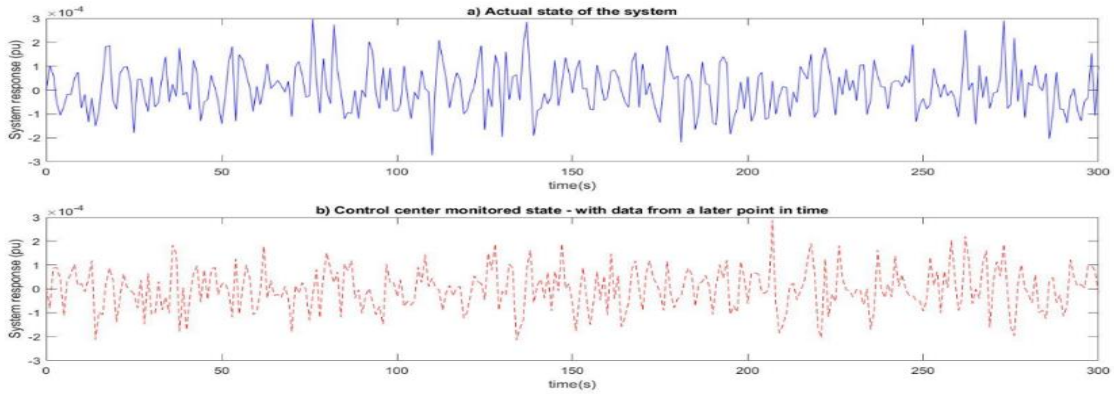

Fig. 8. Actual state of the system and the replayed state of the system

b) The state of the power grid when the cyber-attack is introduced.

Figure 9 depicts the difference between the two states of the system (current state vs. replayed state) and in Figure 10 we can observe the delta values – the difference between the actual state and the replayed state.

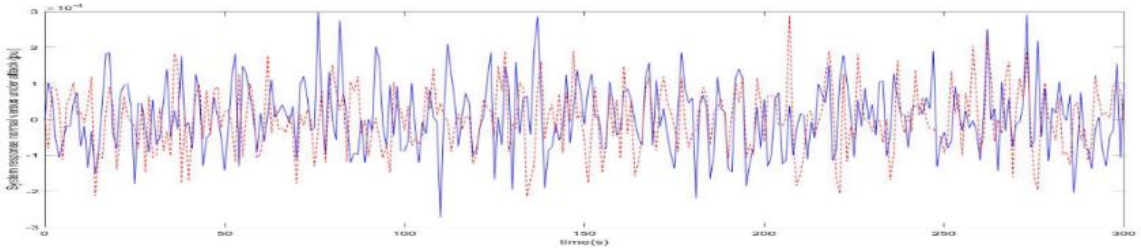

Fig. 9. Actual state of the system against the replayed state

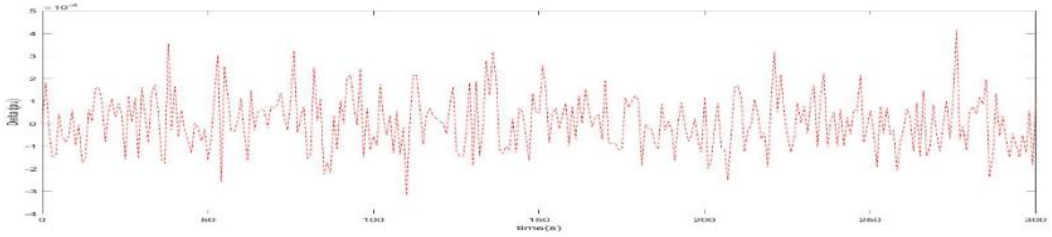

Fig. 10. Delta values of system response of actual state against replayed state

This type of attack is one of the most feasible and effective as it can handle encrypted messages because it doesn't need to know what the played back message is, nor they require an understanding of the communication standard and protocols. The attacker would just need to intercept the data stream and simply communicate it the server which does all the decryption and validation.

Even though the replay data is valid and shows correctly the state of the system, the problem is that the representation is from a past state while a real-time control system needs current data to send the appropriate control commands to the actuators in real-time.

For example, captured control commands over switches or breakers and replayed later as legitimate signals can alter the distribution system by opening or closing regardless of the situation, incorrect control commands being incorrect attributed to actuators can lead to compromising the equipment [11, 12].

7. Conclusions

In this paper, our purpose was to model the dynamic interconnected electrical system and conduct a behavior analysis when the grid is subject to cyber-attacks modelled as disturbances/faults. We reached our goal by providing results of power system response analysis during disruptions caused by cyber-attacks: false data injection and replay attacks. We also proved that cyber-attacks can target any entry point of the cyber network that controls or has access to manipulate physical components and successfully compromise grid operations and physical levels of the power grid having different outcomes.

The power network is a nonlinear model, presented in Section 1, which is difficult to analyze due to its complexity, thus, we provided in Section 2 a simpler linear time-invariant representation to use in the case study in Section 3 of the IEEE 9 bus presented as a multi-machine power system model including non-linear generator dynamics. Upon this linearized time-invariant representation of the network we modeled cyber-attacks, in Section 4, targeting two important properties of the power system: controllability and stability. We consider cyber-attacks to be one of the highest severity disturbances due to their sophistication and unpredictable outcome upon the highly nonlinear complex power system.

R E F E R E N C E S

[1]. *B. Radhakisan, G. Helen*, "Cyber-physical Systems'', The Impact of Control Technology, IEEE Control Systems Society, 2011.

[2]. *I. Dumitrache, D.I. Dogaru*, "Smart Grid Overview: Infrastructure, Cyber–Physical Security and Challenges", International Conference on Control Systems and Computer Science (CSCS), IEEE, 2015.

[3]. *L. Cuadra et. al*., "A Critical Review of Robustness in Power Grids Using Complex Networks Concepts", Energies, vol. 8, 2015, pp 9211-9265.

[4]. *C. Arghir et. al.*, "On the steady-state behavior of a nonlinear power network model", IFAC Proceedings Volumes, vol. 49, issue 22, 2016, pp 061–066.

[5]. *D. I. Dogaru, I. Dumitrache*, "Robustness of Power Systems in the Context of Cyber Attacks", International Conference on Control Systems and Computer Science (CSCS) 2017.

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

[7]. *M. Kezunovic et al.*, "Application of Time-Synchronized Measurements in Power System Transmission Networks", Springer, 2014.

[8]. *L. U. N. de Silva et al.,* "Automatic governor for tie-line control: A teaching tool", Moratuwa Engineering Research Conference (MERCon), 2015.

[9]. *A. F. Taha*, "Secure Estimation, Control and Optimization of Uncertain Cyber-Physical", PhD thesis, Purdue University, 2015.

[10]. *H. Tingshu*, "Control Systems: Controllability and Observability", Course, University of Massachusetts Lowell, [Online] Available: http://faculty.uml.edu/thu/controlsys/note08.pdf

[11]. *S. Amin et al.*, "Cyber security of water SCADA systems: Part II attack detection using an enhanced hydrodynamic model", IEEE Transactions on Control Systems Technology, vol. 21, issue 5, 2013.

[12]. Mitre, "Common Weakness Enumeration", Entry 294, 2015, [Online] Available: https://cwe.mitre.org/data/definitions/294.html

[13]. *F. Miao, M. Pajic, G.J. Pappas*, "Stochastic game approach for replay attack detection", IEEE Conference on Decision and Control, 2013.

[14]. *S. Sridhar, A. Hahn, M. Govindarasu*, "Cyber–Physical System Security for the Electric Power Grid", Proceedings of the IEEE, vol. 100, issue 1, 2012

[15]. *I. Dumitrache, N. Constantin, O. Stoica*, "Some challenges for the Cyber-Physical Energy Systems", pg 3-9, Proceedings of the 2nd IFAC workshop (ICPS-2013) on convergence of Information Technologies And Control Methods With Power Systems – IFAC Paper Plaza, 2013

[16]. *I. Dumitrache*, "Cyber Physical Systems - New Challenges for Electric Power Systems", invited paper on the 7th International Conference on Deregulated Electricity Market Issues in South-Eastern Europe, DEMSEE 2012

[17]. *I. Dumitrache,* "Intelligent Cyber-Energy-Systems" – invited paper on ICTSCC-18th International Conference on System Theory, Control and Computing, 2014

[18]. *F. Ciausiu, M. Eremia*, "Steady-State Stability Limit Identification for Large Power Systems", U.P.B. Sci. Bull., Series C, Vol. 72, Iss. 1, 2010