We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Cognitive Dynamic System for AC State Estimation and Cyber-Attack Detection in Smart Grid

Mohammad Irshaad Oozeer and Simon Haykin

Abstract

The work presented in this chapter is an extension of our previous research of bringing together the Cognitive Dynamic System (CDS) and the Smart Grid (SG) by focusing on AC state estimation and Cyber-Attack detection. Under the AC power flow model, state estimation is complex and computationally expensive as it relies on iterative procedures. On the other hand, the False Data Injection (FDI) attacks are a new category of cyber-attacks targeting the SG that can bypass the current bad data detection techniques in the SG. Due to the complexity of the nonlinear system involved, the amount of published works on AC based FDI attacks have been fewer compared to their DC counterpart. Here, we will demonstrate how the entropic state, which is the objective function of the CDS, can be used as a metric to monitor the grid's health and detect FDI attacks. The CDS, acting as the supervisor of the system, improves the entropic state on a cycle to cycle basis by dynamically optimizing the state estimation process through the reconfiguration of the weights of the sensors in the network. In order to showcase performance of this new structure, computer simulations are carried out on the IEEE 14-bus system for optimal state estimation and FDI attack detection.

Keywords: false data injection, cognitive dynamic systems, cognitive control, AC state estimation, smart grid

1. Introduction

The Cognitive Dynamic System (CDS) is an organized physical model and research tool that is based on certain features of the brain. Following its first introduction in [1], it was later expanded in [2] leading to its first applications in cognitive radio [3] and cognitive radar [4]. Since then, CDS has progressed enormously to give rise to Cognitive Control (CC) [5] and Cognitive Risk Control (CRC) [6] as two of its particular functions. Using those principles, the CDS was first merged in [7] with the Smart Grid (SG) to form a new structure, based on the DC state estimation model, that shows tremendous potential for handling the possible problems that the SG will be facing in the near future. Furthermore, in [8], the construct presented in [7] was expanded to include a more complex CRC that is closer to the brain. In that paper, it was proven how this new approach can to be used to mitigate the problem of cyber-attack in the SG. From a neuroscience perspective, the CDS is founded on Fuster's paradigm of cognition comprising of the following five principles: perception-action cycle (PAC), memory, attention,

intelligence and language [9]. In its simplest form, the CDS is built on two main components: the perceptor, on one side, and the executive on the other with the feedback channel uniting them together. In [7], it was shown that the integration of the over-arching function of CDS, CC, with the SG, is well adapted for slowly progressing cyber-physical systems. In this chapter, the construct presented in [7], where the DC-estimation model was involved, will be re-engineered to be able to carry out AC state estimation optimally and also be able to detect cyber-attacks. In order to do so, the perceptor of the CDS will incorporate a generative model that will allow it to sense and control the environment indirectly. Moreover, in order to bring forward the cognitive ability of the CDS and make it compatible with the current nonlinear state estimation in SG, the steps involved in the state estimation process will be re-engineered in a novel way. It will also be shown how the entropic state, which is the objective function of the CDS, will be instrumental in implementing a control-sensing mechanism that is capable of identifying and handling bad measurements. We will also show how this entropic state serves as the basis for detecting False Data Injection attacks (FDI) in SG.

1.1 Smart grid

The next generation of engineering systems consisting of the Internet of Things (IoT) and Cyber-physical systems (CPSs) are currently paving the way towards the fourth industrial revolution [10]. As those systems are gradually occupying a more prominent role in our daily lives, through applications in critical infrastructures such as electrical power grids or transportation systems, the cyber-security aspects of those systems will also grow in importance [11]. In the context of this chapter, emphasis will be laid upon the SG and its most dangerous threat known as False Data Injection (FDI) attacks. More specifically, compared to our previous research where the DC model for state estimation was investigated [7], focus will be laid upon on the AC model, which is more a realistic representation of the smart grid, and the introduction the CDS for a new way of control and FDI attack detection.

Making use of all the new generation of sensing, monitoring and control strategies, the SG is forecasted to be a more powerful entity than the traditional power grid in many facets such as reliability and efficiency [12, 13]. In the SG, the Supervisory Control and Data Acquisition systems (SCADA) is responsible for monitoring and processing the main control actions by collecting meter measurements from remote terminal units (RTUs) consisting of different field devices or sensors. Through a process known as state estimation, those measurements are then processed and analyzed for errors and inconsistencies after being transmitted to a control center [14, 15]. The state variables that are calculated by this process usually consist of the voltage magnitudes and angles of the different busses in the system [16]. The measurements used for state estimation are the currents, real and reactive power flows, power injections and voltage magnitudes and angles. In the DC model, the state variables are the bus angles only while in the more complex AC model, the voltage magnitudes and angles of the different busses in the network are estimated. Weighted Least Squares (WLS), introduced by Schweppe [14], is the technique used for the power system state estimation using those measurements. In order to enhance the accuracy of the estimated states, another process, known as Bad Data Identification, is carried out to remove bad measurements. Bad measurements are erroneous measurement readings that will impact state estimation negatively. The most commonly applied bad data identification techniques are the Chi-Squared Tests and Largest Normalized Residual Test [15, 17]. Those statistical tests rely on the residuals between the estimated states and the measurement residuals to identify the bad data. In the case of an FDI attack, bad data, which can bypass the

previously mentioned tests, is introduced into the system such that the estimated states can be modified stealthily. Those bad data are maliciously crafted offsets to measurements that are injected to the sensor readings so as the state estimation process is influenced in a particular way. Consequently, with the incorrect calculated states, bad control decisions will be applied.

Although FDI attacks have been a popular topic of research over the past years [18], most of the works, e.g., in [10–13, 19], investigated the FDI attacks on the DC model. Few works have been published on the AC model and those attacks [18, 20, 21]. Nevertheless, the DC model is just a simplified representation of the nonlinear AC state estimation model. There are major differences between the two models that could explain why the AC model has been unpopular. Firstly, in the nonlinear state estimation model, the estimated states are obtained after undergoing iterations, while in the DC model, those states are obtained in closed-form. Moreover, the linear state estimation relies on active power flow analysis [16, 22, 23]. On the other hand, the AC model uses both active and reactive power flow analysis. Furthermore, the state variables in the DC model consist of the voltage angles only while the states in the AC model consist of both the voltage angles and magnitudes. Consequently, these differences raise the complexity and computational expense of nonlinear state estimation as a topic of research when it comes to FDI attacks [24]. In fact, DC based FDI attacks can be detected by AC-based data detection techniques [20]. Hence, since the AC model is commonly applied in power systems, finding a way to detect these attacks and mitigating them under that environment is going to be very important for the coming years.

1.2 Contribution and organization

The main contributions of this chapter can be summarized as follows:

i. The architectural architecture of the CDS, tailored for AC state estimation and FDI attack detection in the SG, is presented. Compared to our earlier work in [7], which was based on the DC model, we will show how that construct can re-engineered with the goal of nonlinear state estimation and computational efficiency in mind. Consequently, it will be shown how the CDS allows for optimal state estimation with relatively less computations, using the principles of cognition rooted in the brain.

ii. To expand on our previous research, the entropic state will be re-introduced for two purposes namely; (1) it serves as a metric of the grid's health on a cycle to cycle basis and (2) it is used in the detection of FDI attacks. The optimization of the entropic state is the goal of the cognitive controller residing in the executive of the CDS. The latter does this by selecting the most optimal actions that will maximize the available information from one PAC to the next. Simulations are performed on the IEEE 14-bus network to show the efficiency of this new approach using the CDS. By learning which measurements to prioritize and which ones to neglect, the CDS showcases a new way of control for bad data correction and FDI attack detection with the SG being the topic of application.

The rest of this chapter is organized as follows: In Section 2, the basic concepts of state estimation and data detection for the AC model will be presented and contrasted. The mathematics of FDI attacks for this model will also be demonstrated. Section 3 expands on the structure of the CDS for the SG. Since this research is an extension of [7], the material presented in that paper will be re-engineered for

this new application. In the context of the CDS, the SG is considered as the environment with which it interacts. Section 4 gives a discussion on the application and simulation results of this approach on the IEEE 14-bus network. It will be shown how this new structure is able to handle the two problems of bad data detection and FDI attack detection simultaneously. Finally, Section 5 concludes this paper by highlighting the key results and presenting new avenues of research for this novel construct.

2. Preliminaries

2.1 Weighted least squares state estimation

In order for the Energy Management System (EMS) to operate properly, it is important for the SCADA to provide the latter with the required measurement data so that correct control decisions can be applied in real-time. However, as those signals are often contaminated with noise, filtering is carried out by both the state estimator and the bad data detector to obtain the most accurate states. However, since power systems comprise of an overdetermined system whereby redundant measurements are taken, the filtering process allows the discarding of those erroneous measurements that will be detrimental for state estimation.

2.2 AC model

The states of a power system refer to the bus voltages angle θ and bus voltage magnitudes V. In the case of the DC model, the states are restricted to the bus angles only and the measurements consist of the real power flows and injections. Additionally, it is assumed that prior knowledge relating to the bus magnitudes is available and those are taken to be close to unity. After choosing a reference bus and setting it to zero radians, state estimation in the linear system is simplified to only estimating the n bus voltage angles $[\theta_1, \theta_2, \ldots, \theta_n]^T$. The DC power flow model has been a popular research tool for power engineers and smart grid cyber-security researchers as it serves as a linearization and approximation of the AC power flow model [14, 25–27]. In fact, this substitution to the AC model has been widely accepted for reasons such as guaranteed faster convergence and reduced algorithmic complexities [28].

In the AC model, the nonlinear power flow equations are fundamental for state estimation since they indicate the link between the measurements and the estimated states. In this model, the active and reactive power for the transmission line between busses k and m are given by

$$P_{km} = V_k^2 g_{km} - V_k V_m g_{km} \cos(\theta_{km}) - V_k V_m b_{km} \sin(\theta_{km}) \tag{1}$$

$$Q_{km} = -V_k^2 b_{km} + V_k V_m b_{km} \cos(\theta_{km}) - V_k V_m g_{km} \sin(\theta_{km}) \tag{2}$$

Additionally, for each bus k, it is calculated using the following equations:

$$P_k = V_k \sum_{m \in S_k} V_m \left(-g_{km} \cos(\theta_{km}) - b_{km} \sin(\theta_{km})\right) + V_k^2 \sum_{m \in S_k} g_{km} \tag{3}$$

$$Q_k = V_k \sum_{m \in S_k} V_m \left(-g_{km} \sin(\theta_{km}) - b_{km} \cos(\theta_{km})\right) - V_k^2 \sum_{m \in S_k} b_{km} \tag{4}$$

where $S_k \subset S$ is the set of all busses that have lines connected to bus k and g_{km} and b_{km} are the conductance and susceptance of the line between busses k and m respectively. θ_{km} denotes and the phase angle difference between bus k and bus m. In AC power flow estimation, the nonlinear relationship between the state variables and the measurements is described as follows:

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{5}$$

where

- $\mathbf{x}$ is the n vector of the true states (voltage magnitudes and angles)
- $\mathbf{z}$ is the m vector of measurements (active and reactive power flows, active and reactive power injections, voltage magnitudes and angles)
- $\mathbf{h}$ is the m x n Jacobian matrix (relates measurements to states)
- $\mathbf{h(x)}$ is the m vector of nonlinear function linking measurements to states
- $\mathbf{e}$ is the m vector of measurement errors
- m is the number of measurements
- n is the number of variables

$\mathbf{H}$ in (5), also known as the Jacobian matrix, is a matrix that defines the theoretical calculations that relates the states to the measurement vector $\mathbf{z}$ and therefore serves as a mathematical description of the power system. These equations are also referred to as the power flow equations and are described as vectors inside $\mathbf{H}$. While in the DC model, those entries consists of a set of linear functions of the state variables, those functions are nonlinear as far as the AC model is concerned. The determination of the state variables is done according to the following criteria:

$$\min J(\mathbf{x}) = (\mathbf{z} - \mathbf{h}(\mathbf{x}))'\mathbf{W}(\mathbf{z} - \mathbf{h}(\mathbf{x}))' \tag{6}$$

$\mathbf{W}$ in (6), is a diagonal matrix that contains the measurement weights. These are based on the reciprocals of the measurement error variance σ:

$$\mathbf{W} = \mathbf{R}_{\mathbf{z}}^{-\mathbf{1}} = \begin{bmatrix} \sigma_1^{-2} & \cdots & \cdots & \cdots \\ \cdots & \sigma_2^{-2} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ \cdots & \cdots & \cdots & \sigma_m^{-2} \end{bmatrix} \tag{7}$$

where $\mathbf{Rz}$ is the covariance matrix of the measurement. The performance index $J(\mathbf{X})$ is then differentiated to obtain the first order optimal conditions which can be solved using iterative methods, such as Honest Gauss Newton method, Dishonest Gauss Newton method and Fast Decoupled State Estimator [23]. The first order optimality condition of (6) to be solved is then expressed as:

$$\frac{\partial J(\mathbf{x})}{\partial \mathbf{x}}|_{\mathbf{x}=\hat{\mathbf{x}}} = -2\mathbf{F}_h^T(\hat{\mathbf{x}})\mathbf{W}(\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}}))' = 0 \tag{8}$$

where $\mathbf{F}_h$ is the Jacobian matrix derived from $\mathbf{h}(\mathbf{x})$ and the $\hat{\mathbf{x}}$ is the estimated state vector. In the case of the CDS, the state estimation process is modified slightly in order to remain compatible with the planning stages in the executive, which will be discussed later. Therefore, for the first t_s cycles, state estimation proceeds similar to the iterative procedures mentioned previously. As from t_s, the preceding calculated state of the AC state estimator, $\mathbf{x}_{k-1}$, is used as the initial guess for the current cycle with any of those iterative techniques. Moreover, the number of iterations is also limited to N_s iterations to save on computational resources.

2.3 Bad data detection

During the state estimation process, faulty measurements have to be detected and identified to be removed as they lead to erroneous calculated states. However, the statistical properties of these errors simplify their detection and identification. In order to determine those errors, the estimated measurements, $\hat{\mathbf{z}}$, are first calculated from (5) using the following equation for the AC case:

$$\hat{\mathbf{z}} = \mathbf{h}(\hat{\mathbf{x}}) \tag{9}$$

The individual estimated measurement error is then obtained using:

$$\hat{\mathrm{e}}_j = \left(z_j - \hat{z}_j\right) \tag{10}$$

As these errors follow a zero mean Gaussian distribution [16], techniques such as the Chi-Squares test and normalized residual have been the most common ones applied for their detection [27]. When Chi-squares test is applied, it is assumed that the state variables are mutually independent from each other and the errors follow a normal distribution. The test involves a number of iterative steps that depend on the number of degrees of freedom of the system, sum of squares $\hat{f}$ and a critical value corresponding to α satisfying the inequality:

$$\hat{f} < \chi^2_{(k,\alpha)} \tag{11}$$

where k is the appropriate number of degrees of freedom and α is a specified probability. Thus, $\hat{f}$ will be large when a large number of bad measurements are present. However, since k is large in power systems, this method allows for the removal of those measurements that are responsible for the largest standardized residuals.

2.4 False data injection attacks

FDI attacks (also known as Bad Injection attacks) is a special category of attacks targeting the SG, whereby bad measurements are injected such that they are able to bypass the bad data detection methods discussed previously. While FDI attacks can also target other cyber-physical systems, various forms of these attacks and consequences have been investigated in [11, 12, 15, 16, 28–38]. In this paper, FDI attacks will be simulated using assumptions from [26], whereby it is assumed that the system parameters and topology (system Jacobian) is known to the attackers, and [18], where a mathematical formulation for simulating the FDI attack in the AC model is provided. Additionally, FDI attacks satisfying the first assumption regarding prior knowledge of the system have been proven to result in more disastrous consequences. Moreover, in [17], the authors demonstrate how an attacker, using

that knowledge of the system matrix $\mathbf{H}_{m\times n}$, can inject an attack vector $\mathbf{a}_{m\times 1}$ to the measurement vector $\mathbf{z}_{m\times 1}$ that remains undetected from the detection techniques mentioned previously. Consequently, with the insertion of $\mathbf{a}_{m\times 1}$, the new corrupted measurement signals $\mathbf{z}'_{m\times 1}$ takes the following form:

$$\mathbf{z}'_{m\times 1} = \mathbf{z}_{m\times 1} + \mathbf{a}_{m\times 1} \tag{12}$$

Hence, this will result in the calculation of an incorrect system state vector $\mathbf{x}'_{m\times 1}$ instead of the original state $\mathbf{x}_{m\times 1}$. The difference between those states is denoted as $\mathbf{c}$ and is calculated as follows:

$$\mathbf{x}' = \mathbf{x} + \mathbf{c} \tag{13}$$

For the AC model, it is shown in [18] that the attack vector will remain undetected when it satisfies the condition:

$$\mathbf{a} = \mathbf{h}(\mathbf{x}_a) - \mathbf{h}(\mathbf{x}) \tag{14}$$

It is then proven as follows:

$$\begin{aligned}
\mathbf{r}_{attack} &= \mathbf{z}' - \mathbf{h}(\mathbf{x}') \\
&= \mathbf{z} - \mathbf{h}(\mathbf{x}') + \mathbf{h}(\mathbf{x}) - \mathbf{h}(\mathbf{x}) \\
&= \mathbf{z} + \mathbf{a} - \mathbf{h}(\mathbf{x}') + \mathbf{h}(\mathbf{x}) - \mathbf{h}(\mathbf{x}) \\
&= \mathbf{r} + \mathbf{a} - \mathbf{h}(\mathbf{x}') + \mathbf{h}(\mathbf{x}) \\
\mathbf{r}_{attack} &= \mathbf{r}_{normal} \quad (\text{since}, \quad \mathbf{a} = \mathbf{h}(\mathbf{x}_a) - \mathbf{h}(\mathbf{x}))
\end{aligned} \tag{15}$$

Consequently, in the case of nonlinear state estimation, it is more complicated to implement the FDI attack. Compared to the attack in the DC case [17], where the attacker only required knowledge of the Jacobian matrix, in the AC model, the latter is now additionally required to have some prior knowledge of the current states of the system. While it is more complicated to meet those conditions, it is still shown in [18] that such an attack is possible and the consequences can be disastrous. In both the DC and AC model, the calculation of wrong state variables, caused by this attack, can start a domino effect of incorrect control decisions leading to dire consequences. As this type of attack targets state estimation in the SG predominantly, the vector $\mathbf{a}$ can be inserted physically by tampering with the meters or wirelessly by injecting the offsets when the readings are transmitted to the SCADA. Hence, the substation state estimator (SSE), which is also an important component of the SG, will also be the target of such attacks as it plays an essential role in state estimation at the substations.

3. Architectural structure of CDS for smart grid

From a neuroscience perspective, the CDS is the entity that matches Fuster's paradigm [9] the closest as far as cognition is concerned. Basically, the CDS is made up of four components namely; environment, perceptor, executive and feedback channel. Moreover they are arranged in a very particular way. The feedback channel links the perceptor and executive, which are situated on two opposite sides. The environment finally closes the global feedback channel whereby the entire CDS is contained within it. Since the focus of this chapter is the nonlinear state estimation

and FDI attack in the SG, the AC state estimator will be considered as the environment with which the CDS interacts since it is the recipient of the measurements in the network. By acting as the supervisor of the network, the CDS empowers the state estimator, through CC, with the cognitive ability to learn during every PAC which measurements to prioritize for optimal state estimation and which to ones to discard. **Figure 1** shows the complex diagram whereby the CDS and AC state estimator are brought together for meeting the goals mentioned previously. In the next subsections, it will be elaborated how the arrangement and the role of each constituent plays a major role for goal-oriented action on the SG.

3.1 Perception-action cycle

When the environment is free of uncertainty, the PAC is responsible for updating the CDS with new information from the environment for every cycle. Thus, with the continuous acquisition of new information from this global feedback loop, the information extraction ability of the perceptor is constantly being improved with each successive cycles. Consequently, this sets up an uninterrupted cyclic directed flow of information from the perceptor to the executive to lead the PAC with the most optimal actions to be performed on the environment. As a result, this hypothesis for a goal-focused scenario is then modified with new information gained from the PAC to allow the executive to improve its current ability to achieve the primary goal that it was designed for.

3.2 Perceptor

Similar to the concept of Percept in the agent of AI [39], both in the brain and CDS, a perception process is performed on incoming measurements. The perceptor of the CDS extracts useful information from the noisy measurements, which

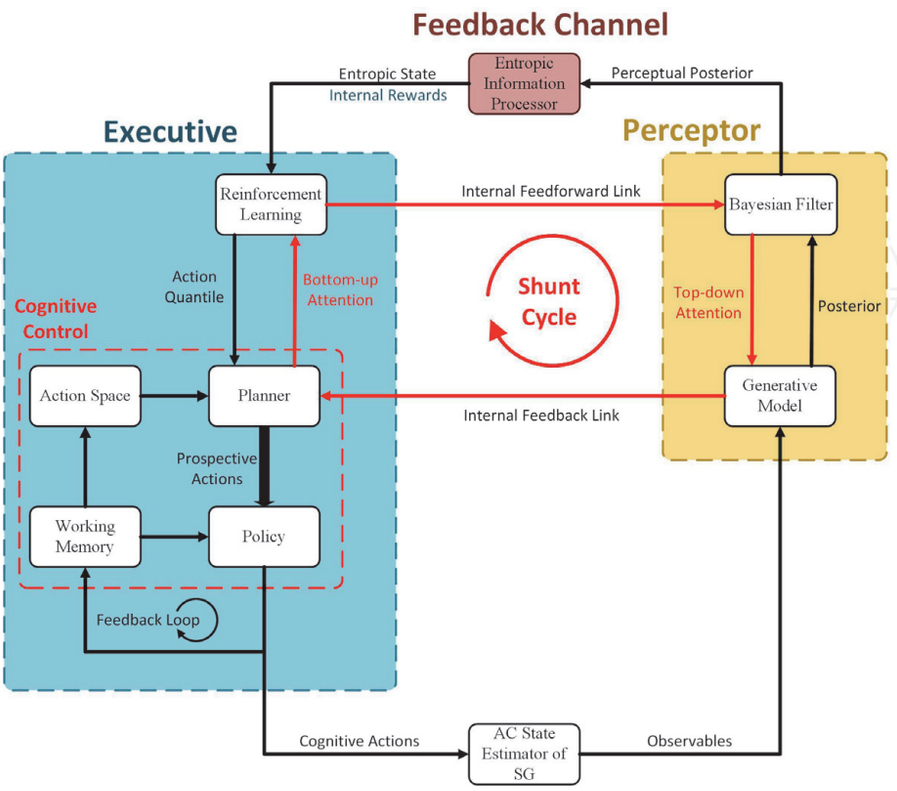


Figure 1.
Architectural structure of CDS for the nonlinear SG.

subsequently the executive uses to optimize its actions and improve the information gain for the next cycles. Those actions, performed by the executive under CC, are called cognitive actions. However unlike the role of the percept in AI, the perceptor perceives the environment directly and extracts relevant information from it which in turn the cognitive controller, residing in the executive, uses to sense the environment indirectly. In order to perform its function, the perceptor is made up of the generative model and the Bayesian filter, which are reciprocally coupled to each other.

3.2.1 Generative model

As defined in [6], the first component of the perceptor for the CDS is conceptually the *Bayesian generative model* [6], which acts as classifier for the observables received from the environment. However, in [7], it was argued that due to the dynamic nature of the SG, the Bayesian generative model would not be suitable for this specific application. Due to the complexity of the SG and its adoption for almost all applications, it is of upmost importance to detect anomalies or cyber-attacks as soon as possible before they can infect the network further, thereby starting a domino effect of cascaded problems throughout the entire network and end users. Therefore, inspired from quickest detection theory, the generative model proposed for the perceptor was based on cumulative sum (CUSUM) and is written as follows:

$$\mathbf{B}_k = \sum_{i=k-L}^{k} \mathbf{x}_i \tag{16}$$

Where k refers to the current cycle number, L is the window over which the past states is being accumulated, $\mathbf{B}_k$ is the vector retaining the cumulative sum for each cycle and $\mathbf{x}_i$ is the vector of the states' output from the AC state estimator for the cycle i. While CUSUM-based detection methods has been very effective in detecting FDI attacks in [40, 41], they fall short when the attacker has prior knowledge of the threshold applied. Indeed, the latter can then craft an attack that remains undetected. However, the CDS allows us to bypass this problem through the use of the dynamic *entropic state*, as will be elaborated later. The entropic state is the foundation of control and attack detection in this CDS structure adapted for the SG. Lastly, the CUSUM based generative model also possesses some other desirable traits such as the smoothing out of noise operating under the slow dynamics of the SG.

3.2.2 Bayesian filter

The second component of the perceptor is the Bayesian filter, which is coupled to the generative model. Although the equations describing the SG for state estimation are nonlinear in nature, we can linearize the state estimates using the *Kalman* filter and assuming that it is operating under additive white Gaussian noise [42]. Since we are assuming that the power system is quasi-static in nature in this paper [43–45], we can use the well-known Kalman filter as the Bayesian filter in the perceptor. The Kalman filter is based on the state-space model which operates on a pair of equations known as the Process equation and the Measurement equation respectively. Moreover, under quasi-static assumptions, we can assume that the state variables $\mathbf{x}$ at the time $k+1$ will only deviate by a small amount from its previous values at its previous cycle k. Consequently we can simplify this relationship to the following equation:

$$\mathbf{x}_{k+1} = \mathbf{x}_k + \omega_k \tag{17}$$

where ω_k is independent Gaussian noise vector with zero mean. Based on (17), we can propose the measurement equation as follows:

$$\mathbf{Y}_k = \mathbf{L}_k \mathbf{B}_k + \omega_k \tag{18}$$

and the covariance of matrix ω_k as:

$$\mathbf{R} = \text{diag}\left[\sigma_\omega^2\right], \sigma_\omega^2 = \text{var}[\omega_i] \tag{19}$$

As we are assuming that the system is operating under quasi-static conditions, a random walk model can be employed as the process equation as follows:

$$\mathbf{B}_{k+1} = \mathbf{F}_k \mathbf{B}_k + \mathbf{v}_k \tag{20}$$

where $\mathbf{v}_k$ is the process noise vector which is assumed to be statistically independent and zero mean. The covariance matrix of $\mathbf{v}_k$ is:

$$\mathbf{Q} = \text{diag}\left[\sigma_\text{v}^2\right], \sigma_\text{v}^2 = \text{var}[\text{v}_i] \tag{21}$$

Referring to (18) and (20), the system matrix $\mathbf{L}_k$ and the predictive transition matrix $\mathbf{F}_k$ are assumed to be identity respectively. In regards to the measurement and process equations mentioned previously, the computational steps of the Kalman filter starts with some predefined initial estimates of the states $\hat{\mathbf{B}}_{k|k}$, and predicted error covariance, $\mathbf{P}_{k|k}$, which are used for the time update steps as follows:

The predicted estimated states of the generative model and predicted error covariance, $\hat{\mathbf{B}}_{k+1|k}$ and $\mathbf{P}_{k+1|k}$ respectively, are calculated using the following equations:

$$\hat{\mathbf{B}}_{k+1|k} = \mathbf{F}_{k+1,k} \hat{\mathbf{B}}_{k|k} + \mathbf{v}_k \tag{22}$$

$$\mathbf{P}_{k+1|k} = \mathbf{F}_{k+1,k} \mathbf{P}_{k|k} \mathbf{F}_{k+1,k}^T + \mathbf{Q} \tag{23}$$

When the next cycle starts, those two estimates are then used for the measurement update stages to calculate the Kalman gain, $\mathbf{K}_k$, filtered accumulated estimate, $\hat{\mathbf{B}}_{k|k}$, and to update the process covariance matrix, $\mathbf{P}_{k|k}$, according to the equations below:

$$\mathbf{K}_k = \mathbf{P}_{k|k-1} \mathbf{L}_k^T \left(\mathbf{L}_k \mathbf{P}_{k|k-1} \mathbf{L}_k^T + \mathbf{R}\right)^{-1} \tag{24}$$

$$\hat{\mathbf{B}}_{k|k} = \hat{\mathbf{B}}_{k|k-1} + \mathbf{K}_k \left(\mathbf{Y}_k - \mathbf{L}_k \hat{\mathbf{B}}_{k|k-1}\right) \tag{25}$$

$$\mathbf{P}_{k|k} = \mathbf{P}_{k|k-1} - \mathbf{K}_k \mathbf{L}_k \mathbf{P}_{k|k-1} \tag{26}$$

As a result, through the iteration of the time update and measurement update steps, the preceding *a posteriori* estimates are used to predict new *a priori* estimates.

3.3 Feedback channel

The feedback channel has very distinctive roles in the CDS as it completes the PAC by bringing together the perceptor and the executive. It is mainly related to control and cyber-attack detection in the SG. In order for the CDS to supervise the SG, the feedback channel holds the entropic-information processor, which is tasked with calculating the *entropic state* and internal rewards during reinforcement

learning in the executive. This will be elaborated in sub-Section 3.4 (Executive) where it is more relevant to the role of the executive during planning.

3.3.1 Entropic-information processor

The directed cyclic flow of information from the perceptor to the executive is known as the *entropic state of the perceptor*. The entropic state is built on the principles of the perceptual posterior, which can be viewed as the incoming filtered posterior embodying the essence of the generative model, Kalman filter and entropy, which is derived from *Shannon's information theory* [46]. The entropic state at time k, in this architecture is calculated using:

$$h_{k|k} = \frac{\mathrm{Tr}\left\{\mathbf{P}_{k|k-1} - \left(\mathrm{diag}\left\{\hat{\mathbf{B}}_{k|k-1} - \mathbf{Y}_k\right\}^2\right)\right\}}{\mathrm{Tr}\left\{\mathbf{P}_{k|k-1}\right\}} \tag{27}$$

where Tr represents trace operator, diag{.} is the diagonal operator and $h_{k|k}$ is the entropic state. In [7], the efficiency of (27) for control and cyber-attack detection was proven and illustrated. For this reason, it will be retained for the CDS architecture being elaborated. Mathematically, (27) simplifies the information between the filtering-error covariance $\mathbf{P}_{k|k-1}$ and the error between the state estimate $\hat{\mathbf{B}}_{k|k-1}$ and current states calculated at cycle k into a single metric. The denominator of (27) normalizes the equation such that $h_{k|k}$ can only take values ranging from 0 to 1 when the environment is operating in the absence of uncertainty. The degree of disturbance affecting the SG can then be characterized through the entropic state; the lower $h_{k|k}$ is, the greater the amount of disturbance or uncertainty in the system. Since the SG will be facing different situations during its operation such as the normal day to day routine and cyber-attacks, we can further dissociate the entropic state with the two following important properties:

i. When the environment is operating in the absence of uncertainty, $h_{k|k}$ will always be positive because of the probabilistic representation of the uncertainties.

ii. When uncertainties are present, $h_{k|k}$ will fluctuate around values which are less than 1. Thus, to distinguish between normal uncertainties, such as process disturbance, due to the probabilistic nature of the environment, and abnormal uncertainties, such as cyber-attack, a suitable threshold γ can be chosen such that if $h_{k|k}$ is below γ, then this would indicate presence of attack and to switch on CRC.

3.4 Executive

From a design perspective, the Executive is the most important entity of the CDS as it is responsible for control of the SG in the absence of uncertainty. With this goal in mind, it consists of Reinforcement Learning (RL) and Cognitive Control (CC), which can be further subdivided into the action space, planner, working memory and policy.

3.4.1 Reinforcement learning: Bayes-UCB

Asides from its role in the calculation of the entropic state during each PAC, the feedback channel is also involved in the calculation of internal rewards during the

planning stages of the RL [39] algorithm in the executive. RL in the CDS is based on the current entropic state at each cycle which is subsequently used to optimize an objective function for optimal control in the network. Before we elaborate on the pivotal role of RL with the other components of the executive, Bayes-UCB [47] RL algorithm will be covered briefly in order to give an overview on how it operates. Bayes-UCB represents the current state of the art from a class of multi-armed bandit algorithms called UCB algorithms [48], which are based on the principle of optimism in the face of uncertainty. In this approach to the multi-armed bandit problem, the algorithm updates the estimate of the reward distribution for each action using a Bayesian method. The action that will be applied is then chosen according to the one that will yield the highest reward. Consequently, Bayes-UCB algorithm is an index policy that uses the prior distribution to pick a dynamic quantile of the posterior estimates for the index for each action. Hence, at each discrete time t, the algorithm will select the action A_t that satisfies the following condition:

$$A_t = \underset{a}{\operatorname{argmax}} q_a(t) = Q\left(1 - \frac{1}{t(\log(t))^c}, \lambda_a^{t-1}\right) \tag{28}$$

where $Q(\alpha, \pi)$ refers to the quantile of order α of the distribution π. Moreover, by assuming that the rewards follow a Bernoulli distribution, and when the prior distribution of each action is Beta(1,1), [49] shows that (28) can be further simplified. To maintain consistency of the used notations in this paper, (28) can be reduced to:

$$A_k = \underset{a}{\operatorname{argmax}} q_a(k) = Q(1 - \frac{1}{k(\log(k))^c}; \text{Beta}(S_a(k) + 1, N_a(k) - S_a(k) + 1) \tag{29}$$

where k is the PAC cycle number, S_a is the cumulative reward for action a, N_a is the number of times action a has been chosen and **c** is real parameter. As the CDS is a construct that draws its origin from the neuroscience of the brain, it is to be emphasized that Bayes-UCB shares many common traits to the Bayesian approach of decision making in human brains [50]. Following this brief coverage of Bayes-UCB, it will be shown in the next section, pertaining to Cognitive Control, how the RL algorithm integrates the system configuration **H** of the power grid, the generative model of the perceptor and the process model in the Kalman filter together for optimal state estimation.

3.4.2 Cognitive control

CC can be considered in many ways as the heart of the CDS as it brings together all the components, described so far, for goal oriented action on the SG. CC is made up of two important modules namely the *planner* and the *policy*. The planner is involved in the extraction of a set of prospective actions from the action-space A and their evaluation during the planning cycles (i.e., shunt cycles [6] in CDS terminology) during each PAC. Consequently, under the influence of attention from one PAC to the next, the policy learns the most appropriate actions yielding the maximum rewards to be applied. In the context of the SG, the action space consists of discrete weight values that can be attributed to the different meters. Thus, under the influence of attention, the CDS will learn the optimal weight values for the different meters for optimal state estimation. Those meters, which are detrimental for the state estimation, will be assigned lower weight values while those, which are crucial, will be given larger weight values as the CDS keeps

learning about its environment to better perform its set goal. Planning in CC brings together all the other modules previously discussed. The process starts with the selection of a randomly chosen prospective action $a_k^{i,j}$ which represents weight value a^i for meter j during cycle k. This hypothesized weight value is then applied virtually to the weight matrix $\mathbf{W}$ in (5) and (6) to form $\mathbf{W}_k^{i,j}$. $\mathbf{W}_k^{i,j}$ is then used to calculate a new planned state estimate, $\hat{\mathbf{x}}_k^p$, using the same procedures mentioned in the last paragraph of Section 2.2. Thus, the same preceding calculated state of the AC state estimator, $\mathbf{x}_{k-1}$, is used as the initial guess for the current cycle using any of those iterative techniques cited. However, the number of iterations is limited to N_p iterations this time around. Due to the different weight matrices being examined, each iteration of using a $\mathbf{W}_k^{i,j}$ will also involve a different hypothesized gain, $\mathbf{G}_k^p$, during planning. Since state estimation is computationally costly, by doing this process with a restricted number of iterations in the methodology explained, this allows the CDS to learn during the planning stages at a lower resource cost. With $\hat{\mathbf{x}}_k^p$ denoting the planned state estimate using the modified weight matrix with the hypothesized weight, the planned cumulative sum involving $\hat{\mathbf{x}}_k^p$ is then calculated:

$$\mathbf{B}_k^p = \sum_{i=k-L}^{k-1} \mathbf{x}_i + \hat{\mathbf{x}}_k^p \tag{30}$$

where $\mathbf{B}_k^p$ is the planned cumulative sum involving $\hat{\mathbf{x}}_k^p$ instead of $\hat{\mathbf{x}}_k$. Using this new cumulative sum, a planned entropic state, $h_{k|k}^p$, is subsequently calculated as follows:

$$h_{k|k}^p = \frac{\det\left\{\mathbf{P}_{k|k-1} - \left(\text{diag}\left\{\hat{\mathbf{B}}_{k|k-1} - \mathbf{B}_k^p\right\}^2\right)\right\}}{\det\left\{\mathbf{P}_{k|k-1}\right\}} \tag{31}$$

The presence of uncertainties in the environment, whether stochastic or probabilistic, will cause a deviation in the output of the generative model of the perceptor from the estimated hidden state of the Kalman filter. Hence, the goal of (31) is to reduce this divergence by finding the best configuration weights for the respective meters. This condition is satisfied whenever the $\mathbf{W}_k^{i,j}$ generates $h_{k|k}^p$ closer to the optimal value of 1, which implies that the planned estimated state of the AC state estimator reduces the propagated variation in the generative model.

3.4.3 Internal rewards

Moving forward with equations that describe the planning steps, the stage is now set to define the relationship between the previous steps and the calculation of the internal rewards during RL. The hypothesized internal rewards, $r_k^{i,j}$, associated with each prospective action $a_k^{i,j}$, for cycle k can be written as:

$$r_k^{i,j} = h_{k|k}^p - h_{k|k} \tag{32}$$

As it can be seen from (32), the objective of RL, when operating under CC, is to minimize the amount of uncertainty in the SG by searching for an improved weight configuration during every PAC that will result in a better entropic state than the previous cycle. In other words, RL attempts to restrict the amount of uncertainty or disturbance during the state estimation process to the range computed by the Kalman filter in the perceptor. Referring back to the steps described so far that led

to (32), we can see that the CDS, as defined in this specific architecture, learns from the past and present actions to pick the best actions for the future. To assist in this task, after undergoing the shunt cycles during every PAC, the working memory holds temporarily the actions that have achieved the highest quantile from Bayes-UCB in (29) and applies them to the system before starting the next PAC. Thus, when the next PAC starts and a new set of prospective actions are evaluated according to their quantile values, if any of those actions achieves a higher quantile than the quantile of its respective meter in the working memory, then the higher achieving action will replace that previously considered best action. This way of performing control in the SG can also be viewed from a Bandit perspective, whereby it can be considered as a Contextual Bandit problem where every cycle presents new situations to be faced. According to those conditions, the actions performed on the SG will modify the system configuration to a new set point, from which the RL algorithm will have to adapt. This then continues on until the CDS is brought to rest. The complete algorithm of the methodology presented in this chapter can be found in [51] where it is integrated with a cyber-attack mitigation strategy known as Cognitive Risk Control, which was not discussed in this chapter. In [51], a greater discussion on the parameters and its selection is provided and contrasted with other popular cyber-attack detection methods.

4. Computational experiments

In this section, two different experiments are carried out to show the capability of CC in this new CDS architecture adapted for the smart grid. The first experiment shows CC's potential for optimal state estimation by using the optimization of the entropic state as objective function. In the second experiment, the capability of the entropic state as an attack detector will be demonstrated in four different scenarios based on the amount of information an attacker has and his access to the sensors. As IEEE bus networks have generally been used as benchmarks for evaluation in the other papers previously referenced and relating to this topic, the IEEE 14-bus network will be used for assessing the architecture proposed in this chapter. Since this particular network comprises of a large number of measurements and states, the results for the two different experiments will focus on certain aspects of the network that are relevant to the actual simulation. For both experiments, the data used to simulate the network configuration comes from the 14-bus case file in *MATPOWER* [53] which is an Electric Power System Simulation and Optimization Tools for MATLAB and Octave. Moreover, in order to bring about the modification for the AC state estimation algorithm, the doSE function of *MATPOWER* was modified for the requirements of the architecture. Originally, the algorithm uses Honest Gaussian Newton method with a maximum number of iterations of 100 and error tolerance of 10^{-5}. It also uses a *Flat Start* initialization each time the function is called. During the *Flat Start*, all the values of the different states for the initial guess is set to 1 unit.

4.1 Cognitive control for BDD

In the first experiment, the measurement signals relating to the state values were available from the case data in *MATPOWER* [52]. For this simulation, a noisy version of those signals was then generated with a signal-to-noise ratio (SNR) of 20 dB to create $\mathbf{z}$. From the case data, 39 measurement signals are used to calculate the 29 state values of the IEEE 14-bus network, half of which are the voltage

magnitudes and the other are the voltage angles for the different busses involved. The total duration of this experiment is 2000s. The parameter L, which is the window over which the past states is being accumulated, of the generative model of the perceptor was set to 20. In regards to the initialization of the Kalman filter, the initial estimates of the values to be received from the generative model are assigned a value of 0 and the diagonal elements of $\mathbf{Q}$ were set to 0.0324. Those of $\mathbf{R}$ were assigned a value of 0.01. On the executive side of the CDS for CC, the action space is made up of 156 actions, whereby each meter can be assigned a weight value from the following: 25, 50, 100, and 200. The goal of this experiment is to highlight this architecture's properties in terms of adaptability and robustness towards optimal state estimation to changing conditions. Consequently, in order to create a perturbation in the system, the SNR of the following meters is changed to 5 dB at the mentioned times: $\mathbf{t = 1000s}$ for meter 2 and $\mathbf{t = 1200s}$ for meter 15. This simulated context can be viewed as meter malfunction or a random attack, where the attacker only has limited access to meters to perform his task. In this simulation, CC is started at $\mathbf{t = 300s}$. As mentioned in the earlier sections, CC is not started at $\mathbf{t = 0s}$ as some time (cycles) have to be allowed so that the Kalman filter can settle on the track in order for the algorithm to be operated effectively.

Referring to **Figure 2**, it can be seen that CC makes the whole network dynamic, whereby the executive of the CDS is assigning the best weight values for the meters for optimal state estimation on a cycle to cycle basis. Consequently, the cognitive controller shows it ability to learn from the current and past cycles to choose the best actions for future. Moreover, the constant modification of the weight values adds another level of nonlinearity on top of the already very complex and nonlinear AC state estimator. While this may appear to be over-complicated at first, the results show that this is not only feasible but it also makes the SG more powerful. As it can be seen in **Figure 2**, at the first instance of meter malfunction for meter 2 at $\mathbf{t = 1000s}$, this has virtually no effect on this system at all as the CDS has assigned a lower weight value to that meter compared from the rest. While **Figure 2** shows the graphs of weight values for the some of the meters pertinent to this simulation, it is left to reader to realize that all the meters are undergoing weight reconfigurations every cycle. Thus, the different respective weight values for the meters are not all the same since the cognitive controller is adapting to the probabilistic nature of the noisy signals continuously. It is also shown that the algorithm is able to apply more than one action during each PAC under a stable manner. At $\mathbf{t = 1200s}$, when meter 15 starts malfunctioning, we can now really see the capability of the architecture. As shown in **Figure 2**, it takes only a couple of cycles for the cognitive controller to learn and adapt to the new situation by lowering the weight assigned to meter 15

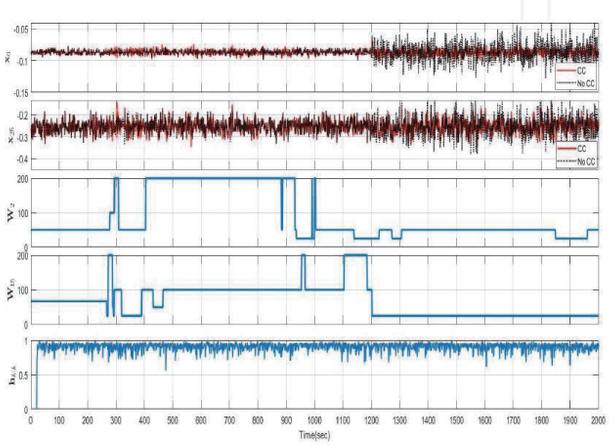


Figure 2.
Graphs of some affected states, weights and entropic state.

and compensating for it by boosting the other meters. Thus, we can see that state 6 is the most affected and state 25 is also afflicted to a lower extent. Compared to the traditional AC state estimator, the CC algorithm is able to keep this perturbation under control as demonstrated in the referenced figure. Consequently, this shows the robustness of the algorithm to adapt and act according to the evolving situations. Although some of those weight values are changed at a later point in time, this is due to the frequentist approach of the Bayes UCB coupled with the probabilistic origin of the noise. As a result of those reconfigurations in earlier situations, this highlights the cognitive ability of the controller to trust certain meters more than the others. This simulation demonstrated CC's ability to pick the best set of meters for state estimation on the go. Referring back to **Figure 2**, it can be seen the CC has performed better than the traditional algorithm. Lastly, the Chi-squares test was not implemented in this experimented as it is based on statistical properties of the signals while the approach proposed is rooted on the principle of cognition of the brain.

4.2 Cyber-attack detection

In this section, the dual property of the entropic state for FDI cyber-attack detection will be demonstrated. Previously, it was shown how the latter is an objective function for the normal running of CC under the absence of uncertainty whereby it is always positive. However, when the presence of uncertainties are no longer probabilistic, such as when an attack takes place, the entropic state will also enable early detection of such attacks. In all the cases, it is assumed that the attacker has knowledge of current states of the system. Although many specialized attacks such as replay attack or Distributed Denial of Service (DDoS) attack exist, four broad categories of FDI attacks will be considered as follows:

i. Case 1: Here we assume that the intruder has perfect knowledge of the network configuration **H** and full access to meters to commit the perfect FDI attack as described earlier. The remaining cases consider more realistic scenarios whereby the hacker faces some restrictions.

ii. Case 2: In this scenario, the intruder still has full knowledge of **H** but has limited access to meters in the grid. To simulate this attack, half of the rows of the attack vector **a** are zeroed to represent the inability to access those sensors.

iii. Case 3: Here the circumstances of case 2 are flipped around; the intruder has access to all the meters but incomplete knowledge of **H**. To carry out the attack, the entries of **H**, used to craft the attack vector, are altered in some way as an indication of the lack of information. Depending on the amount of incomplete information, this attack can have different effects. In order to simulate the attack here, some noise are added to most of the non-zero entries of the attacker's **H**. However, it is important to mention that if the attack vector was generated using an **H** matrix where the zero entries have also been altered, as a representation of more lack of information from the attacker's side, then consequences will vary. In the lower extreme, the attack will still be feasible and detected by the entropic state. In the most extreme cases, the state estimation process will not coverage and fail.

iv. Case 4: Finally, a rogue attack combining case 2 and 3 is considered. The attacker has both imperfect knowledge of **H** and constrained access to the sensors in the grid. In order to simulate this attack, the conditions used in those two cases were combined to create the attack vector.

The mentioned attacks in those different situations were simulated on the IEEE 14 bus network as shown in **Figures 3–6**. In all of the mentioned cases, the hacker's goal is to deflect the value of two of the voltage magnitudes by -0.3 and 0.4 units respectively and one voltage angle by 0.3 radians. Since attack data is not publicly available, the parameters in the *MATPOWER* package will be used to simulate the IEEE 14 bus network.

In all four attack cases, the attack is started at $\mathbf{t = 500s}$. The same parameters were used as in the previous simulation. Additionally, the property of h_k will be demonstrated as a stand-alone utility in the absence of CC. While CC is originally defined for tackling control when the uncertainties are probabilistic and h_k is

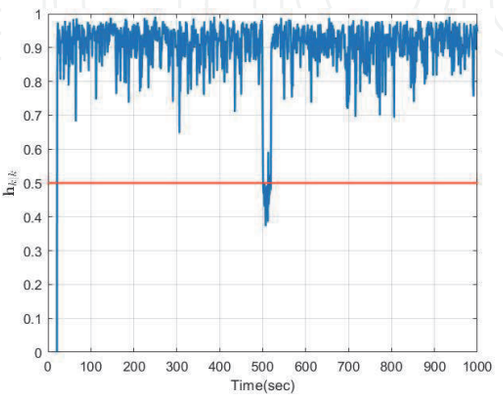


Figure 3.
Case 1.

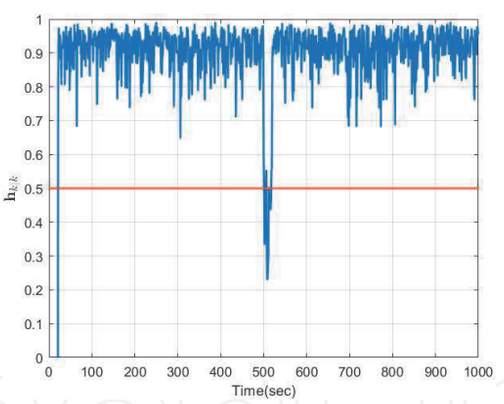


Figure 4.
Case 2.

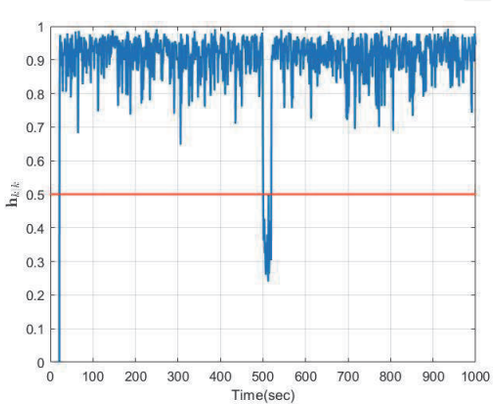


Figure 5.
Case 3.

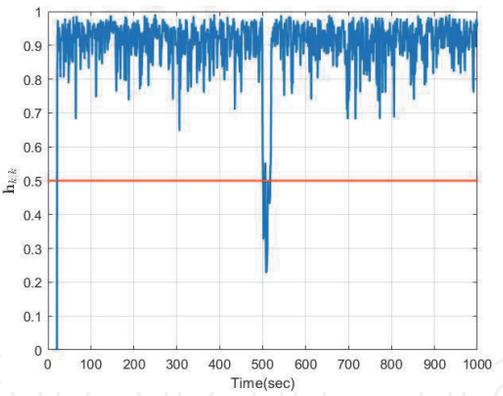


Figure 6.
Case 4.

positive, the CDS has to expand its structure its to include CRC to be able to bring risk under the control in the presence of the cyber-attacks. The implementation of CRC to this architecture can be found in chapter 4 of [51]. The results pertaining to the simulation of the attacks presented earlier are shown in **Figures 3–6**. In all four cases, by assigning a suitable γ, the attack was detected. Furthermore, it can also be seen that as the hacker has less and less information on the current grid, it becomes easier to detect the deflection as the entropic state becomes more negative. The results also displays the efficiency of the generative model, whereby the attack propagates throughout the cumulative sum up to a certain point before the Kalman filter gets back on the current track. This propagation causes h_k to become increasingly negative which consequently lends the property of detection. All the computational experiments were carried out on a system running Windows 10 with an Intel i7-8750H processor. The computational running time of the first experiment was around **40s** and the second experiment took ranged from the shortest time of **3s** for case 1 up to the longest time of **17s** for case 3 and 4. This increase in time for these two specific cases has mostly to do with the increased number of iterations required from the AC state estimator when the sensor data has lost some coherence due to the random attack vector generated as a result of lack of information.

If the CDS architecture proposed in this paper is applied in a medium or large-scale power system, the computational complexity will be lesser compared to the other current detection methods, such as the ones mentioned earlier. A greater elaboration of this technique compared to the other detection methods can be found in [7]. Moreover, the application of the CDS for an application such as the SG is revolutionary as it is a dual system catering to both the control and attack detection aspects of the SG. The main parameter of interest that needs to be scaled up for a more complex grid will be the number of shunt cycles since more meters will have to be evaluated. Nevertheless, it is recommended to keep the action space small so as to make planned rewards, during planning, distinguishable from each other. Another important hyper-parameter in the system, especially for FDI attack detection, are the values in the **Q** matrix. Unlike many tracking applications such as the simulation carried out in [5], which was supported by a mathematical formulation [53], this is not the case in our system. Thus, the contents of **Q** has be defined by the designer depending on the required sensitivity of the system towards disturbances. In order to find proper values for **Q**, prior simulations can be carried out using past historical data. Usually, it is recommended to start with very small values, like the ones used in the simulations carried out in this paper, and then tuning until the desired performance is obtained. Lastly, as the SG is scaled up, that hyper-parameter will have to be increased to reflect the circumstances of a bigger power system.

As voltage fluctuations are common occurrence disturbances in power systems, the second simulation was designed to provide the reader a greater intuition on how the algorithm is able to distinguish between what constitutes a perturbation and the normal condition. When the states of the AC state estimator is experiencing important fluctuations, this is propagated to the generative model and therefore affects the entropic state as a result. Since $h_{k|k}$ serves as an embodiment of the grid's performance, it was illustrated in the earlier simulation how those perturbation would cause a decline in the entropic state. Since the objective function of CC is to always bring $h_{k|k}$ as close as possible to 1, the optimization of $h_{k|k}$ allows CC to reduce fluctuations in the system and keep state estimation under control. Additionally, it was shown in **Figure 2** that when the attack occurred, this caused the estimated states to experience greater deviation. This was then propagated to the generative model and the Kalman filter as result, thereby causing a large drop in $h_{k|k}$ for a number of cycles. This was then successfully detected through the use of the threshold γ. Consequently, those experiments showcases the importance of each of the individual roles of the different components of the CDS and how they work together for goal oriented action on the SG.

5. Conclusion

This chapter covered the following points:

i. This is the first time that a CDS structure has been proposed for handling the nonlinear version of the SG. While previous research in this field, which were focused on bringing the CDS and the SG together, were based on the DC model, the AC model is a more realistic approach to the SG. Consequently, the new construct, which was described in the chapter, shows a lot of potential at tackling the future problems that the grid will face in the coming years as it becomes increasingly interconnected with the other aspects IT such as IoT.

ii. While there are some tradeoffs to be made due to the already inherent computational complexity of the AC state estimation algorithms, it was shown that the CC is revolutionary in the sense that it allows the application of multiple actions during every PAC while still maintaining the stability of state estimation.

iii. The CDS tailored for the AC model of the SG, proposed in this chapter, is a unique architecture that is able to make the SG more powerful by providing a new kind of control and cyber-attack detection, that are both based on cognition from the brain's perspective.

In this chapter, a new CDS based architecture was united with the SG in order to tackle the issues of nonlinear state estimation and cyber-attack detection through CC. Computational experiments were carried out to show the individual benefits of CC for optimal state estimation and FDI attack detection respectively. Moreover, it was also discussed how the algorithm and the parameters can be adjusted so that it can be scaled up to work with bigger networks. In those bigger networks comprising of a large number of meters, a function approximator such as a Neural Network [54] can employed to simplify some of the computations involved. Although this chapter focused on the problems of control on state estimation and cyber-attack in the SG, the architecture covered in this paper, can also be formulated to work for

other similar applications where state estimation is critical such as Vehicular Radar Systems. In order, to adapt the CDS for other applications, the mathematics involving the perceptor and the executive will have to be adjusted accordingly depending on the final goal of the different intended systems.

IntechOpen

IntechOpen

Author details

Mohammad Irshaad Oozeer*† and Simon Haykin†
McMaster University, Hamilton, Canada

*Address all correspondence to: oozeeri@mcmaster.ca

† These authors contributed equally.

IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] S. Haykin, "Cognitive dynamic systems [Point of view]," Proc. IEEE, vol. 94, no. 11, pp. 1910–1911, Nov. 2006.

[2] S. Haykin, "Cognitive Dynamic Systems: Radar, Control, and Radio", Proc. IEEE, Point of View Article, vol. 100, no. 7, pp. 2095–2103, July 2012.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201–220, Feb. 2005.

[4] S. Haykin, "Cognitive radar: A way of the future," IEEE Signal Process.

[5] M. Fatemi and S. Haykin, "Cognitive control: Theory and application," IEEE Access, vol. 2, pp. 698–710, Jun. 2014.

[6] S. Haykin, J. M. Fuster, D. Findlay, and S. Feng, "Cognitive risk control for physical systems," IEEE Access, vol. 5, pp. 14 664–14 679, Jul. 2017.

[7] M. I. Oozeer and S. Haykin, "Cognitive Dynamic System for Control and Cyber-Attack Detection in Smart Grid," in IEEE Access, vol. 7, pp. 78320–78335, 2019. doi: 10.1109/ACCESS.2019.2922410

[8] M. I. Oozeer and S. Haykin, "Cognitive Risk Control for Mitigating Cyber-Attack in Smart Grid," in IEEE Access, vol. 7, pp. 125806–125826, 2019. doi: 10.1109/ACCESS.2019.2939089

[9] J. M. Fuster, "Cortex and Mind: Unifying Cognition", Oxford University Press, 2003.

[10] Y. Wang, M. Amin, J. Fu, H. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids", IEEE Access 2017.

[11] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-Physical Systems Security – A Survey", IEEE Internet of Things Journal, vol. PP, no. 99, pp. 1–1, 2017.

[12] J. Hao, R.J Piechocki, D. Kaleshi, et al: 'Sparse malicious false data injection attacks and defense mechanisms in smart grids', IEEE Trans. Ind. Inf.s, 2015, 11, (5), pp. 1–12 (doi: 10.1109/TII.2015.2475695).

[13] X. Fang, S. Misra, G. Xue, D. Yang, "Smart grid - the new and improved power grid: A survey", IEEE Commun. Surveys Tutorials 2012.

[14] F. C. Scheweppe and J. Wildes, "Power system static-state estimation, Part I: Exact model," IEEE Trans. Power App. Syst., vol. PAS-89, no. 1, pp. 120–125, Jan. 1970.

[15] K. P. V. Priya, J. Bapat, "Bad Data Detection in Smart Grid for AC model", IEEE Indicon 2014.

[16] J J. Grainger and W D. Stevenson JR., "Power System Analysis 1st Edition", McGraw-Hill Series in Electrical and Computer Engineering, 1994.

[17] Y. Liu, P. Ning, M. Reiter, "False data injection attacks against state estimation in electric power grids", ACM CCS pp. 21–32 2009.

[18] Md A. Rahman, and H. Mohsenian-Rad, "False data injection attacks against nonlinear state estimation in smart power grids." In 2013 IEEE Power and Energy Society General Meeting, pp. 1–5. IEEE, 2013.

[19] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber-physical system security for the electric power grid", Proc. IEEE vol. 99 no. 1 pp. 1–15 Jan. 2012.

[20] H. Zhu and G. B. Giannakis, "Robust power system state estimation

for the nonlinear AC flow model," in Proc. IEEE North Amer. Power Symp., 2012, pp. 1–6.

[21] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," IEEE Trans. Smart Grid, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[22] A. Abur and A. Gómez-Expósito,"Power System State Estimation Theory and Implementation", 2004.

[23] A. Monticelli, "State Estimation in Electric Power System A Generalized Approach", Springer Science+Business Media New York, 1999.

[24] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid ac-based state estimation: Vulnerability analysis against cyber attacks." IEEE Transactions on Automatic Control 64.5 (2018): 1784–1799.

[25] Z. Yu, W. Chin, "Blind false data injection attack using PCA approximation method in smart grid", IEEE Trans. Smart Grid vol. 6 no. 3 pp. 1219–1226 May 2015.

[26] J. Kim, L. Tong, and R. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," IEEE Transactions on Signal Processing, vol. 63, no. 5, pp. 1102–1114, March 2015.

[27] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transactions on Smart Grid, vol. 5, no. 2, pp. 612–621, March 2014.

[28] A. Anwar, A. N. Mahmood, M. Pickering, "Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements", J. Comput. Syst. Sci. vol. 83 no. 1 pp. 58–72 2016.

[29] J. Jiang, Y. Qian, "Defense mechanisms against data injection attacks in smart grid networks", IEEE Commun. Mag. vol. 55 no. 10 pp. 76–82 Oct. 2017.

[30] P. McDaniel, S. McLaughlin, "Security and privacy challenges in the smart grid", IEEE Security Privacy vol. 7 no. 3 pp. 75–77 May/Jun. 2009.

[31] R. Deng, G. Xiao, R. Lu, H. Liang, A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks impacts and defense: A survey", IEEE Trans. Ind. Informat. vol. 13 no. 2 pp. 411–423 Apr. 2017.

[32] D. Wang, X. Guan, T. Liu, Y. Gu, Y. Sun, Y. Liu, "A survey on bad data injection attack in smart grid", Proc. IEEE PES Asia-Pac. Power Energy Eng. Conf. pp. 1–6 2013.

[33] K. Manandhar, X. J. Cao, F. Hu, Y. Liu, "Combating false data injection attacks in smart grid using kalman filter", Proceedings of International Conference on Computing Networking and Communications Communications and Information Security Symposium pp. 16–20 2014.

[34] K. Manandhar, X. Cao, F. Hu, Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter", IEEE Trans. Control Netw. Syst. vol. 1 no. 4 pp. 370–379 Dec. 2014.

[35] P.Y. Chen, S. Yang, J. A. McCann, J. Lin, X. Yang, "Detection of false data injection attacks in smart-grid systems", IEEE Commun. Mag. vol. 53 no. 2 pp. 206–213 Feb. 2015.

[36] Y. Liu, L. Yan, J. Ren, D. Su, "Research on efficient detection methods for false data injection in smart grid", International Conference on

Wireless Communication and Sensor Network (WCSN) pp. 188–192 December 2014.

[37] D. B. Rawat, C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems", IEEE Signal Process. Lett. vol. 22 no. 10 pp. 1652–1656 Oct. 2015.

[38] Y. Gu, T. Liu, D. Wang, X. Guan, Z. Xu, "Bad data detection method for smart grids based on distributed state estimation", Proc. IEEE Int. Conf. Commun. pp. 4483–4487 2013.

[39] R. S. Sutton and A. G. Barto, "Reinforcement Learning", Cambridge, MA, USA: MIT Press, 1998.

[40] Y. Huang et al., "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis", IEEE Syst. J. vol. 10 no. 2 pp. 532–543 Jun. 2016.

[41] S. Li, Y. Yilmaz, X. Wang, "Quickest detection of false data injection attack in wide-area smart grids", IEEE Trans. Smart Grid vol. 6 no. 6 pp. 2715–2735 Nov. 2015.

[42] R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems,". Journal of Basic Engineering, 82: 34–45, 1960

[43] A. S. Debs, R. E. Larson "A dynamic estimator for tracking the state of a power system", IEEE Trans. PAS vol. PAS-89 pp. 1670–1673 September/ October 1970.

[44] E. A. Blood, M. D. Ilic, J. Ilic, B. H. Krogh, "A Kalman filter approach to quasi-static state estimation in electric power systems", 38th North American Power Symposium pp. 417–422 2006 2006.

[45] A Saikia, RK Mehta, "Power system static state estimation using Kalman filter algorithm", EDP Sciences. 2016; 7: 1–7.

[46] C. E. Shannon, "A mathematical theory of communication", Bell Syst. Tech. J., vol. 27, no. 3, pp. 379–423, Jul./ Oct. 1948.

[47] E. Kaufmann, O. Cappé and A. Garivier, "On Bayesian upper confidence bounds for bandit problems" Proc. Int. Conf. Artif. Intell. Stat. pp. 592–600 2012.

[48] G. Burtini, J. Loeppky, and R. Lawrence, "A survey of online experiment design with the stochastic multi-armed bandit", CoRR, abs/ 1510.00757, 2015.

[49] E. Kaufmann, "Analysis of bayesian and frequentist strategies for sequential resource allocation", Machine Learning [cs.LG]. Télécom ParisTech, 2014. English. ¡NNT : 2014ENST0056¿. ¡tel-01413183¿

[50] P. Reverdy, V. Srivastava, N. E. Leonard, "Modeling human decision-making in generalized Gaussian multi-armed bandits", Proc. IEEE vol. 102 no. 4 pp. 544–571 Apr. 2014.

[51] Oozeer, M.I., 2020. Cognitive Dynamic System for Control and Cyber Security in Smart Grid (Doctoral dissertation). URL: https://macsphere.mcmaster.ca/handle/11375/25551

[52] R. D. Zimmerman, C. E. Murillo-SÃ¡nchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," Power Systems, IEEE Transactions on, vol. 26, no. 1, pp. 12–19, Feb. 2011.(Digital Object Identifier: 10.1109/TPWRS.2010.2051168)

[53] D. J. Kershaw and R. J. Evans, "Optimal waveform selection for tracking systems," IEEE Trans. Inf. Theory, vol. 40, no. 5, pp. 1536–1550, Sep. 1994.

[54] S. Haykin, "Neural Networks and Learning Machines", 3rd ed. Prentice-Hall, 2009.