8-1-2018

The Resilience Of Smart Energy Systems Against Adversarial Attacks, Operational Degradation And Variabilities

Parth Pradhan
Lehigh University, parth1811@gmail.com

THE RESILIENCE OF SMART ENERGY SYSTEMS AGAINST ADVERSARIAL ATTACKS, OPERATIONAL DEGRADATION AND VARIABILITIES

by

PARTH PRADHAN

Presented to the Graduate and Research Committee

of Lehigh University

in Candidacy for the Degree of

Doctor of Philosophy

in

Electrical Engineering

Lehigh University

August, 2018

Approved and recommended for acceptance as a dissertation in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

____
Date

____
Date Accepted

____
Dissertation Advisor

Committee Members:

____
Prof. Shalinee Kishore
(Committee Chair)

____
Prof. Parv Venkitasubramaniam

____
Prof. Ricky S. Blum

____
Prof. Boris Defourny

Acknowledgements

This dissertation would not have been possible without the care and support of many people during my journey as a PhD student. Their selfless efforts and contributions in transforming me from a disillusioned average Joe to a researcher with a sense of purpose is phenomenal and deserve sincere acknowledgment.

First and foremost, I would like to express utmost gratitude to my academic advisor, Prof. Shalinee Kishore. She is the embodiment of pure intellect working with whom for five years never felt like a dull and tedious experience. It was one of the happiest and proud moments of my life when she bestowed confidence on me and offered to work with her as a PhD student. Since then, she has been playing a pivotal role in shaping my research career in the field of smart energy systems. She provided me with ample support, resource and freedom to pursue research topics of my interest enabled me to grow as an independent researcher. She has also put a positive mark in my personal life by never failing to help my family at the time of trouble as well as trying in numerous ways to make them feel comfortable in the foreign land.

Secondly, I would like to express my great appreciation to Prof. Parv Venkitasubramaniam, Prof. Rick S. Blum and Prof. Boris Defourny for serving on my doctoral committee and carefully reviewing my work and providing necessary feedback. I feel fortunate to have worked with all of my committee members in various research projects where I got to learn from them the different styles of conducting meaningful research. I owe a deep sense of gratitude to Prof. Parv for instilling a passion for research in interesting topics like cyber-physical system security, anonymous networking, etc. The courses like data networks, stochastic control, information theory that he taught have tremendously helped

me deal with complex problems that I encountered in my research work with ease. His intellectual disposition, strong work ethics, ability to think mathematically made him my role model for the rest of my life. I shall also be forever indebted to his financial support during the first year of my PhD studies. I would like to thank Prof. Blum for his research collaboration on two research projects namely ocean wave power grid integration and security of wide area monitoring system. His ingenious insights, active participation, and helpful feedback contributed immensely to the timely completion of the work. Many thanks to Prof. Defourny for all the interesting and informative discussion sessions on stochastic optimization and his generous help in efficiently writing codes for designing offshore renewable farm maintenance strategy.

I would like to thank Prof. Alberto Lamadrid and Prof. Lawrence V. Snyder and Prof. Arindam Banerjee, PORTLAB faculty members, for sharing their wisdom and connecting me with right resources which kept me motivated to work on different ocean wave power technologies. Special thanks to Prof. Lamadrid for advising me on Electricity Market research and helping me learn the technicalities of writing good research papers. Sincere gratitude to staff members of ECE department, David Morrisette, Diane Hubinsky, Ruby Scott and Christine Lake for their help over these years.

I extend my appreciation to my past and present lab-mates, Abhishek Mishra, Kwami Senam Sedzro, Kostas Hatalis, Jiyun Yao, Chengbo Zhang, Omid Javidbakht, K.G. Nagananda for the camaraderie and fun-filled discussions on different research and off-research topics. I would like to thank my friends at SPCRL Lab: Basel Alnajjab, Alireza Famili, Anantha Krishna Kaarthik. Basel proved to be a rare gem as a colleague who provided constant support and motivation to sail through difficult and unfamiliar areas in ocean wave research. I would like to thank my other Lehigh friends and room-mates, Neeraj Dubey, Ramarao Vemula, Rahul Raghavendra, Avinash Balasubramaniam, Sambhawa Priya who made my stay at Lehigh a memorable one. I will forever cherish the time when I had so many around to empathize and patiently hear my common frustrations of PhD life.

This thesis would have never accomplished without the support of my family members.

My wife, Ipsita, left no stone unturned to make my PhD journey a seamless and comfortable one. Her devotion to our family, continual support and selfless desire to see me as a successful researcher have been exemplary. My two and half-year-old son, Priyansh Pradhan, has been a source of joy and positivity. I would like to extend my deepest gratitude to my father Pradip Kumar Pradhan, my mother Jayashree Pradhan and my brother Siddharth Pradhan. They have always had the highest hopes for me, and have held an unwavering faith in my abilities.

Contents

List of Tables

List of Figures

Abstract

The presented research investigates selected topics concerning resilience of critical energy infrastructures against certain types of operational disturbances and/or failures whether natural or man-made. A system is made resilient through deployment of physical devices enabling real-time monitoring, strong feedback control system, advanced system security and protection strategies or through prompt and accurate man-made actions or both. Our work seeks to develop well-planned strategies that act as a foundation for such resiliency enabling techniques.

First (chapter 1), we study the security aspect of cyber-physical systems which integrate physical system dynamics with digital cyberinfrastructure. Smart electricity grid is a common example of this system type. In this work, an abstract theoretical framework is proposed to study data injection/modification attacks on Markov modeled dynamical systems from the perspective of an adversary. The adversary is capable of modifying a temporal sequence of data and the physical controller is equipped with prior statistical knowledge about the data arrival process to detect the presence of an adversary. The goal of the adversary is to modify the arrivals to minimize a utility function of the controller while minimizing the detectability of his presence as measured by the K-L divergence between the prior and posterior distribution of the arriving data. The trade-off between these two metrics controller utility and the detectability cost is studied analytically for different underlying dynamics.

Our second study (chapter 2) reviews the state of the art ocean wave generation technologies along with system level modeling while providing an initial study of the impacts of integration on a typical electrical grid network as compared to the closest related technol-

ogy, wind energy extraction. In particular, wave power is computed from high resolution measured raw wave data to evaluate the effects of integrating wave generation into a small power network model. The system with no renewable energy sources and the system with comparable wind generation have been used as a reference for evaluation. Simulations show that wave power integration has good prospects in reducing the requirements of capacity and ramp reserves, thus bringing the overall cost of generation down.

Our third study(chapter 3) addresses robustness of resilient ocean wave generation systems. As an early-stage but rapidly developing technology, wave power extraction systems must have strong resilience requirements in harsh, corrosive ocean environments while enabling economic operation throughput their lifetime. Such systems are comprised of Wave Energy Converters (WECs) that are deployed offshore and that derive power from rolling ocean waves. The Levelized Cost of Electricity (LCOE) for WECs is high and one important way to reduce this cost is to employ strategies that minimize the cost of maintenance of WECs in a wave farm. In this work, an optimal maintenance strategy is proposed for a group of WECs, resulting in an adaptive scheduling of the time of repair, based on the state of the entire farm. The state-based maintenance strategy seeks to find an optimal trade-off between the moderate revenue generated from a farm with some devices being in a deteriorated or failed state, and the high repair cost that typifies ocean wave farm maintenance practices. The formulation uses a Markov Decision Process (MDP) approach to devise an optimal policy which is based on the count of WECs in different operational states.

Our fourth study (chapter 4) focuses on enabling resilient electricity grids with Grid Scale Storage (GSS). GSS offers resilient operations to power grids where the generation, transmission, distribution and consumption of electricity has traditionally been “just in time”. GSS offers the ability to buffer generated energy and dispatch it for consumption later, e.g., during generation outage and shortages. Our research addresses how to operate GSS to generate revenue efficiency in frequency regulation markets. Operation of GSS in frequency regulation markets is desirable due to its fast response capabilities and the corresponding revenues. However, GSS health is strongly dependent on its operation and understanding the trade-offs between revenues and degradation factors is essential. This study answers whether or not operating GSS at high efficiency regularly reduces its long-term performance (and thereby its offered resilience to the power grid).

Our fifth study (chapter 5) focuses on the resilience of Wide Area Measurement Systems (WAMS) which is an integral part of modern electrical grid infrastructure. The problem of global positioning system (GPS) spoofing attacks on smart grid endowed with phasor measurement units (PMUs) is addressed, taking into account the dynamical behavior of the states of the system. It is shown how GPS spoofing introduces a timing synchronization error in the phasor readings recorded by the PMU and alters the measurement matrix of the dynamical model. A generalized likelihood ratio-based hypotheses testing procedure is devised to detect changes in the measurement matrix when the system is subjected to a spoofing attack. Monte Carlo simulations are performed on the 9-bus, 3-machine test grid to demonstrate the implication of the spoofing attack on dynamic state estimation and to analyze the performance of the proposed hypotheses test. Asymptotic performance analysis of the proposed test, which can be used for large-scale smart grid networks, is also presented.

Chapter 1

Stealthy Attacks in Dynamical Systems: Tradeoffs between Utility and Detectability with Application in Anonymous Systems

1.1 Introduction

Cyber-physical systems such as the smart grid, structural health monitoring, and advanced transportation systems which merge traditional physical control systems with cyber communication networks are vulnerable to adversarial intrusion that aim to cripple the functioning of these systems. In particular, the integration of the cyber information layer exposes the physical system functioning to cyber security vulnerabilities which could result in tangible economic losses and physical damages to our basic infrastructural systems. Real-world incidents and scientific studies have already demonstrated the inability of the power grid to ensure a reliable service in the presence of cyber attacks [2–4]. For instance, consider the Stuxnet worm, which first came to light in 2010, and was designed to target supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes [5]. By injecting false data into the programmable logic controllers (PLC) in the SCADA systems, the worm caused critical malfunctioning of a nuclear power plant. The false injection mechanism stayed undetected for several months whilst jeopardizing a large scale energy operation. This is an example of *disruption of internal physical systems through compromised external communication links.* When our infrastructural systems are vulnerable to mere communication failures, an attack such as Stuxnet demonstrates the potential for large scale disruption at seemingly very little cost to an adversary. The lack of strong cyber-physical security is a severe impediment to the success of future engineering systems that integrate cyber and physical components and are envisioned to transform our critical infrastructures.

Mathematically, cyber physical systems merge the continuous time physical system dynamics with the predominantly discrete time data processing methodologies, which gives rise to modeling challenges [6] and the development of a standardized framework of analysis. Consequently, the study of cyber physical security has focused on specific systems, most notably the smart electricity grid and transportation systems, and the analysis of attacks and countermeasures within the milieu of those specific systems. These studies have typically focused on one-shot attacks where an adversary aims to alter system functioning instantaneously by injecting false data [2, 3, 7–9] while maintaining undetectability under a static model of the system. In this work, our goal is to study an *application independent* stochastic system framework, and investigate a dynamic data modification attack, which we refer to as *under-the-radar* attack. The key intuition behind the study of this class of attacks is the following. In a dynamic framework, every action of the adversary causes an instantaneous loss in utility and simultaneously results in an altering of the system dynamics as perceived by the physical system controller. Consequently, if the controller has prior knowledge of the typical system dynamics, the change in posterior distribution of incoming data can be used effectively to detect the presence of the adversary. From the adversary's perspective, there are two factors to balance, the tangible reward due to loss in system utility and *detectability* factor which we measure using a distance metric between the prior and posterior dynamics. Note that the problem as studied here is one of privacy *as desired by the adversary* while still compromising the operation of the system. Specifically, we present a framework to characterize the tradeoff between the utility loss and the Kullback-Liebler distance between the prior and posterior probability distributions of the captured stream. The K-L distance (or information divergence) is an accepted measure of detectability in hypothesis testing problems [10], and in this work, the detection of the presence or absence of the adversary can be viewed as a hypothesis testing problem as conducted by the control system under attack.

In this work, Markovian dynamics are used to model the prior distribution of the discrete time stochastic process representing the incoming data. In recent years Markov models and in particular discrete time Markov decision processes have been used to model CPSs such as autonomous driving [11] and water monitoring systems [12]. Classical Markov modeled systems such as Linear Quadratic Gaussian control systems (which have broad applicability to CPS), when discretized would also fit the work in this paper. Within the framework of MDPs, part of the data is vulnerable to be modified by the adversary who is aware of the prior dynamics and the detectability threshold of the controller. Under this model, the contributions of the paper are as follows. When the adversary has complete control of the incoming data, or if the state evolution is independent of input, the problem is reduced to a linearly solvable control problem as studied in [13] which provides an exact characterization of the adversary's optimal strategy and the optimal tradeoff between detectability and utility loss. For a general Markovian model, the optimal solution requires the solution of a continuous action Markov Decision Process (MDP) which become computationally impractical as the time horizon increases. For the general case, an achievable tradeoff between detectability and tangible rewards is presented using a greedy heuristic which can be characterized analytically. The proposed model is applied to a networking problem of practical interest, wherein an adversary modifies the timing of an incoming packet stream to a router so as to determine the flow of packets downstream from the router. This problem is studied from the adversary perspective wherein the goal is to balance two costs– the adversary's privacy cost measured by the K-L divergence and the network privacy cost measured by the maximum length of the packet stream whose paths can be hidden by a memory limited router. In this example, it is shown that the general formulation is solvable and yields the optimal adversary strategy.

The rest of the paper is organized as follows. The system model is described in Section 1.2. When the inputs follow an i.i.d arrival distribution, the optimal tradeoffs between utility and K-L divergence, and the optimal adversary policies are derived in Section 1.3. When the inputs follow Markovian dynamics, or an internal controller state is included in the formulation, the tradeoffs and policies are presented in Section 1.4. The network anonymity application is described and solved in detail in Section 1.5, followed by concluding remarks in Section 1.6.

1.1.1 Related Work

The study of false data injection in cyber physical systems has focused on specific applications, most notably, power systems or the smart grid. Attacks on power system state estimation, such as compromising phasor measurement unit (PMU) data streams, has drawn a lot of recent attention due to its potential impact to cripple a national infrastructure. A good majority of the studies have considered "one-shot" attacks [2, 3], wherein an adversary identifies the minimum number of data sources to compromise such that the system moves to an alternate state than the actual one, whilst maintaining perfect complete undetectability of his presence. The undetectability results typically rely on the internal security and stability assessment utilizing static estimation techniques. Introducing dynamics into the security measures can significantly improve the detectability of one-shot attacks. For instance, [14–16] consider continuous-time power system models and apply dynamic techniques to detect malicious data injection. In [15], an accurate power network descriptor model is used and necessary and sufficient conditions for identifiability of attacks based on the network topology are derived, and in [7] dynamic detection and identification procedures based on tools from geometric control theory are proposed to detect power network component failure due to false data injection. Dynamic data injection attacks were also studied in the context of linear quadratic Gaussian (LQG) systems [8,9], wherein the authors study estimation and control when some of the sensors or actuators are corrupted by an attacker with an application in power networks. Specifically, they are concerned with the number of attacks or errors that can be detected and corrected within a specified time as a function of the parameters of system dynamics. They characterize fundamental limits on undetectability of attacks and also provide a secure local control loop design that can make the system more resilient to these attacks. Note that the work in [7–9, 17, 18] also study the problem of false data injection in dynamical systems (LQG controllers and Kalman filter based estimation systems) which is thematically similar to our work. Part of the focus there is on understanding system properties that enable detection of the best adversary over a period of time. A key difference between our model and the work in these references is the MDP model is an open-loop model based on finite state probabilistic automatons whereas LQG and Kalman filter based systems are feedback controllers working with real valued parameters.

Yet another specific application where false data injection has been studied theoretically is the introduction of Byzantine data in Bayesian distributed detection [19, 20]. In Bayesian distributed detection, a group of sensors transmit observations to a fusion center which uses the received data to perform a hypothesis testing problem on the underlying source of observations. In the Byzantine version of the problem explored in [19, 20], the authors included an adversary who compromised a fraction of sensors and determined the most effective attacking strategy of the Byzantine nodes that limits the hypothesis testing performance. Their approach was based on Kullback-Leibler divergence (KLD) as a probabilistic distance between the legitimate and Byzantine data, and aims to maximize the performance of Bayesian detection under a limited Byzantine attack assuming the attack is undetectable and the data are independent across time. While our proposed approach is also based on using an informational distance measure to quantify the deviation of data from the legitimate statistical prior, it is used to study the tension *from the adversary perspective* between preserving his detectability and ability to reduce system utility. The critical challenge in our work is the dynamic nature of the system and the acausal relationship between the key variables in the system.

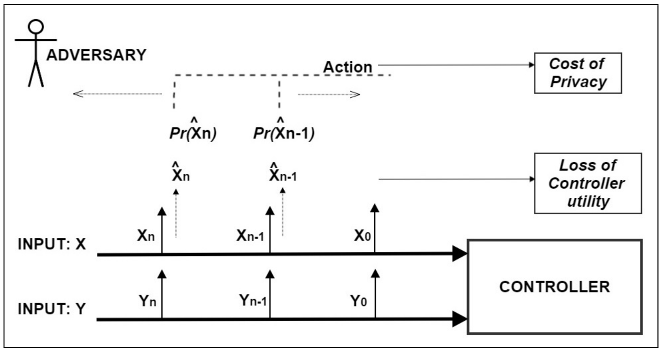


Figure 1.1: System Model

The problem as we explore in this article is similar to a class of cyberattacks referred to by the mnemonic "Frog-Boiling" [21,22], wherein typical intrusion and anomaly detectors of network traffic are fooled by modifying the data streams gradually so that detectors that can maintain limited history of data fail to detect the anomalies built up over several time steps. The work we present here is a theoretical foundational approach operating on the same principle.

1.2 Mathematical Model

Data Arrival Inputs arrive to the controller according to a discrete time stochastic process with wide sense stationary Markovian dynamics. We specifically divide the input into two separate streams $\mathbf{X} = X_1, X_2, \cdots$ and $\mathbf{Y} = Y_1, Y_2, \cdots$ wherein the pair $(x_n, y_n) \in \mathcal{X} \times \mathcal{Y}$ denotes the input data at time step n. $\mathbf{X}, \mathbf{Y}$ represent the legitimate inputs, wherein the initial pair x_0, y_0 is fixed and the inputs at subsequent time points are distributed according to the stationary transition probability matrix $\mathbb{P}_{st} = \{p_{ij|kl} i, k \in \mathcal{X}, j, l \in \mathcal{Y}\}$ and $\Pr\{X_{n+1} = k, Y_{n+1} = l | X_n = i, Y_n = j\} = p_{ij|kl}$ for all n. We represent the inputs by a pair of streams $\mathbf{X}, \mathbf{Y}$ to separate the stream $\mathbf{X}$ which can be modified by the adversary from the stream $\mathbf{Y}$ which is not accessible to him. In practice, the stream $\mathbf{Y}$ could denote information flowing through protected data links, or internal system information that is unavailable to the adversary.

Controller Reward The underlying physical system receives the inputs and performs actions that result in a utility value, denoted by a function $u : \mathcal{X} \times \mathcal{Y} \to \mathcal{R}^+$. In practice, the underlying system has an internal state and, depending on the history, current inputs and state, the controller takes an appropriate action that maximizes the net utility achieved. In this work, our goal is to study the adversarial perspective, and for this purpose the internal actions and internal state of the controller are abstracted into the instantaneous utility function $u(\cdot, \cdot)$. In section 1.4 we will include an explicit internal state variable in the model and derive the corresponding solutions. The controller is equipped with an intrusion detection mechanism whose goal is to identify the presence or absence of adversarial modification using prior knowledge of the legitimate input dynamics.

Adversary The adversary is assumed to have complete access to the data stream $\mathbf{X}$, wherein the data can be modified without restriction prior to being received by the controller. For most of our subsequent results we shall assume that the adversary can observe the stream $\mathbf{Y}$ but not modify the data on it. We denote the modified input stream by $\hat{\mathbf{X}} = \hat{X}_1, \hat{X}_2, \cdots$; the adversary's goal is to generate the modified stream $\hat{\mathbf{X}}$ such that the net utility of the controller is minimized whilst remaining *stealthy* of the intrusion detection mechanism described thenceforth. We assume, for the most part, that the adversary is privy to the internal state process of the controller [1].

Intrusion Detection The controller is equipped with an intrusion detection mechanism which is modeled as a hypothesis testing between the presence and absence of the adversary. Specifically, the mechanism uses the observed inputs $\hat{\mathbf{X}}, \mathbf{Y}$ for the statistical inference. In this work we do not explicitly model the hypothesis testing, but instead use the Kullback-Liebler divergence between the posterior distribution of $(\hat{\mathbf{X}}, \mathbf{Y})$ generated by the adversary and the prior distribution $\mathbb{P}$ as a measure of *detectability* of the adversary's presence. It is well known that under constraints on the false alarm probability, the K-L distance thus computed bounds the probability of missed-detection which the adversary aims to maximize.

Adversary Policy and Net Reward Under this system model, the action of the ad-

[1] When the state transitions are deterministic functions of the inputs, state and action, the adversary can infer the states even if he cannot "observe" them

versary is modeled by the causal conditional distribution:

$$\hat{\mathbb{P}}(\hat{X}_1, \hat{X}_2, \cdots | X_1, Y_1, X_2, Y_2, \cdots) =$$
$$\Pr\{\hat{X}_1 | X_1, Y_1\} \Pr\{\hat{X}_2 | \hat{X}_1, X_2, Y_2, X_1, Y_1\} \cdots$$

which we denote using the policy notation μ. For an n step process, the adversary's goal is to design a policy that maximizes the net reward measured by a weighted sum of the utility of the controller and the K-L divergence between the posterior and prior distributions, given by

$$\mathcal{R}(\mu) = \sum_{i=1}^{n} \lambda \left[\mathbb{E}(u(\hat{X}_i, Y_i)) \right] + (1 - \lambda) D(\hat{\mathbb{P}} || \mathbb{P})$$

where $D(\hat{\mathbb{P}}||\mathbb{P}) =$

$$\sum_{(\mathbf{x},\mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n} \Pr\{\hat{\mathbf{X}} = \mathbf{x}, \mathbf{Y} = \mathbf{y}\} \log \left[\frac{\Pr\{\hat{\mathbf{X}} = \mathbf{x}, \mathbf{Y} = \mathbf{y}\}}{\Pr\{\mathbf{X} = \mathbf{x}, \mathbf{Y} = \mathbf{y}\}} \right]$$

is the K-L divergence between the posterior and prior distributions of the observed inputs. The goal of the adversary is to design the policy μ^* that maximizes the above reward. Inherent in the above discussion is the fact that it is in the adversary's best interests to chose the optimal policy μ^* despite knowing that the controller is aware of the optimal policy μ^* and can design a detector that uses the observed inputs to identify whether the inputs were generated using the prior distribution or the posterior distribution (that is an outcome of the known optimal policy μ^*).

In practice, the optimal distribution q_n is used to randomly generate a specific action (choice of input $\hat{X}_n$) which results in a specific utility and K-L cost achieved by the adversary, which when averaged over the ensemble provides the derived optimal reward. The controller, knowing that the adversary– if he exists– is likely to use the optimal strategy, would perform the hypothesis testing accordingly and flag an alert if the detection metric exceeds a certain threshold. The controller's hypothesis testing is not explicitly considered in this work, but instead abstracted using the K-L distance.

We note that K-L distance requires that the posterior distribution is absolutely continuous with respect to the prior, which in essence limits the adversarial strategies. If the absolute continuity condition were violated, or in other words, the adversary transmitted an input that were not in the prior support, then the presence of the adversary would be revealed instantly, and consequently such scenarios are not considered in this work.

Based on the described model, in the next section, we characterize explicitly the optimal policy of the adversary when the incoming process is i.i.d, and subsequently extend the results for the general Markovian model and when an internal state process is included in Section 1.4. The optimal solution to the general process is expressed as a solution to a continuous state-action Markov Decision Process.

1.3 Optimal Tradeoff and Adversary Policy for i.i.d Input Streams

We first consider a simple system where the inputs to the controller is temporally an i.i.d. process. Mathematically, $\Pr(X_n, Y_n \mid X_{n-1}, Y_{n-1}, \cdots) = \Pr(X_n, Y_n)$. As mentioned in the mathematical model, the instantaneous cost incurred by the adversary in the process is composed of the utility cost and the detectability cost. While the utility cost is a function of instantaneous inputs, $u(X_n, y_n)$(adversary absent) or $u(\hat{X}_n, y_n)$(adversary present), the penalty due to the data modification is measured by the K-L divergence. When the input sequence is i.i.d, the K-L divergence between the distributions $\mathbb{P}$ and $\hat{\mathbb{P}}$ can be split as:

$$\begin{aligned} D(\hat{\mathbb{P}}||\mathbb{P}) = & \sum_{i=1}^{n} \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} \Pr\{\hat{X}_i = x, Y_i = y\} \times \\ & \log\left[\frac{\Pr\{\hat{X}_i = x, Y_i = y\}}{\Pr\{X_i = x, Y_i = y\}}\right] \end{aligned}$$

which is a sum of causal independent terms across time steps. Inherent in the above expansion is the fact that the adversary also chooses a policy independent across time steps. Without proof, we state that this is optimal since the adversary has nothing to gain from a utility perspective using the memory of past actions and the K-L divergence between the distribution of an i.i.d sequence and that of a sequence with memory is higher than that between two i.i.d sequences generated using the marginal distributions. As the compromised input at any given time $\hat{X}_n$ has dependency only with the inaccessible input Y_n, the action to change the probability distribution of $\hat{X}_n$ is a conditional probability $\Pr\{\hat{X}_n|y_n\}$. The unchanged joint probability $\Pr\{X_n, Y_n\}$ and changed probability $\Pr\{\hat{X}_n|y_n\}$ in the analysis below are denoted as $p(X, Y)$ and $q(\hat{X})$ respectively. In the following, the optimal adversary behavior is analyzed depending on whether the adversary can observe the data arriving from input stream $\mathbf{Y}$ or not.

1.3.1 Scenario I: Analysis with Perfect Side Information

Theorem 3.1 Let V_n^* denote the optimal weighted cost as a function of the inputs x_n, y_n realized from the random input variables X_n, Y_n at time n. Then

$$V_n^* = -(1-\lambda)\,\log(\mathbb{E}_{p(\hat{x}|y_n)}\left[\,\exp(\frac{-\lambda}{1-\lambda}u(\hat{x}, y_n))\right]), \hat{x} \in \mathcal{X} \tag{1.1}$$

where the optimal action of the adversary is given by

$$q^*(\hat{x}) = \frac{p(\hat{x} \mid y_n)\,\exp(\frac{-\lambda}{1-\lambda}u(\hat{x}, y_n))}{\Gamma_{iid_1}}, \hat{x} \in \mathcal{X} \tag{1.2}$$

where Γ_{iid_1} is the normalization constant.

Proof: Since the inputs are *i.i.d* and there is no memory utilized in the system dynamics, the optimal cost V_n^* at time n as a function of the inputs is given by solving the the greedy optimality equation from the expected cost-to-go function:

$$\begin{aligned} V_n^* = &\min_{q(\hat{x})} \big[\lambda \sum_{\hat{x}} q(\hat{x}) u(\hat{x}, y_n) + \\ &(1-\lambda) \sum_{\hat{x}} q(\hat{x}) \log\left(\frac{q(\hat{x})}{p(\hat{x} \mid y_n)}\right)\big], \hat{x} \in \mathcal{X} \end{aligned}$$

The minimization uses the idea of K-L minimization similar to linearly solvable control in [13] to derive the optimal policy and cost. The proof details are provided in the appendix as a corollary to the proof of Theorem 4.1 □.

1.3.2 Scenario II:Analysis with Unobservable Side Information

When the side information is observable to the adversary, the achieved utility when the adversary throws away the legitimate input and generates an input with identical distribution to the prior would be perfectly undetectable (and no utility change either) which is a consequence of the use of expected rewards as a metric. For there to be a difference between two sources of input using identical distributions, one legitimate and the other illegal, there ought to be *side information* related to the actual input which can be used to measure the deviation. The unmodified input stream $\mathbf{Y}$ can be viewed as this side information which the controller can use to track the possibly modified input stream $\mathbf{X}$. In particular, when the side information (or state) is not observable to the adversary, his ability to maintain his "stealthiness" is likely to reduce further. In the scenario where the adversary is not able to eavesdrop on input stream $\mathbf{Y}$, only prior knowledge of the probability distribution of Y_n can be used to derive the optimal policy and cost. Since the prior distribution of Y_n is a fixed i.i.d distribution dependent on the observed input X_n, the optimal action at time n is also dependent on the observed input X_n at time n. In the expression below, $q(\hat{X})$ refers to $\Pr(\hat{X}|X_n)$ and $\hat{x} \in \mathcal{X}$. Since the adversary cannot observe Y_n, at best he can compute the marginal distribution of $\hat{X}_n$ from the controller's perspective using his belief about Y_n given the observed X_n. In other words, if

$$\pi(\hat{x}) = \mathbb{E}_{p(Y|x_n)} p(\hat{x} \mid Y)$$

then the K-L divergence between posterior and prior as computed by the adversary is given by

$$D(\hat{\mathbb{P}} \| \mathbb{P}) = D(q(\hat{x}) \| \pi(\hat{x}))$$

The cost minimization function can be written as

$$\min_{q(\hat{x})} \left[\lambda \mathbb{E}_{q(\hat{x})} \mathbb{E}_{p(Y|x_n)} u(\hat{x}, Y) + (1 - \lambda) D(q(\hat{x}) \| \pi(\hat{x})) \right]$$

Theorem 3.2 When the adversary cannot observe the input sequence $\mathbf{Y}$, the optimal cost

$$\bar{V}_n^* = -(1-\lambda)\,\log\left(\mathbb{E}_{\pi(\hat{x})}\left[\,\exp(\frac{-\lambda}{1-\lambda}\sum_{Y} p(Y \mid x_n)u(\hat{x},Y))\right]\right) \tag{1.3}$$

and the optimal action to obtain above cost is given by

$$q^*(\hat{x}) = \frac{\pi(\hat{x})\,\exp(\frac{-\lambda}{1-\lambda}\sum_{Y} p(Y \mid X_n)u(\hat{x},Y))}{\Gamma_{iid_2}} \tag{1.4}$$

where Γ_{iid_2} is the normalization constant.

Proof: The proof follows a similar optimization technique as in Theorem 4.1 □.

Note that when side information is available, the optimal adversary strategy does not depend on the original data X_n. This is a virtue of the i.i.d assumption wherein if the adversary were to choose a policy dependent on the original data X, through a conditional distribution $\Pr\{\hat{X}_n|X_n, Y_n\}$, since the controller does not have access to the original data, the cost function would only be expressed as an expectation over the original data in which case, an equal cost can be obtained using the marginal policy $\Pr\{\hat{X}_n|Y_n\}$. However, when side information is unavailable, the optimal action and tradeoff is dependent on the observed input X_n since the observed input provides information about the unobservable input which in turn influences the expected costs at that time step.

A simple example to illustrate the trade off between the utility cost and detectability cost performed on a binary input model in Figure 1.2. The input tuple $(X_i, Y_i) \in (\{0,0\},\{0,1\},\{1,0\},\{1,1\})$ is generated randomly from an arbitrary joint probability distribution $Pr(x=0,y=0)=0.1546$, $Pr(x=0,y=1)=0.1546$, $Pr(x=1,y=0)=0.2989$ and $Pr(x=1,y=1)=0.2856$. The Utility function of the input tuple (X_i, Y_i) is defined as

$$u(X_i,Y_i) = \begin{cases} -1, & \text{if } X_i = 0, Y_i = 0 \\ -0.75, & \text{if } X_i = 1, Y_i = 1 \\ -0.50, & \text{if } X_i = 1, Y_i = 0 \\ -0.25, & \text{if } X_i = 0, Y_i = 1 \end{cases}$$

By spanning the optimization across different values of λ, a tradeoff between the utility and detectability can be obtained, which is illustrated in Figure 1.2.

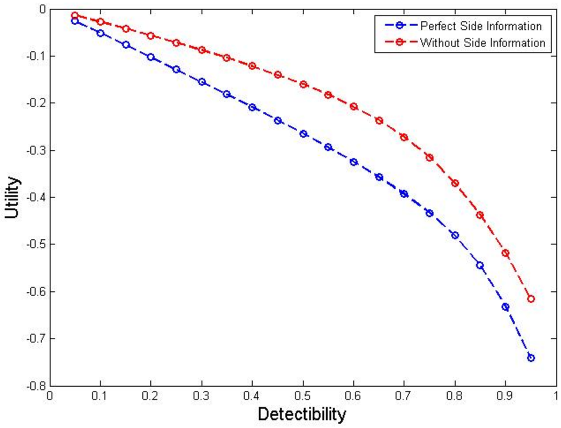


Figure 1.2: Trade Off Between Utility and Detectability in scenario 1 and 2(i.i.d input process)

As observed when adversary chooses to remain completely private (K-L cost is 0), the achieved utility does not depend on whether the adversary can observe the input $\mathbf{Y}$ or not. Since maximum stealth (minimum detectability) implies that the adversary retains the prior distribution of inputs, this observation follows. As expected, the tradeoff for the perfect side information is an *inner bound* on the tradeoff when side information is not observable. This is true mathematically; when optimizing the policy with perfect side information, the adversary can choose to ignore the available information to derive a sub-optimal policy. We shall use this argument to derive an inner bound for the general Markovian framework.

1.4 Adversary Policy and Cost under general Markovian Framework

1.4.1 Continuous State-Action general MDP Formulation for Markov Inputs and Utility independent of Controller's State

In the general Markovian framework, the adversary can arguably use the complete history (until time $n-1$) of the original and modified data sequence when designing the policy for state at time period n. However, we will present an argument that the adversary's state can be effectively captured using four variables namely $\hat{X}_{n-1}, Y_{n-1}, X_n, Y_n$. First, for any adversary policy that utilizes data variables for any time steps prior to $n-1$, the total accrued utility reward can be equivalently obtained using the marginal distribution conditioned only on the present variables. Second, due to the Markovian nature of the incoming data, the difference in K-L rewards between the original policy and the marginalized policy is always positive (since mutual information is always greater than zero). Consequently it is sufficient for the adversary to design a Markov policy based on one step memory alone.

For such a Markovian policy, the K-L cost can be split into a sum of causal rewards as $D(\hat{\mathbb{P}}||\mathbb{P}) =$

$$\begin{aligned}&\sum_{i=1}^{n} \sum_{(x,x',y,y') \in \mathcal{X}^2 \times \mathcal{Y}^2} \Pr\{\hat{X}_i = x, Y_i = y | \hat{X}_{i-1} = x', Y_{i-1} = y'\} \\ &\times \log \left[\frac{\Pr\{\hat{X}_i = x, Y_i = y | \hat{X}_{i-1} = x', Y_{i-1} = y'\}}{\Pr\{X_i = x, Y_i = y | X_{i-1} = x', Y_{i-1} = y'\}} \right]\end{aligned}$$

The reader must note that the inputs at time n , X_n and Y_n are only a part of the information to define the state of the adversary process. The state of the adversary will consist of the current value of input Y_n and X_n(original), input $\hat{X}_{n-1}$(changed) and Y_{n-1} in the previous time step. Note that in the i.i.d case, the original data X_n was not included in the decision making due to the nature of the K-L cost which results in an expectation over the original data and is thus not necessary. However, under Markovian dynamics, the present value of X_n is required for the adversary to estimate the expected future rewards which are a function of X_{n+1}, Y_{n+1} which in turn depend on the current X_n through the Markov transition probability matrix.

Optimal Tradeoff and Adversary Policy with perfect side information

The formulation of a finite horizon general MDP with continuous-state action will require following definitions:

- **Decision Epoch:** $\mathbb{N} = \{1, 2, \ldots, n, \ldots, L\}, L < \infty$

- **Adversary State:** $Z_n \in \mathbb{Z} = \{\mathcal{S}^2 \times \mathcal{T}^2\}$ such that $Z_n = (X_n, Y_n, \hat{X}_{n-1}, Y_{n-1})$. The outcomes of the random state observed at any particular time step n, i.e. $z_n = (x_n, y_n, \hat{x}_{n-1}, y_{n-1})$ is sufficient information available to the adversary.

- **Action:** Continuous action space $q_n \in [0, 1]$ such that $q_n : \mathbb{Z} \to \Pr(\hat{X}_n \in \mathcal{X} : \hat{X}_n = x_n)$. is the probability mass function for the changed input $\hat{X}_n$ that depends on the current process state Z_n.

- **Transition Probability Function:** $\mathbb{F}(z'_{n+1} \mid z_n, q_n) = \mathbb{P} \tilde{\times} q_n$ is the controlled transition of current state $Z_n = (X_n, Y_n, \hat{X}_{n-1}, Y_{n-1})$ to next state $Z_{n+1} = (X_{n+1}, Y_{n+1}, \hat{X}_n, Y_n)$ on applying an action q_n, where the tilde denotes that a matrix operation is done to exchange the 2nd element in the vector resulting from $\mathbb{P} \times q_n$ with the last one. Recollect that $\mathbb{P}$ is the stationary transition probability of uncontrolled markov chain describing the arrival of inputs from streams $\mathbf{X}$ and $\mathbf{Y}$.

- **Instantaneous Cost Function:** $\mathbb{C}_n^{q_n}$ is the weighted sum of the utility cost and the detectability cost for the adversary given by

$$\mathbb{C}_n^{q_n} = \lambda \mathbb{E}_{q_n(\hat{x})} u(\hat{x}, y_n) + (1 - \lambda) \times D(q_n(\hat{x}) \| p_X(\hat{x}))$$

  where

$$p_X(\hat{x}) = \Pr\{X_n = \hat{x} | Y_n = y_n, X_{n-1} = \hat{x}_{n-1}, Y_{n-1} = y_{n-1}\}$$

  is the conditional probability based on the prior distribution. While the state is known to the adversary, the utility cost is an expectation over the action q_n in the problem formulation. The adversary uses the optimal probability distribution, $q_n(\hat{X}_n)$ and randomly picks a value of $\hat{X}_n = x_n$ at each time step which achieves the derived reward in an expected sense.

Having defined the problem at every time step, we can make a finite horizon stochastic planning of the best possible actions or a policy $\mu = \{q_0, q_1, \cdots q_n, \cdots, q_L\}$ for L time epochs to minimize the total expected cost.

Theorem 4.1 When the input sequence $\mathbf{Y}$ is perfectly observable to the adversary, let

V_n^* denote the optimal cost-to-go at time step n. Then the optimal cost for the weighted optimization at time step n is given by

$$V_n{}^*(z_n) = -(1-\lambda)\log\left(\mathbb{E}_{p_X(\hat{x})}\left[\exp(\frac{-\lambda}{1-\lambda}u(\hat{x},y_n))\times \exp\left(\frac{-\mathbb{E}_{\mathbb{P}}[V_{n+1}{}^*(Z_{n+1})]}{1-\lambda}\right)\right]\right)$$

and the optimal action is given by

$$q_n{}^*(\hat{x}_n) = \frac{p_X(\hat{x})\exp\left(\frac{-1}{1-\lambda}(\lambda u(\hat{x},y_n) + \mathbb{E}_{\mathbb{P}}[V_{n+1}{}^*(Z_{n+1})])\right)}{\Gamma_{m1}}$$

where Γ_{m1} is the normalization constant.

Proof: The recursive Bellman equation for finite horizon case is given by

$$V_n^*(z_n) = \min_{q_n}\{\mathbb{C}_n^{q_n} + \mathbb{E}_{q_n}\mathbb{E}_{\mathbb{P}}V_{n+1}^*(Z_{n+1})\}$$

The reduction of the above equation to the form in the theorem is provided in the appendix. □.

Optimal Tradeoff and Adversary Policy with unobservable side information

When the realizations of input sequence $\mathbf{Y}$ are unobservable to the adversary, the state, as defined in the general MDP problem is not completely observable and therefore, the process is similar to a partially observable Markov Decision Process. Accordingly, the adversary maintains a belief vector over $\mathbf{Y}$ using the data sequence from input stream $\mathbf{X}$. If the prior belief (prior to observing X_n) and posterior belief (after observing X_n) of Y_n at any time step n are given by $\pi_n(y_n)$ and $\pi_{n,po}(y_n)$ respectively, the belief updates in step n are as follows:

$$\begin{aligned}
&\pi_n(y_n) \\
= \quad &\sum_y \pi_{n-1}(y) \Pr\{Y_n = y_n | X_{n-1} = x_{n-1}, Y_{n-1} = y\} \\
&\pi_{n,po}(y_n) \\
= \quad &\frac{\sum_y \pi_{n-1}(y) \Pr\{X_n = x_n, Y_n = y_n | X_{n-1} = x_{n-1}, Y_{n-1} = y\}}{\sum_{y,y'} \pi_{n-1}(y) \Pr\{X_n = x_n, Y_n = y' | X_{n-1} = x_{n-1}, Y_{n-1} = y\}}
\end{aligned}$$

In place of the variables Y_n, Y_{n-1} which are unavailable, the sufficient state for the adversary is constituted by the pair of beliefs $\pi_{n-1,po}, \pi_{n,po}$ along with the observed variables $X_n, X_{n-1}\hat{X}_{n-1}$. Conditioned on this new state, which we denote by the random variable ζ_n (realization ϑ_n), the adversary modifies the probability distribution function of $\hat{X}_n$, which we denote by $q_n(\hat{x})$. As with the i.i.d model when the side information was unavailable to the adversary, the best he can do is to compute the K-L divergence between the modified and unmodified marginal distributions. In effect, the single step K-L cost for the adversary can be written as $D(q_n(\hat{x}) \mid p_n(\hat{x}))$ where

$$\begin{aligned}
&p_n(\hat{x}) = \\
&\sum_{y,y'} \pi_{n-1,po}(y')\pi_{n,po}(y) \Pr\{X_n = \hat{x} | Y_n = y', X_{n-1} = \\
&\hat{x}_{n-1}, Y_{n-1} = y\}
\end{aligned}$$

Employing this cost into the backward induction mechanism, we get the following theorem for the optimal cost-to-go function.

Theorem 4.2: The optimal weighted reward at time step n for the general Markovian input system when side information is unobservable is given by

$$\begin{aligned}
V_n{}^*(\vartheta_n) = &-(1-\lambda)\log(\mathbb{E}_{p_n(\hat{x})}[\exp(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_{n,\mathrm{po}}(Y_n)} \\
&[u(\hat{x}, Y_n)]) \times \exp(\frac{-\mathbb{E}_{\pi_{n,po}}[\mathbb{E}_{\mathbb{P}}[V_{n+1}{}^*(\zeta_{n+1})]}{1-\lambda})])
\end{aligned}$$

by taking optimal action ${q_n}^*(\hat{x}) =$

$$\frac{p_n(\hat{x})[\mathcal{U}(\lambda,\hat{x})\text{exp}(\frac{-\mathbb{E}_{\pi_{n,po}}[\mathbb{E}_{\mathbb{P}}[{V_{n+1}}^*(\zeta_{n+1})]}{1-\lambda})]}{\Gamma_{m2}}$$

where Γ_{m2} is the normalization constant

and,

$$\mathcal{U}(\lambda,\hat{x}) = \text{exp}(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_{n,\text{po}}(Y_n)}[u(\hat{x},Y_n)])$$

Proof: The optimal cost for the weighted optimization when side information is unavailable to the adversary is given by the solution to the recursive Bellman equation for the finite horizon case

$$V_n(\zeta_n) = \text{min}_{q_n}\{\mathbb{C}_n^{q_n} + \mathbb{E}_{\pi_{n,po}}\mathbb{E}_{q_n}\mathbb{E}_{\mathbb{P}}V_{n+1}(\zeta_{n+1})\}$$

where

$$\mathbb{C}_n^{q_n} \quad = \quad \lambda\mathbb{E}_{q_n}\mathbb{E}_{\pi_{po}(Y_n)}[u(\hat{x},Y_n)] + (1-\lambda)D(q_n(\hat{x}) \mid p_n(\hat{x})).$$

The rest of the proof relies on the reduction used in the proof of Theorem 4.1 □

Although backward induction can be used to solve for the optimal policy and actions as a function of the belief and state, this process is computationally impractical for more than a few time steps due to uncountable belief space (simplex over $\mathcal{Y}$). In the subsequent section, we therefore briefly discuss methodologies to compute bounds on the optimal tradeoff that are computationally feasible.

Outer bound on the optimal tradeoff

Any sub optimal policy for the adversary would result in an outer bound on the tradeoff between utility and detectability costs. We propose the computation of an outer bound using a greedy heuristic wherein the adversary chooses an action distribution q_n

that optimizes the instantaneous rewards and ignores the rewards in future time steps. When side information is unobservable, the one-step greedy policy when applied yields the optimal cost as

$$\begin{aligned} & {V_n}^*(\vartheta_n) \\ = \quad & -(1-\lambda)\log\left(\mathbb{E}_{p_n(\hat{x})}\left[\exp\left(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_{n,\mathrm{po}}(Y_n)}[u(\hat{x},Y_n)]\right)\right]\right) \end{aligned}$$

which depends on the belief over Y_n. The action probability to achieve the optimal greedy cost turns out to be

$$q_n^*(\hat{x}) = \frac{p_n(\hat{x})\left[\exp\left(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_{n,\mathrm{po}}(Y_n)}[u(\hat{x},Y_n)]\right)\right]}{\mathbb{E}_{p_n(\hat{x})}\left[\exp\left(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_{\mathrm{po}}(Y_n)}[u(\hat{x},Y_n)]\right)\right]}$$

Since the greedy policy only maximizes instantaneous rewards, it can be causally computed (no backward induction) at every time step and is easy to implement.

Inner bound on the optimal tradeoff

Note that when the side information is observable, a sub optimal adversary can choose to ignore the available information, and any policy thus derived will obtain a tradeoff worse than the optimal adversary who uses the available side information. Stated differently, the optimal tradeoff derived for the adversary with perfect side information will serve as an inner bound to evaluate any policy derived for the adversary without side information, for instance, the greedy policy described above.

We illustrate these ideas for the general MDP framework by taking an example of binary model. The input space and utility functions are defined exactly as in the i.i.d binary input model. The 4×4 stationary transition probability matrix $\mathbb{P}$ for the input is chosen to have a form $\begin{bmatrix} \alpha & \beta & \gamma & \delta \\ \alpha & \gamma & \beta & \delta \\ \beta & \alpha & \delta & \gamma \\ \beta & \alpha & \gamma & \delta \end{bmatrix}$.

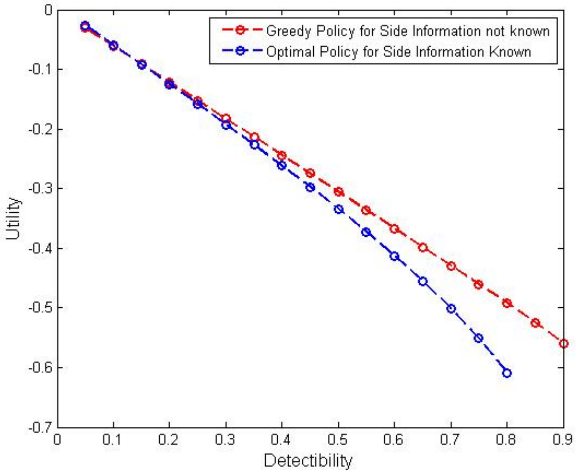


Figure 1.3: Trade Off Between Utility and Detectability for markov input process after greedy policy under scenario I when there is perfect side information(input Y known) and scenario II when there is no side information(input Y not known) and after upper bound under scenario I

For simulation, the value of α, β, γ, δ are arbitrarily assigned as 0.1,0.2,0.3,0.4 respectively. The tradeoff for the greedy policy when side information is unavailable is compared with the optimal tradeoff when side information is available. The results are plotted in Figure 1.3.

1.4.2 Continuous State-Action general MDP Formulation for I.I.D inputs with Controller's Internal State Evolution Observable

There has been no notion of Controller's State in the theoretical analysis so far. We have only considered a stylized model of the controlled dynamical system in which the incoming data to the controller directly results in its utility. In typical cyber physical systems, controllers have internal state processes which evolve as functions of the inputs and controller actions. In this section, we expand our analysis by modeling the internal state process of the controller using Markovian dynamics. Specifically, the physical system has an instantaneous internal state S_t at time instant t, where $S_t \in \mathcal{S}$ is a discrete random variable. The system receives the inputs and performs actions that result in an internal state transition, which is denoted by the stationary transition probability $w_{x,y}(s', s) = \Pr(S_{n+1} = s' \mid S_n = s, X_n = x, Y_n = y)$. As mentioned in Section 1.2, the optimal controller policy (actions) are assumed to be solved for (and history independent [2]), and consequently the transition probability can be denoted using an action independent distribution $w_{x,y}(s', s)$. Likewise, the utility is also dependent on the controller's state S_n along with the inputs at time step n and is denoted as $u(S_n, X_n, Y_n)$. Note that when the internal state process is part of the system dynamics, there is a Markovian evolution even with i.i.d inputs. In the following analysis, we shall consider the two input sequences to be i.i.d in nature and have a joint distribution $p(X, Y)$. The adversary also has complete information about the input sequences and the internal state sequence.

We note that the term state used in the paper denotes the state of the adversary's optimization. We shall continue to use it thus and apply the terminology "internal state" to denote the internal state of the controller. The state of the adversary in this model at time n is (S_n, Y_n) due to the i.i.d assumption. The value of original input variable X_n is irrelevant for the identical reason as stated in the beginning of Section III. In the following we derive the optimal policy and action for the internal state based model.

Theorem 4.3: When the internal state is observable to adversary, the optimal cost for the weighted optimization is given by

$$\begin{aligned} &{V_n}^*(s_n, y_n) \\ &= -(1-\lambda)\log\left(\mathbb{E}_{p_X(\hat{x})}\left[\exp\left(\frac{-\lambda}{1-\lambda}u(s_n, \hat{x}, y_n)\right)\times\right.\right. \\ &\left.\left.\exp\left(\frac{-\mathbb{E}_{w_{\hat{x},y_n}}\mathbb{E}_{\mathbb{P})}[V^*_{n+1}(S_{n+1}, Y_{n+1})]}{1-\lambda}\right)\right]\right) \end{aligned}$$

and the optimal action

$${q_n}^*(\hat{x}) = \frac{p(\hat{x})\exp\left(\frac{-\lambda}{1-\lambda}u(s_n, \hat{x}, y_n)\right)\exp\left(\frac{-H}{1-\lambda}\right)}{\mathbb{E}_{p_X(\hat{x})}\left[\exp\left(\frac{-\lambda}{1-\lambda}u(s_n, \hat{x}, y_n)\right)\exp\left(\frac{-H}{1-\lambda}\right)\right]}$$

where $H = \mathbb{E}_{w_{x_n,y_n}}\mathbb{E}_{\mathbb{P}}[{V_{n+1}}^*(Y_{n+1}, S_{n+1})]$

[2] For finite horizon systems with bounded rewards, the conditions for history independence can be found in [23]

Proof: The recursive Bellman's equation for finite horizon case is given by

$$V_n(s_n, y_n) = \min_{q_n}\{\lambda \mathbb{E}_{q_n(\hat{X})}[u(s_n, \hat{x}, y_n)] + (1-\lambda)\times$$
$$D(q_n(\hat{x})\,||\,p_X(\hat{x}))+\sum_{s_{n+1}}\sum_{\hat{x}}\sum_{y_{n+1}}[w_{x_n,y_n}(s_{n+1}, s_n)q_n(\hat{x})$$
$$p_Y(y_{n+1})V_{n+1}(s_{n+1}, y_{n+1})]\}$$

and the rest of the proof is a straightforward extension of Theorem 4.1. □

Note that although the inputs are i.i.d, the optimal solution requires a backward induction as stated in the theorem. This is, as mentioned earlier, an outcome of the state introducing temporal dependency across the adversarial actions. That being said, the availability of the state information results in a straightforward optimization of the action and the cost-to-go function in the Bellman equation.

1.4.3 Continuous State-Action general MDP Formulation for I.I.D. inputs with Controller's Internal State Evolution Unobservable

When the controller's internal state is unobservable to adversary, the overall adversary state is $(\pi_n(S_n), Y_n))$ that includes the adversary's belief $\pi_n(S_n) = \Pr\{S_n|Y_1^n, \hat{X}_1^n\}$ over the controller's state S_n. Based on this prior belief and the input Y_n observed, the adversary modifies the input to $\hat{X}$ using a probability distribution conditioned on the state $(\pi_n(S_n), y_n))$, which we denote by $q_n(\hat{x})$. Due to the adversarial data modification, the instantaneous utility cost as measurable by the adversary is given by $\mathbb{E}_{\pi_n}\mathbb{E}_{q_n}[u(S_n, \hat{X}_n, y_n)]$. Since there is no feedback from the state evolution to the input process, the adversary, unlike in the situation with unobservable side information, is not required to maintain a prior and posterior belief. The present input y_n, modified input $\hat{x}_n$ and the belief over present state π_n can be used to obtain the belief of the state in the subsequent step as:

$$\pi_{n+1}(s_{n+1}) = \sum_s \pi_n(s) w_{\hat{x_n},y_n}(s_{n+1}, s)$$

The optimal adversary cost from the weighted optimization is given by the solution to the recursive Bellman equation for finite horizon case of non-observable controller's state and i.i.d input process

$$\begin{aligned} V_n(\pi_n, y_n) = &\min_{q_n}\{\lambda \mathbb{E}_{\pi_n}\mathbb{E}_{q_n(\hat{X})}[u(S_n, \hat{X}, y_n)] + \\ &(1-\lambda)D(q_n(\hat{x})\,|\,p(x)) + \mathbb{E}_{\pi_n}\mathbb{E}_{q_n}\mathbb{E}_{\mathbb{P}}V^*_{n+1}(\pi_{n+1}, Y_{n+1})\} \end{aligned}$$

When the state is unobservable to the adversary, the problem of reducing the Bellman equation beyond its stated form above is as yet intractable. The primary difference between unobservable state and unobservable side information (under Markovian dynamics) is the fact that unlike the side information which evolves as an uncontrolled Markov chain with fixed transition probability, the state evolution depends on the adversary action through the modified input process $\hat{\mathbf{X}}$. Consequently the minimization in the Bellman equation is complicated by the non-standard dependence between the action and subsequent belief. We can however derive inner and outer bounds on the optimal tradeoff as was done in Section 1.4.1. An outer bound can be obtained using the greedy heuristic, wherein the action is applied to maximize the expected instantaneous reward. The optimal value function obtained on applying greedy policy is

$$V_n{}^* = -(1-\lambda)\log\left(\mathbb{E}_{p_X(\hat{X})}\left[\exp\left(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_{\mathrm{pr}}(S)}u(S, \hat{X}, y_n)\right)\right]\right)$$

which is obtained by applying an optimal action probability

$$q(\hat{x}) = p_X(\hat{x})\frac{\exp\left(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_n(S_n)}u(S_n, \hat{x}, y_n)\right)}{\mathbb{E}_{p_X(\hat{X})}\left[\exp\left(\frac{-\lambda}{1-\lambda}\mathbb{E}_{\pi_n(S)}u(S, \hat{X}, y_n)\right)\right]}.$$

While the greedy policy provides an outer bound, the optimal tradeoff between utility and detectability cost for the adversary who can perfectly observe the state would serve as an inner bound to the tradeoff when the state is not observable.

Thus far in the preceding discussion we have considered the optimal action and the detectability-utility cost tradeoff for the adversary under different scenarios. In the most general model, wherein the inputs are Markovian and the internal state and side information are not observable to the adversary, the resulting optimization would combine the POMDP framework as described in Section 4 with the state evolution factor described above; since further simplification of the Bellman equation is intractable as yet, this has been omitted here for ease of presentation. In the rest of this work, we present in detail, a practical example of an internal state based system which can be solved analytically using recursive optimization.

We consider the binary example in Section III and introduce an internal state whose transitions occur with arriving inputs. Let the controller exist in two states, denoted by S_1 and S_2. The state transition occurs as follows.

If $X = Y$, $\begin{bmatrix} p & 1-p \\ q & 1-q \end{bmatrix}$ And, if $X \neq Y$ $\begin{bmatrix} 1-p & p \\ 1-q & q \end{bmatrix}$ where p=0.2 and q=0.3.

Adversary cost is defined as

$\mathbb{C}= \begin{cases} -0.9, & \text{if } S_n = S_1 \text{and} X_n = Y_n \\ -0.1, & \text{if } S_n = S_1 \text{and} X_n \neq Y_n \\ -0.6, & \text{if } S_n = S_2 \text{and} X_n = Y_n \\ -0.4, & \text{if } S_n = S_2 \text{and} X_n \neq Y_n \end{cases}$ where X_n and Y_n are the inputs arrived at controller at time n.

Figure 1.4 plots the optimal tradeoff between utility and detectability for the adversary who can observe the internal state process and the sub optimal tradeoff derived from the greedy heuristic when the adversary cannot observe the internal state process.

1.5 Application in the study of admissible length in Anonymous Communication

In any datagram network, timing analysis can be used to trace flows of packets and thus can compromise users' anonymity [24, 25]. Specifically, the correlation between in-

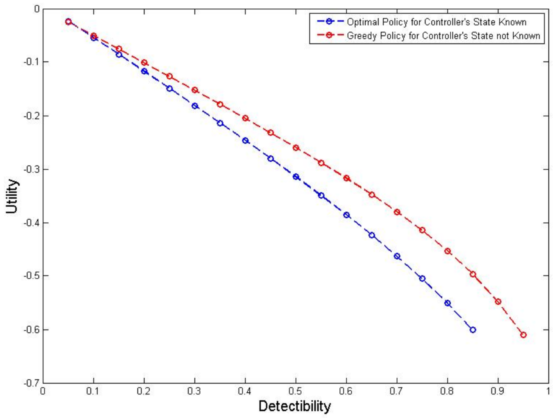


Figure 1.4: Comparison between the optimal tradeoff for an i.i.d input process when internal state of the controller is observable, and the greedy policy tradeoff when internal state is not observable

coming and outgoing streams at shared routers induced by the router scheduling policy can be used to track flows from sources to corresponding destinations. On the Internet, senders' *anonymity* is achieved using networks of Chaum mixes [26]. Chaum mixes are relay nodes or proxy servers that use a combination of encryption, packet padding and random reordering to obfuscate the source destination information of a packet. Specifically, every user transmits packets to the desired destination through a sequence of mix nodes. Each packet is encrypted in layers using public key encryption such that, every mix on the path decrypts a layer of encryption, determines the identity of the subsequent mix on the path, and transmits the packet to that mix, which in turn removes the next layer of encryption and so on. The anonymous system Tor [27] is a popular mix network used by more than half a million users.

Encryption and packet padding, however, serve only to limit information retrieval from the contents of packets. To limit the information retrieval through timing analysis, mixes typically wait until they receive packets from multiple users, randomly reorder the collected packets and transmit them in batches, thus reducing the correlation between the timing on incoming and outgoing flows. As expected, the anonymity achievable from timing analysis severely deteriorates in the presence of resource constraints on the mix such as limited memory and bandwidth. Consider a router in a data network serving packet streams from

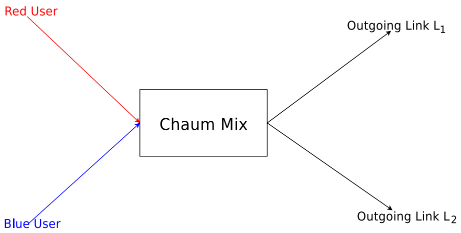


Figure 1.5: Mix receives packets from two users, encrypts and randomly reorders them, and transmits them in their corresponding outgoing link. Eve observes the arrival and departure processes.

two users with equal arrival rates as shown in Figure 1.5. If an eavesdropper does not observe any arrival or departure process, and has no prior knowledge about the sources of outgoing links, the probability of associating an outgoing link with any particular source would be the prior probability (in this case $\frac{1}{2}$ for each user). A mixing strategy provides **perfect anonymity**, if it ensures that the probability of Eve predicting the outgoing links of users correctly remains $\frac{1}{2}$, independent of the number of packets observed. No mixing strategy can, however, provide perfect anonymity using a limited buffer capacity; this can be ascertained from the fact that for a random arrival model, the probability that the sequence of arrivals contains a preponderance of packets from a single source exceeds the finite buffer size is non zero. A formal proof of this statement can be found in [28].

In effect, the objective of a memory limited mix is to maintain perfect anonymity for as long as possible, whereas the objective of the adversary is to detect the source of outgoing packets as quickly as possible. In [28], the maximum average length of the packet stream– referred to as admissible length– for which the mix can maintain perfect anonymity was evaluated for a variety of scenarios. In each of the scenarios, the mix's goal is to use a scheduling policy so that the admissible length is maximized, whereas the adversary's goal is to match the outgoing links with the respective sources as quickly as possible, or in other words, reduce the admissible length. Note that the admissible length is directly related to the duration of time before which the adversary can perfectly match the incoming and outgoing streams. In this work, we study the admissible length when the adversary can control the incoming timing in one of the processes[3]. In [31],

[3] This can be accomplished in a variety of ways including compromising access points, filling queues with spurious packets, jamming acknowledgments and suchlike [29, 30]

this problem was studied when the adversary had limited ability to modify the timing (by capturing a finite number of packets). Here we make no limiting assumptions on the adversary ability, but instead study the problem wherein the adversary aims to optimize the tradeoff between the admissible length and the detectability of his presence which fits into the main theoretical model described in this work.

1.5.1 System Model

We characterize the system model under following headings:

- **Arrival Process** Arrival process is a discrete-time system which is independent for both the users. For ease of understanding we refer to packets from the two users and red and blue packets respectively. Packets arrive at each time step according to Bernoulli process with associated probability of arrival defined below for 2 users system.

  $$\begin{aligned}\mathbb{P}_r : p_r &= \text{probability that a red packet arrives}\\ 1 - p_r &= \text{probability that a red packet does not arrive}\end{aligned}$$

  Similarly,

  $$\begin{aligned}\mathbb{P}_b : p_b &= \text{probability that a blue packet arrives}\\ 1 - p_b &= \text{probability that a blue packet does not arrive}\end{aligned}$$

- **Chaum Mix** The mix receives packets from both the users and transmits a pair of packets, one from each user, every time the buffer contains at least one packet from each user. The maximum number of packets that can be stored in the buffer is m. However, when the buffer is full of packets from only one user, the mix is forced to transmit on only one stream (and not a pair) thus revealing the source of the outgoing stream to the adversary. The total number of slots until this event occurs is defined as the *admissible length* of the system. In [28], transmitting packets from each user when the buffer has packets from all the users has been proved to be optimal strategy for maximizing admissible length.

Optimal Mixing Strategy Note that the adversary determines the source of an outgoing stream by analyzing the correlations between the timing on incoming and outgoing streams. Consequently, as long as each outgoing stream is equally correlated to all incoming streams, the system will remain in perfect anonymity (each stream equally likely to belong to each source). More specifically, if the mix ensures that at all times the number of departed packets on any outgoing link is less than the minimum number of arrivals across all incoming links, then it is possible to design a scheduling policy for all outgoing streams to have identical timing, thus maintaining perfect anonymity. This idea was used in [28] to prove that the optimal strategy for the mix is to transmit one packet of each user if and only if at least one packet from each user is present in the buffer and the buffer is not full. If the buffer is full and only packets from one user are present, then the mix is forced to transmit a single packet, at which point any adversary can identify the source of that outgoing stream. The expected number of slots required to reach this condition is defined as the **admissible length** of the system.

- **Adversary:** The adversary is allowed to alter the dynamics of the red packet arrival process. In effect the arrival probability of a red packet can be altered in every slot. In practice this can be accomplished by capturing packets or regenerating old packets by modifying acknowledgments. The objective of the adversary is to shorten the time in which the buffer is filled with packets from one user only. The adversary can only modify the red packet stream but can observe the packets on the blue packet stream.

Adversary MDP Model: By virtue of the Bernoulli arrival model and the mixing strategy, the buffer can only contain packets from one user. Since the mixing strategy is deterministic, the adversary can perfectly determine the number of packets present in the mix's buffer at every time slot. This scenario therefore falls under the observable internal state-input adversary model described in Section 4.3. Following are the specifics of the model as it pertains to this problem.

Time Horizon: The time horizon is infinite but the process has a stopping condition (when the buffer is full and a new packet arrives from the same source as that of the packets in the buffer).

Inputs: The two input processes $\{X_n\}$ and $\{Y_n\}$ are i.i.d Bernoulli processes with probabilities p_r and p_b respectively.

Internal State: The internal state at time n is defined as the number of red packets in the buffer or the negative of the number of blue packets in the buffer. The state transition is deterministic given the inputs.

$$p(s'|s,x,y) = \begin{cases} 1 \quad s' = s+1, s < M, x = 1, y = 0 \\ \quad s' = s-1, s > -M, x = 0, y = 1 \\ s' = s, x = y \\ s = M+1 \text{ or } s = -M-1 \end{cases}$$

Utility Cost: The utility cost measures the admissible length which is incremented by 1 at every step until the state reaches one of the boundaries $M+1$ or $-M-1$. In other words

$$u(s,x,y) = \begin{cases} 1 & |s| < M+1 \\ 0 & \text{o.w.} \end{cases}$$

At any state s, let $\varphi(s)$ denote the utility cost-to-go in the absence of any adversarial modification. Then, $\varphi(s)$ can be solved using the following recursion:

$$\begin{aligned} \varphi(s) = & p_r p_b \varphi(s) + (1-p_r)(1-p_b)\varphi(s) + p_r(1-p_b)\varphi(s+1) \\ & + (1-p_r)p_b\varphi(s-1) + 1 \end{aligned}$$

The proof of the above equation is available in [28] and is a special case of the Bellman equation derived in Section 4 where the adversary has no actions and $\lambda = 0$. The solution to the above recursion using boundary conditions,$\varphi(m+1) = \varphi(-m-1) = 0$ is found to be

$$\varphi(s) = 4\left[(m+1)^2 - s^2\right] \tag{1.5}$$

Now, consider a situation where adversary is allowed to change the dynamics of the red packet stream and eavesdrops to know the arrival information of blue(B) packets at each time step. Following the model is Section 4, the adversary's state at time n is given by the pair (S_n, Y_n).When the current state is $(s, B = 0)$, let the probability of a red packet arrival (as altered by the adversary) be denoted by $q_r(y, B = 0)$ and the action probability function $Q_r = [q_r \ (1-q_r)]$. Similarly, when the process state is $(s, B = 1)$, the probability mass function is denoted as $\bar{Q}_r = [\bar{q}_r \ (1-\bar{q}_r)]$. The problem is formulated as infinite horizon total cost MDP in which the action is continuous. Let the value function at state (s, B) be denoted by $\vartheta(s, B)$.

The boundary conditions are then modified accordingly as $\vartheta(m, 0) = 0$, $\vartheta(m+1, 1) = 0$
$\vartheta(-m-1, 0) = 0$, $\vartheta(-m, 1) = 0$

The Bellman equation to minimize the weighted cost for the adversary, following the result in Section 4, is given by

$$
\begin{aligned}
\vartheta(s,0) = \min_{0 \le q_r \le 1} [\lambda \mathbb{1}_{\{s \neq {}^{(m+1)}_{-(m+1)}\}} &+ (1-\lambda) D(Q_r \| \mathbb{P}_r) \\
&+ q_r p_b \vartheta(s+1,1) + q_r(1-p_b)\vartheta(s+1,0) + \\
&(1-q_r) p_b \vartheta(s,1) + (1-q_r)(1-p_b)\vartheta(s,0)] \\
\vartheta(s,1) = \min_{0 \le \bar{q}_r \le 1} [\lambda \mathbb{1}_{\{s \neq {}^{(m+1)}_{-(m+1)}\}} &+ (1-\lambda) D(\bar{Q}_r \| \mathbb{P}_r) \\
&+ \bar{q}_r p_b \vartheta(s,1) + \bar{q}_r(1-p_b)\vartheta(s,0) + \\
&(1-\bar{q}_r) p_b \vartheta(s-1,1) + (1-\bar{q}_r)(1-p_b)\vartheta(s-1,0)]
\end{aligned}
$$

where, $\mathbb{1}_{\{A\}}$ is the indicator function identifying even A.

Theorem 5.1 In a system of two users which generate packets with equal probability and a chaum mix with buffer capacity m, when the adversary can control the probability of arrival of one input stream while eavesdropping the arrival of packets from other stream, the admissible length is given by

$$\vartheta(s,0) = -2(1-\lambda)\log\Big(\frac{{k_1}^{(m+1)}({k_2}^{2(m+1)}-1)}{{k_2}^{2(m+1)}-{k_1}^{2(m+1)}}{k_1}^{s} + \frac{{k_2}^{(m+1)}(1-{k_1}^{2(m+1)})}{{k_2}^{2(m+1)}-{k_1}^{2(m+1)}}{k_2}^{s}\Big)$$

$$\vartheta(s,1) = -2(1-\lambda)\log\Big(\frac{{k_1}^{(m+1)}({k_2}^{2(m+1)}-1)}{{k_2}^{2(m+1)}-{k_1}^{2(m+1)}}{k_1}^{s-1} + \frac{{k_2}^{(m+1)}(1-{k_1}^{2(m+1)})}{{k_2}^{2(m+1)}-{k_1}^{2(m+1)}}{k_2}^{s-1}\Big)$$

where,

$$k_1 = \frac{1+\sqrt{1-\exp\left(\frac{-\lambda}{1-\lambda}\right)^2}}{\exp\left(\frac{-\lambda}{1-\lambda}\right)}, k_2 = \frac{1-\sqrt{1-\exp\left(\frac{-\lambda}{1-\lambda}\right)^2}}{\exp\left(\frac{-\lambda}{1-\lambda}\right)}$$

Proof: Using the technique similar to the theory developed in sec III and IV implemented for the infinite horizon average reward MDP, the average cost to fill the mix's buffer starting from any buffer state is found out. Details are available in the appendix. □

The admissible length is plotted against the detectability (K-L cost) in Figure 1.6. These tradeoffs are plotted for different initial state of the mix's buffer. For a system that initializes with an empty buffer the outer curve represents the adversarial detectability-utility tradeoff. When maximum stealth (zero detectability) of the adversary is imposed (no detectability), the admissible length expectedly converges to the result in [28] given by $4[(m+1)^2 - s^2]$. Figure 1.7 plots the admissible length as a function of the initial buffer state; interestingly although the mix can only alter the red packet dynamics, the admissible length-to-go as a function of the internal buffer state is symmetric– identical stopping time regardless of whether the buffer contains blue or red packets.

A Note on Countermeasures

The natural counterpart to the adversary perspective discussed thus far in this paper is that of the intrusion detection mechanism as implemented within the control system. To

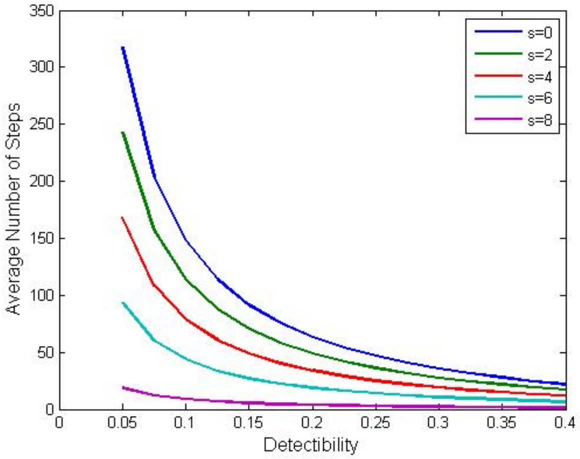


Figure 1.6: Utility Vs Detectability trade-off in a mix of buffer capacity m=8

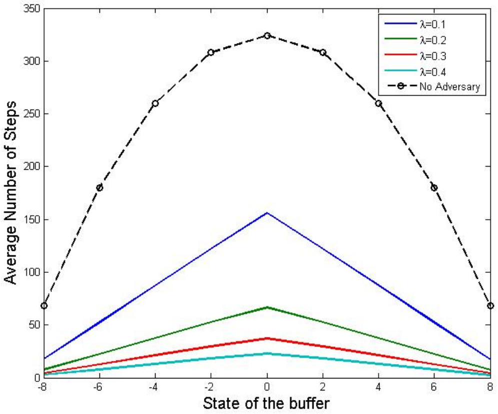
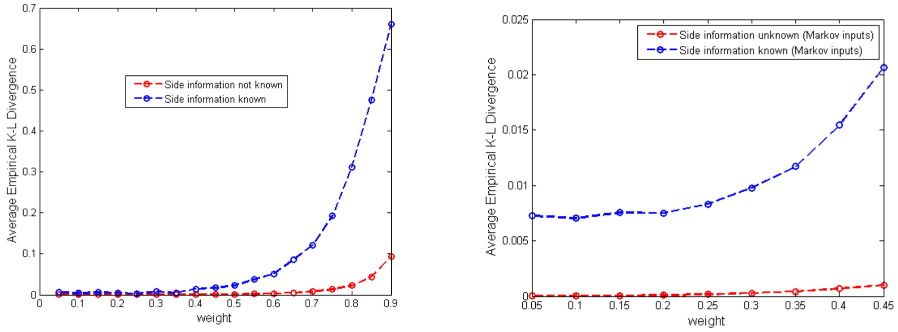


Figure 1.7: Admissible length Vs buffer state y in a mix of buffer capacity m=8

that end, Figures 1.8(a) and 1.8(b) plot the empirical K-L divergence between the observed data pattern and the prior (or expected) data pattern. The empirical K-L divergence can be computed using the empirical probability distribution of the state transitions on the pair of inputs, as when compared to the underlying prior probability distribution. From the figure one can discern that as the adversary reduces the weight on the detectability, the detection statistics increase and consequently his actions are *more detectable*. As noted in the figures, the performance by an adversary with knowledge of side information is apparently more detectable than one without side information. The primary reason for this is that as optimized, the utility function when side information is unavailable is taken as expectation over all possible side information Y which limits the ability of the adversary to increase his utility beyond a certain degree. In effect although the detectability of such an adversary is apparently lower for the same weight, the resulting utility for the adversary is also proportionately lower. In effect the availability of side information to the adversary emboldens him to cause additional damage to the system albeit at the cost of higher detectability.

Any detection mechanism that uses such an empirical statistic would likely apply a threshold depending on its tolerance for false alarm and requirement on detection rate. Depending on the chosen threshold, were the adversary to operate under the threshold his actions may fall into the ”missed detection” category and he would thus remain undetected, and were he to operate above the threshold his actions would be detected whilst causing higher damage to system operation. We do note that this is a specific example of detection statistics that can feed countermeasures but are not necessarily optimal. We do note that when the controller is aware of the attacker’s policy, then the KL divergence as derived by the attacker would be a tight bound assuming the controller utilizes an optimal detection mechanism. Were the attacker to use an alternate policy (which would have higher KL divergence than μ^*), the higher KL would result in easier detectability by the controller.



(a) Detection Statistics across the λ spectrum

(b) Detection Statistics for $\lambda < 0.5$

Figure 1.8: Empirical Kullback-Leibler Divergence as a function of weighting factor for optimal adversarial strategies with and without side information

1.6 Concluding Remarks

In this work, we presented a model to study dynamic *under-the-radar* attacks by an adversary on a dynamical system. Here, the adversary is trying to impact a system without revealing his presence. Using a weighted reward that included the utility cost and the K-L divergence, we characterized analytically, under different conditions on the underlying system dynamics, the tradeoff between the tangible impact to the system and the adversary's "stealthiness". For the Markovian model, we note that the independence over time for the attacker's policy is a mathematical consequence of the positivity of KL divergence and the fact that the randomness in one state transition is independent of the previous. Intuitively, were the adversary to use a strategy that wasnt memoryless, then the dependency across time would serve as additional information revealing his presence. A natural way forward beyond intrusion detection would be the design of countermeasures that alter the controller strategy having detected the adversary presence to obtain a desired performance whilst showing resistance to intrusion. We believe that a stochastic/multistage game formulation that includes detection and mitigation as controller actions would serve as a likely framework for the course of such an investigation.

1.7 Appendices

1.7.1 Proof of theorem 3.1,4.1

It is well known that the K-L divergence between two probability distributions $D(q(x) \mid p(x)) \geq 0$ with equality if and only if $q(x) = p(x) \forall x$. This follows from the fact that for any function $g : \mathcal{X} \mapsto \mathcal{R}^+$,

$$q(x) = \frac{g(x)}{\sum_x g(x)}$$

minimizes the divergence expansion: $\sum_x q(x) \log \frac{q(x)}{g(x)}$ The reductions in the different proofs in this work shall use the above as a fact. For a Markovian input stream with observable side information:

$$\begin{aligned}
&{V_n}^* = \min_{q_n} \{ \sum_{\hat{x}} q_n(\hat{x})[\lambda u(\hat{x}, y_n) + (1-\lambda) \times \\
&\log(\frac{q_n(\hat{x})}{p_n(\hat{x})}) + \mathbb{E}_{p_{n+1}(X_{n+1}, Y_{n+1})}[{V_{n+1}}^*]]\} \\
&= \min_{q_n} \{(1-\lambda) \sum_{\hat{x}} q_n(\hat{x})[\log(q_n(\hat{x}) \div \\
&(\exp(\frac{-\lambda}{1-\lambda} u(\hat{x}, y_n)) \times p_n(\hat{x}) \times \\
&\exp(\frac{-\mathbb{E}_{p_{n+1}(X_{n+1}, Y_{n+1})}[{V_{n+1}}^*]}{1-\lambda})))]\} \\
&= \min_{q_n} \{(1-\lambda) D(q_n(\hat{x}) \| F(\hat{x}))\} - \\
&(1-\lambda) \log(\mathbb{E}_{p_n(\hat{x})}[\exp(\frac{-\lambda}{1-\lambda} u(\hat{x}, y_n)) \times \\
&\exp(\frac{-\mathbb{E}_{p_{n+1}(X_{n+1}, Y_{n+1})}[{V_{n+1}}^*]}{1-\lambda})])
\end{aligned}$$

Using the optimal divergence expansion stated at the beginning of the proof, the Optimal cost function,

$$\begin{aligned}
{V_n}^*(z_n) = &-(1-\lambda) \log \left(\mathbb{E}_{p_X(\hat{x})} \left[\exp(\frac{-\lambda}{1-\lambda} u(\hat{x}, y_n)) \times \right.\right. \\
&\left.\left. \exp\left(\frac{-\mathbb{E}_{\mathbb{P}}[{V_{n+1}}^*(Z_{n+1})]}{1-\lambda} \right) \right] \right)
\end{aligned}$$

and the optimal action is given by

$$
\begin{aligned}
& {q_n}^*(\hat{x}_n) \\
= \quad & \frac{p_X(\hat{x})\text{exp}\left(\frac{-1}{1-\lambda}(\lambda u(\hat{x},y_n)+\mathbb{E}_{\mathbb{P}}[{V_{n+1}}^*(Z_{n+1})])\right)}{\sum_{\hat{x}} p_X(\hat{x})\text{exp}\left(\frac{-1}{1-\lambda}(\lambda u(\hat{x},y_n)+\mathbb{E}_{\mathbb{P}}[{V_{n+1}}^*(Z_{n+1})])\right)}
\end{aligned}
$$

where Γ_{m1} is the normalization constant.

Corollary We follow from the the above solution for optimal action probability when the input stream is I.I.D in nature. In that case, the expected future reward need not be considered to take a decision at the present state. The optimal decision for a given state will be independent of time n. In this scenario, the formulated problem for the markov case will be reduced to

$$
V^* = \text{min}_q\{\sum_{\hat{x}} q(\hat{x})[\lambda u(\hat{x},y_n)+(1-\lambda)\log(\frac{q(\hat{x})}{p(\hat{x})})
$$

1.7.2 Proof of theorem 5.1

We minimize

$$
\begin{aligned}
& \vartheta(s,0) = \min_{Q_r}[\lambda + (1-\lambda)[q_r[\log(\frac{q_r}{p_r}) + \frac{p_b}{(1-\lambda)}\vartheta(s+1,1) \\
& + \frac{(1-p_b)}{(1-\lambda)}\vartheta(s+1,0)] + (1-q_r)[\log(\frac{1-q_r}{1-p_r})+ \\
& \frac{p_b}{(1-\lambda)}\vartheta(s,1) + \frac{(1-p_b)}{1-\lambda}\vartheta(s,0)]]] \\
& = \lambda + (1-\lambda)\min_{Q_r}[q_r\log(\frac{q_r}{p_r\mu_1}) + (1-q_r)\log(\frac{1-q_r}{(1-p_q)\mu_2})]] \\
& = \lambda + (1-\lambda)\min_{Q_r}[\sum_{i=1}^{2} Q_r(i)\log\left(\frac{\frac{Q_r(i)}{R(i)}}{R(1)+R(2)}\right)]] \\
& -(1-\lambda)\log(R(1)+R(2))
\end{aligned}
$$

where $\mu_1 = \exp(\frac{-\lambda}{1-\lambda}[p_b\vartheta(s+1,1)+(1-p_b)\vartheta(s+1,0)])$,$\mu_2 = \exp(\frac{-\lambda}{1-\lambda}[p_b\vartheta(s,1)+(1-p_b)\vartheta(s,0)])$, $R(1) = p_r\mu_1, R(2) = (1-p_r)\mu_2$.

The optimal value function is $\vartheta(s,0) = \lambda - (1-\lambda)\log(R(1)+R(2))$. when an optimal action $Q_r(i) = \dfrac{R(i)}{\sum_{j=1}^{2} R(j)}, i \in \{1,2\}$ is applied. We can also rewrite the value function as

$$\exp\left(\frac{-\vartheta^*(s,0)}{(1-\lambda)}\right) = \exp(\frac{-\lambda}{1-\lambda})[p_r\mu_1 + (1-p_r)\mu_2] \tag{1.6}$$

Similarly,

$$\vartheta(s,1) = \min_{\bar{q}_r}[\lambda \mathbb{1}_{\{s\neq(m+1),-(m+1)\}} + (1-\lambda)D(\bar{Q}_r \mid \mathbb{P}_r)$$
$$+ \bar{q}_r p_b \vartheta(s,1) + \bar{q}_r(1-p_b)\vartheta(s,0)+$$
$$(1-\bar{q}_r)p_b\vartheta(s-1,1) + (1-\bar{q}_r)(1-p_b)\vartheta(s-1,0)]$$

gives $\exp\left(\dfrac{-\vartheta^*(s,1)}{(1-\lambda)}\right) = \exp(\dfrac{-\lambda}{1-\lambda})[p_r\bar{\mu}_1 + (1-p_r)\bar{\mu}_2]$ by taking optimal action $\bar{Q}(i) = \dfrac{\mathbb{P}_r(i)\bar{\mu}_i}{\mathbb{P}_r(1)\bar{\mu}_1 + \mathbb{P}_r(2)\bar{\mu}_2}, i \in \{1,2\}$
where $\bar{Q}(1) = q_r, \bar{Q}(2) = 1-q_r = \bar{q}_r$, $\bar{\mu}_1 = \exp[\dfrac{-1}{1-\lambda}(p_b\vartheta^*(s,1) + (1-p_b)\vartheta^*(s,0))]$ and $\bar{\mu}_2 = \exp[\dfrac{-1}{1-\lambda}(p_b\vartheta^*(s-1,0) + (1-p_b)\vartheta^*(s-1,1))]$

We are now left to solve the homogeneous non-linear recurrence equation (6) and (7). Substituting,

$$\alpha_s = \exp(\frac{-\vartheta(s,0)}{2(1-\lambda)}), \beta_s = \exp(\frac{-\vartheta(s,1)}{2(1-\lambda)}), \rho = \exp(\frac{-\lambda}{1-\lambda})$$

for better readability and assuming $p_r = p_b = \dfrac{1}{2}$ for the ease of solving the equations by making them linear, we can write ${\alpha_s}^2 = \dfrac{\rho}{2}(\beta_{s+1}\alpha_{s+1} + \beta_s, \alpha_s)$ and ${\beta_s}^2 = \dfrac{\rho}{2}(\beta_s\alpha_s + \beta_{s-1}, \alpha_{s-1})$. However, ${\alpha_s}^2 = {\beta_{s+1}}^2$. Since, both α_s and β_s are defined as positive variables, $\alpha_s = \beta_{s+1}$. Replacing the β_{s+1} with α_s and β_s with α_{s-1} in equation 5 gives

$$\alpha_s = \frac{\rho}{2}(\alpha_{s+1} + \alpha_{s-1})$$

The general solution of the above linear homogeneous recurrence equation is

$$\alpha_s = B_1 {k_1}^s + B_2 {k_2}^s$$

where $k_1 = \dfrac{1+\sqrt{1-\rho^2}}{\rho}$, $k_2 = \dfrac{1-\sqrt{1-\rho^2}}{\rho}$. Using the boundary conditions, we determine unknown coefficients to be $B_1 = \dfrac{{k_1}^{(m+1)}({k_2}^{2(m+1)}-1)}{{k_2}^{2(m+1)}-{k_1}^{2(m+1)}}$, $B_2 = \dfrac{{k_2}^{(m+1)}(1-{k_1}^{2(m+1)})}{{k_2}^{2(m+1)}-{k_1}^{2(m+1)}}$. This gives the values of $\vartheta(s,0)$ and $\vartheta(s,1)$.

Chapter 2

Prospects of Wave Power Grid Integration

2.1 Introduction

The abundance of ocean wave energy resources and their free availability have long brought interest into exploring new ways to harness their energy efficiently and profitably. The development of wave energy production towards its commercialization, however, is still in its infancy. In the seventies, key theoretical studies on wave power extraction were conducted and efforts were initiated to design and improve wave energy converter devices. Development suffered a deceleration after a few years when other means of energy became more lucrative for investment. Wind and solar technologies had a significant lead from the beginning over ocean wave energy technologies and their market grew over the years. Their levelized capital cost also dropped because of improvement in conversion efficiency. In recent years, wave energy converters (WECs), although still lagging far behind solar and wind in the scale of power production, are gaining attention and renewed confidence globally on their role to meet ever increasing demands while also complying to stringent environmental norms. Wave power extraction, now a third generation renewable, is rapidly maturing to compete with some of the costly energy alternatives like diesel while establishing itself as a valuable member of many renewable portfolios. It also fits the distributed generation model which stresses local consumption of electricity whereby reducing some of the inefficiencies of the T&D system. Several utility scale WEC projects are at various stages of development in the U.S., Coastal Europe and Australia.

The objective of this paper is to propose a methodology to study wave power extraction and analyze its potential for integration into electricity markets. A major drawback of integrating renewable resources into the grid lies in their inherent variability. Current literature on wave energy is unclear on what is the inherent variability of wave power and what this variability means to integrating WECs and arrays of WECs to the grid. In this work, we develop a preliminary model and results to close this knowledge gap. Specifically, we demonstrate that wave power integration may in fact be economically promising based on certain performance criteria. This article is organized as follows. Section 2.2 reviews the state of the art of wave energy converters and some of the underlying principles of wave power extraction. In section 2.3, we explain the calibration and data processing for the model. Section 2.4 describes the electrical bus network system employed for the integration study, and analyzes the system level impacts for wave power penetration close to 10%. A comparison to a similar deployment with wind power is also provided. Section 2.5 concludes the paper.

2.2 Background

2.2.1 Current status of wave power generation technologies

There are different techniques proposed for on-shore, near-shore and off-shore wave energy extraction. The process of energy generation goes through a series of steps which includes absorption of energy from ocean waves by different types of energy capture mechanisms, transmission of mechanical power to the electrical generator by power take off mechanisms, and control of the output power with suitable power electronics [32]. The conditioning of power to make it appropriate for an electrical grid using battery storage has also been proposed, along with systems employing arrays of WECs.

A closer look at the recent developments of wave energy technologies gives a very promising picture. The leading energy capture designs, based on their operating principles, are broadly classified into Oscillating water column (OWC) type, Oscillating body and Overtopping device. Although OWC technology was initially developed to work onshore, the feasibility of offshore deployment is also being explored. The changing ocean water level inside a chamber causes the trapped air above it to contract or expand thus driving the turbine. LIMPET, with a total installed capacity of 500kW was one of the first successful projects built on OWC technology at the Scottish Island of Islay, UK [33]. The OCEANLINX project is another effort with a cluster of offshore OWCs operated as a single unit by the Australian Renewable Energy Agency (ARENA) and is expected to generate 91,000 terawatt-hours of electricity annually [34]. Oscillating Body, as the name suggests, makes use of translational and/or rotational motion of a shaft as the first step of the wave energy conversion process. The PowerBuoy by Ocean Power Technologies (OPT), and Pelamis, by Pelamis Wave Power, are two projects based on the principle of the oscillating body technique which have shown good prospects to move from lab scale devices to utility scale plants. Six commercial wave farm projects of Pelamis P2 devices are at various stages of development in Europe with installed capacities ranging from 10 to 50 MW [35]. The PowerBuoy has already been tested in Scotland, Spain and Hawaii, and future large-scale projects are underway for Portland (Australia), Cornwall (UK), and Coos Bay (Oregon, US) [36]. Overtopping devices are a third type of energy capture mechanism which harness energy from the incoming waves by capturing them in a central reservoir and releasing them back to the sea through a number of hydroelectric turbines. The multi MW Wave Dragon projects is an example of this type developed in Denmark and Portugal [37].

The power take off (PTO) unit is an internal system connecting the energy capture device to the electrical generator. Based on the medium of energy transfer, it can be broadly classified as having OWC PTO, Hydraulic PTO, or direct drive PTO mechanisms. The air turbine in OWC operates as its PTO system while employing an active control strategy to match the turbine speed with the air velocities driving it. The hydraulic PTO makes use of a combination of two accumulators and a piston with check valves which functions as a half-wave rectifier allowing the oil to only flow in one direction, either to the motor or turbine. It is a complicated system with many moving parts that can cause regular wear-and-tear and oil leakage. Pelamis devices employ this kind of PTO inside each one of the segments in their long structure. Direct drive PTOs, as the name suggests, have a single shaft or a shaft coupled with rotating gears to generate electrical energy through its movement in between two permanent magnets. Most of the point-absorber-based WECs including Power Buoys and AWS, have adopted direct drive PTO mechanisms [32]. These are active and passive control mechanisms proposed for both the hydraulic type and direct drive PTOs.

The development of efficient power conditioning makes use of most of available technologies. Optimizing the output power from a number of wave energy converters under a stochastic ocean environment before injecting it to the grid, generally involves more challenging issues.

2.2.2 Variability Studies of wave

Significant wave height and average wave period contribute to wave power variability [32]. [38] argues that there is seasonal variability of wave power and that the capacity value of wind and wave power is comparable. On the other hand, the variability of the wave power was compared to wind power in [39] and it was shown that there is a significant difference in the variability of wind and wave power outputs based on the wave data collected from different locations around the globe. The capacity value for wind power is also reported to be lower than that for wave power in that paper. It seems that the studies so far have conflicting rather than concrete findings regarding the relative variability of wave and wind. [40] demonstrates that a judicious mix of different renewable power resources (which includes wind, solar, and wave) instead of a single dominant power source can lower the reserve requirements on the transmission network. In this kind of set-up, net generation becomes more stable because the various variabilities tend to average out as these variabilities are unrelated.

2.2.3 Need for short term variability assessment

While hourly wind and wave data can effectively assess annual power production and help one decide on site selection for wind and wave farm installation, it may prove insufficient for intra-hour operation and planning such as frequency regulation, power dispatch scheduling, providing price signals to generator owners for bidding, and making short-term prediction of power outputs necessary for electricity markets. These opportunities may receive serious consideration once this renewable power is viewed as a dispatchable generation. Active studies are being carried out to understand the effect of increased penetration of these renewable resources in European Electricity market on a short-term, medium-term, and long-term scales [41].

2.3 Methodology

2.3.1 Data Description, Wave Data

This study focuses on quantifying the short-term variability of wave power by using high resolution measured data of ocean waves. The wave data is obtained from Belmullet Berth B (Lat 54.23, Long -10.14), a high wave energy potential region in the northwest coast of Ireland. The energy density in this area is estimated to be around 76kW [42].

The two months of sampled raw wave data include significant wave height and average period reported three times every ten minutes. We pre-processed this data to eliminate missing values and irregularities, and obtain data for every ten-minute interval compatible with available wind data. The reason for choosing ten minutes as data resolution is explained later.

Instead of solving for the potential wave analytically, we obtain wave power outputs using the Pelamis P2 device with rated capacity of 750kW power matrix of the wave energy converter [43]. The power matrix provides the average power with significant wave height and wave period as inputs. The power matrix was originally designed to estimate the change in power production corresponding to changes larger than 0.5 meters and 0.5 seconds in significant wave height and wave period, respectively. As this study aims to

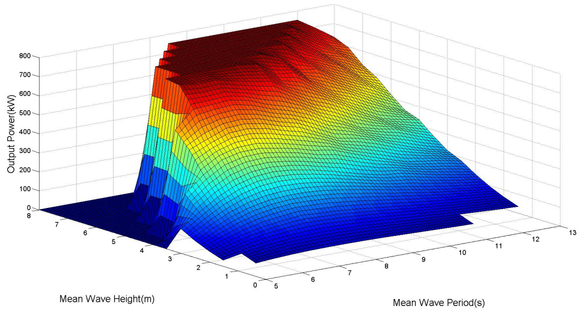


Figure 2.1: Interpolated power matrix

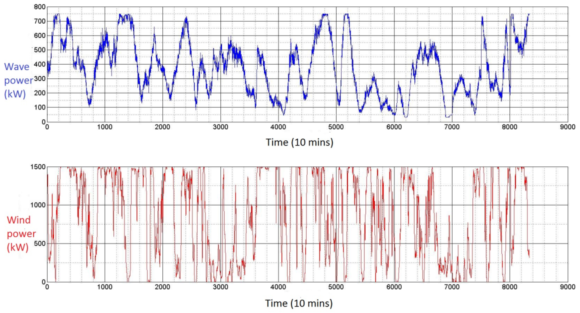


Figure 2.2: Time series of wind power (top) and wave power (bottom)

capture smaller variability of wave power, a bilinear interpolation method is employed to extend the power matrix to such cases. Figure 2.1 shows the interpolated power matrix.

2.3.2 Data Description, Wind Data

The wind speed is obtained from the NREL-EWITS data set [44] of wind speed reported in ten minute intervals. The wind data is coherent with the wave data in terms of number of samples and time during which it is collected. The wind speeds are then applied to power curve of a commercial wind turbine [45].

Figure 2.2 shows the output power obtained from wind and wave.

Figure 2.3 shows an example time series plot of wave height and wave power. The wave power depends on both the mean wave height and the average wave period, with wave height dominating the relation over time. This observation allows us to simplify the state transitions over time, assuming that the wave period plays no role in the wave power variability. Thus, potential wave power is approximated using only the information on

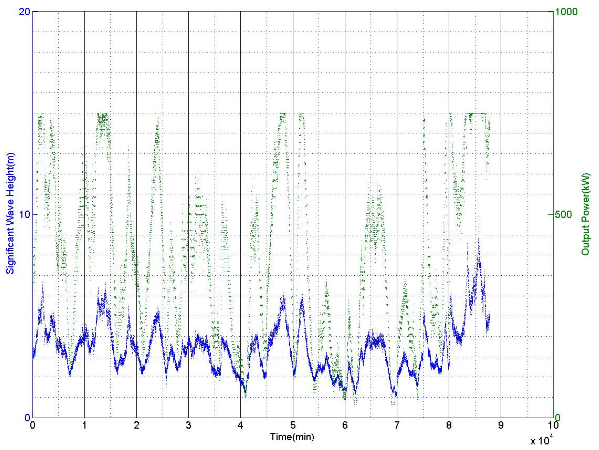


Figure 2.3: Wave height and wave power comparison

wave height, and state transition probability matrices are calculated using this parameter for the clustering. In future work we will use both wave height and wave frequency to determine the clustering for the determination of the transition probability matrices.

Wind power, on the other hand, depends only on the wind speed.

2.3.3 Time Transitions of simulation inputs

The wave height and wind speed of the renewable resources are modeled using Markov chains for the quantification of short-term variability. To characterize the variability of wind speed and wave height, the wind speed and the wave height are partitioned into four groups using a k-means clustering methodology [46]. The number of clusters, corresponding to a number of expected states of the system, is chosen to be four for simplification of the stochastic optimization problem discussed in Section 2.4. For the transition probability matrix, the entire data is divided into blocks of 24 hours and each day is divided into 144 time horizons (24 hours × 6 10-minute intervals). This kind of multi-period approach helps to capture the similarity in the nature of variability at a particular time period every day [47]. Therefore, 144 transition probability matrices are required for every the transitions which are then used for scheduling day-ahead power dispatch and provision of ancillary services. The values of the available power for 10-minute intervals belong to one of these states, namely high power availability, low power availability, and two intermediate scenarios.

The 144 standardized vectors of maximum power availability in each state are also created for each one of the 10-minutes intervals in a day. Thus, two sets of the above two inputs are created, one each for the wind and wave. This kind of model allows tractability of the problem.

We assume nameplate capacity levels of 100 MW for both wave and wind power. This penetration level, slightly over 10%, provides observable effects. We simulated single wave and wind generators, as opposed to farms of devices. There is little to no study on the variability of the power from several wave devices. Therefore, the maximum power availability from wave generators is linearly scaled. Although there are methodologies to estimate wind farm output from a single representative time series of wind power, we scaled linearly the power availabilities for wind, to ensure a level playing field.

Two standard load profiles are used, one for the summer and one for the winter, to study the effect of renewable power in the electrical grid in two different seasons. The summer load profile has a prominent peak at the middle of the day whereas in the winter profile, there are two peaks one occurring during the late morning hours and second one is a large peak occurring during late evening hours There is no uncertainty in the load profile considered in the simulation. The variability comes from the wave and wind inputs only.

2.4 Simulation and Analysis

The results in this section assume that the market is deregulated. Figure 2.4 shows the power network used, a highly stylized version of the PJM system, with 5-buses used to assess the planning and operation of the electrical system under market conditions [48].

We used MATPOWER 4.1 [49] as the software tool for the simulation. The simulation compares the difference in the response of the system when each of the two renewable resources are available as part of the total generation portfolio, using a Security Constrained, Optimal Power Flow with Endogenous Reserves [50]. Three cases are formulated as follows:

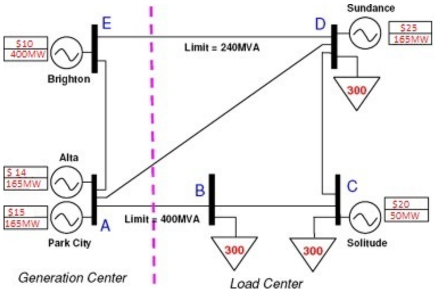


Figure 2.4: One-line diagram of 5-Bus test network

1. Case I: Only conventional generators, base case
2. Case II: Case I + 100 MW of wave energy added at bus 4
3. Case III: Case I + 100 MW of wind energy added at bus 4

The system evaluation is made using four metrics: 1) total power generated by renewable resource compared to maximum capacity; 2) reserve and ramping requirements in the day-ahead market; 3) total cost of serving the system; and 4) Load Not Served (LNS). The base case is designed with conventional generators whose capacity sum up to 945MW. The load is 900MW in the system, all of which is dispatchable.

The Multi-period SuperOPF framework [47] is used to optimize the allocation of resources. The results are obtained by optimizing over 144 dispatching schedules with four possible renewable resource availability states and one contingency assumed. Following is the analysis of the simulation results:

Power generated by wind and wave

We calculate the percentage of nominal maximum power and effective power dispatched. The % of nominal power (Table **??**, e[% W^a]) refers to the percentage of actual power dispatched to its rated capacity. This provides a rough measure of the capacity factor of these devices. The rated capacity of both the wind and the wave farm is set to 100MW. It is observed that both wave and wind resources deliver power for more than 60% on average over the entire optimization horizon (1 day). Also, the availability of wave power is somewhat lower than wind power. It is reasonable to conjecture that

Criteria for evaluation	Case I	Case II	Case III
	Summer Load Profile		
1. e[% W^a], e[% W^e]	N/A	64.64, 75.51	77.41, 77.78
2a. ±Av[Cp. Res.] (MW/d)	0.45, 0.180	58.28, 1.07	87.03, 0.5951
2b. ±Av[Rp Res.] (MW/d)	2.67, 2.55	59.28, 58.78	88.05, 87.27
3(a). E[Cost]($) (% dev. w.r.t. Case I)	9,853 -	9,291 (5.70)	9,832 (0.21)
3(b). MaxGen-Cap (MW)	735	636	635
	Winter Load Profile		
1. e[% W^a], e[% W^e]	N/A	64.77, 76.2	77.43, 77.71
2a. ±Av[Cap. Res.] (MW/d)	1.24, 0.49	58.63, 0.79	87.44, 0.76
2b. ±Av[Rp Res.] (MW/d)	2.53, 1.98	58.63, 57.88	88.54, 87.52
3(a). E[Cost]($) (% dev. w.r.t. Case I)	10,530 -	9,897 (6.01)	10,469 (00.57)
3(b). MaxGen-Cap (MW)	780	679	680

Table 2.1: Analysis of electrical System under high penetration of renewables under three criteria for evaluation

the differences in average power dispatched between wind and wave generators is driven by the power curve and power matrix used respectively to determine output power. In both cases we use a generic power curve and power matrix. Figure 2.2 shows that the low cut-off value of wind turbine makes it deliver power close to its rated capacity more often. The device configuration favors wind by reducing some of its variability and allowing it to operate as a bimodal resource, either at the maximum rated capacity or at zero power. The wave energy converter, on the other hand, operates below its operating limits most of the time translating most of the variability of the wave height into wave power. Belmullet Berth B, where the wave data is collected, has no full scale wave energy converters installed. Therefore, the power matrix selected in this study is not optimized for that specific location. The expected value of effective power (Table **??**, [% W^e]) is calculated to take into account the variable expected availability over the optimization horizon. Effective power is the percentage of actual power dispatched compared to the expected value of the maximum power available. We observe that the expected wind dispatches are higher than the wave dispatches. In this case, the power curve which points to the same reason explained above. The good availability of renewable power throughout the day clearly imply that the electricity prices at peak loads are likely to go down with higher penetrations of Renewable Energy Sources (RES) to the grid.

Capacity and Ramp Reserves

Reserve capacity is the additional amount of power made available online by the generator units for system balance and to cover unforeseen outages (contingencies). If a generator can adequately supply the demand promised with lesser usage of reserve capacity, the overall system cost will be less. Figure 2.5 shows that the system with wind requires considerably more reserve capacity than the system with wave during a summer day owing to the wind's high short-term variability. Table **??** shows that wave power outperforms wind in terms of the positive and negative reserve capacity, requiring almost 33 percent less positive capacity reserve than does the corresponding system with wind. The negative capacity reserve requirements are almost negligible. The ramp reserves are

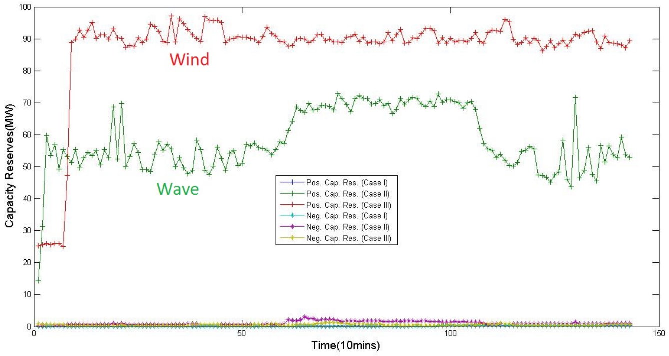


Figure 2.5: Capacity reserves in a typical summer day

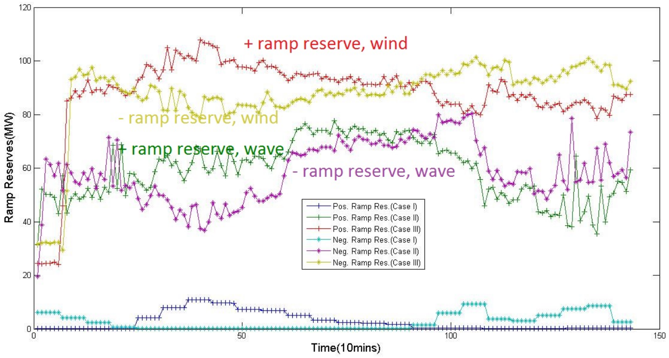


Figure 2.6: Ramp reserves in a typical summer day

necessary to allow load following in the system and cover the electricity demanded. The system operator determines ramp reserves based on the expected load following needs using day-ahead forecasts of generation and load. Figure 2.6 shows that Case II has comparatively lesser requirements for both up and down ramping than Case III. This would also make wave power more favorable in deregulated markets as the cost of ramping has a considerable share in the total cost of generation. The positive ramp reserve is used to cover cases in which the power from the RES becomes unavailable. Due to the bimodal behavior of the wind resource, the requirements are biased towards upwards reserves.

Expected generation Cost

Row 3(a) in Table **??** shows the expected cost of generation in all the three cases under the two load types. Case I with no renewables has the highest expected cost of generation due to exclusive use of conventional generators. Case II has lower cost of generation possibly due to lesser usage of reserves amongst all possible cases (including Case III). Row 3(b) in Table **??** shows the the peak conventional generation capacity. The two renewable cases (Cases II and III) have significant lower capacity, displaced by either wave or wind. This simulations then support some capacity value provided by both resources in short time scales.

Value of LNS

All system demand is modeled as dispatchable load, with the value of lost load set to $10,000/MWh [51]. Because the system trades off the cost of providing energy and ramping the generators to follow the load, with the penalty for load not served, the optimization allows shedding loads in cases with low probability of occurrence, therefore minimizing expected system cost. From the simulation, we observe that there is not much load shedding in any of the three cases, i.e., LNS is almost always close to zero.

2.5 Conclusion

Wave energy is an abundant resource along the coastlines of the US, Europe and Australia. The efficiency of wave energy converters is improving and their low cost of production has scope for increased participations in the generation fleets. In this simulation study, wave power integration looks economically promising with the proposed set of evaluation criteria. Our results show that the effects of short term variability of wave is less pronounced compared to wind which makes wave energy a promising choice for grid operation. From the operational point of view, the variability of power from WEC is lower, lowering the requirement for ancillary services to compensate their variability. The expected operation costs including the procurement of ancillary services (ramp reserves) are therefore lower, and the impact on capacity requirements for reliability purposes is similar to those of a wind turbine. Our future work includes analysis of WEC's arrays compared to wind farms.

Chapter 3

Optimal Predictive Maintenance Policy for an Ocean Wave Farm

3.1 Introduction

Providing clean electricity from wave is a renewable energy option expected to grow and develop in the years ahead and become a key aspect of energy portfolio. In U.S, Australia and several western European countries, the commercialization of these technologies is being encouraged through large scale funding programs and tax credits [52] [53] [54]. The deployment of commercial-scale wave energy converters like “Azura”, in Kaneohe Bay, on the islands of Oahu, Hawaii [55] and APB powerbuoy off the coast of Atlantic City, New Jersey [36] are some examples of projects carried out in the U.S. The credit of world’s first grid-connected wave power goes to Carnegie Wave Energy in Western Australia [56]. Offshore wind generation systems have preceded wave generation systems. While several wind farms with capacity in the order of hundreds of MWs already operating in Europe [57], U.S. witnessed its first offshore wind farm generating electricity commercially at Rhode Island in the end of 2016 [58].

Compared to conventional generation and onshore renewable generation, the Levelized Cost of Electricity (LCOE) of offshore renewable power generation systems is still high [59]-[62]. This is in part because the technology is earlier in its development cycle than onshore wind or solar generation but also because these energy converters are installed offshore and operate in harsh in-ocean conditions. For wave power to become an economically viable second generation renewable technology, the cost components of its LCOE need to be lowered. In this paper, we focus on strategies that minimize the maintenance costs of WEC installations. Maintenance cost has been noted as a major share of the LCOE of offshore renewable energy conversion and has not yet been optimally evaluated. We find that the Operation and Maintenance (O&M) costs of the wave energy generation system differ from conventional generation system. Unlike conventional generators which are typically large stand-alone systems capable of generating substantial amounts of power with high degree of certainty, Wave Energy Converters (WECs) are smaller and deliver small to moderate amounts of power subject to some uncertainty. For this reason, a number of WECs are often co-deployed within the same geographic region to exploit economies of scale and to increase both the amount and reliability of power production. The maintenance and replacement of any one WEC is expensive since it requires dispatching a maintenance vessel as well as specialized equipment and manpower. Savings are possible by scheduling joint maintenance operations for several WECs. The question then is when to schedule joint maintenance across a farm of WECs. The intuitive answer is when the cost of maintenance of failed or failing WECs is justifiable in relation to the status quo, i.e., the revenue generated from producing power from functional WECs. The focus of this paper is to quantify this intuition.

This paper is specifically concerned with the determination and analysis of an optimal maintenance policy for wave farms. Such a policy will lower the LCOE of these farms by minimizing the expected maintenance costs over the life of the wave farm. The formulation studied here is a stochastic control problem where the decision is whether and when maintenance work should be performed. It features specific modeling and optimization challenges: 1) the modeling of correlations between random deterioration processes of individual WECs subject to a common harsh environment; 2) the modeling of weather which affects the deployment of maintenance ships; and 3) the curse of dimensionality that describes the state of the wave farm as the number of WECs grows.

We note that the structural aspects of the problem are also present in offshore wind farm maintenance problems. Therefore, we believe our work could be adapted to offshore wind farm maintenance. We discuss related work in offshore wind farm maintenance along with WEC maintenance in our literature review below.

3.1.1 Contributions and Related Work

Maintenance is a key part of the asset management activities of electric utilities and power producers. According to the survey in [63], maintenance approaches of electric utility companies can be categorized as either (a) *scheduled maintenance*, where times between maintenance operations are fixed in advance; (b) *predictive maintenance*, based on monitoring the state of the equipment; and (c) *emergency maintenance*, when some equipment has failed. The survey in [64] examines maintenance of offshore wind farms with a focus on the logistics involved; each of the three maintenance approaches is well represented. A comprehensive review of condition-based maintenance methodologies currently employed in marine renewable energy systems is provided by [65]. It states that implementing predictive maintenance increases availability and reduces maintenance costs, thereby improving the competitiveness of wave farms.

Several utilities have implemented Reliability-Centered Maintenance (RCM) programs, where the performance of several maintenance strategies are monitored and the best one is adopted over time based on historical performance [63] [66]. For example, in [66], an Artificial Neural Network (ANN) model utilizes system health monitoring measurements to predict the remaining useful life of each wind turbine in the onshore wind farm. This helps to decide which turbines and exactly which components should be maintained. However, when historical data is scarce, which is the case with offshore WECs, it makes sense for a utility to optimize maintenance policies based on a probabilistic model, such as the model proposed in this paper, and study the sensitivity of the policies to parameters that remain uncertain due to the lack of experience.

In probabilistic models, the evolution of the state of a piece of equipment is represented through a Markov or semi-Markov chain model, where transitions happen randomly towards states of higher deterioration, until repair or replacement is made. The structure of the optimal policy for single equipment replacement problems is well known in the Markov Decision Process (MDP) literature, and described for instance in [67], §8-2.

Transition probabilities can be estimated from historical time series relative to identical pieces of equipment. In [68], Bayesian estimation methods are proposed and evaluated on a steam turbine crack propagation data set. Alternatively, in [69], maximum-likelihood methods are proposed to reverse-engineer the transition probabilities by finding those most consistent with a maintenance policy assumed to be optimal. The approach is evaluated on a bus engine fleet maintenance problem.

Maintenance activities for offshore wind and wave farms are similar in various ways. In both cases, the costs of arranging maintenance crews, repair tools and transportation to offshore locations are high. In both cases, O&M activities are influenced by weather. Finally, in both cases, the installations will be unmanned except during maintenance [70].

Scheduled maintenance of wave energy converters are discussed in [71] and categorized as on-site service and mid-life refit. In the former case, routine farm visits are envisioned to occur at a chosen frequency to permit regular servicing and repair onsite. The mid-life refit involves towing WEC units for onshore maintenance and therefore involves major component replacement or repair. [71] estimates maintenance schedules assuming random breakdown events with failure rates given a Failure Modes and Effects Analysis (FMEA) table. In such cases, given the nature of failure and availability of repair equipment and team, the type of operation and recovery time is also adjusted. [72] [73] describe how maintenance activities can be affected by weather and other environmental factors.

Offshore wind farm maintenance models have been explored in recent literature. In [74], an opportunistic model is proposed that exploits low wind power production and unexpected failures to perform preventive maintenance tasks at lower costs. In [75], a method for assessing the reliability of potential wind farm site is presented in which wind-speed dependent failure rates are considered. This approach takes into account the impact of seasonable changes on wind turbine operation. In [76], the predictive maintenance of wind turbines subject to stochastic weather events is considered. The main difference between this work and ours is that [76] studies the maintenance of a single wind turbine, whereas the present paper considers the problem of maintaining the entire wave farm based on the state of each WEC. In [77] [78] [79], optimization models for selection and/or scheduling of maintenance activities for an offshore wind farm are presented. For example, [77] considers decisions regarding the location of maintenance accommodation, number of technicians, choice of transfer vessels, and use of helicopter. However, our work seems to be the first to examine the design of optimal maintenance policy for the offshore renewable farm as a stochastic system that is grid-connected, participates in the electricity market and takes into account the weather conditions before taking maintenance decisions. Our goal is to provide a maintenance strategy under these assumptions. As such our model and results are expected to be broadly applicable. Comparisons with existing approaches are subject to the caveat that different objective functions are being optimized. For example, many earlier studies for renewable farms address maintenance of individual devices or certain aspects of maintenance activities such as fleet size or scheduling, for instance [76] [77] [80]. Other existing studies employ a data driven solution, leveraging the existence of historical data, whereas ours is a model-based approach.

The approach proposed in this paper relies on a reduction of the state space where we count the number of WECs in each given state. This is a technique employed for instance in routing problems for operating a large fleet of vehicles [81]. The approach relies on the assumption that WECs in the same state are exchangeable. This assumption is natural if the WECs are identical, located in the same geographical area, and thereby subject to the same sources of stress; it could be relaxed by augmenting the number of WEC states that are distinguished and counted. The state space reduction that ensues is sometimes referred to as "state space collapse". The effectiveness of the approach is demonstrated on a wave farm model made of $N = 30$ WECs. Originally the problem has 3^N states, but in the reduced state space the number of distinct states is $\mathcal{O}(N^2)$. This makes it possible to solve dynamic programs exactly and to perform sensitivity studies reliably.

In the wave farm maintenance problem, weather events affect the deterioration processes as well as the ability of the maintenance vessels to be dispatched. Data driven models for marine weather are able to capture seasonal variabilities by utilizing the concept of weather windows [61] [72]. In the literature, weather window analysis gives the percentage of time in a year that a device can be accessed. For ease of presentation and analysis, our work considers a system model in which the evolution of wave farm state as well as exogenous variables such as weather are independent. The extension to a model featuring seasonality, lending itself to weather window analysis, is possible however, for instance using the device of p-periodic Markov Decision Processes [82].

Following nomenclature in IEEE standard [83], a simple weather model with the following states is adopted: Normal weather (ξ^N), Adverse weather (ξ^A), and Major storm disaster (ξ^M). The Markov chain modeling the weather environment is assumed to be time-homogeneous. This assumption could be relaxed by computing a time-dependent maintenance policy over a finite horizon, or a periodic policy over an infinite horizon using the algorithmic approach of [82]. The device of a periodic policy can be used for instance to model a winter season during which vessels cannot be dispatched.

Finally, our work contributes to visual analytics by proposing a graphical representation of the high-dimensional state of the offshore renewable farm, that can be used by operators to visualize probabilistic predictions and to analyze the sensitivity of the maintenance policy to important inputs of the problem.

3.1.2 Organization

The remainder of the paper is organized as follows. The main notation used in this paper is summarized in Section 3.2. The offshore renewable farm maintenance problem is formulated in Section 3.3. Section 3.4 presents numerical results and our analysis. Finally, Section 5.5 concludes the paper.

3.2 Nomenclature

N = number of WECs in the wave farm.

i or j = index for the state of a single WEC, in {1,2,3} where 1, 2 and 3 denote healthy state, unhealthy state and faulty state, respectively.

t = time period index.

$N_{i,t}$ = number of WECs in state i at time t.

p_{ij} = one-step marginal transition probability from state i to j for a WEC.

$W_{ij,t+1}$ = number of WECs in state j at time $t+1$ that originated from state i, if the random transitions are independent, identically distributed (i.i.d.)

p_c = probability of common cause.

ρ_{ij} = correlation coefficient between transitions from i to j for pairs of WECs.

ω_1, ω_2 = coefficients based on weather severity that change failure probabilities of healthy and unhealthy WECs, respectively.

$W^c_{ij,t+1}$ = number of WECs in state j at time $t+1$ that originated from state i, if the random transitions are correlated.

S_t = information state at time t.

A_t = decision at time t which is based on S_t.

R_t = expected reward (negative cost) of being in state S_t and selecting decision A_t.

C^{rep} = expected cost of maintenance, including fixed and variable costs.

c_f =fixed cost of maintenance.

c_2 = unit cost per WEC of repairing $N_{2,t}$ WECs.

c_3 = unit cost per WEC of repairing $N_{3,t}$ WECs.

R^{gen} = expected profit of operating $N_{1,t} + N_{2,t}$ WECs.

$1 + \eta$ = interaction coefficient among WECs influencing mean power from the wave farm.

$1 + \theta$ = interaction coefficient among WECs influencing variance of the power from the wave farm.

σ = variance of power from a single WEC.

P_1 = power from a single WEC.

π^f = forward hourly price of power.

π^s = random penalty hourly price of a shortfall in committed production.

ϕ = probability density function (pdf) of the standard Gaussian distribution.

Φ = cumulative density function (cdf) of the standard Gaussian distribution.

$Bern(p)$ = Bernoulli distribution with parameter p.

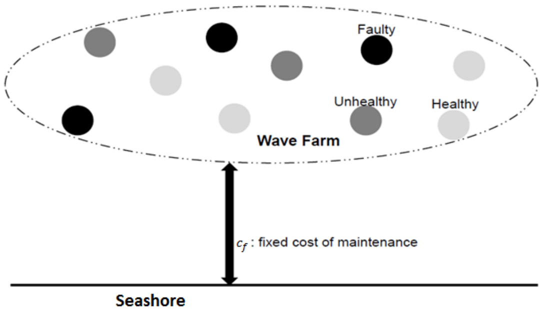


Figure 3.1: Ocean wave farm consisting of energy converters in 3 possible states: (1) Healthy, (2) Unhealthy, (3) Faulty.

$Bin(n, p)$ = binomial distribution with parameters n and p.

$CB(n, p, \rho)$ = correlated binomial distribution with parameters n, p, ρ.

$Beta(\alpha, \beta)$ = Beta distribution with α, β as shape parameters.

γ = discount factor in $(0, 1)$.

3.3 Mathematical Model

The ocean wave farm consists of N WECs (Figure 3.1), each of them being in one of the following states:

- 1 : Healthy, delivers power as expected;
- 2 : Unhealthy, experiencing deteriorations;
- 3 : Faulty, severe deteriorations, no power output.

3.3.1 Wave Farm States and State Space Collapse

The number of converters in states 1,2,3 at time t are denoted $N_{1,t}$, $N_{2,t}$, $N_{3,t}$. The counts satisfy the relation

$$N_{1,t} + N_{2,t} + N_{3,t} = N. \tag{3.1}$$

The state of the wave farm is described by

$$N_t = (N_{1,t}, N_{2,t}, N_{3,t}). \tag{3.2}$$

Due to (3.1) two variables suffice to determine the third one, so $N_{2,t}$ can be omitted in (3.2). It can be checked that

- An integral N_t is a feasible farm state iff

$$0 \leq N_{3,t} \leq N - N_{1,t} \leq N. \tag{3.3}$$

- The total number of wave farm states N_t is

$$(N+1)(N+2)/2 = \mathcal{O}(N^2).$$

- To a wave farm state N_t corresponds a number of WEC configurations equal to

$$\binom{N}{N_{1,t}, N_{2,t}, N_{3,t}} = \frac{N!}{N_{1,t}!N_{2,t}!N_{3,t}!}.$$

3.3.2 Weather States

The weather is modeled as a Markov chain, following standard practice in reliability evaluation [84]. The weather state is denoted ξ_t. As in [83], three types of weather states are distinguished:

- Normal weather (ξ^N),
- Adverse weather (ξ^A),
- Major storm weather (ξ^M).

Adverse weather is viewed as an alert state, potentially evolving to the major storm types. The transition probabilities can be chosen to approximate the storm interarrival time distribution and the weather alert system characteristics. The occurrence of severe cyclonic storms is often well explained by a Poisson process [85–87]. The Bernoulli process, which is a discrete-time process with geometric interarrival times and state-independent transition probabilities, can be used as a device to approximate the Poisson process, which is a continuous-time process with exponential interarrival times and constant hazard rate. Historical data are sometimes available to estimate the proportion of storms and depressions which actually evolved into a cyclonic stage [88].

3.3.3 Decisions

Regardless of whether the repair activities are carried out onshore or offshore, dispatching a vessel is costly but a crucial step in the maintenance process. The model assumes that if a repair vessel is dispatched, all necessary repairs will be performed on unhealthy and faulty WECs to bring them back to the healthy state. Therefore, the decision at time t reduces to whether or not the vessel is dispatched. It also assumes that the vessel to carry out offshore maintenance activities is available immediately after the decision to repair is taken. This is a reasonable assumption when the discrete time periods have a sufficiently long duration. By the same rationale the model assumes that completing the repair activities takes a single time step. The decision at time t is denoted A_t with values

- 0: Do not dispatch the vessel or do not repair,
- 1: Dispatch the vessel and repair.

The decision A_t depends on the wave farm state N_t and the weather state ξ_t. The maintenance policy π describes the action to take for each state. If the policy is stationary, this can be written as

$$A_t = A^{\pi}(S_t) \tag{3.4}$$

where $S_t = (N_t, \xi_t)$ is the information state and A^{π} is the mapping from states to decisions.

3.3.4 State Transitions

The wave farm state transition probabilities are computed from the WEC state transition probabilities. When the decision is to repair ($A_t = 1$), the next state is defined as

$$N_{1,t+1} = N, \quad N_{2,t+1} = 0, \quad N_{3,t+1} = 0. \tag{3.5}$$

The remainder of this section describes the evolution of the wave farm state without intervention ($A_t = 0$).

The transition probabilities from state i to j for any particular WEC are described by $p_{12} > 0$ and $p_{23} > 0$; the other probabilities p_{ij} for $i \neq j$ are set to 0. This describes a gradual deterioration process with state 3 as an absorbing state.

Let $W_{ij,t+1}$ be the number of WECs that enter state j at time $t+1$ while being in state i at time t. Since only p_{11}, p_{12}, p_{22}, p_{23}, p_{33} are nonzero, the wave farm state transition under $A_t = 0$ can be described by

$$\begin{aligned} N_{1,t+1} &= N_{1,t} - W_{12,t+1}, \\ N_{2,t+1} &= N_{2,t} + W_{12,t+1} - W_{23,t+1}, \\ N_{3,t+1} &= N_{3,t} + W_{23,t+1}. \end{aligned} \tag{3.6}$$

Models for the joint distribution of the nonnegative random vector $(W_{12,t+1}, W_{23,t+1})$ are given in Appendix 3.6.1.

The evolution of the expectation of the wave farm state N_t under the "do not repair" action, and normal weather throughout, is presented for a particular numerical example in Figure 3.2. The probabilities p_{12} and p_{23} used in the simulation are 0.04 and 0.1 respectively, with the WEC transitions assumed to be mutually independent (zero probability of common cause, see Appendix 3.6.1). It can be observed that the WECs in healthy state gradually decrease in number over time and WECs in faulty state increase in number over time. As the number of WECs in unhealthy state changes depending on the sign of

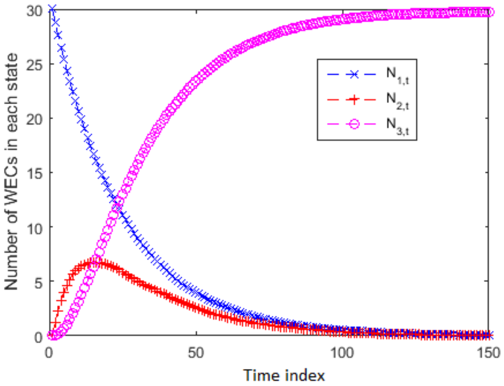


Figure 3.2: Expectation of ocean wave farm's state (excluding weather state) as a function of time under "Do not repair" action

$(W_{12,t+1} - W_{23,t+1})$, on average, it increases initially and then steadily decreases.

Weather-Dependent Failure Probabilities: When a WEC is subjected to bad weather conditions, its likelihood of failure may increase. Wear and tear is one cause of failure, but other causes such as slamming [89] may be specific to extreme sea weather, leading to our assumption of increased overall failure rate in these conditions.

This phenomenon is included in the model by making failure probabilities a function of weather severity. As the weather deteriorates, the failure probabilities can be modified as follows:

$$\Pr\{W_{12,t+1}\} = \Pr\{W_{12,t+1}\} + \omega_1(1 - \Pr\{W_{12,t+1}\})$$

$$\Pr\{W_{23,t+1}\} = \Pr\{W_{23,t+1}\} + \omega_2(1 - \Pr\{W_{23,t+1}\}) \tag{3.7}$$

where ω_1 and ω_2 can be tuned depending on the weather condition (adverse weather or major storm). If the weather is normal, ω_1 and ω_2 are zero.

Survival strategies of WECs have not been perfected yet. As suggested in [**?**] [**?**], research on designing WEC devices that can survive extreme conditions and on the effectiveness of current life-extending controls to reduce system loading during bad weather conditions needs to be further carried out.

3.3.5 Rewards

The model assumes that a reward $R_t = R(S_t, A_t)$ is obtained at each period. A reward function R of the following form is adopted:

$$R(S_t, A_t) = (1 - A_t) \cdot R^{\text{gen}}(N - N_{3,t}) - A_t \cdot C^{\text{rep}}(N_t), \tag{3.8}$$

$$\begin{aligned} C^{\text{rep}}(N_t) &= c_f + c_2 N_{2,t} + c_3 N_{3,t} \\ &= c_f + c_2(N - N_{1,t}) + (c_3 - c_2)N_{3,t}. \end{aligned} \tag{3.9}$$

Here R^{gen} is the expected profit of operating $N_t^{\text{op}} := N_{1,t} + N_{2,t} = N - N_{3,t}$ non-faulty converters, and C^{rep} is the expected cost of repairing the $N_{2,t}$ unhealthy and $N_{3,t}$ faulty converters. Healthy converters continue to operate at the time of maintenance. The methodology to derive the overall expected profit R^{gen} is explained in Appendix 3.6.2.

The C^{rep} function has a fixed cost component c_f for sending the vessel, and a variable cost component where $c_2 \leq c_3$ are the expected cost of repair per converter in unhealthy and faulty states, respectively. Note that the repair cost coefficients c_2,c_3 are costs per single WEC being repaired.

Weather-Dependent Reward Function

In the weather-dependent model, the reward function is also a function of the weather state. Specifically, both the revenue component and maintenance cost component of the reward function are different under different weather conditions. The cost of maintenance increases with deterioration in weather conditions as

$$C^{\text{rep}}(N_t, \xi^N) < C^{\text{rep}}(N_t, \xi^A) < C^{\text{rep}}(N_t, \xi^M). \tag{3.10}$$

With the worsening of weather conditions, the height of the ocean waves increases to dangerous levels more frequently. It is expected that the WEC production efficiency reduces due to protection systems that operate more frequently during adverse ξ^A and major adverse ξ^M weather. This leads to lower expected revenues from generation. Thus,

$$R^{\text{gen}}(N - N_{3,t}, \xi^N) > R^{\text{gen}}(N - N_{3,t}, \xi^A) > \\ R^{\text{gen}}(N - N_{3,t}, \xi^M). \tag{3.11}$$

Remark 1: Given $S_t = (N_t, \xi_t)$, let $\mathcal{Z}(S_t)$ be the set of states $Z = (Y, \xi_t)$ such that the wave farm state $Y = (Y_1, Y_2, Y_3)$ is reachable from N_t under the "passive" policy $A_{t'} = 0$ for all $t' = t, t+1, \ldots$. Then it holds that

$$R(Z, 0) \leq R(S_t, 0) \text{ for all } Z \in \mathcal{Z}(S_t),$$
$$R(Z, 1) \leq R(S_t, 1) \text{ for all } Z \in \mathcal{Z}(S_t).$$

To see this, note that when the system evolves without repair, it evolves towards states where, relative to the current state, the repair costs can never decrease and the generating instantaneous reward can never increase.

Remark 2: Along state trajectories generated with $A_{t'} = 0$ for $t' \leq t - 1$, it holds that for both actions $a \in \{0, 1\}$,

$$R(S_{t+1}, a) \leq R(S_t, a). \tag{3.12}$$

To see this, note that the set of feasible wave farm states can be described as

$$\{(N - N_1, N_3) : N_1 \geq 0, N_3 \geq 0, N_1 + N_3 \leq N\}.$$

Regardless of weather, the set of feasible next states while being in state (N_1, N_3) and choosing action $A_t = 0$ can be described by

$$S'(N - N_1, N_3) = \\ \{(N - N_1', N_3') : 0 \leq N_1' \leq N_1,\ N_3 \leq N_3' \leq N - N_1\}.$$

In the case $A_t = 0$,

$$R(S_{t+1}, 0) = R^{\text{gen}}(N - N_3') \leq R^{\text{gen}}(N - N_3) = R(S_t, 0),$$

using R^{gen} nondecreasing and $N_3' \geq N_3$.

In the case $A_t = 1$,

$$\begin{aligned} R(S_{t+1}, 1) &= -C^{\text{rep}}(N_{t+1}) \\ &= -(c_f + c_2(N - N_1') + (c_3 - c_2)N_3') \\ &\leq -(c_f + c_2(N - N_1) + (c_3 - c_2)N_3) \\ &= -C^{\text{rep}}(N_t) = R(S_t, 1), \end{aligned}$$

using $N_1' \leq N_1$, $N_3' \geq N_3$, and $0 \leq c_2 \leq c_3$.

Remark 3: Along state trajectories generated with $A_{t'} = 0$ for $t' \leq t - 1$, it holds that the function $\Delta R(S_t) := R(S_t, 1) - R(S_t, 0)$ satisfies

$$\Delta R(S_{t+1}) \geq \Delta R(S_t). \tag{3.13}$$

To see this, note that we have

$$\Delta R(S_t) = -C^{\text{rep}}(N_t) - R^{\text{gen}}(N - N_{3,t}).$$

Along transitions with $A_t = 0$, it holds that $R^{\text{gen}}(N - N_{3,t}) = R(S_t, 0)$ is nonincreasing, and $-C^{\text{rep}}(N_t) = R(S_t, 1)$ is nondecreasing.

3.3.6 Objective Function

Using the states, decisions, transition and reward function described above, the problem is formulated as the search for a policy that maximizes the expected discounted cumulated reward over an infinite horizon:

$$V(S_0) = \max_{\pi \in \Pi} \mathbb{E}^{\pi} \left[\sum_{t=0}^{\infty} R(S_t, A^{\pi}(S_t)) \, \Big| \, S_0 \right], \tag{3.14}$$

where $\gamma \in (0,1)$ is the discount factor and Π denotes the space of stationary Markov decision policies. The optimal value function V^* satisfies

$$V^*(S) = \max_{A \in \{0,1\}} \left[R(S,A) + \gamma \sum_{S'} Pr(S'|S,A) V^*(S') \right]. \tag{3.15}$$

The optimal policy π^* can be computed using standard dynamic programming algorithms such as value iteration or policy iteration [90].

3.4 Results and Analysis

In this section, we present the solution of the infinite horizon problem defined in (3.14). At first, we define the baseline case and then consider different cases to compare and contrast the optimal policies. First, the results on the structure of the optimal policy under different cases are discussed. Then, other results of the optimization problem that include the steady-state transition probabilities and trajectory of the wave farm states under optimal policy are presented. In our simulation, we have defined the parameters for a typical ocean wave farm to generate the results. The numerical values of the parameters used are based on communication from wave farm energy industry experts and believed to be practically possible. We make the numerical analysis of the following cases.

Baseline: The number of wave energy converters in the wave farm is taken as $N = 30$. The probability p_c that explains the dependencies among random transitions of the wave farm states is set to zero. η is set to zero which means that no interaction among WECs is assumed. Refer to Appendix 3.6.2 for the detailed description of p_c and η. The fixed cost of dispatching maintenance vessel and crew c_f is set to 500. The weather is assumed to remain in normal state throughout. The parameters used to define the reward function in the system model are defined in Table 3.1. The parameters for the sensitivity analysis

c_2	10	P_1	0.4
c_3	15	V_1	0.04
π^f	30	η	-0.3
π^s	100	θ	-0.5

Table 3.1: Parameters in Reward Function

	p_{12}	p_{23}	p_c	c_f	η
Baseline	0.01	0.3	0	500	0
Case I.A	**0.001**	0.3	0	500	0
Case I.B	0.01	**0.01**	0	500	0
Case II.A	0.01	0.3	**0.5**	500	0
Case II.B	0.01	0.3	**0.9**	500	0
Case III.A	0.01	0.3	0	**70**	0
Case III.B	0.01	0.3	0	**4000**	0
Case IV.A	0.01	0.3	0	500	**0.2**
Case IV.B	0.01	0.3	0	500	$-$**0.8**
Case V	0.01	0.3	0	500	0

Table 3.2: Parameters for Sensitivity Analysis of Optimal Policy Under Baseline and Five Cases.

of the optimal policy under baseline and five cases described next are tabulated in Table 3.2.

Cases:

I. *Sensitivity of the optimal policy to failure probabilities*

II. *Sensitivity of the optimal policy to common cause indicator* p_c

III. *Sensitivity of the optimal policy to fixed cost of maintenance* c_f

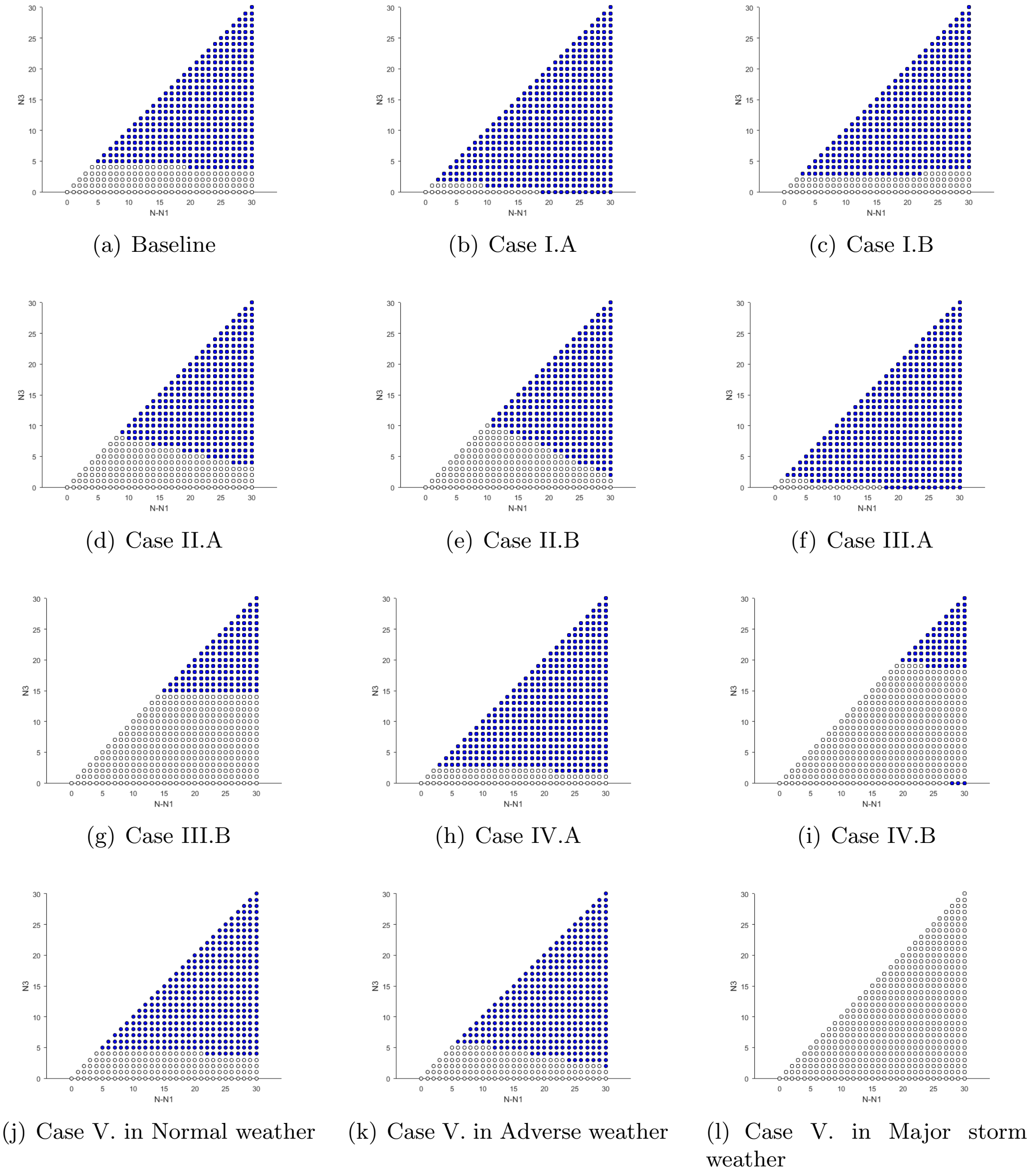
IV. *Sensitivity of the optimal policy to interaction coefficient* η

V. *Effect of different weather conditions:* The state transitions of the Markovian weather are shown on Table 3.3. The cost of repair of each WEC in adverse and major storm weather is set as $c_{2,\xi^A} = 5c_2$, $c_{3,\xi^A} = 10c_2$ and $c_{2,\xi^M} = 10c_2$, $c_{3,\xi^M} = 30c_3$, respectively with c_2, c_3 as in Table 3.1.

We solve (3.14) using the linear programming approach to dynamic programming. While any linear optimization or conic optimization solver can be used for this purpose,

	ξ_{t+1}^N	ξ_{t+1}^A	ξ_{t+1}^M
ξ_t^N	0.995	0.0049	0.0001
ξ_t^A	0.5	0.0001	0.4999
ξ_t^M	0.5	0.5	0

Table 3.3: Transition Probabilities of a 3-state Markov Model of Weather [1]



(a) Baseline

(b) Case I.A

(c) Case I.B

(d) Case II.A

(e) Case II.B

(f) Case III.A

(g) Case III.B

(h) Case IV.A

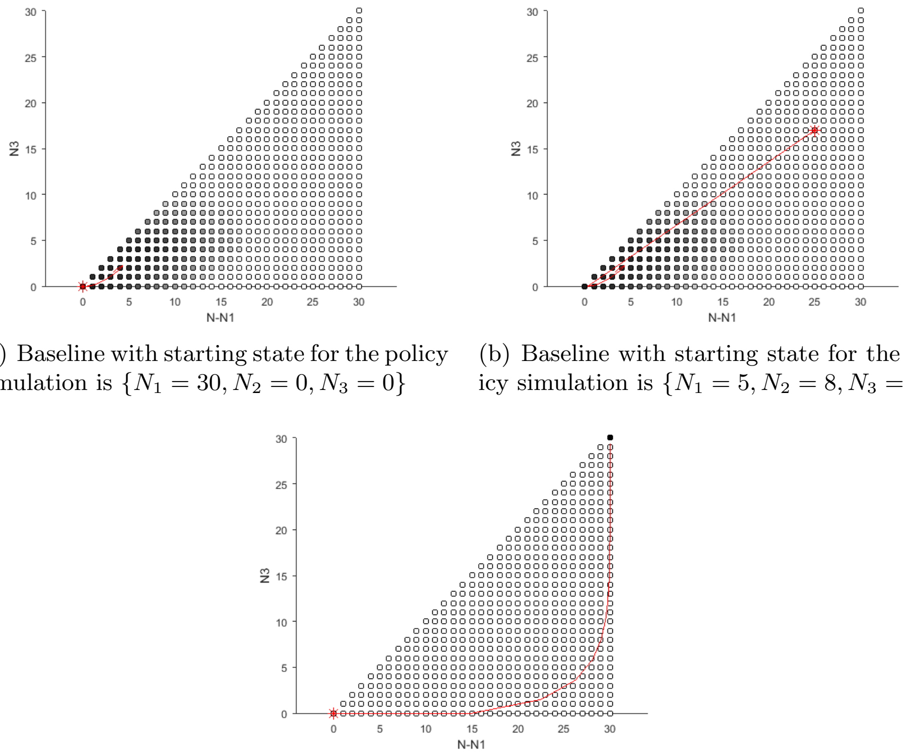
(i) Case IV.B

(j) Case V. in Normal weather

(k) Case V. in Adverse weather

(l) Case V. in Major storm weather

Figure 3.3: Optimal Policy for the studied cases(Filled circle: Repair. White circle: Do not repair)



(a) Baseline with starting state for the policy simulation is $\{N_1 = 30, N_2 = 0, N_3 = 0\}$

(b) Baseline with starting state for the policy simulation is $\{N_1 = 5, N_2 = 8, N_3 = 17\}$

(c) Case with $p_{12} = 0.3$ and starting state $\{N_1 = 30, N_2 = 0, N_3 = 0\}$ for which "do not repair" at any state is the optimal policy

Figure 3.4: Steady-state probabilities in greyscale (darker means higher probability value). The trajectory of expected wave farm state under optimal policy is indicated by a continuous curve that starts from an initial state marked with the asterisk (*).

	V^*(Adaptive)	J^*(Scheduled)	T_s^* [a]
Baseline	208060	77922	14
Case I.A	228840	77922	14
Case I.B	221110	188220	41
Case II.A	182450	-1573	50
Case II.B	166130	-8636	50
Case III.A	227410	114040	10
Case III.B	142490	-31324	50
Case IV.A	373640	148620	10
Case IV.B	82019	27640	23

[a] For each value of J^*, T_s^* is the corresponding optimal inter-maintenance time

Table 3.4: Comparison of Objective Values under Different Maintenance Strategies

we use the solver Sedumi [91], called from Matlab. The optimal policies for the above cases are illustrated in Figure 3.3. In these plots, the X-axis represents the number of WECs that are not in healthy state ($N - N_1 = N_2 + N_3$) and the Y-axis represents the number of WECs that are in faulty state (N_3) in the wave farm. All the possible states of the wave farm are represented as small circles. The state on the origin is the wave farm state with all healthy WECs ($N - N_1 = 0, N_3 = 0$).

In all the plots of optimal policy, one can identify a curve that separates the decision region "Do not repair" (represented with white circles) and the decision region "Repair" (represented with filled circles). In the sequel, this curve is being referred to as the threshold line.

Case I: In Figure 3.3(b), the shifting of threshold line in the optimal policy depends on the change of the probability of a WEC transitioning from healthy to unhealthy state and from unhealthy to faulty state. When the failure probability p_{12} is increased, the threshold shifts upwards compared to the baseline threshold line, indicating it is better to wait until a larger number of WECs turn faulty. This would avoid frequent repairs which are expensive. On the other hand, when p_{12} is decreased, the threshold line shifts downwards. This indicates that the incentive to do frequent repair is higher as the WECs can be expected to stay in healthy state for longer durations of time. A similar behavior is observed regarding the shifting of the threshold line by varying failure probability p_{23} as shown in Figure 3.3(c). The decrease of p_{23} leads to WECs staying in unhealthy state for longer durations of time to generate power. Therefore, it is economical to wait for more WECs to turn faulty before selecting the repair action. Figure 3.3(c) reflects this phenomenon.

Case II: In Figure 3.3(d) and 3.3(e), the effect of having a common cause influencing failure probabilities of a WEC on the threshold line is presented. We employ joint failure model 2 given by (3.20) and (3.21) in Appendix 3.6.1 to illustrate this. Upon increasing the value of p_c, it can be observed that the threshold line shifts to the right indicating that a common cause might cause the WECs to turn faulty faster. This is because $q_{12,1}$ and $q_{23,1}$ are respectively higher than $q_{12,0}$ and $q_{23,0}$. Therefore, the failure correlation coefficient should also be assessed to determine the best maintenance strategy.

Case III: In Figure 3.3(f) and 3.3(g), we study how the fixed maintenance cost c_f impacts the optimal policy. Decreasing or increasing c_f leads to an optimal policy whose threshold line shifts to the left or right compared to the baseline threshold line, respectively. For example, the overall maintenance cost owing to high fixed maintenance cost at a wave farm state lying on the baseline threshold line would be higher than the accumulated revenue of generating power from operating WECs under no repair.

Case IV: In Figure 3.3(h) and 3.3(i), the sensitivity of the optimal policy to the interaction coefficient of a WEC is illustrated. As the interaction coefficient directly influences the revenue from each WEC, the threshold line also shifts with the interaction coefficient. When the interaction coefficient is greater than one, there is constructive interference of the waves created by the WECs resulting in higher expected reward. This provides the incentive to go for maintenance more often as the revenue from power generation is expected to be high. When the interaction coefficient is less than one, there is destructive interference of the waves resulting in lower expected reward. As a result, the threshold line moves upwards, meaning that the repair of the wave farm when a greater number of WECs are in the deteriorated state is more economical.

Case V: To study the impact of weather on the wave farm maintenance strategy, the weather state is introduced as an exogenous variable in the overall system state. The wave farm state transition function and reward function are defined under three different types of weather state. The solution of the dynamic program gives an optimal policy corresponding to each weather type as illustrated in Figure 3.3(j), 3.3(k) and 3.3(l). We can observe that during major storm (ξ^M) conditions, one cannot repair. This is consistent with the typical perception and industry practice. It is best to carry out repair action in normal weather as the cost of dispatching maintenance vessel as well as failure probabilities are small. In adverse weather condition, the repair is to be done only if many WECs have fallen into faulty state as the cost of maintenance is higher than under normal weather condition.

3.4.1 Steady-state probabilities and Policy Simulation

The steady-state probabilities are defined by $q_\infty = q_\infty \mathbf{Q}^\pi$ where $\mathbf{Q}^\pi$ is the transition probability matrix under policy π and q_∞ satisfies $\sum_j q_{\infty,j} = 1$. Under the optimal policy π^*, the elements $\mathbf{Q}^{\pi^*_{ik}}$ are given by $\Pr(S_t = k | S_{t-1} = i, A^{\pi^*}_{t-1}(i))$. The policy simulation is executed by picking an initial probability q_0 concentrated on the starting state and calculating the trajectory of next states using state probabilities $q_t = q_0(\mathbf{Q}^\pi)^t$ until the end of truncated time horizon. The values of q_∞ for each state and the expected state evolution under the optimal policy π^* are illustrated in Figure 3.4. The steady-state probability is represented in levels of gray varying from black at the highest probability to white at the lowest probability. From the figure, one can get information on the most likely wave farm states in steady-state under the optimal maintenance policy. In the baseline case, it can be observed that the wave farm is likely to have predominantly healthy WECs. In Figure 3.4(c), an extreme case is considered in which the probabilities of failure, $p_{12} = 0.9$ and $p_{23} = 0.9$, are reasonably high. In such cases, it is economical not to perform repair as healthy WECs quickly turn into unhealthy and eventually faulty states. The non-zero steady-state probabilities of the wave farm are concentrated on the vertex $(N_1 = 0, N_2 = 0, N_3 = 30)$ where the system state consists of faulty WECs only.

In Figure 3.4, policy simulation results are illustrated as the continuous line trajectory with starting state marked by asterisk $(*)$. Figure 3.4(a) shows that when the starting state is at the origin (all the WECs are in healthy state), after several time steps, the wave farm state settles around a medium-size region where the steady-state probabilities of the wave farm states are high. In Figure 3.4(b), the starting wave farm state is taken as $\{N_1 = 5, N_2 = 8, N_3 = 13\}$. The immediate optimal action at that particular state is to "repair". As a result, the wave farm is renewed to all healthy WECs and then the state evolves as in the previous case. The optimal policy is simulated for extreme case in Figure 3.4(c) with starting state $\{N_1 = 30, N_2 = 0, N_3 = 0\}$. We can observe that after a few time steps, the system deteriorates to the state with all faulty WECs.

3.4.2 Comparison with Scheduled Maintenance Policy

Scheduled maintenance is also a commonly suggested strategy for ocean wave farm. Scheduled maintenance is carried out by dispatching a maintenance vessel at fixed time intervals to repair or replace the WECs that are not operating well. In the proposed system model, we refer to those WECs as unhealthy and faulty WECs. Let T_s be the time interval between two consecutive maintenance activities.

We make a comparison between the expected cumulative discounted reward from the scheduled maintenance policy that employs the best possible inter-maintenance parameter T_s, and the optimal adaptive policy π^* studied in this paper. We consider the case where the weather remains in normal state throughout. Under "do not repair" action, the wave farm state evolves according to the failure probabilities of individual WECs until $T_s - 1$ time steps. The "repair" action at time step T_s restores the wave farm to a state with all healthy WECs. Let the transition matrix under no repair be denoted by $\mathbf{Q}$. The elements of $\mathbf{Q}$ are determined by (3.21) in Appendix 3.6.1. The probability of being in each state at time t is described as the row vector $p_t = p_0\mathbf{Q}^t$ where p_0 is the row vector of initial probabilities. Assuming that $p_0 = [1\ 0\ \ldots\ 0]$ to start from full healthy state, the expected discounted return during the first T_s periods is

$$\begin{aligned} J_1(T_s) &= \sum_{t=0}^{T_s-2} \gamma^t [\sum_S [p_t(S)R(S, A=0)]] \\ &\quad + \gamma^{T_s-1}[\sum_S [p_{T_s-1}(S)R(S, A=1)]] \end{aligned}$$

Thus, the total expected return and corresponding best time interval for scheduled maintenance is given by

$$J^* = \max_{T_s \in \{2,\ldots,T_f\}} J_1(T_s)/(1-\gamma^{T_s})$$

and $T_s^* = \underset{T_s}{\operatorname{argmax}} \quad J_1(T_s)/(1-\gamma^{T_s})$, respectively. T_f is the maximum time interval being considered for the scheduled maintenance. The value of T_f can be set to be much higher than the average time it takes for the probability that all the WECs in faulty state to be close to 1. In our simulations, T_f is set to 50. Table 3.4 reports the values of J^* for the baseline case and cases I-IV. The table also reports the corresponding optimal value of T_s. The values of J^* are compared to the values V^* obtained with the optimal state-based maintenance policy. We can clearly see that the proposed maintenance policy outperforms the scheduled maintenance policy in all four cases. We can also notice that in a few cases, carrying out scheduled maintenance may even result in negative expected return. In such situation, no value of T_s less than T_f can be selected before all the WECs in the wave farm turn into faulty states.

3.5 Conclusion

In this work, we propose an adaptive maintenance strategy for a group of WECs. Today's WECs are characterized by low output power and high failure probability which are incorporated in the system model of the wave farm to be maintained. The optimal policies under different system parameters are analyzed. Results from solving maintenance optimization problem for wave farms may help farm owners to schedule maintenance activities efficiently for different farm sizes. Instead of going for arbitrary maintenance of individual devices, repairing a group of devices all at once can substantially lower the cost of dispatching maintenance vessel fleets.

Although the numerical studies have been carried out with $N = 30$ WECs, the proposed approach could accommodate much larger fleets, since the number of states in our formulation only grows quadratically with N rather than exponentially. The proposed maintenance strategy is also general enough to be applicable not just to the maintenance of wave farms but also to offshore wind farms and other arrays of devices that are expensive to reach, such as offshore weather monitoring sensors. This can be done by appropriately defining the reward and transition probabilities of the deterioration states in those systems.

In future work, one could consider the case where the wave farm state is only partially observable and an inspection is required from time to time to know the exact number of WECs in different states. There have been several studies on maintenance decision under uncertainty. However, a maintenance and inspection strategy for a group of devices in the context of wave energy production has not been explored yet. Future work would also investigate the structure of the optimal policy under partial observability.

3.6 Appendices

3.6.1 Joint Failure Models

If the random transitions at the level of each WEC are statistically independent, $W_{12,t+1}$ and $W_{23,t+1}$ are easily found to follow binomial distributions:

$$W_{12,t+1} \sim Bin(N_{1,t}, p_{12}),$$
$$W_{23,t+1} \sim Bin(N_{2,t}, p_{23}).$$

It is more realistic to assume, however, that the random transitions are not independent, for instance to model deteriorations due to common causes. There are several ways to achieve this:

1. WEC deteriorations are assumed to be pairwise correlated. $W_{ij,t+1}$ given $N_{i,t}$ is decomposed as a sum of dependent Bernoulli random variables,

   $$W_{ij,t+1} = \sum_{k=1}^{N_{i,t}} W^k_{ij,t+1}, \tag{3.16}$$

   where $\mathbb{E}[W^k_{ij,t+1}] = p_{ij}$, $\text{var}[W^k_{ij,t+1}] = p_{ij}(1 - p_{ij})$, and $\text{covar}[W^k_{ij,t+1}, W^\ell_{ij,t+1}] = \rho_{ij} p_{ij}(1 - p_{ij})$. Here ρ_{ij} is the correlation coefficient, assumed to be nonnegative. In this case, $W_{ij,t+1}$ given $N_{i,t}$ follows a *correlated binomial distribution* [92]:

   $$W_{ij,t+1} \sim CB(N_{i,t}, p_{ij}, \rho_{ij}), \tag{3.17}$$

which is statistically equivalent to

$$
\begin{aligned}
W'_{ij,t+1} &= (1-Z)W_1 + Z(N_{i,t}W_2), \\
Z &\sim Bern(\rho_{ij}), \\
W_1 &\sim Bin(N_{i,t}, p_{ij}), \\
W_2 &\sim Bern(p_{ij}),
\end{aligned} \tag{3.18}
$$

that is, a mixture distribution between a binomial and a rescaled Bernoulli with values in $\{0, N_{i,t}\}$. The probability mass function (pmf) of $W_{ij,t+1}$ is

$$
\begin{aligned}
\mathbb{P}[W_{ij,t+1} = w] = (1-\rho_{ij})\binom{N_{i,t}}{w} p_{ij}^{w}(1-p_{ij})^{N_{i,t}-w} \\
+ \begin{cases} \rho_{ij}(1-p_{ij}) & \text{if } w = 0, \\ 0 & \text{if } w = 1, \dots, N_{i,t}-1, \\ \rho_{ij}p_{ij} & \text{if } w = N_{i,t}. \end{cases}
\end{aligned} \tag{3.19}
$$

Thus, higher values of ρ_{ij} lead to greater probabilities of the extreme outcomes $w = 0$ and $w = N_{i,t}$.

2. Let $Z_{0,t+1} \sim Bern(p_c)$ be a common cause indicator, and let $W_{ij,t+1}$ be i.i.d. conditionally to $Z_{0,t+1}$, with $W_{ij,t+1}|(Z_{0,t+1} = 0) \sim Bern(q_{ij,0})$ and $W_{ij,t+1}|(Z_{0,t+1} = 1) \sim Bern(q_{ij,1})$. By marginalizing out $Z_{0,t+1}$, $W_{ij,t+1}$ becomes a mixture of binomials:

$$
\begin{aligned}
\mathbb{P}[W_{ij,t+1} = w] = p_c\binom{N_{i,t}}{w} q_{ij,1}^{w}(1-q_{ij,1})^{N_{i,t}-w} \\
+ (1-p_c)\binom{N_{i,t}}{w} q_{ij,0}^{w}(1-q_{ij,0})^{N_{i,t}-w}.
\end{aligned} \tag{3.20}
$$

The common cause indicator can be shared among $W_{12,t+1}$ and $W_{23,t+1}$, leading to a joint distribution

$$\begin{aligned}
&\mathbb{P}[W_{12,t+1} = w_{12}, W_{23,t+1} = w_{23}] \\
&= p_c[\binom{N_{1,t}}{w_{12}} q_{12,1}^{w_{12}} (1 - q_{12,1})^{N_{1,t} - w_{12}}] \\
&\cdot [\binom{N_{2,t}}{w_{23}} q_{23,1}^{w_{23}} (1 - q_{23,1})^{N_{2,t} - w_{23}}] \\
&+ (1 - p_c)[\binom{N_{1,t}}{w_{12}} q_{12,0}^{w_{12}} (1 - q_{12,0})^{N_{1,t} - w_{12}}] \\
&\cdot [\binom{N_{2,t}}{w_{23}} q_{23,0}^{w_{23}} (1 - q_{23,0})^{N_{2,t} - w_{23}}]. \qquad (3.21)
\end{aligned}$$

3. The probability p_{ij} is assumed to be drawn from a Beta distribution at each transition: $p_{ij,t} \sim Beta(\alpha_{ij}, \beta_{ij})$. Then $W_{ij,t} | p_{ij,t} \sim Bin(N_{i,t}, p_{ij,t})$. That is to say, $W_{ij,t}$ follows a Beta-binomial distribution, the pmf of which is given by

$$\mathbb{P}[W_{ij,t+1} = w] = \binom{N_{i,t}}{w} \frac{B(w + \alpha_{ij}, N_{i,t} - k + \beta_{ij})}{B(\alpha_{ij}, \beta_{ij})},$$

where $B(\alpha, \beta)$ is the beta function.

Methods to estimate α_{ij}, β_{ij} from data are described in [93], since the Beta-binomial is a particular case of the Dirichlet-multinomial distribution.

3.6.2 Derivation of Expected Profit

The R^{gen} function can be estimated by fitting a power output model to data from lab or at-sea experiments on arrays of converters, and taking into account dispatchability and electricity market considerations, as we now describe.

For instance, suppose that from reported lab experiments, the average output of a single WEC is P_1, and the average output of an array of N converters is

$$P_N := (1 + \eta) N P_1,$$

where $(1+\eta)$ is an interaction coefficient. If the interactions are positive ($\eta > 0$), the output is superlinear in N, as documented in [94]. If the interactions are negative ($-1 < \eta < 0$), the output is sublinear in N, as documented in [95]. Given the points $(0,0)$, $(1,P_1)$, (N,P_N), a quadratic power output model can be fitted to estimate the average power output P as a function of $x = N_t^{\mathrm{op}}$:

$$P(x) = P_1(1 - \tfrac{\eta}{N-1})x + P_1\tfrac{\eta}{N-1}x^2.$$

In our system model, $N_t^{\mathrm{op}} = N_{1,t} + N_{2,t}$. The output model could of course be refined by conducting lab experiments with different array sizes.

Suppose it is optimal for the wave farm to bid a certain quantile of its predicted power distribution, in order to maximize its expected profit, as described for instance in [96] and also justified below. As documented in [97], arrays of converters decrease the standard deviation of the aggregated power. Therefore, an increase in $x = N_t^{\mathrm{op}}$ should also help to increase the optimal offer and expected profit.

For instance, suppose the variance of the power output of a single WEC is σ_1^2, and the variance of the power output from the array is

$$\sigma_N^2 = (1+\theta)N\sigma_1^2,$$

where $\theta < 0$ as documented in [97]. Given the points $(0,0)$, $(1,\sigma_1^2)$, (N,σ_N^2), a quadratic model can be fitted to estimate the variance V as a function of $x = N_t^{\mathrm{op}}$:

$$V(x) = \sigma_1^2(1 - \tfrac{\theta}{N-1})x + \sigma_1^2\tfrac{\theta}{N-1}x^2.$$

In the absence of other information on the distribution of the power output, we adopt the maximum entropy distribution for a nonnegative random variable with given mean $P(x)$ and variance $V(x)$. This is known to correspond to a truncated Gaussian distribution on $\mathbb{R}^+$. The mean and standard deviation (μ_x, σ_x) of the Gaussian to be truncated can be obtained by solving numerically for (μ, σ) the nonlinear system of equations

$$\left.\begin{aligned} \mu + \sigma\tfrac{\phi(\mu/\sigma)}{\Phi(\mu/\sigma)} &= P(x) \\ \sigma^2\left[1 - (\mu/\sigma)\tfrac{\phi(\mu/\sigma)}{\Phi(\mu/\sigma)} - \left(\tfrac{\phi(\mu/\sigma)}{\Phi(\mu/\sigma)}\right)^2\right] &= V(x) \end{aligned}\right\} \tag{3.22}$$

which expresses the mean and variance of a truncated Gaussian supported on $[0, +\infty)$ (see e.g. [98]). The quantile function (inverse cdf) at level p of the truncated Gaussian is then given by

$$F^{-1}_{\mu_x,\sigma_x^2}(p) = \mu_x - \sigma_x\Phi^{-1}((1-p)\Phi(\mu_x/\sigma_x)).$$

For the type of two-stage settlement markets studied in [96], the expected hourly profit is then obtained as the optimal value to a newsvendor-type problem (see e.g. [96]),

$$R^{\text{gen}}(x) = \max_{q\geq 0}\{\pi^f q - \mathbb{E}_{p|x}[\pi^s(q-p)^+]\},$$

where π^f is a known forward hourly price of power, π^s is the random penalty hourly price of a shortfall in committed production, $\bar{\pi}_s = \mathbb{E}[\pi^s]$, and power spillage has been assumed to have no penalty. It is optimal to offer a newsvendor-type quantity

$$C_x = F^{-1}_{\mu_x,\sigma_x^2}(\pi^f/\bar{\pi}^s),$$

to get (see e.g. [96])

$$R^{\text{gen}}(x) = \pi^f C_x - \bar{\pi}^s \int_0^{C_x} (C_x - p) f_{\mu_x,\sigma_x^2}(p)dp.$$

Lengthy but straightforward calculations lead to the following particular result for the truncated Gaussian density f_{μ_x,σ_x^2}:

$$R^{\text{gen}}(x) = \pi^f\mu_x + \bar{\pi}^s\sigma_x\frac{\phi(\mu_x/\sigma_x) - \phi(\frac{C_x-\mu_x}{\sigma_x})}{\Phi(\mu_x/\sigma_x)}, \tag{3.23}$$

where (μ_x, σ_x) solves (3.22).

Chapter 4

Optimal Control Strategy of Battery participating in Frequency Regulation Market

4.1 Introduction

In this work, we devise control strategies for GSS systems participating in wholesale FR markets. In particular, control rules are devised by inspecting optimal control solutions that trade off battery health factors such as energy throughput vs. market factors such as the performance score and revenues.

The AGC signals are generated on short time scales (seconds) which implies that accurately following it would lead to high energy exchange rate for the GSS. Such operation clearly affects battery life. Thus, the questions this work answers are twofold. First, what is the trade-off between battery degradation factors and market participation and can it result in improved revenue over the battery life? If so, what control strategy or rules would enable these benefits?

In papers [99] [100] [101], the issues of degradation of batteries participating in FR have been discussed. Papers [99] and [100] focus on evaluating battery degradation and do not provide practical control strategies for market participation. These articles provide good depth on the battery health aspects but make several assumptions such as a zero-mean AGC signal (which may not always be the case). In addition, they do not analyze the tradeoffs between degradation and market revenues making it challenging to devise control strategies with a desired tradeoff. In [101], authors propose a control strategy of intentionally deviating from the regulation signal to achieve higher long term profits though they do not guarantee any performance through optimization. Moreover, the proposed strategy does not account for daily differences in AGC signal and the multitude of battery degradation factors.

The main contribution of our work is to evaluate the optimal trade-off between the GSS performance and degradation factors and devise control rules based on this evaluation. Several control strategies are compared based on the weights assigned to the performance and degradation factors. Co-optimizing revenue and degradation brings more control over GSS degradation factors. We show that the market price as an input and past performance as a feedback to the GSS controller provides control over revenues and guarantees an improved performance. Simple rules for the response signal are devised from the results of the optimization problem and their impact in terms of revenue performance and degradation factors is shown to be better than existing strategies.

The remainder of this chapter is organized as follows. Section II details the problem formulation that includes a brief overview of a typical GSS performance evaluation process, types of degradation models and the optimal control formulations. Section III presents the results obtained and discusses their impact.

4.2 Optimal Battery Control Strategy acknowledging Continuous Degradation

4.2.1 Performance Factor

PJM interconnection evaluates the performance of a resource in FR markets by computing an hourly performance factor pf_h which is defined as weighted sum of following three scores. [102].

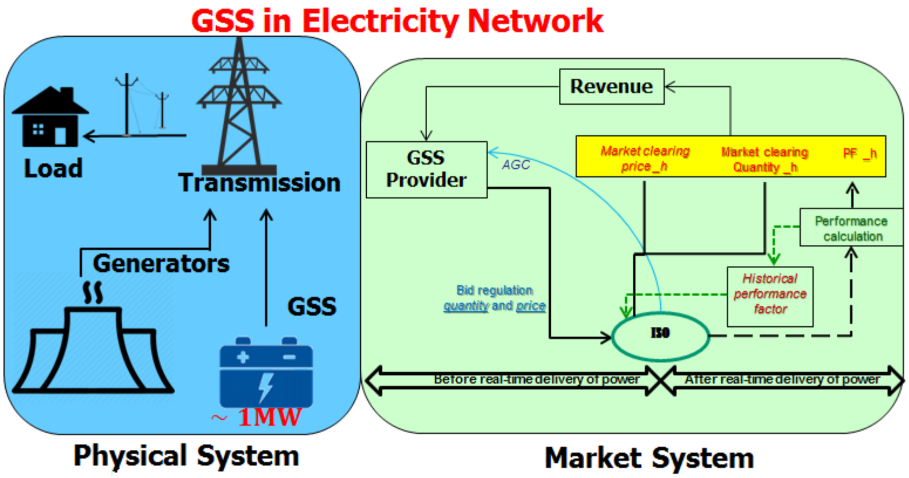

GSS in Electricity Network
Load
Transmission
Generators
GSS
~ 1MW
Physical System
Revenue
GSS Provider
AGC
Market clearing price _h
Market clearing Quantity _h
PF _h
Performance calculation
Historical performance factor
Bid regulation quantity and price
ISO
Before real-time delivery of power
After real-time delivery of power
Market System

Figure 4.1: GSS in electricity network

- Correlation score $= \max_{(\delta=0 \text{ to } 5Min)} \sigma_{Signal,Response}(\delta, \delta + 5Min)$ calculated every 10s. Here σ is correlation function and δ is shifted time steps.
- Delay score $= \dfrac{\delta - 5Min}{5Min}$ calculated every 10s
- Precision score = 1-Abs$\left[\dfrac{\sum Abs(P_t) - \sum Abs(AGC_t)}{\sum Abs(AGC_t)}\right]$ where AGC_t and P_t are AGC and response signal respectively.

4.2.2 Revenue

Resources once qualified to participate in the PJM FR market submit bids for power quantity and price (both capacity and mileage). The day-ahead market is cleared for every hour and hourly market prices α_h are set. In real-time, each market cleared resource is paid an amount adjusted by a performance factor evaluated by SO. Roughly, the hourly payment to a resource i can be described as

$$r_{i,h} = \alpha_h \times pf_{i,h} \tag{4.1}$$

Market regulations has set minimum acceptable performance score below which the participating resource shall be disqualified. The past hourly performance values also impact its future bid selection process. In this regard, SO uses the past performance scores and computes their average in a rolling horizon fashion. This moving average is termed as historical performance score (pf_h^{hs})

4.2.3 Dynamic Programming (DP) Framework

Under the assumption that daily AGC signal, AGC_t, is known in advance, a GSS operator with battery capacity C maximizes total reward over the time horizon T, i.e.

$$\max_{P_t} \sum_{t}^{T} R(P_t, S_t) \tag{4.2}$$

where S_t is the system state and P_t is the action or response signal. The GSS reward function, R_t at each time step t is a weighted sum of instantaneous revenue (r_t) and degradation factor (d_t) written as

$$R = \lambda r_t + (1 - \lambda) d_t, \lambda \in (0, 1) \tag{4.3}$$

The state of charge SoC_t constrained between 0 to 1 defines the physical dynamics of the GSS. Using the above market mechanisms and making following assumptions, we define baseline model(Type 0) and three proposed revenue models(Type I,II,III) to be used in the DP formulation.

- The time horizon, T is chosen as 24 hours.
- A unified time step t for all system variables are chosen as $10s$. AGC signal is interpolated accordingly.
- The hourly performance score pf_h is simplified as only the precision score obtained every 10s defined as

  $$pf_t = 1 - Abs[AGC_t - P_t], t \in (10, 20, \ldots, T = 86400) \tag{4.4}$$

  where AGC_t is interpolated to time step t. Note that the area under the response signal in 10s is energy in/out of GSS (otherwise defined as instantaneous energy-throughput, CtP_t) The correlation and delay scores are removed to maintain causality of revenue variables (from GSS perspective, calculating correlation involves the prediction of its own action to decide current action). In addition, calculating correlation of two signals is computationally expensive and does not provide new insights in market participation.

- Similar to pf_h^{hs} defined by PJM as an average of past 100 steps pf_h, our historical performance definition pf_t^{hs} is a moving-average of fewer past pf_t.
- The dynamic market prices are uniform (same) within an hour.

Degradation Factors

Two types of instantaneous degradation factors (or degradation functions), d_t similar to [103] are defined below:

- Instantaneous normalized energy throughput: $|E|_t^2$
- Instantaneous SoC deviation level: $|\frac{SoC_t - SoC_{ref}}{SoC_{max} - SoC_{ref}}|$

Like performance factor, the value of a degradation factor is normalized from 0 to 1. The instantaneous degradation cost is defined as kd_t where k is a constant that denotes the cost of replacement, maintenance etc incurred due to degradation scaled down to dollar per 10s. The accumulated degradation cost over battery life time signifies lost revenue due to low operating life.

System Models

To incorporate different market elements such as pf_t, α_h, pf_t^{hs}, four types of system models are defined. For each type of revenue models, the system state S_t and objective R_t are defined as follows.

- Type 0: $S_t = (SoC_t, AGC_t)$, $R_t = pf_t$
- Type I: $S_t = (SoC_t, AGC_t)$, $R_t = \lambda pf_t + (1 - \lambda)d_t$

- Type II: $S_t = (SoC_t, AGC_t, \alpha_h)$, $R_t = \lambda C \alpha_h pf_t + (1-\lambda)kd_t$
- Type III: $S_t = (SoC_t, AGC_t, \alpha_h, pf_t^{hs})$, $R_t = \lambda(C\alpha_h pf_t + f(pf_t^{hs}, \alpha_h)) + (1-\lambda)kd_t$

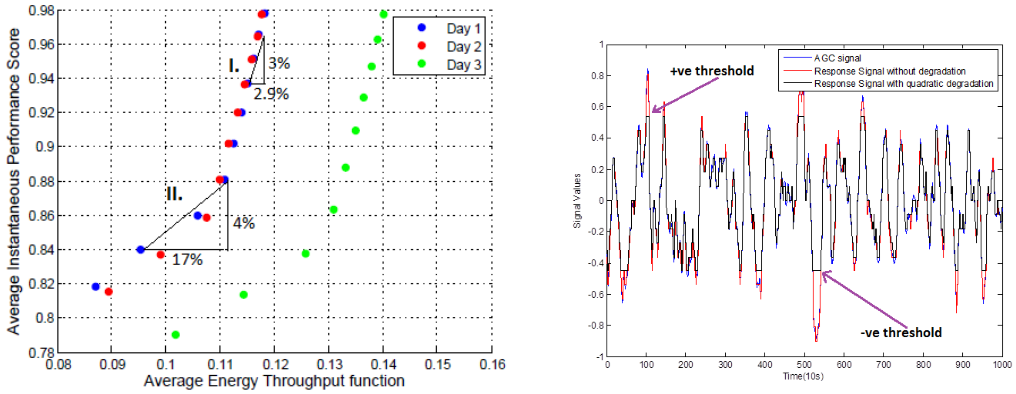
Type 0 is the baseline revenue model in which high performance score can be ensured just by following the AGC signal without violating SoC constraint at all time instant. In type I formulation, only the performance factor pf_t is sought to be maximized and the reward function trades off pf_t vs. the degradation factor d_t. In type II formulation, price is added as a state variable and is considered in the reward function and the revenues are traded off against d_t. In type III, historical performance factor pf_t^{hs} is incorporated in the reward function and $f(.)$ denotes a penalty function for low pf_t^{hs}. In all the above cases d_t is based only on the energy throughput unless SoC based degradation is specifically specified.

In the optimal problem formulation, SoC is discretized into 1000 values, response signal into 22 values and historical performance factor into 50 values. The DP problem formulation is based on the Bellman equation and is solved backward in time for different values of λ to obtain the optimal states and actions.

4.3 Results and Analysis

Results from solving optimization of finite horizon net reward(eq. 4.2) under different problem formulations are presented. In particular, the revenue-degradation trade-off is analyzed using optimal performance factor pf_t^* and optimal degradation factor d_t^* and subjective assessment of the optimal action signal, P_t^* (or response) is discussed. A hypothesis of control rules based on Type I problem result is described and tested using a simulation case study. Type I problem is discussed in detail because its results can be compared to current industry practices(similar to Type 0).

Type II and III problem results and the subsequent control strategies are extensions of the Type I results. They substantiate our argument that there are key market factors' information can help optimize net revenue for the GSS. Finally, results on trade-off and corresponding response signal are obtained using degradation as a function instantaneous



(a) Type I: instantaneous performance-degradation factor (energy throughput) trade-off

(b) Response signal for 3 hours from type I problem formulation

SoC level as types I-III focus only on energy throughput based degradation.

Type I Problem: In Figure 4.2(a), we observe that the trade-off is more pronounced in region II compared to region I suggesting reduction of average degradation($d_{av} = \sum_{t=0}^{T} d_t^*/T$) by lowering average performance factor($pf_{av} = \sum_{t=0}^{T} pf_t^*/T$) can be economically beneficial in long run. However, this trade-off is not as attractive if the current average performance factor is already quite high (region I).

This characteristic of the trade-off is attributed to the fact that the instantaneous energy in and out decreases with more weight,λ, on the degradation compared to revenues. Therefore, the response corresponding to increasing weights on degradation give increasing value of total energy throughput for the same AGC signal in a day. More importantly, the optimal response signal exhibits a cut-off value beyond which AGC signal need not be followed as shown in Figure 4.2(b). Based on these observations, we conjecture that the cut-off value or threshold of the response signal is a function of average instantaneous degradation and devise the following control rules

1. To reduce the value of average degradation factor to "x$\in [0,1]$", the response signal should follow AGC signal till

$$|AGC_t| \leq \frac{k_1 - \sqrt{k_2 - k_3 x}}{2(k_4 - k_1 + \sqrt{k_2 - k_3 x})} \tag{4.5}$$

where k_1, k_2, k_3 and k_4 are constants obtained from curve fitting the degradation factor as a function of the relative weight. The degradation depends on the AGC signal on that particular day. Therefore, we can expect similar values of constants under similar AGCs obtained on different days.

2. This rule should be followed as long as the performance factor is high enough to not run the risk of facing disqualification in the market which is discussed in Type III later.

Type II Problem: The trade-off curve shown in Figure 4.2 is obtained using a periodic bi-level(High-Low) hourly market price structure. As the revenue is a function of market price along with performance score, the trade-off curve is influenced by it. When the market prices are low, the optimal solution aggressively reduces instantaneous cost of degradation d_{av}. Another observation is that the optimal response signal has a cut-off limit which varies linearly in this problem set-up(not shown due to space limitation) with market price and desired hourly cost of degradation. It is understood that when the hourly market price is high, the AGC signal should be followed as closely as possible and when market price is low, the threshold is lower. This threshold can be determined through a similar curve fitting exercise as the one in the discussion of the type I problem above. Figure 4.3 shows the existence of threshold(that also shifts with λ) in optimal response signal under low hourly market price.

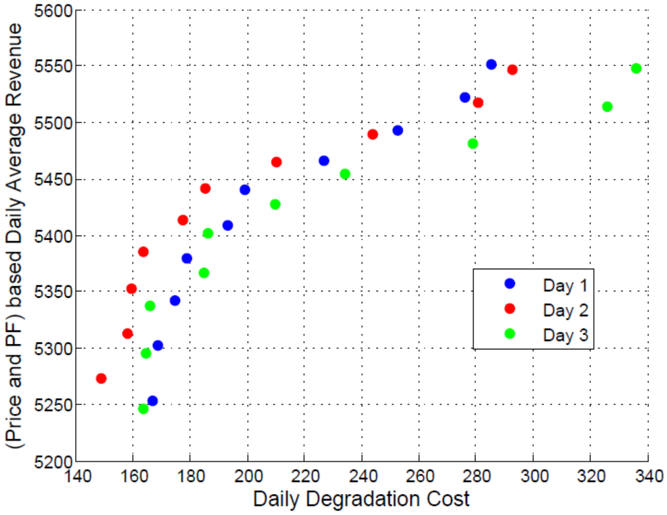


Figure 4.2: Trade-off plot obtained from type II problem formulation

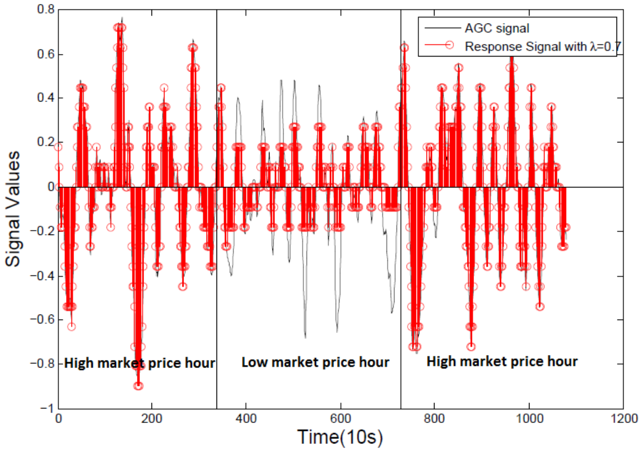


Figure 4.3: Optimal response signal trajectory under type II problem formulation

Type III Problem The results of type III show that control strategies can be developed specifically to prevent the performance score from dropping continuously in Type II problem when market prices are low. The historical performance score is added to the state information to facilitate this. The optimal results are compared against type II problem results under an hourly market price sequence $\{Pr\} = 20, 80, 40, 60$ (i.e. not Type II bi-level prices). As illustrated in figure 4.4, the performance factor stays above 0.7 even in the low market price hour and under reasonable weight to degradation cost in a four hour horizon. The optimal response signal as shown in figure 4.5 tracks the AGC closer during the low price period compared to its counterpart from type II problem solution and achieves close to the same overall reduction in the cost of battery degradation.

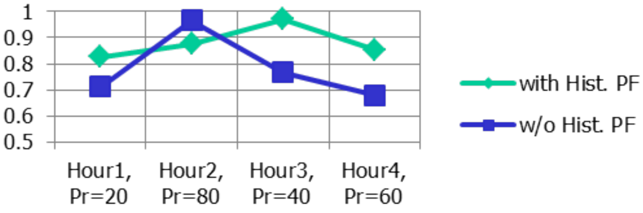


Figure 4.4: Performance score in four hours corresponding to each hourly market price under type III problem formulation

Results from these simple problem formulations show that a rule on response signal can be developed based on the values of historical performance score, SoC and market prices.

The results from using an SoC based degradation factor in the type I problem formu-

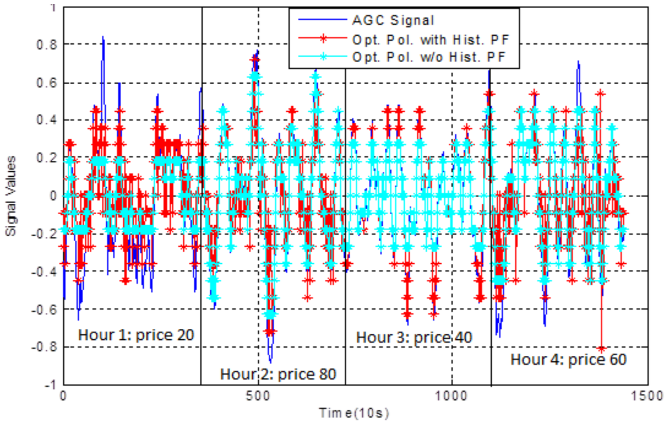


Figure 4.5: Optimal response signal in four hours under type III problem formulation

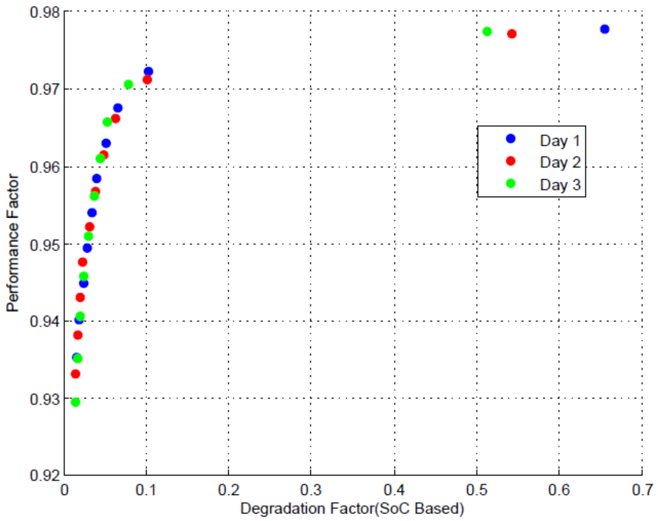


Figure 4.6: Trade-off plot under type I problem formulation that has SoC based degradation factor

lation includes the trade off curve shown in figure 4.6. The SoC and response signal are shown in figure 4.7. Trade-off curve shows that performance factor is not very sensitive to a large range of values of weight on instant degradation cost. This is due to the fact that the SoC transitions are not very drastic in a particular time interval so as to influence the instantaneous energy throughput significantly. However, the SoC level is increasingly tightened around the reference SoC level as more weight is given to instantaneous degradation cost. A reference SoC of 0.5 is chosen in this problem. This hints at control rules based on the acceptable SoC window similar to the AGC threshold discussed in the above cases.

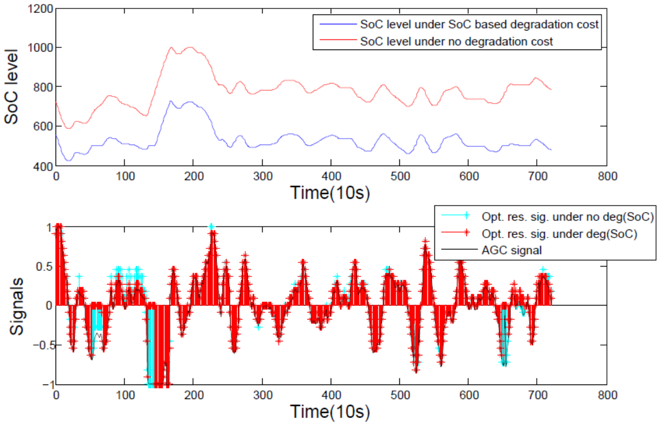


Figure 4.7: SoC level and response signal trajectories obtained from type I problem formulation that has SoC based degradation factor

Chapter 5

GPS Timing Synchronization Attack: Characterization and Detection in Smart Grid Networks

5.1 Introduction

A modern wide area monitoring system supporting the future grid will include a vastly improved information and communications functionality that allow service providers to sense, monitor, and manage electricity flows throughout the grid [104]. While the cyber-physical integration improves the performance and efficiency of the grid, it increases the vulnerability of the grid to potential cyber-attacks. Security of the power grid has received significant attention in the literature [105] - [110]. In this paper, we address the problem of cybersecurity in smart grid networks involving PMUs taking into account the dynamical nature of the power system.

A PMU can record synchrophasors at a high sampling rate, and the measurements are synchronized to an absolute time reference provided by the GPS. It is possible to deceive the GPS receiver by transmitting spurious signals resembling the normal GPS signals, leading to timing synchronization errors and this referred to as a GPS-spoofing attack [111]. In an electric grid with PMUs, GPS spoofing results in counterfeit time stamps to the true phasors and is referred to as the timing synchronization attack (TSA) [112]. Since a TSA only alters the time stamps without inducing changes in the actual measurements, it results in confusing the command center with erroneous system operation status. Evaluating the threat to PMUs and the countermeasures to combat TSA is a topic that has received considerable attention in the literature [113] - [123].

We analyze the implications of TSAs on the dynamical behavior of the power system. The dynamical model of the power system [124] is considered, and it is assumed that PMUs are installed on all the generator buses. We show how TSAs, characterized using a scalar parameter, alter the phasor readings by transforming the system matrix in the measurement equation of the model. In our analysis, the time of attack and the scalar parameter which results in the TSA are assumed unknown. For this setup, we develop a generalized likelihood ratio-based hypotheses testing procedure to detect changes from the normal operating behavior when the system is subjected to a TSA. Monte Carlo simulations using a 9-bus, 3-machine test system are performed to demonstrate (a) the implication of a TSA on the dynamic state estimation (DSE) and (b) the performance of the proposed test. Asymptotic performance results of the test which are applicable to practical (large) smart grid networks are also presented. To the best of our knowledge, this is the first time a characterization of the impact of a TSA on the *dynamic behavior* of power system and its detection is reported in the literature. These studies are important for efficient wide area monitoring and to initiate timely action in the event of a security threat to the grid. The initial results of this work appeared in [125].

In Section 5.2, we present the dynamical model of the power system and characterize the TSA. The hypothesis test to detect the spoofing attack is presented in Section 5.3. Simulation results are in Section 5.4. Concluding remarks are provided in Section 5.5. Asymptotic analysis is relegated to the appendix.

5.2 System Model

5.2.1 Dynamic Model of the Power System

The power system comprising generators, electrical loads and the transmission network is modeled using differential and algebraic equations. At the ith generator, the rotor angle (δ_i), the rotor speed (ω_i) and the internal voltage (E_i) of the synchronous generator are the state variables of the system governed by differential equations, while the nodal voltage magnitudes (V_i) and the phasor angles (θ_i) are the algebraic variables. To analyze the system's behavior we consider the 3$^{\text{rd}}$-order differential equations, which can sufficiently capture the dynamics of state variables [126].

We consider an n-bus, m-generator system where the state vector of the linearized model for synchronous generator is denoted by $\boldsymbol{x}_i = [\Delta\delta_i \; \Delta\omega_i \; \Delta E_i]'$, $i = 1, \ldots, m$ and $[\cdot]'$ denotes the transpose of the vector. The state $\boldsymbol{x}_i$ captures the change of the i^{th} generator's variables around an operating point, which depends on the network topology, generator parameters and the load. In the absence of a control mechanism, a perturbation caused by a change in these components can alter the system stability. We model the evolution of the $3m \times 1$ state vector $\boldsymbol{x}_t = (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_m)$ by

$$\boldsymbol{x}_t \quad = \quad \boldsymbol{A}\boldsymbol{x}_{t-1} + \boldsymbol{v}_t, \tag{5.1}$$

where $\boldsymbol{A}$ is the $3m \times 3m$ (for the 3$^{\text{rd}}$-order model) state transition matrix. The modes given by the eigenvalues of $\boldsymbol{A}$ are assumed to be sufficiently damped for the system to be stable. In other words, a stable open loop system is considered so a zero control input can be employed for simplification. The entries of $\boldsymbol{A}$ are given by the following sub-matrices each of size $m \times m$: $\boldsymbol{A}_{11} = \boldsymbol{0}$ (zero matrix), $\boldsymbol{A}_{12} = \boldsymbol{I}$ (identity matrix), $\boldsymbol{A}_{13} = \boldsymbol{0}$, $\boldsymbol{A}_{21} = g_a(\delta_o, E_o, \theta_o, V_o, Y_L)$, $\boldsymbol{A}_{22} = -\text{diag}(D_i)$, $\boldsymbol{A}_{23} = g_b(\delta_o, E_o, \theta_o, V_o, Y_L)$, $\boldsymbol{A}_{31} = g_c(\delta_o, E_o, \theta_o, V_o, Y_L)$, $\boldsymbol{A}_{32} = \boldsymbol{0}$, $\boldsymbol{A}_{33} = g_d(\delta_o, E_o, \theta_o, V_o, Y_L)$, where D_i is the damping of the i^{th} generator, Y_L is the load admittance, and $(\delta_o, E_o, \theta_o, V_o, Y_L)$ is the operating point around which the system is linearized to make it viable for small signal analysis. The functions $g_a(\cdot)$, $g_b(\cdot)$, $g_c(\cdot)$ and $g_d(\cdot)$ can be written in matrix form [127] and are not presented here for the sake of brevity. The $3m \times 1$ state transition noise vector $\boldsymbol{v}_t$ is assumed to be independently and identically distributed (iid) and Gaussian with $3m \times 1$ zero mean vector and $3m \times 3m$ covariance matrix $\boldsymbol{C}_{v,t}$.

The i^{th}PMU records the voltage magnitude V_i and the phasor angles θ_i, while the rotor speed ω_i is typically measured using a separate sensor and is incorporated into the measurement equation. The $3m \times 1$ measurement vector at time t is the deviation of the measurements from steady state measurement values denoted by $\boldsymbol{y}_{ti} \triangleq [\Delta V_{ri}, \Delta\omega_i, \Delta V_{j_i}]$ where $V_{ri} = V_i \cos(\theta_i), V_{j_i} = V_i \sin(\theta_i)$ and is given by

$$\tilde{\boldsymbol{y}}_t \quad = \quad \boldsymbol{S}\boldsymbol{x}_t + \boldsymbol{w}_t, \tag{5.2}$$

where $\boldsymbol{w}_t$ is the $3m \times 1$ measurement noise vector assumed to be i.i.d. Gaussian with $3m \times 1$ zero mean vector and $3m \times 3m$ covariance matrix $\boldsymbol{C}_{w,t}$. The measurement matrix is given by

$$\boldsymbol{S} \quad = \quad \begin{bmatrix} \boldsymbol{S}_{11} & \boldsymbol{0} & \boldsymbol{S}_{12} \\ \boldsymbol{0} & \boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{S}_{21} & \boldsymbol{0} & \boldsymbol{S}_{22} \end{bmatrix}, \tag{5.3}$$

Here, $\boldsymbol{S}$ is $3m \times 3m$ square block matrix of 9 entries with each entry being a matrix of size $m \times m$ given by

$$
\begin{aligned}
\boldsymbol{S}_{11} &= (-Y_{f_r}\mathrm{diag}_{1:m}(E_{oi}\mathrm{sin}(\delta_{o_i})) \\
&\quad -Y_{f_j}\mathrm{diag}_{1:m}(E_{oi}\mathrm{cos}(\delta_{o_i}))), \qquad (5.4) \\
\boldsymbol{S}_{12} &= (Y_{f_r}\mathrm{diag}_{1:m}(\mathrm{cos}(\delta_{o_i})) \\
&\quad -Y_{f_j}\mathrm{diag}_{1:m}(\mathrm{cos}(\delta_{o_i}))), \qquad (5.5) \\
\boldsymbol{S}_{21} &= (Y_{f_r}\mathrm{diag}_{1:m}(E_{oi}\mathrm{cos}(\delta_{o_i})) \\
&\quad -Y_{f_j}\mathrm{diag}_{1:m}(E_{oi}\mathrm{sin}(\delta_{o_i}))), \qquad (5.6) \\
\boldsymbol{S}_{22} &= (Y_{f_r}\mathrm{diag}_{1:m}(\mathrm{sin}(\delta_{o_i})) \\
&\quad +Y_{f_j}\mathrm{diag}_{1:m}(\mathrm{cos}(\delta_{o_i}))), \qquad (5.7)
\end{aligned}
$$

where $\mathrm{diag}_{1:m}(u_i)$ denotes a square diagonal matrix of size m having u_i at diagonal entry i. Y_{f_r} and Y_{f_j} are the real and imaginary parts of $(Y_G + Y_L + Y_{bus})^{-1}Y_G$ where Y_G and Y_N are the generator and bus admittance matrices [127].

5.2.2 Characterization of TSA

In this subsection, we show how a TSA alters the measurement matrix $\boldsymbol{S}$ in (5.2). The voltage represented in complex phasor form at generator i is given by $\tilde{V}_i = V_{ri} + jV_{j_i}$, where V_{ri} and V_{j_i} denote the real and imaginary components, respectively. A time synchronization attack on a PMU at node i, denoted by the time-shift $\beta_i(t_c)$, modifies the instantaneous nodal voltage signal by introducing a phase change as follows:

$$
\begin{gathered}
\tilde{V}_i(t+\beta_i(t_c)) = V_i(t+\beta_i(t_c)) \times \\
\cos\left[2\pi f_c(t+\beta_i(t_c)) + \theta_i(t+\beta_i(t_c))\right], \qquad (5.8)
\end{gathered}
$$

where t_c denotes the time instant of the spoofing attack. Assuming normal steady state operation before attack (SSOBA), so that the unattacked version of (5.8) is a sinusoid (constant V_i and θ_i over time), the synchronization delay attack changes the model by adding a factor $2\pi f_c\beta_i(t_c)$ to the phase at time t_c, where f_c denotes the operating frequency of the system. The voltage phasor after a TSA can be written as $\tilde{V_i} = V_i\angle(\theta_i + 2\pi f_c\beta_i(t_c)) = \bar{V}_{ri} + j\bar{V}_{ji}$, where $\angle(\cdot)$ denotes the phase. We thus have

$$\begin{aligned}\bar{V}_{ri} &= V_i\cos(\theta_i + 2\pi f_c\beta_i(t_c)) \\ &= V_i\cos(\theta_i)\cos(2\pi f_c\beta_i(t_c)) \\ &\quad -V_i\sin(\theta_i)\sin(2\pi f_c\beta_i(t_c)) \\ &= V_{ri}\cos(2\pi f_c\beta_i(t_c)) - V_{j_i}\sin(2\pi f_c\beta_i(t_c)), \qquad (5.9) \\ \bar{V}_{ji} &= V_i\sin(\theta_i + 2\pi f_c\beta_i(t_c)) \\ &= V_i\sin(\theta_i)\cos(2\pi f_c\beta_i(t_c)) \\ &\quad +V_i\cos(\theta_i)\sin(2\pi f_c\beta_i(t_c)) \\ &= V_{ji}\cos(2\pi f_c\beta_i(t_c)) + V_{ri}\sin(2\pi f_c\beta_i(t_c)), \qquad (5.10)\end{aligned}$$

which can be compactly written as follows:

$$\begin{bmatrix}\bar{V}_{ri} \\ \bar{V}_{ji}\end{bmatrix} = \begin{bmatrix}\cos(2\pi f_c\beta_i(t_c)) & -\sin(2\pi f_c\beta_i(t_c) \\ \sin(2\pi f_c\beta_i(t_c)) & \cos(2\pi f_c\beta_i(t_c))\end{bmatrix}\begin{bmatrix}V_{ri} \\ V_{ji}\end{bmatrix}. \qquad (5.11)$$

However, SSOBA results in

$$\begin{bmatrix}\Delta\bar{V}_{ri} \\ \Delta\bar{V}_{ji}\end{bmatrix} = \begin{bmatrix}\cos(2\pi f_c\beta_i(t_c)) & -\sin(2\pi f_c\beta_i(t_c) \\ \sin(2\pi f_c\beta_i(t_c)) & \cos(2\pi f_c\beta_i(t_c))\end{bmatrix}\begin{bmatrix}\Delta V_{ri} \\ \Delta V_{ji}\end{bmatrix}. \qquad (5.12)$$

Using $[\Delta V_r \ \Delta V_j]' = [\Delta V_{r1}, \ldots, \Delta V_{rm}, \Delta V_{j1}, \ldots, \Delta V_{jm}]'$

$$\begin{bmatrix}\Delta V_r \\ \Delta V_j\end{bmatrix} = \begin{bmatrix}\boldsymbol{S}_{11} & \boldsymbol{S}_{13} \\ \boldsymbol{S}_{31} & \boldsymbol{S}_{33}\end{bmatrix}\begin{bmatrix}\Delta\delta \\ \Delta E\end{bmatrix}, \qquad (5.13)$$

we can write

$$\begin{bmatrix}\Delta\bar{V}_r \\ \Delta\bar{V}_j\end{bmatrix} = \begin{bmatrix}\boldsymbol{M}_1 & -\boldsymbol{M}_2 \\ \boldsymbol{M}_2 & \boldsymbol{M}_1\end{bmatrix}\begin{bmatrix}\boldsymbol{S}_{11} & \boldsymbol{S}_{13} \\ \boldsymbol{S}_{31} & \boldsymbol{S}_{33}\end{bmatrix}\begin{bmatrix}\Delta\delta \\ \Delta E\end{bmatrix}, \qquad (5.14)$$

where $\boldsymbol{M}_1 = \text{diag}_{1:m}(\cos(2\pi f_c \beta_i(t_c)))$ and $\boldsymbol{M}_2 = \text{diag}_{1:m}(\sin(2\pi f_c \beta_i(t_c))$. The new measurement equation after a TSA is given by

$$\boldsymbol{y}_t \quad = \quad \boldsymbol{M}\boldsymbol{S}\boldsymbol{x}_t + \boldsymbol{v}_t, \tag{5.15}$$

where

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{M}_1 & \boldsymbol{0} & -\boldsymbol{M}_2 \\ \boldsymbol{0} & \boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{M}_2 & \boldsymbol{0} & \boldsymbol{M}_1 \end{bmatrix}. \tag{5.16}$$

In effect, the GPS spoofing attack under SSOBA can be modeled as modification of the observation matrix based on the attack parameters $\beta_i(t_c)$. Using the measurements $\boldsymbol{y}_t$, the goal of this paper is detect changes in the observation matrix due to a TSA in the given power network.

5.3 Detection of TSA

The theory of hypothesis testing has been well developed in the statistics literature [128], while being further refined for many practical applications by the signal processing community [129]. Given fully known statistical models for a set of sensor observations under two different possible circumstances which are called hypotheses H_0 and H_1, the theory will allow one to make optimum decisions on which hypothesis is true. The optimality criterion is related to the probability that one makes the wrong decisions. In this paper, the observations are made by some PMUs (augmented by some other sensors), and H_0 represents the hypothesis that the no PMU is subjected to a GPS spoofing attack, while H_1 represents the hypothesis that some PMU was subjected to an attack.

For the observation model in (5.15), let $p(\boldsymbol{y}|H_j), j = 0, 1$, denote the probability density function (PDF) of the observations evaluated when H_j is true. This is proportional to the probability that the observations are in an infinitesimally small region around the actual observations $\boldsymbol{y}$ when H_j is true. We can compute the probability that the observations $\boldsymbol{y}$

lie in some set by integrating the appropriate PDF (under H_0 or H_1) over all $\boldsymbol{y}$ in that set. Let $\Pr(H_j)$ denote the probability of H_j being true; note that, $\Pr(H_0) = 1 - \Pr(H_1)$. There are two types of errors the test can make, and thus two types of probabilities of error: the probability the test picks H_1 when H_0 is true, or the probability the test picks H_0 when H_1 is true. Let Γ be the the set of all $\boldsymbol{y}$ for which the test will decide H_1. Thus for any $\boldsymbol{y} \notin \Gamma$ the test will decide for H_0. The total (average) probability of error is

$$\begin{aligned} p_e &\overset{(a)}{=} \Pr(H_0) \int_{x \in \Gamma} p(\boldsymbol{y}|H_0) d\boldsymbol{y} + \Pr(H_1) \int_{y \notin \Gamma} p(\boldsymbol{y}|H_1) d\boldsymbol{y} \\ &= \Pr(H_0) \int_{y \in \Gamma} p(\boldsymbol{y}|H_0) d\boldsymbol{y} \\ &\quad + \Pr(H_1) \left(1 - \int_{y \in \Gamma} p(\boldsymbol{y}|H_1) d\boldsymbol{y} \right) \\ &= \Pr(H_1) + \\ &\quad \int_{y \in \Gamma} \left(\Pr(H_0) p(\boldsymbol{y}|H_0) - \Pr(H_1) p(\boldsymbol{y}|H_1) \right) d\boldsymbol{y}, \end{aligned} \tag{5.17}$$

where the first term in (a) is $\Pr(H_0)$ times the probability the test makes an error by deciding for H_1 when H_0 is true, denoted as $\Pr(\text{decide } H_1|H_0)$ and called the probability of false alarm (P_f). The second term in (a) is $\Pr(H_1)$ times the probability the test makes an error by deciding for H_0 when H_1 is true, denoted as $\Pr(\text{decide } H_0|H_1) = 1 - \Pr(\text{decide} H_1|H_1)$. $\Pr(\text{decide } H_1|H_1)$ is called the probability of detection (P_d).

In order to make p_e as small as possible, we include $\boldsymbol{y}$ in Γ if these $\boldsymbol{y}$ make $\Pr(H_0)p(\boldsymbol{y}|H_0) < \Pr(H_1)p(\boldsymbol{y}|H_1)$ since including these $\boldsymbol{y}$ in Γ will make p_e smaller from the last line of (5.17). For any $\boldsymbol{y}$ such that $\Pr(H_0)p(\boldsymbol{y}|H_0) > \Pr(H_1)p(\boldsymbol{y}|H_1)$, these $\boldsymbol{y}$ must be kept out of Γ since they will make p_e larger if they are included. Note that any $\boldsymbol{y}$ that provide $\Pr(H_0)p(\boldsymbol{y}|H_0) = \Pr(H_1)p(\boldsymbol{y}|H_1)$ can be either put into or left out of Γ, and they will have no impact on p_e. This optimum test is called the likelihood ratio test, which compares the ratio of $p(\boldsymbol{y}|H_1)$ to $p(\boldsymbol{y}|H_0)$ to the threshold $\tau = \Pr(H_0)/\Pr(H_1)$. If $\Pr(H_0) = \Pr(H_1)$ then the likelihood ratio test chooses H_1 if the probability that the observations are in an infinitesimally small region around the measured value of $\boldsymbol{y}$ when H_1 is true is larger than the probability that the observations are in an infinitesimally small region around the measured $\boldsymbol{y}$ when H_0 is true. Now if we have prior knowledge that H_0 or H_1 are more likely, then this should bias our decision, which is what the likelihood ratio tells us to do from the threshold $\tau = \Pr(H_0)/\Pr(H_1)$. In fact there is a trade off between the two types of errors $\Pr(\text{decide } H_1|H_0)$ or $\Pr(\text{decide } H_0|H_1)$ set by the threshold. Thus if we make $\tau < 0$ then we can make $\Pr(\text{decide } H_0|H_1) = 0$ since we always decide for H_1 but we also make $\Pr(\text{decide } H_1|H_0) = 1$. If we set $\tau = \infty$ then we never decide for H_1 and so $\Pr(\text{decide } H_1|H_0) = 0$ but $\Pr(\text{decide } H_0|H_1) = 1$. In general we can prove that making τ larger always makes $\Pr(\text{decide } H_1|H_0)$ smaller and $\Pr(\text{decide } H_0|H_1)$ larger.

In our problem, $p(\boldsymbol{y}|H_1)$ contains some unknown parameters (say, θ), and so we denote this as $p(\boldsymbol{y}|\theta, H_1)$. In such cases, it is common to employ the generalized likelihood ratio test (GLRT) which replaces the likelihood ratio with

$$\frac{\max_{\theta} p(\boldsymbol{y}|\theta, H_1)}{p(\boldsymbol{y}|H_0)}. \tag{5.18}$$

The interpretation is that we employ an estimate of the unknown parameter θ which maximizes the likelihood function of the observation. If the estimate of θ is very accurate, then the GLRT is close to the optimum test (*i.e.* the likelihood ratio test). In our problem, the performance loss of GLRT compared to the likelihood ratio test is not very large and the loss tends to decrease as we employ more high quality data.

We now present a test to detect changes in the measurement matrix in the event of a TSA. Let us suppose that a TSA has been initiated at the time instant t_c, leading to an alteration of the measurement matrix $\boldsymbol{S}$. We denote the resulting measurement matrix by $\boldsymbol{S}_c \triangleq \boldsymbol{MS}$ (see (5.15)). Given the set $\boldsymbol{y}^T \triangleq \{\boldsymbol{y}_0, \ldots, \boldsymbol{y}_{T-1}\}$ of measurements, the problem is formulated as one of devising a statistical testing procedure to detect the change - owing to an attack - in the measurement matrix as reliably as possible. More precisely, we need to devise a test to distinguish between the following two hypotheses:

$$\begin{cases} H_0 : \boldsymbol{y}^T \text{ in } (5.2), \boldsymbol{S} = \boldsymbol{S}_0, \quad t = 0, \ldots, T-1 \\ H_1 : \boldsymbol{y}^T \text{ in } (5.2), \boldsymbol{S} = \begin{cases} = \boldsymbol{S}_0, \quad t = 0, \ldots, t_c - 1 \\ = \boldsymbol{S}_c \neq \boldsymbol{S}_0, \quad t = t_c, \ldots, T-1. \end{cases} \end{cases}$$

The hypotheses test involves comparing a test statistic to a threshold and is of the form $\Lambda \overset{[}{H_0}]H_1\gtrless\rho$ where Λ is the test statistic and ρ is the test threshold. We adopt the Neyman-Pearson criterion to set ρ for a given false alarm probability [129]. The likelihood ratio test statistic is given by

$$\Lambda \;=\; \frac{p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1};\boldsymbol{S}_c)\times\cdots\times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c};\boldsymbol{S}_c)}{p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1})\times\cdots\times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c})}. \tag{5.19}$$

The conditional probability $p(\boldsymbol{y}_t|\boldsymbol{y}_{t-1};\boldsymbol{S}_c)$ under hypothesis H_1 is given by, for $t=t_c,\ldots,T-1$,

$$p(\boldsymbol{y}_t|\boldsymbol{y}_{t-1};\boldsymbol{S}_c) \;=\; \frac{\exp\left\{-\frac{1}{2}(\boldsymbol{y}_t-\boldsymbol{\mu}_{1t})'\boldsymbol{\Sigma}_{1t}^{-1}(\boldsymbol{y}_t-\boldsymbol{\mu}_{1t})\right\}}{(2\pi)^{K/2}|\boldsymbol{\Sigma}_{1t}|^{1/2}},$$

where $\boldsymbol{\mu}_{1t}\triangleq\mathbb{E}[\boldsymbol{y}_t|\boldsymbol{y}_{t-1}]=\boldsymbol{S}_c\boldsymbol{A}\boldsymbol{S}_c^{-1}\boldsymbol{y}_{t-1}$ is the mean vector and $\boldsymbol{\Sigma}_{1t}\triangleq\mathrm{Cov}[\boldsymbol{y}_t|\boldsymbol{y}_{t-1}]=\boldsymbol{S}_c\boldsymbol{A}\boldsymbol{S}_c^{-1}\boldsymbol{C}_{w,t-1}(\boldsymbol{S}_c\boldsymbol{A}\boldsymbol{S}_c^{-1})'+\boldsymbol{S}_c\boldsymbol{C}_{v,t}\boldsymbol{S}_c'+\boldsymbol{C}_{w,t}$ is the covariance matrix. For the likelihood function under H_0, $\boldsymbol{\mu}_{1t}$ and $\boldsymbol{\Sigma}_{1t}$ will be replaced by $\boldsymbol{\mu}_{0t}$ and $\boldsymbol{\Sigma}_{0t}$, respectively, while the matrix $\boldsymbol{S}_c$ will be replaced by $\boldsymbol{S}_0$. In our problem setup, the measurement matrix $\boldsymbol{S}_c$ after a TSA and the time instant t_c when the spoofing attack is launched on the PMUs are unknown, and will have to be estimated; therefore, GLRT (5.18) is employed. From (5.15) and (5.16), we see that estimating the matrix $\boldsymbol{S}_c$ is equivalent to estimating the parameter β, which results in GPS spoofing. The GLRT statistic is given by

$$\frac{\max\limits_{t_c}\max\limits_{\beta}\left[p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1};\boldsymbol{S}_c)\times\cdots\times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c};\boldsymbol{S}_c)\right]}{p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1})\times\cdots\times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c})}. \tag{5.20}$$

The maximum likelihood (ML) estimates of β and t_c are obtained as follows. We consider a discrete set $\mathcal{T}_c$ of time instants at which TSA can be launched. For every $t_c\in\mathcal{T}_c$, the value of β that maximizes the likelihood function $[p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1};\boldsymbol{S}_c)\times\cdots\times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c};\boldsymbol{S}_c)]$ is the ML estimate of β, and is denoted by $\hat{\beta}$. The value of t_c that maximizes the function $\max_\beta\,[p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1};\boldsymbol{S}_c)\times\cdots\times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c};\boldsymbol{S}_c)]$ is the ML estimate of t_c and is denoted by $\hat{t}_c$.

Taking logarithms on both sides of (5.20), the test becomes

$$
\begin{aligned}
\ln \Lambda &= \Lambda' \overset{[}{H}_0]H_1 \gtrless \ln \rho = \rho', && (5.21)\\
\Lambda' &= \sum_{t=\hat{t}_c}^{T-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})' \boldsymbol{\Sigma}_{0t}^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{0t}) \\
&\quad - (\boldsymbol{y}_t - \boldsymbol{\mu}_{1t})' \boldsymbol{\Sigma}_{1t}^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{1t}), && (5.22)\\
\rho' &= \sum_{t=\hat{t}_c}^{T-1} 2\rho - \ln \left\{ \frac{|\boldsymbol{\Sigma}_{0t}|}{|\boldsymbol{\Sigma}_{1t}|} \right\}, && (5.23)\\
\boldsymbol{\mu}_{0t} &= \boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1} \boldsymbol{y}_{t-1}, && (5.24)\\
\boldsymbol{\mu}_{1t} &= \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{y}_{t-1}, && (5.25)\\
\boldsymbol{\Sigma}_{0t} &= \boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1} \boldsymbol{C}_{w,t-1} \left(\boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1} \right)' \\
&\quad + \boldsymbol{S}_0 \boldsymbol{C}_{v,t} \boldsymbol{S}_0' + \boldsymbol{C}_{w,t}, && (5.26)\\
\boldsymbol{\Sigma}_{1t} &= \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{C}_{w,t-1} \left(\hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \right)' \\
&\quad + \hat{\boldsymbol{S}}_c \boldsymbol{C}_{v,t} \hat{\boldsymbol{S}}_c' + \boldsymbol{C}_{w,t} && (5.27)
\end{aligned}
$$

Under hypothesis H_0, $(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})'\boldsymbol{\Sigma}_{0t}^{-1}(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})$ is central Chi squared, while $(\boldsymbol{y}_t - \boldsymbol{\mu}_{1t})'\boldsymbol{\Sigma}_{1t}^{-1}(\boldsymbol{y}_t - \boldsymbol{\mu}_{1t})$ is the generalized Chi squared each with $3m$ degrees of freedom (d.o.f.). For $t = 0, \ldots, T-1$, we thus see that the under H_0, the test statistic Λ in (5.19) is the difference between the central Chi squared and the generalized Chi squared random variables each with $3m \times (T - t_c)$ d.o.f. whose PDF is difficult to establish in closed-from [130]. We, therefore, resort to numerical evaluation to analyze the performance of the test in Section 5.4.

For sake of comparison, we also present one ad hoc test that has been employed in similar problems. This test is sometimes called the residual test. The residual is given by $\boldsymbol{r}_t = \boldsymbol{y}_t - \hat{\boldsymbol{y}}_{t|t-1}$, where $\hat{\boldsymbol{y}}_{t|t-1}$ is the predicted measurement vector computed by a Kalman filter. The residual test compares $||\boldsymbol{r}_t||^2$ to a threshold chosen to fix the false alarm probability.

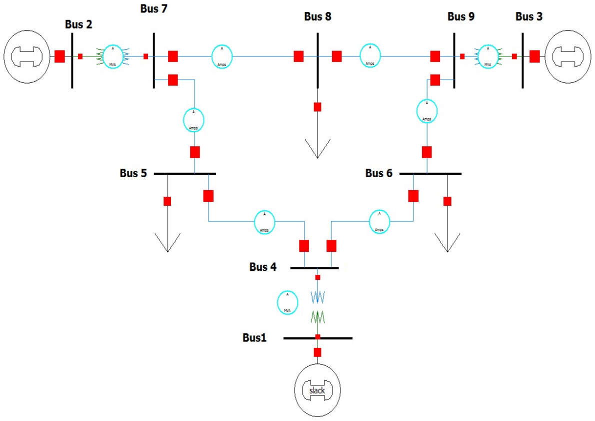


Figure 5.1: A 3 Machine, 9 bus test system (known as P.M Anderson 9 Bus).

5.4 Simulation Results

We conduct experiments on the 9−bus 3−machine Western System Coordinating Council (WSCC) test case with the state space model specified in [126] to demonstrate the effect of a TSA and to verify the performance of the hypotheses test in (5.21). A block diagram of the test bus system is shown in Fig. 5.1. A PMU is assumed to be located at each of the generator nodes. Although TSAs can be launched on several PMUs simultaneously, in this paper we give detailed discussion for the case of a single PMU (on node $i = 1$) being compromised. The results are based on $L = 5 \times 10^4$ Monte Carlo (MC) simulations. First we linearize our system model around an operating point as described in [127]. Let S_0 denote the output matrix of this linearized state space model. In the linearized state space model, we choose the covariance matrices $C_{w,t}$ (corresponding to noise vector in input-output equation) and $C_{v,t}$ (corresponding to the noise vector in state update equation) to be $\sigma^2 \boldsymbol{I}$ with $\sigma = 0.01$. The dynamic state estimation (DSE) procedure is implemented by employing the discrete-time Kalman Filter (KF) for $t = 0.1$ to 10s at a sampling rate of 100 samples/s.

At the time instant $t = 5$s, we launch a TSA by setting the attack parameter at node 1 equal to 8.33ms and the attack parameter for all other nodes equal to 0, *i.e.*, $\beta_i(t_c) = b_1 = 1/2f_c = 8.33$ms for $i = 1$ and $\beta_i(t_c) = 0$ for $i \neq 1$, where $f_c = 60$Hz is the grid frequency and β_i denotes the attack parameter at the i^{th} node which alters the

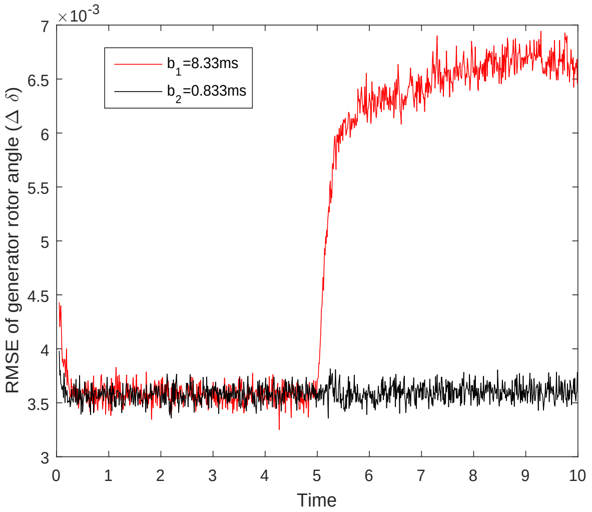


Figure 5.2: RMSE of the rotor angle $\Delta\delta_1$ when the TSA is induced at $t_c = 5$s. $\beta_1(t_c) = b_1$ or b_2 where $b_1 = 8.33$ms and $b_2 = 0.833$ms.

measurement matrix of the model. After the attack, the KF continues to update the state estimate on receiving a new observation y_t according to $\hat{x}_{t|t} = \hat{x}_{t|t-1} + K_t(y_t - S_0\hat{x}_{t|t-1})$ when the output matrix has changed from S_0 to $S_c = MS_0$, where M is given in (5.16). The performance of the filtering algorithm is assessed by plotting the root mean squared error (RMSE) of the estimated state variable as a function of time. The RMSE for the rotor angle $\Delta\delta_i$ at time t is given by

$$\text{RMSE}_{\Delta\delta_i,t} = \sqrt{\frac{1}{L}\sum_{\ell=1}^{L}\left(\hat{\Delta\delta}^{\ell}_{i,t} - \Delta\delta^{\ell}_{i,t}\right)^2}, \tag{5.28}$$

where $\hat{\Delta\delta}^{\ell}_{i,t}$ and $\Delta\delta^{\ell}_{i,t}$ denote the estimate and the true value, respectively, of the rotor angle at time t in the ℓ^{th} MC simulation. The RMSE for the internal voltage ΔE_i of the i^{th} generator is defined analogously. In Fig 2, we plot the RMSE of the rotor angle of the synchronous generator at node 1 as a function of time for normal operating conditions and when a TSA is launched on the bus system. It can be seen that, due to TSA at $t = 5$s there is a sudden increase in the RMSE; such a drastic performance change is not observed under normal operating conditions. A similar behavior is observed in the plot of the RMSE of the internal voltage of the generator at node 1 as shown in Fig 3. Such

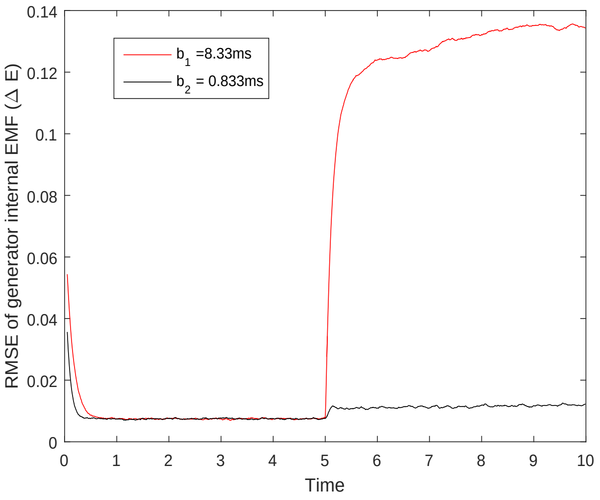


Figure 5.3: RMSE of the internal voltage ΔE_1 of the generator 1 when the TSA is induced at $t_c = 5$s. $\beta_1(t_c) : b_1 = 8.33$ms or $b_2 = 0.833$ms.

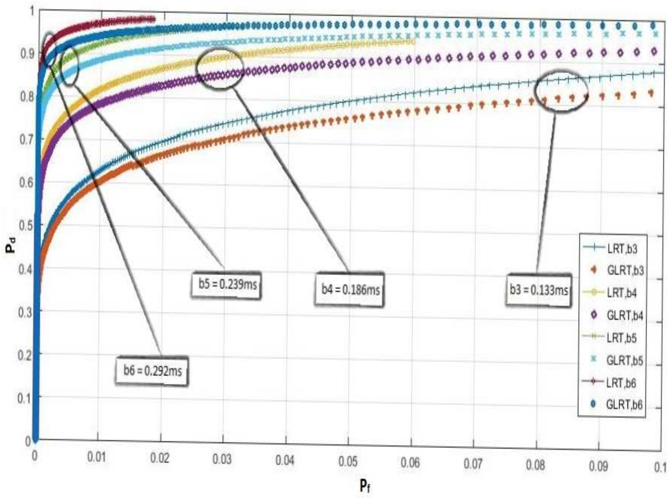


Figure 5.4: The ROCs of the proposed test compared to that of LRT for different values of the attack parameter.

drastic degradation in the performance is hazardous, since erroneous state estimates can result in wrong control signals issued by the command center. When $\beta_1(t_C) = b_1$ the change in performance is easily recognizable. However, when the magnitude of the TSA is small, say $\beta_1(t_c) = b_2 = 0.1b_1$, the change is not recognizable as shown in Fig. 5.2 and Fig. 5.3. Our proposed hypotheses test can efficiently detect whether the system is under attack even for small magnitudes of TSA.

To analyze the performance of the proposed detection scheme, we plot the receiver operating characteristics (ROC) of the test in (5.21) which is the most well accepted measure [129]. For the false alarm probability $P_f \in (0, 1]$, the detection probability P_d is computed using L Monte Carlo instantiations. The ROCs are plotted for different attack parameters: $\beta_1(t_c) = b_3 = 0.133$ms, $\beta_1(t_c) = b_4 = 0.186$ms, $\beta_1(t_c) = b_5 = 0.239$ms, and $\beta_1(t_c) = b_6 = 0.292$ms. As shown in Fig. 5.4 the detection performance improves with increased magnitudes of the attack parameter. In the literature, it is discussed that attack parameters smaller than 0.013ms are insignificant since they do not affect normal system operations. Thus, TSAs caused by $\beta_1(t_c) < 0.013$ms need not be detected. We also compare the ROC of the proposed test with the clairvoyant likelihood ratio test (LRT), in which $\beta_1(t_c)$ is assumed to be known and gives an upper bound on the performance of the proposed test. As shown in Fig. 5.4, the performance of the proposed test is comparable to that of LRT.

In the next experiment, we show the effect of window size (*i.e.* the time span over which the system is observed) on the performance of the test. Increased window size provides more data samples, which enables a better characterization of the TSA and also reduces the effect of noise. However, it also increases the delay in making the decision, since the hypotheses test can be performed only after collecting all the samples in the specified timeframe. In Fig. 5.5, we plot of ROCs of the proposed test and that of LRT for different window sizes. It can be seen that for 60 samples, the performance of the test is quite reasonable even for a small value for β. This result is important from the standpoint of practical implementation, since the test can provides a reasonably good performance even with a smaller number of samples and for short time windows. For the attack parameter of 0.278ms, the results in Fig. 5.5 indicate significant improvement in performance for increasing time windows, suggesting a tradeoff between the desired performance and tolerable delay.

Next, we demonstrate the performance degradation of the test when the time of attack t_c is unknown. The ROCs of the proposed test and LRT are obtained for $\beta = 0.236$ms and window sizes 100 and 200. As shown in Fig. 5.6, the performance of the test expectedly

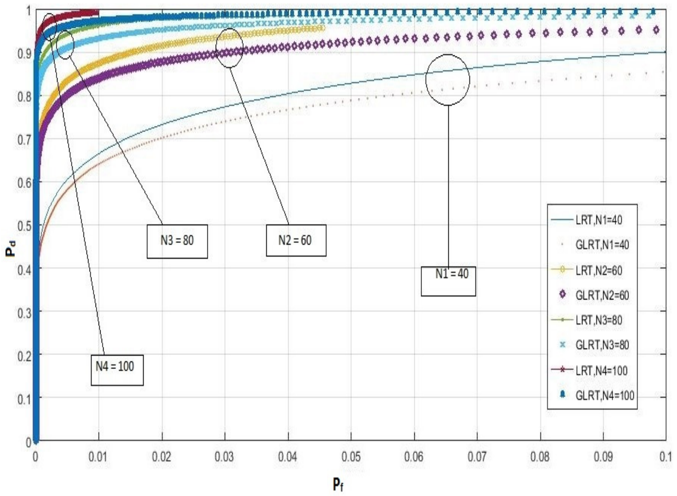


Figure 5.5: The ROCs of the proposed test and that of LRT for different window sizes: $N_1 = 100$, $N_2 = 80$, $N_3 = 60$, $N_4 = 40$.

degrades when t_c is unknown (hence, estimated). The degradation in performance is mainly due to the error incurred in estimating t_c. However, the performance degradation is negligible for larger window sizes.

We also compare the performance of the proposed test with the standard residual test, which is an ad-hoc test that has been frequently employed in the power systems literature. For a given false alarm rate, the probability of detection can be easily computed using known procedures. We plot the ratio of detection probabilities of the residual test and the proposed test for different sample sizes. As shown in Fig. 5.7, the proposed test consistently outperforms the residual test for small magnitudes of the TSA. This shows considerable improvement in performance of detection of the TSA using the proposed test over an ad-hoc test.

5.5 Concluding remarks

A natural extension of this work is to analyze the performance of our test when multiple PMUs are attacked leading to a larger separation between the two distributions $p(\boldsymbol{y}|H_0)$ and $p(\boldsymbol{y}|H_1)$. This suggests an improved performance of the proposed test when more than one PMU in the network is subject to a TSA. Simulation results confirmed that

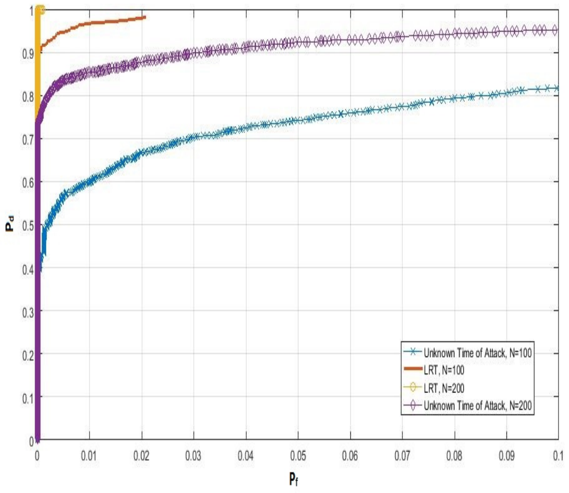


Figure 5.6: The ROCs of the proposed test for unknown time of attack. The ROC of the clairvoyant LRT is also plotted.

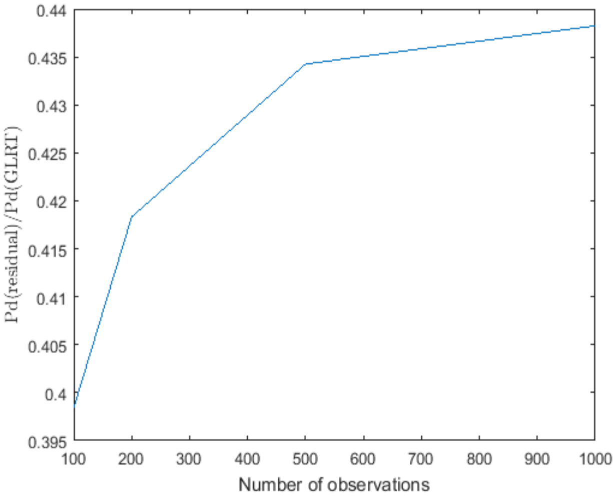


Figure 5.7: The ratio of Probability of detection obtained from residual test and GLRT test versus number of observations used in the tests

when multiple PMUs in the grid were attacked, the ROC of proposed test was more favorable than the ROC when a single PMU was subject to a TSA. In the interest of space, we do not include those results in this paper. We have reported the results of our proposed test for a small bus system (see Fig. 5.1) as an aid to present the main part of the paper clearly. However, the number of nodes in a wide-area smart grid network is quiet large, and with the initiative of power utilities to populate the grid with a greater number of PMUs, it is important to extend the analysis of this work to large scale networks. From an engineering viewpoint, the characterization of the performance of the test for a very large number m of buses demands attention. In the appendix, we derive the asymptotic (large m) expressions for the threshold and probability of detection P_d which can be used to analyze the performance of the test in these practical (large) scenarios.

For real world power networks spread over a wide geographical area, *i.e.*, when the number of buses in the grid is very large ($m \to \infty$), we can efficiently approximate the test statistic to derive its asymptotic PDF under both hypotheses H_0 and H_1. Using these asymptotic PDFs, computable expressions for the test threshold ρ' and the probability of detection P_d are derived. These expressions are not applicable to the WSCC test case (since m is very small) considered in this paper. Note that, the test statistic is the same as given in (5.21).

.0.1 Asymptotic ($m \to \infty$) PDF of the test statistic under H_0

We denote $z_{0t,H_0} = (\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})'\boldsymbol{\Sigma}_{0t}^{-1}(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})$ and $z_{1t,H_0} = (\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})'\boldsymbol{\Sigma}_{1t}^{-1}(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})$ when $\boldsymbol{y}_t$ is sampled from the distribution corresponding to the null hypothesis H_0. It is seen that $(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})$ is Gaussian distributed with the $3m \times 1$ mean vector $\boldsymbol{\gamma}_{0t,H_0} = \mathbb{E}_{H_0}[\boldsymbol{y}_t - \boldsymbol{\mu}_{0t}] = \boldsymbol{S}_0\boldsymbol{A}\boldsymbol{S}_0^{-1}\boldsymbol{y}_{t-1} - \boldsymbol{S}_0\boldsymbol{A}\boldsymbol{S}_0^{-1}\boldsymbol{y}_{t-1} = \boldsymbol{0}$ and the $3m \times 3m$ positive definite covariance matrix $\boldsymbol{\Omega}_{0t,H_0} = \mathbb{E}_{H_0}[(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})']$. Further, $(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})$ is Gaussian distributed with the $3m\times1$ mean vector $\boldsymbol{\gamma}_{1t,H_0} = \mathbb{E}_{H_0}[\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t}] = \boldsymbol{S}_0\boldsymbol{A}\boldsymbol{S}_0^{-1}\boldsymbol{y}_{t-1} - \hat{\boldsymbol{S}}_c\boldsymbol{A}\hat{\boldsymbol{S}}_c^{-1}\boldsymbol{y}_{t-1}$ and the $3m\times3m$ positive definite covariance matrix $\boldsymbol{\Omega}_{1t,H_0} = \mathbb{E}_{H_0}[(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t} - \boldsymbol{\gamma}_{1t,H_0})(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t} - \boldsymbol{\gamma}_{1t,H_0})']$.

Thus, both z_{0t,H_0} and z_{1t,H_0} follow the generalized Chi square distribution [131]. It has been shown that the generalized Chi square distribution can be approximated as the noncentral Chi square distribution $\chi^2_{3m}(\lambda)$ with $3m$ degrees of freedom (d.o.f.) and noncentrality parameter λ [132]. In our problem setup, $z_{0t,H_0} \sim \chi^2_{3m}(\lambda_{0t,H_0})$ with $\lambda_{0t,H_0} = \frac{1}{2}\boldsymbol{\gamma}'_{0t,H_0}\boldsymbol{\Sigma}_{0t}^{-1}\boldsymbol{\gamma}_{0t,H_0} = 0$, and $z_{1t}|H_0 \sim \chi^2_{3m}(\lambda_{1t,H_0})$ with $\lambda_{1t,H_0} = \frac{1}{2}\boldsymbol{\gamma}'_{1t,H_0}\boldsymbol{\Sigma}_{1t}^{-1}\boldsymbol{\gamma}_{1t,H_0}$. Under hypothesis H_0, the test statistic Λ is, therefore, the difference between a central Chi square RV with $3m(T-\hat{t}_c)$ d.o.f. and a noncentral Chi square RV with $3m(T-\hat{t}_c)$ d.o.f. and noncentrality parameter $\sum_{t=\hat{t}_c}^{T-1}\lambda_{1t,H_0}$. Since the distribution of the difference between a central Chi square RV and a noncentral Chi square RV is very difficult to characterize and does not permit a closed-form expression [130, Chapter 4A], we resort to approximation. The analysis is especially applicable for wide-area smart grid networks, *i.e.*, for large m the following approximations hold:

$$\sum_{t=\hat{t}_c}^{T-1} z_{0t,H_0} \sim \chi^2_{3m(T-\hat{t}_c)} \approx \mathcal{N}\left(3m(T-\hat{t}_c), 6m(T-\hat{t}_c)\right), \tag{.29}$$

$$\sum_{t=\hat{t}_c}^{T-1} z_{1t,H_0} \sim \chi^2_{3m(T-\hat{t}_c)}\left(\sum_{t=\hat{t}_c}^{T-1}\lambda_{1t,H_0}\right), \tag{.30}$$

which can be approximated as follows:

$$\sum_{t=\hat{t}_c}^{T-1} z_{1t,H_0} \approx \varphi_0 B_0, \text{ where } B_0 \sim \chi^2_{\nu_0}, \tag{.31}$$

$$\varphi_0 \triangleq \frac{3m(T-\hat{t}_c) + 2\left(\sum_{t=\hat{t}_c}^{T-1}\lambda_{1t,H_0}\right)}{3m(T-\hat{t}_c) + \left(\sum_{t=\hat{t}_c}^{T-1}\lambda_{1t,H_0}\right)}, \tag{.32}$$

$$\nu_0 \triangleq \frac{\left[3m(T-\hat{t}_c) + \left(\sum_{t=\hat{t}_c}^{T-1}\lambda_{1t,H_0}\right)\right]^2}{3m(T-\hat{t}_c) + 2\left(\sum_{t=\hat{t}_c}^{T-1}\lambda_{1t,H_0}\right)}, \tag{.33}$$

$$\sum_{t=\hat{t}_c}^{T-1} z_{1t,H_0} \sim \Gamma\left(\frac{\nu_0}{2}, 2\varphi_0\right) \approx \mathcal{N}(\nu_0\varphi_0, 2\nu_0\varphi_0^2), \tag{.34}$$

where $\Gamma\left(\frac{\nu_0}{2}, 2\varphi_0\right)$ denotes the Gamma distribution with parameters $\frac{\nu_0}{2}$ and $2\varphi_0$. Therefore, we have

$$\Lambda|H_0 \quad \sim \quad \mathcal{N}(\mu_{\Lambda|H_0}, \sigma^2_{\Lambda|H_0} - 2\kappa_{H_0}), \tag{.35}$$

where

$$\begin{aligned}
\mu_{\Lambda|H_0} &= 3m(T - \hat{t}_c) - \nu_0\varphi_0, & (.36)\\
\sigma^2_{\Lambda|H_0} &= 6m(T - \hat{t}_c) + 2\nu_0\varphi_0^2, & (.37)\\
\kappa_{H_0} &= \text{cov}\left(\sum_{t=\hat{t}_c}^{T-1} z_{0t,H_0}, \sum_{t=\hat{t}_c}^{T-1} z_{1t,H_0}\right). & (.38)
\end{aligned}$$

The covariance κ_{H_0} under hypothesis H_0 is computed as follows: we first generate L samples from two normal distributions $\mathcal{N}\left(3m(T - \hat{t}_c), 6m(T - \hat{t}_c)\right)$ and $\mathcal{N}(\nu_0\varphi_0, 2\nu_0\varphi_0^2)$, where φ_0 and ν_0 are given by (.32) and (.33), respectively. The covariance κ_{H_0} is given by

$$\kappa_{H_0} = \frac{1}{L-1}\sum_{\ell=1}^{L}\left[z^{\ell}_{H_0} - 3m(T - \hat{t}_c)\right]\left[x^{\ell}_{H_0} - \nu_0\varphi_0\right], \tag{.39}$$

where, $z^{\ell}_{H_0}$ denotes the realization of the RV $\sum_{t=\hat{t}_c}^{T-1} z_{t,H_0}$ at the ℓ^{th} instantiation; similarly for $x^{\ell}_{H_0}$. We let $\Lambda^{\text{std}}|H_0 = \frac{\Lambda|H_0 - \mu_{\Lambda|H_0}}{\sqrt{\sigma^2_{\Lambda|H_0} - 2\kappa_{H_0}}} \sim \mathcal{N}(0, 1)$. For a fixed false alarm rate $P_f = \alpha$, according to the Neyman-Pearson criterion [129],

$$\begin{aligned}
\int_{\rho'}^{\infty} p(\Lambda^{\text{std}}|H_0)d\boldsymbol{y} = Q\left(\frac{\rho' - \mu_{\Lambda|H_0}}{\sqrt{\sigma^2_{\Lambda|H_0} - 2\kappa_{H_0}}}\right) = \alpha&\\
\Rightarrow \rho' = \sqrt{\sigma^2_{\Lambda|H_0} - 2\kappa_{H_0}}Q^{-1}(\alpha) + \mu_{\Lambda|H_0},& \qquad (.40)
\end{aligned}$$

where $Q(\cdot)$ denotes the $Q-$function [129]. The covariance κ_{H_0} can be calculated using computer simulations.

.0.2 Asymptotic ($m \to \infty$) PDF of the test statistic under H_1

We denote $z_{0t,H_1} = (\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})'\boldsymbol{\Sigma}_{0t}^{-1}(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})$ and $z_{1t,H_1} = (\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})'\boldsymbol{\Sigma}_{1t}^{-1}(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})$ when $\boldsymbol{y}_t$ is sampled from the distribution corresponding to the hypothesis H_1. For $t = \hat{t}_c, \ldots, T-$

1, we see that $(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t})$ is Gaussian distributed with the $3m \times 1$ mean vector $\boldsymbol{\gamma}_{0t,H_1} = \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{y}_{t-1} - \boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1} \boldsymbol{y}_{t-1}$ and the $3m \times 3m$ positive definite covariance matrix $\boldsymbol{\Omega}_{0t,H_1} = \mathbb{E}_{H_1}[(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t} - \boldsymbol{\gamma}_{0t,H_1})(\boldsymbol{y}_t - \boldsymbol{\mu}_{0t} - \boldsymbol{\gamma}_{0t,H_1})']$. Similarly, $(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})$ is Gaussian distributed with the $3m \times 1$ mean vector $\boldsymbol{\gamma}_{1t,H_1} = \mathbb{E}_{H_1}[\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t}] = \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{y}_{t-1} - \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{y}_{t-1} = \boldsymbol{0}$ and the $3m \times 3m$ positive definite covariance matrix $\boldsymbol{\Omega}_{1t,H_1} = \mathbb{E}_{H_1}[(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})(\boldsymbol{y}_t - \hat{\boldsymbol{\mu}}_{1t})']$.

Thus, for $t = \hat{t}_c, \ldots, T-1$, $z_{0t,H_1} \sim \chi^2_{3m}(\lambda_{0t,H_1})$ with $\lambda_{0t,H_1} = \frac{1}{2}\boldsymbol{\gamma}'_{0t,H_1} \boldsymbol{\Sigma}_{0t}^{-1} \boldsymbol{\gamma}_{0t,H_1}$, and $z_{1t,H_1} \sim \chi^2_{3m}(\lambda_{1t,H_1})$ distributed with $\lambda_{1t,H_1} = \frac{1}{2}\boldsymbol{\gamma}'_{1t,H_1} \boldsymbol{\Sigma}_{1t}^{-1} \boldsymbol{\gamma}_{1t,H_1} = 0$. Therefore, under H_1, Λ is the difference between a noncentral Chi square RV with $3m(T - \hat{t}_c)$ d.o.f. and noncentrality parameter $\sum_{t=\hat{t}_c}^{T-1} \lambda_{0t,H_1}$ and a central Chi square RV with $3m(T - \hat{t}_c)$ d.o.f. whose distributions are difficult to characterize and does not permit closed-form expressions [130, Chapter 4A]. For large m, we use the following approximations:

$$\sum_{t=\hat{t}_c}^{T-1} z_{1t,H_1} \sim \chi^2_{3m(T-\hat{t}_c)} \approx \mathcal{N}\left(3m(T - \hat{t}_c), 6m(T - \hat{t}_c)\right) \tag{.41}$$

$$\sum_{t=\hat{t}_c}^{T-1} z_{0t,H_1} \sim \chi^2_{3m(T-\hat{t}_c)} \left(\sum_{t=\hat{t}_c}^{T-1} \lambda_{0t,H_1} \right), \tag{.42}$$

which can be approximated as follows:

$$\sum_{t=\hat{t}_c}^{T-1} z_{0t,H_1} \approx \varphi_1 B_1, \text{ where } B_1 \sim \chi^2_{\nu_1}, \tag{.43}$$

$$\varphi_1 \triangleq \frac{3m(T - \hat{t}_c) + 2\left(\sum_{t=\hat{t}_c}^{T-1} \lambda_{0t,H_1}\right)}{3m(T - \hat{t}_c) + \left(\sum_{t=\hat{t}_c}^{T-1} \lambda_{0t,H_1}\right)}, \tag{.44}$$

$$\nu_1 \triangleq \frac{\left[3m(T - \hat{t}_c) + \left(\sum_{t=\hat{t}_c}^{T-1} \lambda_{0t,H_1}\right)\right]^2}{3m(T - \hat{t}_c) + 2\left(\sum_{t=\hat{t}_c}^{T-1} \lambda_{0t,H_1}\right)}, \tag{.45}$$

$$\sum_{t=\hat{t}_c}^{T-1} z_{0t,H_1} \sim \Gamma\left(\frac{\nu_1}{2}, 2\varphi_1\right) \approx \mathcal{N}(\nu_1\varphi_1, 2\nu_1\varphi_1^2), \tag{.46}$$

where $\Gamma\left(\frac{\nu_1}{2}, 2\varphi_1\right)$ is the Gamma distribution with parameters $\frac{\nu_1}{2}$ and $2\varphi_1$. We thus have

$$\Lambda | H_1 \sim \mathcal{N}\left(\mu_{\Lambda|H_1}, \sigma^2_{\Lambda|H_1} - 2\kappa_{H_1}\right), \tag{.47}$$

where

$$\begin{aligned}
\mu_{\Lambda|H_1} &= \nu_1\varphi_1 - 3m(T-\hat{t}_c), && (.48)\\
\sigma^2_{\Lambda|H_1} &= 2\nu_1\varphi_1^2 + 6m(T-\hat{t}_c), && (.49)\\
\kappa_{H_1} &= \operatorname{cov}\left(\sum_{t=\hat{t}_c}^{T-1} z_{0t,H_1}, \sum_{t=\hat{t}_c}^{T-1} z_{1t,H_1}\right). && (.50)
\end{aligned}$$

The covariance κ_{H_1} is computed in a manner similar to κ_{H_0}. We let $\Lambda^{\mathrm{std}}|H_1 = \frac{\Lambda|H_1 - \mu_{\Lambda|H_1}}{\sqrt{\sigma^2_{\Lambda|H_1} - 2\kappa_{H_1}}} \sim \mathcal{N}(0,1)$. P_d is given by

$$\begin{aligned}
P_d &= \int_{\rho'}^{\infty} p(\Lambda^{\mathrm{std}}|H_1)d\boldsymbol{y} = Q\left(\frac{\rho' - \mu_{\Lambda|H_1}}{\sqrt{\sigma^2_{\Lambda|H_1} - 2\kappa_{H_1}}}\right)\\
&= Q\left(\frac{\sqrt{\sigma^2_{\Lambda|H_0} - 2\kappa_{H_0}}Q^{-1}(\alpha) + \mu_{\Lambda|H_0} - \mu_{\Lambda|H_1}}{\sqrt{\sigma^2_{\Lambda|H_1} - 2\kappa_{H_1}}}\right). \qquad (.51)
\end{aligned}$$

Bibliography

[1] R. Billinton and G. Singh, "Application of adverse and extreme adverse weather: modelling in transmission and distribution system reliability evaluation," *IEE Proceedings on Generation, Transmission and Distribution*, vol. 153, no. 1, pp. 115–120, Jan 2006.

[2] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on.* IEEE, 2010, pp. 220–225.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[4] W. Liu, C. Kwon, I. Aljanabi, and I. Hwang, "Cyber security analysis for state estimators in air traffic control systems," in *AIAA Conference on Guidance, Navigation, and Control*, 2012.

[5] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, no. 3, pp. 49–51, 2011.

[6] E. A. Lee, "Cyber physical systems: Design challenges," in *Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on.* IEEE, 2008, pp. 363–369.

[7] F. Pasqualetti, F. Dorfler, and F. Bullo, “Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design,” in *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on.* IEEE, 2011, pp. 2195–2201.

[8] H. Fawzi, P. Tabuada, and S. Diggavi, “Secure state-estimation for dynamical systems under active adversaries,” in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on.* IEEE, 2011, pp. 337–344.

[9] ——, “Secure estimation and control for cyber-physical systems under adversarial attacks,” 2012.

[10] H. V. Poor, *An introduction to signal detection and estimation.* Springer, 1994.

[11] J. Wei, J. M. Dolan, J. M. Snider, and B. Litkouhi, “A point-based mdp for robust single-lane autonomous driving behavior under uncertainties,” in *Robotics and Automation (ICRA), 2011 IEEE International Conference on.* IEEE, 2011, pp. 2586–2592.

[12] A. Nasir, B.-H. Soong, and S. Ramachandran, “Framework of wsn based human centric cyber physical in-pipe water monitoring system,” in *Control Automation Robotics Vision (ICARCV), 2010 11th International Conference on*, Dec 2010, pp. 1257–1261.

[13] K. Dvijotham and E. Todorov, “Linearly solvable optimal control,” *Reinforcement Learning and Approximate Dynamic Programming for Feedback Control*, pp. 119–141, 2012.

[14] A. D. Domínguez-García and S. Trenn, “Detection of impulsive effects in switched daes with applications to power electronics reliability analysis,” in *Decision and Control (CDC), 2010 49th IEEE Conference on.* IEEE, 2010, pp. 5662–5667.

[15] F. Pasqualetti, A. Bicchi, and F. Bullo, “A graph-theoretical characterization of power network vulnerabilities,” in *American Control Conference (ACC), 2011.* IEEE, 2011, pp. 3918–3923.

[16] A. Teixeira, H. Sandberg, and K. H. Johansson, “Networked control systems under cyber attacks with applications to power networks,” in *American Control Conference (ACC), 2010.* IEEE, 2010, pp. 3690–3696.

[17] F. Pasqualetti, F. Dorfler, and F. Bullo, “Attack detection and identification in cyber-physical systems,” *Automatic Control, IEEE Transactions on*, vol. 58, no. 11, pp. 2715–2729, 2013.

[18] C.-Z. Bai, F. Pasqualetti, and V. Gupta, “Security in stochastic control systems: Fundamental limitations and performance bounds,” in *American Control Conference (ACC), 2015.* IEEE, 2015, pp. 195–200.

[19] B. Kailkhura, S. Brahma, Y. S. Han, and P. K. Varshney, “Optimal distributed detection in the presence of byzantines.” in *ICASSP*, 2013, pp. 2925–2929.

[20] M. Gagrani, P. Sharma, S. Iyengar, V. S. S. Nadendla, A. Vempaty, H. Chen, and P. K. Varshney, “On noise-enhanced distributed inference in the presence of byzantines,” in *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on.* IEEE, 2011, pp. 1222–1229.

[21] E. Chan-Tin, D. Feldman, N. Hopper, and Y. Kim, “The frog-boiling attack: Limitations of anomaly detection for secure network coordinate systems,” in *Security and Privacy in Communication Networks.* Springer, 2009, pp. 448–458.

[22] Z. Wang, A. Serwadda, K. S. Balagani, and V. V. Phoha, “Transforming animals in a cyber-behavioral biometric menagerie with frog-boiling attacks,” in *Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on.* IEEE, 2012, pp. 289–296.

[23] M. L. Puterman, *Markov decision processes: discrete stochastic dynamic programming.* John Wiley & Sons, 2009, vol. 414.

[24] A. Back, U. Möller, and A. Stiglic, “Traffic analysis attacks and trade-offs in anonymity providing systems,” in *Information Hiding.* Springer, 2001, pp. 245–257.

[25] T. He and L. Tong, "Detection of information flows," *Information Theory, IEEE Transactions on*, vol. 54, no. 11, pp. 4925–4945, 2008.

[26] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[27] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," DTIC Document, Tech. Rep., 2004, `http://www.torproject.org`.

[28] A. Mishra and P. Venkitasubramaniam, "Admissible length study in anonymous networking: A detection theoretic perspective," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1957–1969, 2013.

[29] X. Wang, S. Chen, and S. Jajodia, "Network flow watermarking attack on low-latency anonymous communication systems," in *Security and Privacy, 2007. SP'07. IEEE Symposium on.* IEEE, 2007, pp. 116–130.

[30] A. Serjantov, R. Dingledine, and P. Syverson, "From a trickle to a flood: Active attacks on several mix types," in *Information Hiding.* Springer, 2003, pp. 36–52.

[31] A. Mishra and P. Venkitasubramaniam, "Anonymity of a buffer constrained chaum mix: Optimal strategy and asymptotics," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on.* IEEE, 2013, pp. 71–75.

[32] J. Cruz, *Ocean Wave Energy: Current Status and Future Prespectives*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[33] C. B. Boake, T. J. T. Whittaker, M. Folley, and H. Ellen, "Overview and initial operational experience of the limpet wave energy plant."

[34] S. Adee. (2009, Oct) This renewable energy source is swell. [Online]. Available: spectrum.ieee.org/energy/renewables/this-renewable-energy-source-is-swell

[35] [Online]. Available: http://www.pelamiswave.com/pelamis-technology

[36] (2015) Ocean power technologies successfully deploys apb350 powerbuoy off the coast of atlantic city, new jersey. [Online]. Available: http://globenewswire.com/news-release/2015/09/08/766562/10148445/

[37] S. Parmeggiani, J. F. Chozas, A. Pecher, E. Friis-Madsen, H. Sørensen, and J. P. Kofoed, "Performance assessment of the wave dragon wave energy converter based on the equimar methodology," in *9th European Wave and Tidal Energy Conference (EWTEC)*, vol. 9, 2011.

[38] D. Kavanagh, A. Keane, and D. Flynn, "Capacity value of wave power," *IEEE Transactions on Power Systems*, vol. 28, no. 1, pp. 412–420, Feb 2013.

[39] T. Denniss, "Comparing the variability of wind speed and wave height data," *Energetech Australia*, 2005.

[40] D. A. Halamay, T. K. A. Brekken, A. Simmons, and S. McArthur, "Reserve requirement impacts of large-scale integration of wind, solar, and ocean wave power generation," in *IEEE PES General Meeting*, July 2010, pp. 1–7.

[41] [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachmentdata/file/48128/2167-uk-renewable-energy-roadmap.pdf

[42] [Online]. Available: http://www.seai.ie/Publications/Renewables-Publications-/Ocean/Tidal-Current-Energy-Resources-in-Ireland-Report.pdf

[43] L. Rusu and C. G. Soares, "Wave energy assessments in the azores islands," *Renewable Energy*, vol. 45, pp. 183 – 196, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0960148112001668

[44] D. Corbus, J. King, T. Mousseau, R. Zavadil, B. Heath, L. Hecker, J. Lawhorn, D. Osborn, J. Smit, R. Hunt *et al.*, "Eastern wind integration and transmission study," *NREL (http://www. nrel. gov/docs/fy09osti/46505. pd f), CP-550-46505*, vol. 13, pp. 1–8, 2010.

[45] P. Norgaard and H. Holttinen, “A multi-turbine power curve approach,” in *Nordic wind power conference*, vol. 1, 2004, pp. 1–2.

[46] G. Gan, C. Ma, and J. Wu, *Data clustering: theory, algorithms, and applications.* Siam, 2007, vol. 20.

[47] A. J. Lamadrid, S. Maneevitjit, T. D. Mount, C. E. Murillo-Sanchez, R. J. Thomas, and R. D. Zimmerman, “A ”superopf” framework,” Tech. Rep., 12/2008 2008.

[48] R. Bo and F. Li, “Comparison of lmp simulation using two dcopf algorithms and the acopf algorithm,” in *Electric Utility Deregulation and Restructuring and Power Technologies, 2008. DRPT 2008. Third International Conference on.* IEEE, 2008, pp. 30–35.

[49] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, “Matpower: Steady-state operations, planning, and analysis tools for power systems research and education,” *IEEE Transactions on power systems*, vol. 26, no. 1, pp. 12–19, 2011.

[50] A. J. Lamadrid, T. Mount, R. Zimmerman, C. E. Murillo-Sanchez, and L. Anderson, “Alternate mechanisms for integrating renewable sources of energy into electricity markets,” in *Power and Energy Society General Meeting, 2012 IEEE.* IEEE, 2012, pp. 1–8.

[51] L. Lawton, M. Sullivan, K. Van Liere, A. Katz, and J. Eto, “A framework and review of customer outage costs: Integration and analysis of electric utility outage cost surveys,” Ernest Orlando Lawrence Berkeley National Laboratory, Berkeley, CA (US), Tech. Rep., 2003.

[52] P. Pradhan, K. Hatalis, S. Kishore, R. Blum, and A. Lamadrid, “Prospects of wave power grid integration,” in *PES General Meeting — Conference Exposition, 2014 IEEE*, July 2014, pp. 1–5.

[53] (2015). [Online]. Available: http://energy.gov/savings/renewable-electricity-production-tax-credit-ptc

[54] (2016). [Online]. Available: https://www.theguardian.com/environment/2016/jul/27/european-offshore-wind-investment-hits-14bn-in-2016

[55] (2015) Innovative wave power device starts producing clean power in hawaii. [Online]. Available: http://energy.gov/eere/articles/innovative-wave-power-device-starts-producing-clean-power-hawaii

[56] (2015) World?s first grid-connected wave power station switched on in australia. [Online]. Available: http://www.sciencenewspost.com/worlds-first-grid-connected-wave-power-station-switched-on-in-australia/

[57] "The european offshore wind industry," 2017. [Online]. Available: https://windeurope.org/wp-content/uploads/files/about-wind/statistics/WindEurope-Annual-Offshore-Statistics-2016.pdf

[58] (2016, Dec.) America's first offshore wind farm powers up. [Online]. Available: http://dwwind.com/press/americas-first-offshore-wind-farm-powers/

[59] S. Astariz, A. Vazquez, and G. Iglesias, "Evaluation and comparison of the levelized cost of tidal, wave, and offshore wind energy," *Journal of Renewable and Sustainable Energy*, vol. 7, no. 5, p. 053112, 2015.

[60] G. Buigues, I. Zamora, A. Mazon, V. Valverde, and F. Pérez, "Sea energy conversion: problems and possibilities," in *International Conference on Renewable Energies and Power Quality (ICREPQ'06), 8p*, 2006.

[61] B. Teillant, R. Costello, J. Weber, and J. Ringwood, "Productivity and economic assessment of wave energy projects through operational simulations," *Renewable Energy*, vol. 48, pp. 220 – 230, 2012.

[62] M. O'Connor, T. Lewis, and G. Dalton, "Operational expenditure costs for wave energy projects and impacts on financial returns," *Renewable Energy*, vol. 50, pp. 1119 – 1131, 2013.

[63] J. Endrenyi, S. Aboresheid, R. N. Allan, G. J. Anders, S. Asgarpoor, R. Billinton, N. Chowdhury, E. N. Dialynas, M. Fipper, R. H. Fletcher, C. Grigg, J. McCalley, S. Meliopoulos, T. C. Mielnik, P. Nitu, N. Rau, N. D. Reppen, L. Salvaderi, A. Schneider, and C. Singh, "The present status of maintenance strategies and the impact of maintenance on reliability," *IEEE Transactions on Power Systems*, vol. 16, no. 4, pp. 638–646, 2001.

[64] M. Shafiee, "Maintenance logistics organization for offshore wind energy: Current progress and future perspectives," *Renewable Energy*, vol. 77, pp. 182–193, 2015.

[65] A. Mrigaud and J. V. Ringwood, "Condition-based maintenance methods for marine renewable energy," *Renewable and Sustainable Energy Reviews*, vol. 66, pp. 53 – 78, 2016.

[66] Z. Tian, T. Jin, B. Wu, and F. Ding, "Condition based maintenance optimization for wind power generation systems under continuous monitoring," *Renewable Energy*, vol. 36, no. 5, pp. 1502 – 1509, 2011.

[67] D. Heyman and M. Sobel, *Stochastic Models in Operations Research*. Mineola, NY: Dover, 2003, vol. II: Stochastic Optimization.

[68] A. Pasanisi, S. Fu, and N. Bousquet, "Estimating discrete Markov models from various incomplete data schemes," *Computational Statistics & Data Analysis*, vol. 56, no. 9, pp. 2609–2625, 2012.

[69] J. Rust, "Optimal replacement of GMC bus engines: An empirical model of Harold Zurcher," *Econometrica*, vol. 55, no. 5, pp. 999–1033, 1987.

[70] D. Bull, M. Ochs, D. Laird, B. Boren, and R. Jepsen, "Technological cost-reduction pathways for point absorber wave energy converters in the marine hydrokinetic environment," Sandia National Laboratories, U.S., Tech. Rep., 09 2013.

[71] D. Jarocki and J. H. Wilson, "Wave energy converter performance modeling and cost of electricity assessment," in *ASME 2010 International Mechanical Engineering*

Congress and Exposition. American Society of Mechanical Engineers, 2010, pp. 333–342.

[72] M. O'Connor, T. Lewis, and G. Dalton, "Weather window analysis of irish west coast wave data with relevance to operations & maintenance of marine renewables," *Renewable energy*, vol. 52, pp. 57–66, 2013.

[73] K. Abdulla, J. Skelton, K. Doherty, P. O'Kane, R. Doherty, G. Bryans *et al.*, "Statistical availability analysis of wave energy converters," in *The Twenty-first International Offshore and Polar Engineering Conference.* International Society of Offshore and Polar Engineers, 2011.

[74] F. Besnard, M. Patrikssont, A. B. Strombergt, A. Wojciechowskit, and L. Bertling, "An optimization framework for opportunistic maintenance of offshore wind power system," in *PowerTech, 2009 IEEE Bucharest*, June 2009, pp. 1–7.

[75] G. Wilson and D. McMillan, "Assessing wind farm reliability using weather dependent failure rates," *Journal of Physics: Conference Series*, vol. 524, no. 1, p. 012181, 2014. [Online]. Available: http://stacks.iop.org/1742-6596/524/i=1/a=012181

[76] E. Byon and Y. Ding, "Season-dependent condition-based maintenance for a wind turbine using a partially observed markov decision process," *IEEE Transactions on Power Systems*, vol. 25, no. 4, pp. 1823–1834, Nov 2010.

[77] F. Besnard, K. Fischer, and L. B. Tjernberg, "A model for the optimization of the maintenance support organization for offshore wind farms," *IEEE Transactions on Sustainable Energy*, vol. 4, no. 2, pp. 443–450, April 2013.

[78] A. Gutierrez-Alcoba, G. Ortega, E. M. Hendrix, E. E. Halvorsen-Weare, and D. Haugland, "A model for optimal fleet composition of vessels for offshore wind farm maintenance," *Procedia Computer Science*, vol. 108, pp. 1512 – 1521, 2017, international Conference on Computational Science, ICCS 2017, 12-14 June 2017, Zurich, Switzerland.

[79] C. A. Irawan, D. Ouelhadj, D. Jones, M. Stlhane, and I. B. Sperstad, “Optimisation of maintenance routing and scheduling for offshore wind farms,” *European Journal of Operational Research*, vol. 256, no. 1, pp. 76 – 89, 2017.

[80] C. Gundegjerde, I. B. Halvorsen, E. E. Halvorsen-Weare, L. M. Hvattum, and L. M. Nons, “A stochastic fleet size and mix model for maintenance operations at offshore wind farms,” *Transportation Research Part C: Emerging Technologies*, vol. 52, pp. 74 – 92, 2015.

[81] W. B. Powell and B. V. Roy, “Approximate dynamic programming for high-dimensional dynamic resource allocation problems,” in *Handbook of Learning and Approximate Dynamic Programming*, J. Si, A. G. Barto, W. B. Powell, and D. Wunsch, Eds. Hoboken, NJ: Wiley-IEEE Press, 2004, pp. 261–279.

[82] Y. Hu and B. Defourny, “Near-optimality bounds for greedy periodic policies with application to grid-level storage,” in *IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning (ADPRL-2014)*, December 2014, pp. 1–8.

[83] “IEEE standard terms for reporting and analyzing outages occurrences and outage states of electrical transmission facilities,” Piscataway, NJ, 2008.

[84] R. Billinton and L. Chen, “Incorporation of weather effects in transmission system models for composite system adequacy evaluation,” *IEE Proceedings C – Generation, Transmission and Distribution*, vol. 133, no. 6, pp. 319–327, 1986.

[85] D. Mooley, “Severe cyclonic storms in the Bay of Bengal, 1877–1977,” *Monthly Weather Review*, vol. 108, no. 10, pp. 1647–1655, 1980.

[86] P.-S. Chu and J. Wang, “Modeling return periods of tropical cyclone intensities in the vicinity of Hawaii,” *Journal of Applied Meteorology*, vol. 37, pp. 951–960, 1998.

[87] G. Villarini, G. A. Vecchi, and J. A. Smith, “Modeling the dependence of tropical storm counts in the North Atlantic basin on climate indices,” *Monthly Weather Review*, vol. 138, no. 7, pp. 2681–2705, 2010.

[88] M. Alam, A. Hossain, and S. Shafee, "Frequency of Bay of Bengal cyclonic storms and depressions crossing different coastal zones," *International Journal of Climatology*, vol. 23, no. 9, pp. 1119–1125, 2003.

[89] W. Van Paepegem, C. Blommaert, I. De Baere, J. Degrieck, G. De Backer, J. De Rouck, J. Degroote, J. Vierendeels, S. Matthys, and L. Taerwe, "Slamming wave impact of a composite buoy for wave energy applications: design and large-scale testing," *Polymer Composites*, vol. 32, no. 5, pp. 700–713, 2011.

[90] D. Bertsekas, *Dynamic Programming and Optimal Control*, 3rd ed. Belmont, MA: Athena Scientific, 2005.

[91] J. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization Methods and Software*, vol. 11–12, pp. 625–653, 1999.

[92] A. Luceño, "A family of partially correlated Poisson models for overdispersion," *Computational Statistics and Data Analysis*, vol. 20, pp. 511–520, 1995.

[93] T. Minka, "Estimating a dirichlet distribution," M.I.T., Tech. Rep., 2000.

[94] S. D. Weller, T. J. Stallard, and P. K. Stansby, "Interaction factors for a rectangular array of heaving floats in irregular waves." *IET Renewable Power Generation*, vol. 4, pp. 628–637, 2010.

[95] V. Stratigaki, P. Troch, T. Stallard, D. Forehand, J. P. Kofoed, M. Folley, M. Benoit, A. Babarit, and J. Kirkegaard, "Wave basin experiments with large wave energy converter arrays to study interactions between the converters and effects on other users in the sea and the coastal area," *Energies*, vol. 7, pp. 701–734, 2014.

[96] E. Y. Bitar, R. Rajagopal, P. P. Khargonekar, K. Poolla, and P. Varaiya, "Bringing wind energy to market," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1225–1235, 2012.

[97] M. Rahm, O. Svensson, C. Bostrom, R. Waters, and M. Leijon, "Experimental results from the operation of aggregated wave energy converters," *IET Renewable Power Generation*, vol. 6, no. 3, pp. 149–160, 2012.

[98] N. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions*, 2nd ed. Hoboken, NJ: Wiley, 1994.

[99] B. Xu, A. Oudalov, J. Poland, A. Ulbig, and G. Andersson, "Bess control strategies for participating in grid frequency regulation," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 4024 – 4029, 2014, 19th IFAC World Congress. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1474667016422329

[100] J. Donadee and M. Ilić, "Estimating the rate of battery degradation under a stationary markov operating policy," in *PES General Meeting— Conference & Exposition, 2014 IEEE*. IEEE, 2014, pp. 1–5.

[101] F. Matthey, T. Kamijoh, K. Takeda, S. Ando, T. Nomura, T. Shibata, and A. Honzawa, "Cost-benefit analysis tool and control strategy selection for lithium-ion battery energy storage system," in *Power & Energy Society General Meeting, 2015 IEEE*. IEEE, 2015, pp. 1–5.

[102] Regulation performance evaluation process. [Online]. Available: http://www.pjm.com/~/media/committees-groups/task-forces/rpstf20110810/20110810-item-03-regulation-performance-evaluation-process.ashx

[103] M. Koller, T. Borsche, A. Ulbig, and G. Andersson, "Defining a degradation cost function for optimal control of a battery energy storage system," in *PowerTech (POWERTECH), 2013 IEEE Grenoble*. IEEE, 2013, pp. 1–6.

[104] A. Phadke and J. Thorp, "Communication needs for wide area measurement applications," in *Proc. IEEE Int. Conf. Critical Infras.*, Sep. 2007, pp. 1–7.

[105] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 220–225.

[106] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.

[107] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," in *Proc. IEEE Allerton Conf. Commun, Control, Comput.*, Oct. 2012, pp. 212–219.

[108] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE J. Select. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[109] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[110] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation," *IEEE J. Select. Areas Commun.*, vol. 32, no. 7, pp. 1460–1470, Jul. 2014.

[111] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. Int. Tech. Meet. Satellite Div. The Ins. Navigation*, Sep. 2008, pp. 2314–2325.

[112] S. Gong, Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "GPS spoofing based time stamp attack on real time wide area monitoring in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2012, pp. 300–305.

[113] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator - a case study on co-simulation platform GECO," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2012, pp. 587–592.

[114] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Critical Infras. Protect.*, vol. 5, no. 3-4, pp. 146–153, Dec. 2012.

[115] I. Akkaya, E. A. Lee, and P. Derler, “Model-based evaluation of GPS spoofing attacks on power grid sensors,” in *Proc. IEEE Workshop Model. Simul. Cyber-Phys. Ener. Syst.*, May 2013, pp. 1–6.

[116] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, “Time synchronization attack in smart grid: Impact and analysis,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Jan. 2013.

[117] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domínguez-García, “Spoofing GPS receiver clock offset of phasor measurement units,” *IEEE Trans. Power Systems*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.

[118] S. Mousavian, J. Valenzuela, and J. Wang, “A probabilistic risk mitigation model for cyber-attacks to PMU networks,” *IEEE Trans. Power Systems*, vol. 30, no. 1, pp. 156–165, Jan. 2015.

[119] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, “A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids,” *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Aug. 2015.

[120] F. Zhu, A. Youssef, and W. Hamouda, “Detection techniques for data-level spoofing in GPS-based phasor measurement units,” in *IEEE Int. Conf. Select. Topics Mobile Wireless Net.*, Apr. 2016, pp. 1–8.

[121] A. K. Mattei, W. M. Grady, P. J. Caspary, and S. A. McBride, “Detection of time spoofing attacks on GPS synchronized phasor measurement units,” in *Ann. Conf. Protect. Relay Eng.*, Apr. 2016, pp. 1–8.

[122] P. Risbud, N. Gatsis, and A. Taha, “Assessing power system state estimation accuracy with GPS-spoofed PMU measurements,” in *IEEE Power Energy Soc. Inn. Smart Grid Tech. Conf.*, Sep. 2016, pp. 1–5.

[123] X. Fan, L. Du, and D. Duan, “Synchrophasor data correction under GPS spoofing attack: A state estimation based approach,” *IEEE Trans. Smart Grid*, 2017, to appear.

[124] J. J. Grainger and W. D. Stevenson, *Power System Analysis.* McGraw-Hill, 2003.

[125] P. Pradhan, K. G. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in *Proc. IEEE Conf. Commun. Net. Security*, Oct. 2016, pp. 391–395.

[126] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability.* Prentice Hall, 1998.

[127] A. Chakrabortty and P. P. Khargonekar, "Introduction to wide-area control of power systems," in *Proc. IEEE American Control Conf.*, Jun. 2013, pp. 6758–6770.

[128] E. L. Lehmann and J. P. Romano, *Testing Statistical Hypotheses.* Springer, 1959.

[129] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. Springer-Verlag, 1994.

[130] M. K. Simon, *Probability Distributions Involving Gaussian Random Variables.* Springer, 2006.

[131] J. R. Schott, *Matrix Analysis for Statistics*, 3rd ed. John Wiley & Sons, 2017.

[132] H. Liu, Y. Tang, and H. H. Zhang, "A new chi-square approximation to the distribution of non-negative definite quadratic forms in non-central normal variables," *Comp. Stat. Data Analy.*, vol. 53, no. 4, pp. 853–856, Feb. 2009.

Vita

Parth Pradhan was born on September 18, 1987 at Bhurkunda, a small town in Hazaribagh district, Jharkhand, India to a bank officer, Pradip Kumar Pradhan, and a primary school teacher, Jayashree Pradhan. He attended Kendriya Vidyalaya Giddi A, Jharkhand and DAV Public School Chandrasekharpur Bhubaneswar, Odisha before completing his Xth board matriculation exam in 2002. After finishing his higher secondary education from BJB Science College Bhubaneswar, he enrolled at the prestigious National Institute of Technology (NIT) in Rourkela, India, where he earned his Bachelor of Technology (B. Tech) in Electronics and Instrumentation Engineering in 2009.

Between 2009 and 2012, He worked with NTPC Limited as operations engineer and control and instrumentation engineer. In 2012, he joined Energy Systems Engineering Institute (ESEI), Lehigh University, and earned his Masters of Engineering (M.E) degree in Energy Systems Engineering in 2013. Since then, he has been working towards the Ph.D. degree in the Department of Electrical and Computer Engineering, Lehigh University, Bethlehem, PA. He worked as an intern with Energy Management group, at NEC Laboratories America, Cupertino, CA in 2015. During the summer of 2017, he interned with Applied Solutions group at PJM Interconnections, Norristown, PA. His research interests include stochastic control and optimization in smart grids, electricity markets, attack detection in wide area monitoring systems, and renewable generation grid integration and maintenance.