Security Games for Risk Minimization in Automatic Generation Control

Yee Wei Law, Tansu Alpcan, *Senior Member, IEEE*, and Marimuthu Palaniswami, *Fellow, IEEE*

***Abstract*—The power grid is a critical infrastructure that must be protected against potential threats. While modern technologies at the center of the ongoing smart grid evolution increase its operational efficiency, they also make it more susceptible to malicious attacks such as false data injection to electronic monitoring systems. This paper presents a game-theoretic approach to smart grid security by combining quantitative risk management techniques with decision making on protective measures. The consequences of data injection attacks are quantified using a risk assessment process where the well-known conditional value-at-risk (CVaR) measure provides an estimate of the defender's loss due to load shed in simulated scenarios. The calculated risks are then incorporated into a stochastic security game model as input parameters. The decisions on defensive measures are obtained by solving the game using dynamic programming techniques which take into account resource constraints. Thus, the formulated security game provides an analytical framework for choosing the best response strategies against attackers and minimizing potential risks. The theoretical results obtained are demonstrated through numerical examples. Simulation results show that different risk measures lead to different defense strategies, but the CVaR measure prioritizes high-loss tail events.**

***Index Terms*—Automatic generation control, cyber-physical system security, security games, smart grid.**

I. Introduction

THE power grid, on which most economic activities rely, is a critical infrastructure that must be protected against potential threats. As it evolves to a "smart grid" with better efficiency, however, the concerns increase due to emergence of new attack vectors exploiting increasing system complexity. While security (against malicious attacks) is an important issue for grid operators, real-world constraints such as resource limitations necessarily force adoption of a risk management approach to the problem rather than complete elimination of all potential threats. Protective measures are usually taken based on a cost-benefit analysis balancing available defensive resources with perceived security risks.

This paper investigates the important class of false data injection attacks to smart grids which directly affect the operation of automatic generation control systems and potentially lead to blackouts. The problem is formulated first as one of quantitative risk management using the well-known conditional value-at-risk (CVaR) measure, which in turn provides the input to a stochastic (Markov) security game formulation. The resulting game analysis helps smart grid operators to make informed decisions on their security strategies while taking into account their resource constraints. Although the paper focuses on a certain type of attack and subsystem, the approach can be applied to similar security problems in smart grid, and hence, can be extended to develop the foundation of a systematic framework for smart grid security.

Security risk analysis can be defined as "the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact" [1]. A simple but elegant definition of *risk* is "the probability and magnitude of a loss, disaster, or other undesirable event" [2]. The *expected shortfall* or CVaR measure is used extensively for financial risk management. Most smart grid standards and guidelines, e.g., IEC 62351-1, NISTIR 7628, identify risk assessment as a critical part of a security framework. For instance, the Australian Government advocates the use of the Australian and New Zealand Standard for Risk Management (AS/NZS ISO 31000:2009) by owners and operators of critical infrastructure. However, the standard ISO 31000:2009 is "not mathematically based", and has "little to say about probability, data, and models" [3].

Security games provide an analytical framework for modelling the interaction between malicious attackers who aim to compromise a smart grid, and operators defending it. The rich mathematical basis provided by the field of game theory facilitates formalizing the strategic struggle between attackers and defenders for the control of the smart grid [4]. Using the risk framework and some of the concepts of earlier studies [5], [6], this work applies game theory to the modelling of attacks on and defenses for the critical power system component, automatic generation control (AGC).

The **main contributions** of this paper include

- assessment and identification of risks faced by the AGC, which constitute an important part of a smart grid, due to false data injection attacks;
- quantifying risks faced by the AGC using the CVaR measure, in terms of potential blackouts caused by attacks;
- a stochastic (Markov) security game formulation for analysis of best defensive actions building upon the risk analysis conducted and under resource limitations;
- a numerical study illustrating the framework developed, and demonstrating the dependence of the optimal strategy on the employed risk measure.

The rest of the paper is organized as follows. Section II discusses related work. Section III states the problem of assessing the cyber-security risks in AGC. Section IV presents our game

Manuscript received August 21, 2013; revised January 15, 2014 and April 17, 2014; accepted May 20, 2014. The work of Y. W. Law was supported in part by the ARC under contracts LP120100529 and LE120100129, and in part by the EC under contract CNECT-ICT-609112 (SOCIOTAL). Paper no. TPWRS-01079-2013.

The authors are with the Department of Electrical and Electronic Engineering, The University of Melbourne, Parkville, VIC 3010, Australia.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2014.2326403

and risk model. In Section V, we specify an informal threat model; we also discuss attack and defense actions under this threat model. In Section VI, we apply the game and risk model to automatic generation control, and present our simulation results. Section VII concludes this paper.

II. Related Work

As a complex system, smart grid presents a number of security challenges. Due to the infancy of the discipline, a substantial research effort is dedicated to exploring cyber-attacks and their effects on power system components.

The most relevant attacks targeting smart grid are either denial-of-service attacks [7], [8] or false data injection attacks (data integrity attacks) [9]–[16]. The attacked systems can be classified as

- remote terminal units and intelligent electronic devices acting as sensors feeding measurements such as voltage phasors [11], [13], [16], power [12], frequency [15], to critical power system components;
- communication networks [7], [8]; and
- critical power system components such as FACTS devices [13], the load-frequency control or automatic generation control system [9], [10].

Risk assessment is an important research imperative in smart grid security. We note that some authors erroneously refer to risk assessment as *vulnerability assessment*, which is a different concept [1]. *Attack trees* or attack graphs is a common starting point for most of the work in this area. An attack tree represents attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes. Ten *et al.* [17] propose a framework based on attack trees for evaluating system security. They focus on attacks originating from substations connecting to the control center through a *virtual private network*. They limit cyber-intrusions to firewall penetration and password cracking, singling out password policies and port auditing as the two most important security measures—these assumptions are used in other work by the same research team [18], [19]. Liu *et al.* [20] take an attack tree as input, and assign a "difficulty level" to each action on the tree using Analytic Hierarchy Process. Their methodology produces a *vulnerability factor*, an artificial measure of the success probability of an attack. Analytic Hierarchy Process is a decision making methodology that is often applied to risk management, but it relies on subjective scoring and it does not satisfy several statistical axioms (e.g., transitivity) [2]. In comparison, only empirical evidence is used in this work.

The limitations of attack trees are widely recognized. Sommestad *et al.* [21] propose *defense graphs* as an alternative to attack graphs, to take into account the countermeasures already in place within a system. They model defense graphs using *influence diagrams*, which are essentially Bayesian networks enhanced with indicators that express *beliefs* on *likelihood* values. The output of their assessment methodology is the expected loss associated with a successful attack. Hahn *et al.* [22] propose *privilege graphs* to model the privilege states in a system and the paths exploitable by an attacker. The essence of their proposal is an algorithm for computing an *exposure metric*, that takes into account 1) the number of attack paths through the security mechanisms protecting a target asset, and 2) the path length representing the effort required to exploit a path.

Ten *et al.* [18] model attacks using *stochastic Petri Nets*, which encapsulate the probability and risk of attacks. Sridhar *et al.* [19] use stochastic Petri Nets to model computers, firewalls and intrusion protection systems. To assess the *steady-state impact* of attacks on the power system itself, they present the impact study of coordinated attack scenarios, where coordination is in the sense of targeting multiple power system components simultaneously. Like [19], our work involves detailed modelling and simulation of attacks on a power system component, which in our case is the AGC system.

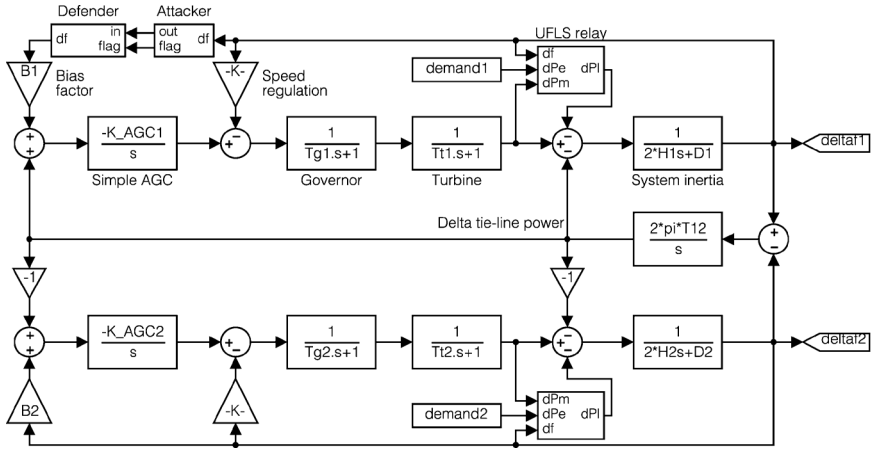
Game theory provides the basis for generalizing decision making methods such as Markov decision processes [23] and stochastic control/programming [24] to a multiagent setting. Chen *et al.* [7] use two-player zero-sum static games between a so-called *intentional attacker* and a *fusion-based defender* to compute the equilibrium network robustness corresponding to the minimax strategies. Our previous work [15], [16] use two-player zero-sum stochastic games for assessing security risks and optimal defenses for the smart grid. In comparison to these work, our current work 1) provides a more intuitive definition of risk states, 2) studies concrete clustering-based intrusion detection algorithms instead of hypothetical ones, and 3) provides alternative definitions of the players' payoffs, one of which is based on the financial risk measure of "conditional value-at-risk".

III. Automatic Generation Control in Power Grid

The most critical aspect of a power system is stability, and one of the most important parameters to stabilize is frequency. This is because the frequency of a power system rises/falls with decreased/increased loading. Failure to stabilize frequency may lead to damage to equipment (utility's or end users'), harm to human safety, reduction of or interruption to electricity supply. Violation of frequency stability criteria is one of the main reasons for numerous power blackouts [25]. Less tangible secondary impacts, including loss of data or information and damage to reputation, are equally undesirable.

The frequency control system operates at three levels. Primary frequency control takes the form of a turbine governor's *speed regulator*, a proportional controller of gain $1/R$, where R is the *droop characteristic* (drop in speed or frequency when combined machines of an area change from no load to full load). Secondary frequency control is for correcting the steady-state error residue left by the proportional controller, and may take the form of an integral controller; in which case, primary and secondary frequency control form a parallel proportional-integral controller, capable of driving frequency deviations to zero whenever a step-load perturbation is applied to the system. Tertiary frequency control is supervisory control based on offline optimizations for ensuring adequate spinning reserve for primary control, and optimal dispatch of units participating in secondary control. While primary and secondary control respond in seconds and tens of seconds respectively, tertiary control is usually manually activated minutes after secondary control. Our study concerns only the *dynamics* of frequency control, and hence does not consider tertiary control.

In an interconnected system with two or more *control areas*, in addition to frequency, the generation within each area must



Symbols	Definition
H, D	Inertia constant, damping coefficient
T_g, T_t	Time constants for turbine governor
R	Droop characteristic
B	Frequency bias factor
K_{AGC}	Gain of secondary frequency control
T_{12}	Tie-line synchronizing coefficient

Unit	$K_{\mathrm{AGC}\,i}$ (s)	D_i (p.u./Hz)	$2H_i$ (p.u. s)	R_i (Hz/p.u.)
$i=1$	0.3	0.015	0.1667	3.00
$i=2$	0.2	0.016	0.2017	2.73

Unit	T_{gi} (s)	T_{ti} (s)	B_i (p.u./Hz)
$i=1$	0.08	0.40	0.3483
$i=2$	0.06	0.44	0.3827

Fig. 1. Simulink representation and simulation parameters for a two-area AGC system model based on Bevrani's [25, Fig. 2.10 and Table 2.2]. The top area is labeled area 1. The demand time series `demand1` and `demand2` are the demand profiles of Victoria on June 4–5, 2012 and of South Australia on June 7–8, 2012, respectively, provided by the Australian Energy Market Operator. Nominal frequency = 60 Hz.

also be controlled to maintain scheduled power interchanges over *tie lines* (inter-area transmission lines). The control of both frequency and generation is called *load-frequency control*. Within each area, each generation unit has primary control, while secondary control is centralized. Together, decentralized primary control and centralized secondary control achieve the purpose of load-frequency control. **Automatic generation control (AGC)** is load-frequency control with the additional objective of *economic dispatch* (distributing the required change in generation among units to minimize costs) [26], [27]. However, AGC is sometimes referred to as automated (versus manual) load-frequency control [28], or even the entire frequency control system itself [29]. AGC is an indispensable part of the "central nervous system" of a power grid called the **energy management system (EMS)**, and possibly the only automatic closed loop between the IT and power system of a control area [9]; because of this, it is subject to attacks propagated through the IT system. A detailed threat model is given in Section V.

When system frequency deviates from the nominal frequency (60 Hz for the Americas, 50 Hz for most other parts of the world) by a certain threshold, overfrequency and underfrequency protection relays execute tripping logic defined by a protection plan that varies from operator to operator. Assuming a nominal frequency of 60 Hz, overfrequency relays start tripping thermal plants when frequency rise exceeds 1.5 Hz [29], [30], but these relays are usually set to tolerate deviations due to post-fault transients for short periods of time. Underfrequency relays perform **underfrequency load shedding (UFLS)**, which is the sole concern of our study because it results in directly measurable revenue loss. For our study, we adopt Mullen's UFLS scheme [31]. The gist of the scheme is, when the system frequency drops by more than 0.35 Hz below the nominal frequency, to shed this much load:

$$\Delta P_m - \Delta P_e - 0.3/R$$

where ΔP_m is the change in generator's mechanical power, ΔP_e is the change in generator's electrical power, and R is the droop characteristic. Our goal is to model and quantify the risks posed by an attacker who aims to inflict revenue loss on the electricity provider by injecting false data to the automatic generation controller in the hope of triggering load shedding.

For this work, we use the two-area AGC system model and associated simulation parameters in Fig. 1. The automatic generation controller is an integral controller of gain K_{AGC}. AGC design is an established discipline with designs dating back to the 1950s; a simple integral controller seems to be a logical starting point. The UFLS relay in each area decides on the necessity to shed load, and the amount of load to shed if necessary, using Mullen's algorithm [31]. Once the system frequency has stabilized for at least 30 s, the UFLS relays reconnect the shed loads in the reverse order they were shed.

In this sample configuration, the maximum sheddable loads are capped at 4 p.u. and 1 p.u. for the areas 1 and 2 respectively. "p.u." stands for "per unit" and is simply the ratio of an absolute value in some unit to a base/reference value in the same unit. The base load for both areas is taken to be 1000 MW.

IV. Security Game Model

We first explore formulating our cyber-security risk assessment problem as a decision making problem, then show how the problem entails game-theoretic treatment, and further show how our security game model, based on the framework in [4], can be applied.

Define the decision maker as the cyber-defense component of the AGC of a multi-area power system. At each *stage* (time point) t, the decision maker takes an *action* d, for which it receives a *reward* r_d (positive for gain, negative for loss). In general, the reward depends on the *state* s of the power system. Furthermore, the action may trigger the system to transition into another state. Assuming the state transition is Markovian (memoryless), then the decision making problem can be formulated as a *Markov decision process* (MDP), defined by the 4-tuple $(\mathcal{S}, \mathcal{A}^D, M, r)$, where

- $\mathcal{S} \stackrel{\text{def}}{=} \{s_1, \ldots, s_{N_S}\}$ is the system's state space;
- $\mathcal{A}^D \stackrel{\text{def}}{=} \{d_1, \ldots, d_{N_D}\}$ is the decision maker's action space;
- $M_{s,s'}(d) \stackrel{\text{def}}{=} \Pr\{s[t+1] = s' \mid s[t] = s, d[t] = d\}$ is the state transition probability, for $s, s' \in \mathcal{S}$ and $d \in \mathcal{A}^D$;

- $r_d(s, s')$ is the reward for triggering state transition $s \to s'$ by action $d \in \mathcal{A}^D$.

The decision maker's objective is to maximize its cumulative reward by deciding on the optimal policy $d[t]$, for all t.

The effect of an attack manifests as a change to M and r_d—this is equivalent to modeling attacks as the actions of an "attacker" agent, that at every stage, takes an action from a set of actions. In other words, the attacker comes into the picture as another decision maker. While the theory of multiagent MDP deals with cooperative agents [23], the theory of *stochastic games* (equivalently, *Markov games*) is applicable here. A stochastic game is a "competitive MDP" where the agents/players execute their actions simultaneously to maximize their own reward. We define a *security game* as a stochastic game with a finite state space, and two players (attacker versus defender) that choose their actions from their respective finite action space; or more formally, as a 6-tuple $(\mathcal{S}, \mathcal{A}^A, \mathcal{A}^D, \mathbf{M}, \mathbf{G}^A, \mathbf{G}^D)$, where

- $\mathcal{S} \stackrel{\text{def}}{=} \{s_1, \ldots, s_{N_S}\}$ is the system's state space;
- $\mathcal{A}^A \stackrel{\text{def}}{=} \{a_1, \ldots, a_{N_A}\}$ is the attacker's action space;
- $\mathcal{A}^D \stackrel{\text{def}}{=} \{d_1, \ldots, d_{N_D}\}$ is the defender's action space;
- $\mathbf{M}(a, d) = [M_{s_i,s_j}(a, d)]_{N_S \times N_S}$ is the system's state transition matrix corresponding to attack action $a \in \mathcal{A}^A$ and defense action $d \in \mathcal{A}^D$;
- $\mathbf{G}^A(s) = [G^A_{a,d}(s)]_{N_A \times N_D}$ is the attacker's expected payoff for playing action $a \in \mathcal{A}^A$ against defense action $d \in \mathcal{A}^D$ in in system state $s \in \mathcal{S}$;
- $\mathbf{G}^D(s) = [G^D_{a,d}(s)]_{N_A \times N_D}$ is the defender's expected payoff for playing action $d \in \mathcal{A}^D$ against attack action $a \in \mathcal{A}^A$ in system state $s \in \mathcal{S}$.

Let $\boldsymbol{p}^{\mathcal{S}}[t]$ be the stage-t probability distribution on the state space $\mathcal{S}$:

$$\boldsymbol{p}^{\mathcal{S}}[t] \stackrel{\text{def}}{=} [\Pr\{s[t] = s_1\}, \Pr\{s[t] = s_2\}, \ldots, \Pr\{s[t] = s_{N_S}\}]^T$$

then $\boldsymbol{p}^{\mathcal{S}}[t+1] = \mathbf{M}(a, d)\boldsymbol{p}^{\mathcal{S}}[t]$. The matrix entry $M_{s_i,s_j}(a, d)$ represents the probability of state s_i transitioning to state s_j under attack action a and defense action d.

We associate a different level of risk with each state. In this work, we define a **risk state** as a tuple $(\Delta f_1, \Delta f_2)$, i.e., a tuple consisting of area 1's frequency deviation and area 2's frequency deviation. Four risk states are defined by partitioning $(\Delta f_1, \Delta f_2)$:

- State s_{00}: $-0.35 < \Delta f_1$ and $-0.35 < \Delta f_2$;
- State s_{01}: $-0.35 < \Delta f_1$ and $\Delta f_2 \leq -0.35$;
- State s_{10}: $\Delta f_1 \leq -0.35$ and $-0.35 < \Delta f_2$;
- State s_{11}: $\Delta f_1 \leq -0.35$ and $\Delta f_2 \leq -0.35$.

This definition follows the intuition that s_{00} is the least underfrequency (least risky) state while s_{11} is the most underfrequency (most risky) state. Note that -0.35 Hz is the threshold used in the UFLS algorithm in Section III.

In the next two subsections, we define the attacker's and defender's payoffs, and present the algorithm for determining the optimal attack and defense strategies.

A. Attacker's and Defender's Payoffs

For each state $s \in \mathcal{S}$, the attacker (defender) incurs a net gain (net loss):

$$\begin{aligned}\text{Attacker's net gain} &= \text{Attacker's gain} - \text{Attacker's cost},\\ \text{Defender's net loss} &= \text{Defender's loss} - \text{Defender's gain}\\ &= \text{Defender's loss}.\end{aligned}$$

Above, the defender's gain is taken to be zero, because no profit is made by merely countering attacks. There are many ways to model the remaining variables, namely the attacker's gain, the attacker's cost and the defender's loss, by making different assumptions about the attacker and defender. For example, we can assume the attacker to be a corporate adversary or a nation-state attacker—either way, we need to make very specific assumptions about the nature of the attacker. Depending on the assumptions, the attacker's net gain may be much larger, much smaller, or close to the defender's net loss. In this work, we assume the attacker's net gain to be close to the defender's net loss, and hence the security games to be *zero-sum*, i.e.,

$$\text{Attacker's gain} - \text{Attacker's cost} = \text{Defender's loss}.$$

By estimating the defender's loss, which is more readily quantifiable from a power system perspective, we essentially also estimate the attacker's net gain. Our zero-sum formulation is a simplification that 1) is based on the loose principle: "whatever the defender loses the attacker gains", 2) absolves us from making very specific assumptions about the attacker, 3) guarantees convergence, and 4) provides an accessible demonstration of the utility of our security game framework.

The defender's loss has multiple cost components, including primarily 1) the cost of load shed, 2) the development and runtime costs of the defense actions, and 3) the costs of false positives. We discuss each of these cost components below:

- **Cost of load shed**: In our previous work [15], this cost component is taken to be the cost of the expected total load shed in state s under attack action a and defense action d. The limitation of this formulation is that for loss distributions that are heavy-tailed, as many empirical loss distributions are [32], the expected value cannot capture the severity of a rare event. In a heavy-tailed distribution, the loss probability decreases with the loss magnitude more slowly than an exponent, so although a successful attack is a rare event, when it does happen, the loss is usually far greater than the expected loss. In this work, following Varaiya *et al.*'s proposal [33], we additionally adopt the financial measure *expected shortfall* or CVaR for estimating the defender's loss. To explain CVaR, we first define *value-at-risk* (VaR). VaR at significance level $\alpha \in (0, 1)$ (α is typically small) is the minimum value ζ such that the probability that the loss exceeds ζ is no larger than α [32]. Mathematically, for a loss P_{shed} with cumulative distribution function (cdf) $F_{P_{\text{shed}}}$, the VaR at significance level α is

$$\begin{aligned}\text{VaR}_\alpha(P_{\text{shed}}) &\stackrel{\text{def}}{=} \inf\{\zeta \mid F_{P_{\text{shed}}}(\zeta) \geq 1 - \alpha\}\\ &= F^{-1}_{P_{\text{shed}}}(1 - \alpha) \qquad (1)\end{aligned}$$

where the last equality is only valid for smooth and continuous $F_{P_{\text{shed}}}$. CVaR at significance level α is the expected loss when VaR_α is exceeded [32]. Mathematically, the CVaR at significance level α is

$$\mathrm{CVaR}_\alpha(P_{\mathrm{shed}}) \stackrel{\mathrm{def}}{=} \mathsf{E}\{P_{\mathrm{shed}} \mid P_{\mathrm{shed}} \geq \mathrm{VaR}_\alpha(P_{\mathrm{shed}})\} = \frac{1}{\alpha}\int_{1-\alpha}^{1} F^{-1}_{P_{\mathrm{shed}}}(a)\, da. \quad (2)$$

Formulae (1) and (2) are immediately calculable given the loss distribution $F_{P_{\mathrm{shed}}}$. In this work, the loss distribution is given by the cdf of load shed.

- **Development and runtime costs of defense actions**: This cost component should be negligible relative to the cost of load shed, for the implementation of the actions to be justified in the first place. Thus, this cost component is ignored in our security game model.
- **Cost of false positives**: A false positive refers to the scenario where a defense action—in the form of an intrusion detection algorithm—misdiagnoses a harmless anomaly as an attack. A positive diagnosis can lead to the replacement of a piece of software or hardware or both, hence a high false positive rate is clearly undesirable. Taking into account the cost of false positives in our security game model ensures the trivial defense action that marks all system input signals as malicious (thereby exhibiting a 100% false positive rate in the absence of attacks) does not get chosen. The expected cost of false positives is $c_{\mathrm{fp}}p_{\mathrm{fp}}$, where c_{fp} is the cost of a false positive in the same unit as load shed, and p_{fp} is the probability of getting a false positive. Note that c_{fp} is a fixed cost and does not change with p_{fp}, so the expected cost sufficiently reflects the impact of false positives.

Based on the discussion above, we provide two alternative definitions of $G_{a,d}(s)$:

$$G^{\mathrm{mean}}_{a,d}(s) \stackrel{\mathrm{def}}{=} \mathsf{E}\{P_{\mathrm{shed}}(a,d,s)\} + c_{\mathrm{fp}}p_{\mathrm{fp}}(a,d,s), \quad (3)$$

$$G^{\mathrm{CVaR}}_{a,d}(s) \stackrel{\mathrm{def}}{=} \mathrm{CVaR}_\alpha(P_{\mathrm{shed}}(a,d,s)) + c_{\mathrm{fp}}p_{\mathrm{fp}}(a,d,s). \quad (4)$$

Note both P_{shed} and c_{fp} depend on the actions and state.

Summarizing this subsection, $\mathbf{G}(s) = \mathbf{G}^A(s) = -\mathbf{G}^D(s)$. $G_{a,d}(s)$ represents the defender's loss (attacker's net gain) in risk state s by taking action d against attack action a. In game-theoretic terms, given a stage-t state of $s[t]$, the attacker and defender play a zero-sum matrix game represented by $\mathbf{G}(s[t])$.

B. Optimal Attack and Defense Strategies

The objective of a rational attacker (defender) is to maximize (minimize) its expected cumulative payoff $\bar{Q}$. For a game played in a sufficiently long time, we can adopt the *future-discounted reward* model [23] and write $\bar{Q}$ as

$$\bar{Q} \stackrel{\mathrm{def}}{=} \sum_{t=0}^{\infty} \gamma^t G_{a[t],d[t]}(s[t]) \quad (5)$$

where $a[t] \in \mathcal{A}^A$, $d[t] \in \mathcal{A}^D$, $s[t] \in \mathcal{S}$, $\forall t \in \mathbb{N}$, and $\gamma \in [0,1)$ is the *discount factor*. The discount factor γ is a logical construct for de-emphasizing the payoff at future stages (a smaller γ leads to lower future payoffs).

As per game theory, the attacker's *strategy* is defined as a probability distribution on $\mathcal{A}^A$ for a given state $s[t]$, i.e.,

$$\boldsymbol{p}^A(s[t]) \stackrel{\mathrm{def}}{=} [\Pr\{a(s[t]) = a_1\}, \ldots, \Pr\{a(s[t]) = a_{N_A}\}]^\top.$$

$\boldsymbol{p}^A(s[t])$ is a *mixed strategy* when none of the entries of $\boldsymbol{p}^A(s[t])$ is 1. When implementing a mixed strategy, for state $s[t]$, the attacker adopts action a_i at probability $\Pr\{a(s[t]) = a_i\}$, for $i = 1, \ldots, N_A$. A *pure strategy* is where one and only one entry of $\boldsymbol{p}^A(s)$ is 1, and the attacker always adopts the action corresponding to this entry for state $s[t]$. The defender's strategy, $\boldsymbol{p}^D(s[t])$, is similarly defined. The (optimal) $\boldsymbol{p}^D(s[t])$ that minimizes $\bar{Q}$ depends on $\boldsymbol{p}^A(s[t])$, $\forall t \in \mathbb{N}$. For this "reference" attack strategy to be meaningful, we adopt the notion of *Nash equilibrium*, where the equilibrium attack strategy and equilibrium defense strategy are the *best responses* to each other. The question is: are these equilibrium strategies stationary (same for all t)?

Fink [34] proved that any n-player ($n \geq 2$) discounted stochastic game has at least one Nash equilibrium in stationary strategies. For two-player zero-sum discounted stochastic games, Shapley [35] proved that there exists a unique Nash equilibrium in stationary strategies. Hence there is no need to compute a separate optimal attack/defense strategy for each t. Furthermore, the problem can be solved recursively using *dynamic programming* to obtain the stationary optimal strategy (solving a zero-sum matrix game at each stage) [23], [35]. At stage t, the optimal cost $Q_t(a,d,s)$ (the dependency of s, a and d on t is omitted for notational brevity) can be computed iteratively using the dynamic programming recursion

$$Q_{t+1}(a,d,s) = G_{a,d}(s) + \gamma \sum_{s' \in \mathcal{S}} M_{s,s'}(a,d) \cdot \min_{\boldsymbol{p}^D(s')} \max_a \sum_{d \in \mathcal{A}^D} Q_t(a,d,s')\boldsymbol{p}^D_d(s') \quad (6)$$

for $t \in \mathbb{N}$ and a given initial condition Q_0. In (6), $\boldsymbol{p}^D_d(s')$ is the element of $\boldsymbol{p}^D(s')$ that corresponds to d. (6) converges to the optimal Q^* as $t \to \infty$.

There are multiple ways to implement (6). The algorithm called *value iteration* is prescribed here due to its scalability. To describe the algorithm, we first split (6) into the two-part mutually recursive Bellman equations:

$$V(s) = \min_{\boldsymbol{p}^D(s)} \max_a \sum_{d \in \mathcal{A}^D} Q_t(a,d,s)\boldsymbol{p}^D_d(s), \quad (7)$$

$$Q_{t+1}(a,d,s) = G_{a,d}(s) + \gamma \sum_{s' \in \mathcal{S}} M_{s,s'}(a,d)V(s') \quad (8)$$

for $t \in \mathbb{N}$. We can formulate (7) as a linear program:

$$\min_{\boldsymbol{p}^D(s)} V(s) \quad \mathrm{s.t.} V(s) \geq \sum_{d \in \mathcal{A}^D} Q_t(a,d,s)\boldsymbol{p}^D_d(s), \forall a \in \mathcal{A}^A, \quad \boldsymbol{p}^D_d \geq 0, \sum_d \boldsymbol{p}^D_d = 1, \forall d \in \mathcal{A}^D. \quad (9)$$

The strategy $\boldsymbol{p}^D(s), \forall s \in \mathcal{S}$ computed from (9) is the *minimax* strategy w.r.t. Q. The fixed points of equations (7) and (8), V^* and Q^*, lead to the optimal minimax solution for the defender. By the Fundamental Theorem of Game Theory [36, Theorem 9.5.1], the optimal attack strategy $\boldsymbol{p}^A(s), \forall s \in \mathcal{S}$ can be obtained by solving the dual of linear program (9). Pseudocode for the value iteration algorithm, using (9) and (8) to find V^* and Q^*, can be found in [4, Algorithm 4.1].

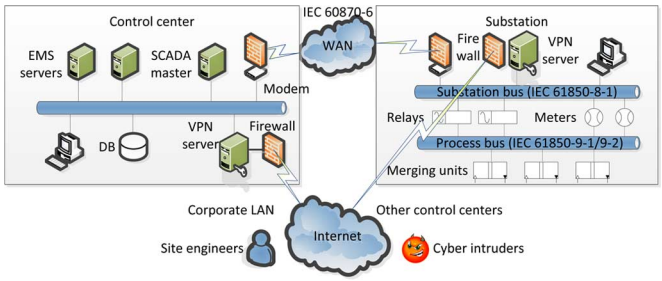


Fig. 2. Accessibility of a power system control center and substation from the Internet. AGC is executed on one of the EMS servers. In our threat model, an attacker can feed the AGC software with false frequency deviation data.

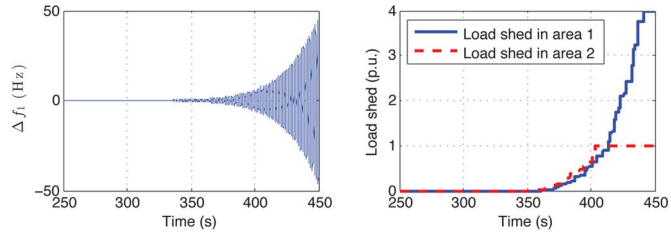


Fig. 3. An example of "overcompensation" attack, where the attacker substitutes Δf_1 with $8\Delta f_1$ as frequency input to the area-1 integral controller. As long as the attack persists, neither generator tripping nor load shedding helps stabilize the system.

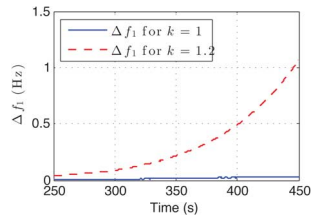


Fig. 4. Negative compensation attack: for large enough k (e.g., 1.2), the system frequency $\to +\infty$.

V. Threat Analysis

Fig. 2 shows the communication architecture involving a control center and a substation based on the international standard IEC 61850 [18], [27]. Access to the control system in either the control center or the substation is enabled through a virtual private network (VPN). Some authors [17] equate the compromise of an entire control center or substation to the successful cracking of a VPN access password and the penetration of an Internet-facing firewall (see Fig. 2). This strong attacker model is not entirely unrealistic, however, our goal is to investigate the strategy of an attacker that has successfully penetrated the protected network but whose actions within the AGC system are bounded by several resource constraints. We assume the following resource constraints:

- The attacker cannot directly trip generators, or transmission lines (by opening circuit breakers).
- The attacker cannot tamper with turbine governors.
- The attacker cannot tamper with UFLS relays. Some commercial relays (e.g., SEL-387E) have an integrated frequency meter, and are thereby not subject to false frequency data injection attacks.
- The attacker cannot tamper with the EMS.
- The attacker can reduce but not block the input/output of the EMS.

Without the above constraints, it is a trivial exercise for any attacker that has successfully penetrated the protected network to trigger cascading failures across the power grid. It is therefore conceivable that an energy provider would make protecting its generators, circuit breakers, turbine governors, UFLS relays, and EMS its foremost priority. Despite the above constraints, an attacker can forge and send false *frequency deviation* (Δf) data to the AGC software executing on one of the EMS servers, by compromising one of the meters in the substation (see Fig. 2). In the spirit of stealthy attacks as embodied by Stuxnet, Duqu and Flame, it is also conceivable that a persistent attacker would adopt this subtle and stealthy strategy. Then, it is up to the AGC software to detect such attacks.

A. Basic Attacks

It is impossible to exhaust all injection patterns, but there are four basic patterns on which more sophisticated attacks are based:

- **Constant injection**: If an attacker injects a constant false Δf, then it effectively disables the integral control loop, causing the system frequency to converge to a non-nominal frequency. If the false Δf is positive, then the system will settle on a below-nominal frequency, causing loads to be shed; otherwise, the system will settle on an above-nominal frequency, causing generators to be tripped. Both cases lead to cascading failures.
- **Bias injection**: When the false Δf is a constant displacement from the true Δf, the effect is similar to that of constant injection because normally the true $\Delta f \approx 0$.
- **Overcompensation**: If the false Δf is k times the true Δf, where k is a large positive number, then the attack effectively causes overcompensation by the integral control loop, and consequently unstable oscillations. As the system frequency sweeps past the overfrequency and underfrequency thresholds, generators will be tripped and loads will be shed, followed by cascading failures. Fig. 3 shows the result of an attack using $k = 8$.
- **Negative compensation**: If the false Δf is $-k$ times the true Δf, where k is a positive number, then the attack effectively reverses the intended effect of the integral control loop, causing the system frequency to diverge from the nominal frequency (see Fig. 4). This attack directly triggers generator tripping.

Once a generator is tripped, spinning reserve will be engaged to fill the supply hole. If this fails, as the final measure, underfrequency relays will start shedding loads. In other words, attacks that directly trigger generator tripping can also cause load shedding. For our study, we concentrate only on the overcompensation attack, as it inflicts maximal damage in terms of directly triggering both generator tripping and load shedding.

B. Basic Defenses

Basic defences against the overcompensation attack include:

- **Saturation filter**: We can constrain the attack by limiting the Δf input to the integral controller to $[-4.5, 3.5]$ Hz (i.e., passing the input through a saturation filter), because at $\Delta f = -4.5$ Hz, not only should all sheddable loads have been shed, but also all generators would be tripped. At $\Delta f = 3.5$ Hz, all generators would be tripped [30].

- **Redundancy**: Measurement redundancy is routinely provisioned for critical grid parameters [37]. Multiple frequency meters of different grades can be installed, so that the likelihood of all meters being compromised is small and the AGC software has a non-zero chance of getting genuine frequency data.
- **Detection**: Saturation filtering and redundancy only limit the effect of an attack, stopping an attack requires the attack to be detected and the source be removed. A threshold-based algorithm can be designed to observe the metric $\sum_t |\Delta f(t)|$ or $\sum_t |\Delta f(t) - \Delta f(t-1)|$; if the metric is larger than a certain threshold, the system could be under attack. Alternatively, a clustering-based algorithm can be designed to count the number of clusters in the time series $\{\Delta f(t)\}$; if more than one cluster are observed, the system could be under attack because $\Delta f(t)$ values tend to cluster around 0 under normal circumstances. In general, clustering is a more versatile approach than thresholding for anomaly detection.

There are unlimited ways to improve upon the overcompensation attack to counter the above defenses. Correspondingly, there are unlimited ways to detect these improved attacks with varying accuracy, and certainly there are more advanced controllers that are less susceptible to these attacks. Nevertheless, our interest is not on the design of attacks, defenses or the controller, but on the modelling of system risk dynamics under the actions of the attacker and defender for any given system.

VI. Simulation Study

The simulation workflow is to

1) first define the attack and defense actions;
2) simulate the effect of interactions between the attack actions and defense actions on an AGC system, to observe the state transition matrix $\mathbf{M}(a,d) = [M_{s_i,s_j}(a,d)]_{N_S \times N_S}$ and the game matrix $\mathbf{G}(s) = [G_{a,d}(s)]_{N_A \times N_D}$; and finally
3) feed the observed $\mathbf{M}(a,d)$ and $\mathbf{G}(s)$ to the value iteration algorithm to solve (7) and (8) for the optimal defense strategy $\boldsymbol{p}^D(s), \forall s \in \mathcal{S}$.

To keep this simulation study numerically simple, we define only two attack actions and two defense actions, although the proposed framework can be applied to any finite number of actions of any specifications. Note that the optimal attack strategy $\boldsymbol{p}^A(s), \forall s \in \mathcal{S}$ can be obtained by solving the dual of linear program (9).

Attack actions: The chosen attack actions are:

a_1	attack at "half power": corrupt half of the observed samples;
a_2	attack at "full power": corrupt all of the observed samples.

The attack actions are predicated on the successful compromise of the meter. We model the attacker to take 4 sessions and 8 sessions to compromise Meter 1 and Meter 2 respectively ("session" is defined later). The corruption takes the following form: the attacker sets a false Δf to -4.5 Hz if the true Δf is negative, or 3.5 Hz if the true Δf is positive. This implements the overcompensation attack, and takes into account the saturation filter in Section V.

Defense actions: The defender implements the saturation filter and redundancy measure described in Section V. For redundancy, the defender reads N consecutive samples alternately from two frequency meters of different builds (one is more secure than the other). N consecutive samples from one meter constitute one *session* (see Fig. 5). Upon collecting N samples, the defender runs a clustering-based algorithm on the latest N samples to detect intrusions. The clustering algorithm used for this simulation study is Sledge *et al.*'s cluster count extraction algorithm [38]. Sledge *et al.*'s algorithm consists of a cross-correlation filter whose size determines the "fuzziness" or "sharpness" of clusters and therefore influences the cluster count. The following defense actions are defined:

d_1	set the filter size to $0.25N$ (5 pixels if $N = 20$), and label the corresponding meter as malicious if at least two clusters are found;
d_2	set the filter size to $0.40N$ (8 pixels if $N = 20$), and label the corresponding meter as malicious if at least two clusters are found.

These filter sizes are chosen because simulations indicate that a filter size of less than $0.25N$ is prone to false negatives whereas a filter size of more than $0.40N$ is prone to false positives.

Disinfection and load reconnection: If the detection result of d_1 or d_2 is positive, the defender *always* disinfects the meter (e.g., by refreshing its firmware, cryptographic keys and so on). Disinfection is assumed to complete within one session (see Fig. 5). After a meter is disinfected, the attacker will discover it has lost control of the meter, and will start compromising the meter again—we model the attacker to take 4 sessions and 8 sessions to compromise Meter 1 and Meter 2 respectively. Furthermore, we also model the system to reconnect shed loads in

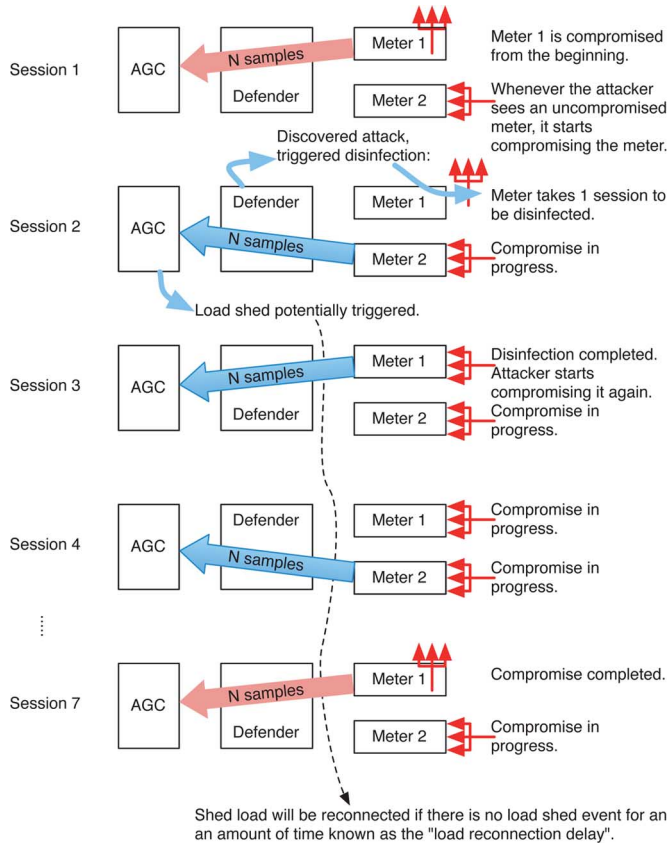


Fig. 5. Sample sessions in our attacker-defender interaction model.

TABLE I
COMPARING DEFENSE ACTIONS

	d_1				d_2			
	TN	FP	TP	FN	TN	FP	TP	FN
a_1	99.8%	0.2%	100%	0%	99%	1%	100%	0%
a_2	99%	1%	100%	0%	98.8%	1.2%	100%	0%

TN=True Negative; FP=False Positive; TP=True Positive; FN=False Negative.

the order they were shed, after some time there has not been any load shedding event—we call this time the *load reconnection delay*. It turns out the load reconnection delay plays a significant role in the game outcome, as we will see later.

Obtaining $\mathbf{M}(a, d)$: The AGC samples its input every few seconds, and at each sampling point, the system is in one of the four risk states $s_{00}, \ldots, s_{11}$. $M_{s_i,s_j}(a, d)$ is readily obtained by fixing attack action at a, defense action at d, and calculating the probability of the system transitioning from state s_i to state s_j by counting the number of transitions.

Obtaining $\mathbf{G}(s)$: Based on (3) and (4), two cost components need to be measured through simulations:

1) $\mathsf{E}\{P_{\text{shed}}(a, d, s)\}$ or $\text{CVaR}_\alpha(P_{\text{shed}}(a, d, s))$: At every time instant the system is in state s under attack action a and defense action d, the total amount of load shed in areas 1 and 2, denoted $P_{\text{shed}}(a, d, s)$, follows a cdf. Given sufficient samples of $P_{\text{shed}}(a, d, s)$, we can estimate the pdf (for which we use *kernel density estimation*) and then the cdf, which then allows us to calculate the CVaR of $P_{\text{shed}}(a, d, s)$ through (2). $\mathsf{E}\{P_{\text{shed}}(a, d, s)\}$ is estimated by taking the average of $P_{\text{shed}}(a, d, s)$ over time.
2) $c_{\text{fp}} p_{\text{fp}}(a, d, s)$: Recall two frequency meters are used in the system for redundancy, of which one is more secure and presumably more costly than the other. We set $c_{\text{fp,Meter1}} = 0.01$ for Meter 1 and $c_{\text{fp,Meter2}} = 0.02$ for Meter 2 (one order of magnitude smaller than the expected cost of load shed). Let x be the number of time instants the system is in state s under attack action a and defense action d. Then, $p_{\text{fp}}(a, d, s)$ is the fraction of x where d makes a diagnosis and the diagnosis is a false positive.

For simulations, we use the two-area AGC system model and associated simulation parameters in Fig. 1. We set $N = 20$, i.e., 20 samples are read from a meter in each session. Using MATLAB/Simulink, each simulation is conducted for 200 virtual minutes. Attacks are simulated to start at time 100 s. In practice, AGC signals are transmitted to the generating plant once every 2 to 4 s [26], but knowing a faster sampling rate alleviates the effects of attacks [15], we set the sampling rate of the "Defender" and "Attacker" blocks to 1 Hz. The obtained $\mathbf{M}$ and $\mathbf{G}$ are fed into Algorithm 2. The simulation results enable the comparisons in the subsequent subsections.

A. Comparing Defense Actions

Table I compares d_1's and d_2's performance. Both d_1 and d_2 have a 100% detection rate of a_1 and a_2, but d_2 has a slightly higher false positive rate. Due to the low false positive rates, the cost of false positives has little impact on the game outcome in this study.

B. Comparing Expectation and CVaR of Total Load Shed

The expected total load shed, $\mathsf{E}\{P_{\text{shed}}\}$, does not generally reflect the α-level CVaR of total load shed, $\text{CVaR}_\alpha(P_{\text{shed}})$.

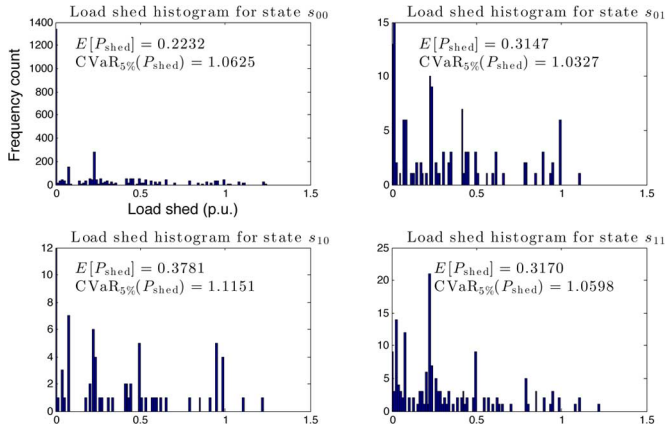


Fig. 6. Expected total load shed and at 5%-level CVaR of total load shed corresponding to the risk states (attack action $= a_1$, defense action $= d_2$). Load reconnection delay is set to 30 s.

As Fig. 6 shows for attack action a_1 and defense action d_1, the least risky state s_{00} has the lowest expected total load shed but the second highest CVaR of total load shed. This seemingly counter-intuitive phenomenon is a result of underfrequency load shedding: the largest portion of load shed is for returning the system to the least risky state. Therefore, as subsequent results will show, cost/risk quantification using different measures—$\mathsf{E}\{P_{\text{shed}}\}$ versus $\text{CVaR}_\alpha(P_{\text{shed}})$—can lead to different optimal strategies for the attacker and defender.

C. Comparing Optimal Strategies

Fig. 7(a)–(b) and Fig. 7(c)–(d) show the optimal strategies when the load reconnection delay is set to 30 s:

- When $\mathsf{E}\{P_{\text{shed}}\}$ is used for cost/risk quantification, the optimal attack and defense strategies are mostly mixed strategies, which vary only slightly with different discount factors. In the limit, a pure defense strategy using only d_2 should suffice. This result may seem surprising considering d_1 and d_2 are similar, with d_2 having just a slightly higher false positive rate (hence causing slightly more disinfections). However, it is the combination of a short load reconnection delay and slightly more frequent disinfections that accentuates the distinction between d_1 and d_2. Later, we will see that a long load reconnection delay suppresses the distinction between d_1 and d_2.
- When $\text{CVaR}_\alpha(P_{\text{shed}})$ is used for cost/risk quantification, the optimal attack and defense strategies turn out to be a_1 and d_1, respectively. This can be explained by the observation that a_1, as a less aggressive attack, actually causes more fluctuation in the observed Δf_1 and Δf_2, and hence longer tails in the loss distribution. Corresponding to a_1, Table I suggests d_1 is the better strategy.

The defender can prioritize average or tail events by choosing the appropriate cost/risk measure. Given the high costs of tail events, the CVaR measure is potentially more favorable.

Fig. 8(a)–(b) and Fig. 8(c)–(d) show the optimal strategies when the load reconnection delay is set to 60 s. When the system is less aggressive on reconnecting shed loads, d_2 has a similar effect as d_1 on the system, so it is not surprising that Fig. 8(a)–(b) shows the optimal defense strategy is a 50%/50% mixed strategy. Moreover, with a longer load reconnection delay, there is less fluctuation on the load level, and the loss

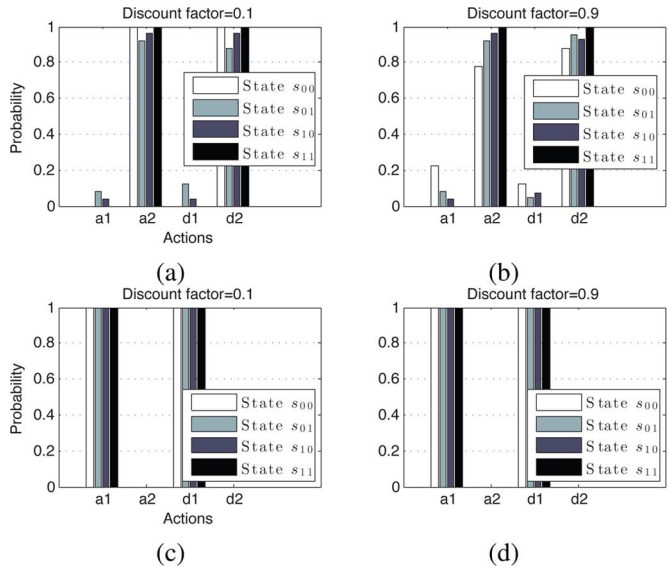


Fig. 7. Optimal attack and defense strategies when the game matrix is defined using $\mathsf{E}\{P_{\rm shed}\}$ (sub-figures a, b), and $\mathrm{CVaR}_\alpha(P_{\rm shed})$ (sub-figures c, d). Load reconnection delay is set to 30 s.

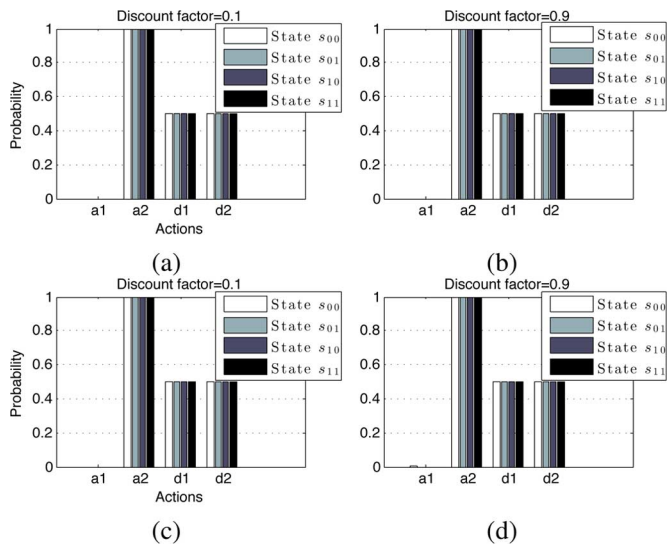


Fig. 8. Optimal attack and defense strategies when the game matrix is defined using $\mathsf{E}\{P_{\rm shed}\}$ (sub-figures a, b), and $\mathrm{CVaR}_\alpha(P_{\rm shed})$ (sub-figures c, d). Load reconnection delay is set to 60 s.

distribution gets smaller tails. Hence comparing Fig. 8(a)–(b) with Fig. 8(c)–(d), we can see that using either $\mathsf{E}\{P_{\rm shed}\}$ or $\mathrm{CVaR}_\alpha(P_{\rm shed})$ as the cost measure gives us the same optimal attack and defense strategies.

We conclude this section with a general remark. In theory, there is an optimal strategy corresponding to each state. In practice, the optimal strategy may turn out to be the same for all states, in which case, the attacker or defender can apply the same strategy throughout the entire course of its attack or defense. For example, in Fig. 7(a)–(b), a_2/d_2 is approximately optimal for all states, whereas in Fig. 7(c)–(d), a_1/d_1 is exactly optimal for all states.

VII. Conclusion and Future Directions

Risk assessment for power grids has been identified as a critical area by the public sector, industry and academia. However, existing risk management standards such as ISO 31000:2009 are more about general principles and guidelines than concrete mathematical techniques. In this work, we identify and assess the risks faced by the critical power system component AGC. Our discussion of potential attacks to AGC and countermeasures is based on an explicit security threat model. We propose the use of the quantitative risk measure CVaR capturing the probability and magnitude of security threats faced by the AGC system due to false data injection attacks. Building upon the risk analysis, we model attacker-defender interactions using stochastic (Markov) security games to analyze the best defensive actions under resource constraints. The developed framework is illustrated with a detailed AGC model and simulation results. As evident in the simulation results, different risk measures may lead to different defense strategies, but the CVaR measure allows a decision maker to prioritize high-loss tail events.

A. Future Directions

In zero-sum security games, by the definition of Nash equilibrium, the attacker cannot increase its gain and thereby the defender's loss by unilaterally deviating from its equilibrium strategy—this feature is however lost when security games are formulated as general-sum games. Furthermore, in zero-sum games, all Nash equilibria are *Pareto-optimal* (i.e., there is no other game outcome that gives both players higher payoffs, or give one player the same payoff but the other player a higher payoff), but this feature is again missing in general-sum games.

To formulate a risk assessment framework based on general-sum security games, we consider an attacker and a defender that are *rational* (i.e., seeking convergence to a stationary strategy that is a best response to their opponent's strategy). Although attackers often do not act rationally in real life partly due to limitations on observations and available information, security games are meant to provide organizations—"within the boundaries of the models"—with rational guidelines for defensive strategies and principles for algorithms that can also be implemented in (semi)automated security systems. For risk assessment, the optimal defense strategy is devised against the optimal attack. In practice, a defense measure should be implemented to adapt to attacks, based on guidelines provided by the optimal defense strategy.

For general-sum games, a Nash equilibrium is not necessarily Pareto-optimal and vice versa. Finding a Nash equilibrium of an n-player ($n \geq 2$) general-sum finite game is already a PPAD-complete problem, let alone finding a Pareto-optimal equilibrium. Recognizing the difficulty of converging to a Nash equilibrium, *multiagent learning* seeks alternative convergence criteria, e.g., correlated equilibrium, Hannan consistency, targeted optimality (best response against a specific class of players) [23]. Efficient and scalable multiagent learning is an ongoing challenge [39], for which domain-specific (power system in our case) heuristics is likely necessary.

In summary, generalizing the current framework to model general-sum attacker-defender interactions involves prescribing a meaningful equilibrium with a lower complexity than Nash equilibrium, and designing the corresponding multiagent learning rules for efficient convergence to that equilibrium.

REFERENCES

[1] NIST, Glossary of Key Information Security Terms, Feb. 2011, IR 7298 Revision 1.

[2] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*. New York, NY, USA: Wiley, 2009.

[3] M. Leitch, "ISO 31000:2009—The new international standard on risk management," *Risk Anal.*, vol. 30, no. 6, pp. 887–892, 2010.

[4] T. Alpcan and T. Başar, *Network Security: A Decision and Game Theoretic Approach*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[5] J. Mounzer, T. Alpcan, and N. Bambos, "Dynamic control and mitigation of interdependent IT security risks," in *Proc. 2010 IEEE Int. Conf. Communications (ICC)*, May 2010, pp. 1–6.

[6] P. Bommannavar, T. Alpcan, and N. Bambos, "Security risk management via dynamic games with learning," in *Proc. 2011 IEEE Int. Conf. Communications (ICC)*, Jun. 2011, pp. 1–6.

[7] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24–29, 2012.

[8] S. Liu, X. Liu, and A. El Saddik, "Denial-of-Service (DoS) attacks on load frequency control in smart grids," in *Proc. 2013 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2013, pp. 1–6.

[9] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. IEEE Conf. Decision and Control*, Dec. 2010.

[10] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," in *Proc. American Control Conf.*, June 2010.

[11] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, 2011.

[12] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," *Int. J. Security Netw.*, vol. 6, no. 1/2011, pp. 2–13, 2011.

[13] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *Proc. 2011 IEEE Power and Energy Society General Meeting*, Jul. 2011, pp. 1–6.

[14] A. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667–674, 2011.

[15] Y. W. Law, T. Alpcan, M. Palaniswami, and S. Dey, "Security games and risk minimization for automatic generation control in smart grid," in *Proc. 3rd Conf. Decision and Game Theory for Security (GameSec 2012)*, 2012, vol. 7638, pp. 281–295, ser. LNCS, Springer Heidelberg, Germany.

[16] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," in *Proc. IEEE 50th Annual Allerton Conf. Communication, Control, and Computing*, 2012.

[17] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[18] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[19] S. Sridhar, M. Govindarasu, and C.-C. Liu, "Risk analysis of coordinated cyber attacks on power grid," in *Control and Optimization Methods for Electric Smart Grids*. New York, NY, USA: Springer, 2012, vol. 3, pp. 275–294.

[20] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010.

[21] T. Sommestad, M. Ekstedt, and L. Nordstrom, "Modeling security of power communication systems using defense graphs and influence diagrams," *IEEE Trans. Power Del.*, vol. 24, no. 4, pp. 1801–1808, Oct. 2009.

[22] A. Hahn and M. Govindarasu, "Cyber attack exposure evaluation framework for the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 835–843, Dec. 2011.

[23] Y. Shoham and K. Leyton-Brown, *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[24] A. J. Conejo, M. Carrión, and J. M. Morales, *Decision Making Under Uncertainty in Electricity Markets*. New York, NY, USA: Springer Science+Business Media, 2010.

[25] H. Bevrani, *Robust Power System Frequency Control*, ser. Power Electronics and Power Systems. New York, NY, USA: Springer, 2009.

[26] P. Kundur, *Power System Stability and Control*. New York, NY, USA: McGraw-Hill Professional, 1994.

[27] F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proc. IEEE*, vol. 93, no. 11, pp. 1890–1908, Nov. 2005.

[28] G. Andersson, Dynamics and Control of Electric Power Systems ETH Zürich, Switzerland, Feb. 2010, lecture notes 227-0528-00.

[29] J. Machowski, J. W. Bialek, and J. R. Bumby, *Power System Dynamics: Stability and Control*, 2nd ed. New York, NY, USA: Wiley, 2008.

[30] C. Luo, H. Far, H. Banakar, P.-K. Keung, and B.-T. Ooi, "Estimation of wind penetration as limited by frequency deviation," *IEEE Trans. Energy Convers.*, vol. 22, no. 3, pp. 783–791, Sep. 2007.

[31] S. K. Mullen, "Plug-in hybrid electric vehicles as a source of distributed frequency regulation," Ph.D. dissertation, Univ. Minnesota, Minneapolis, MN, USA, 2009.

[32] C. Alexander, *Market Risk Analysis: Value at Risk Models*. New York, NY, USA: Wiley, 2009, vol. 4.

[33] P. Varaiya, F. Wu, and J. Bialek, "Smart operation of smart grid: Risk-limiting dispatch," *Proc. IEEE*, vol. 99, no. 1, pp. 40–57, Jan. 2011.

[34] A. M. Fink, "Equilibrium in a stochastic n-person game," *Hiroshima Math. J.*, vol. 28, no. 1, pp. 89–93, 1964.

[35] L. Shapley, "Stochastic games," *Proc. Nat. Acad. Sci. USA. (PNAS)*, vol. 39, pp. 1095–1100, 1953.

[36] P. R. Thie and G. E. Keough, *An Introduction to Linear Programming and Game Theory*. New York, NY, USA: Wiley, 2008.

[37] D. Lefebvre, S. Bernard, and T. Van Cutsem, "Undervoltage load shedding scheme for the hydro-Québec system," in *Proc. IEEE Power Engineering Society General Meeting*, Jun. 2004, vol. 2, pp. 1619–1624.

[38] I. Sledge, T. Havens, J. Huband, J. Bezdek, and J. Keller, "Finding the number of clusters in ordered dissimilarities," *Soft Comput.*, vol. 13, no. 12, pp. 1125–1142, 2009.

[39] L. Busoniu, R. Babuska, and B. De Schutter, "A comprehensive survey of multiagent reinforcement learning," *IEEE Trans. Syst., Man, Cybern. C*, vol. 38, no. 2, pp. 156–172, Mar. 2008.

Yee Wei Law received the Ph.D. degree from University of Twente, The Netherlands.

He was a Research Fellow at The University of Melbourne, Australia, and starting from mid-2014, he is a Lecturer at the University of South Australia. His main research interests are the security and privacy aspects of smart grids, sensor networks, and more generally the Internet of Things. He is an Associate of $(ISC)^2$ and a member of Smart Grid Australia.

Dr. Law received the Best Paper Award at ICTC 2012.

Tansu Alpcan (SM'13) received the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Illinois at Urbana-Champaign, Urbana, IL, USA, in 2001 and 2006, respectively.

His research involves applications of distributed decision making, game theory, and control to various security and resource allocation problems in networked and power systems. He has been a Senior Lecturer at The University of Melbourne, Australia, since October 2011.

Marimuthu Palaniswami (F'12) received the Ph.D. degree from the University of Newcastle, Australia.

He is now a Professor at The University of Melbourne, Australia, and the Convener of the ARC Research Network on ISSNIP. His research interests include control, machine learning, signal processing and their applications to smart grids, biomedical engineering, wireless sensor networks, and the Internet of Things.

Dr. Palaniswami became an IEEE Distinguished Lecturer in machine learning in 2012.