Author copy. Accepted for publication. Do not distribute.

Cyber-Physical Resilience: Definition and Assessment Metric

Andrew Clark, *Member, IEEE,* and Saman Zonouz, *Member, IEEE*

***Abstract*—Resilient operation of cyber-physical infrastructures in adversarial environments requires *i)* toughness: maintenance of core crucial sub-functionalities despite ongoing intrusions, and *ii)* elasticity: recovery of the normal system operation in a timely manner. Put in other words, it does not require unrealistic assumptions about absolute preventative *protection* of complex cyber-physical platforms that would disable any type of malicious penetration and damage against the physical plant at the first place. Instead, resilience is based on the assumption that a sophisticated intrusion may succeed to evade the deployed protection and runtime *detection* mechanisms and impact the underlying system services and assets partially (except the core sub-functionalities). The resilient system fights back through reactive and proactive intrusion *tolerance* mechanisms to respond to ongoing misbehaviors and recover the affected system services and components within a reasonable time interval. In this paper, we present a formal definition of resilience and assessment metric for resilience. Our resilience metric quantifies the ability of the system to recover from an attack provided the attack is discovered within a fixed time interval, as well as the cost of recovery. We analyze the metric properties for linear systems and linear systems with actuator saturation. We then formulate cyber defense policies that ensure the resilience conditions are satisfied and validate our approach using a power system case study.**

***Index Terms*—Cyber-physical systems, cyber security, intrusion resilience.**

I. Introduction

Traditionally, security intrusions would target cyber assets through various attack vectors such as software vulnerability exploitations and social engineering channels. Recent advances in practical deployment of orchestrated operation of the cyber computations and physical processes in safety-critical infrastructures, so-called cyber-physical systems (CPS), have expanded the attack surfaces and their ultimate impact. As shown by the past real incidents, e.g., Stuxnet [1] and BlackEnergy3 [2] malware, cyber-originated misbehaviors can target physical components through a variety of domain-specific attack vectors such as sensor-based data corruptions, malicious control command injection, and the controller compromises.

Recently increasing number and complexity of fast-spreading and high-impact cyber-physical intrusions call for effective protection solutions. Cyber-physical security handling techniques can be categorized into three groups. First, intrusion prevention techniques (e.g., end-to-end data encryption), attempt to ideally prevent any attacks from happening in the first place. Second, intrusion detection solutions (e.g., host-based malware detection by anti-virus solutions) are designed based on the practical assumption that absolute security is infeasible and the attacks will still occur and need to be identified. Finally, intrusion tolerance solutions (e.g., infected asset containment by network firewalls) employ reactive and proactive response and recovery mechanisms to bring the affected system functionalities as the result of the successful and ongoing attacks.

Cyber-physical intrusion resilience aims at *i)* full correctness maintenance of the core (possibly empty) set of *crucial* sub-functionalities despite ongoing adversarial misbehaviors. Put in other words, it is acceptable for non-crucial sub-functionalities to be affected (partially degraded or complete failure) temporarily; and *ii)* guaranteed recovery of the normal operation of the affected sub-functionalities within a predefined cost limit, so-called *resilience threshold*. The cost limit can be formulated using various criteria such as time (recovery deadline), money (recovery expenses), etc. The abovementioned functionalities may involve integrated sub-components of the cyber network and physical platform.

Consequently, the required protection and Intrusion resilience is an overarching system property that requires a well-integrated and targeted design and deployment of the defense mechanisms (prevention, detection and tolerance) within various components of the target system. To guarantee permanent correct functionality of the crucial services, the corresponding system components have to either implement absolutely secure preventative measures, or leverage tolerance techniques (e.g., redundancy) to eliminate the possibility of any adversarial impact. The remaining components need the security protection mechanisms to an extent that satisfies the resilience threshold.

Our contributions in this paper are as follows:

- We provide a formal and abstract mathematical definition for intrusion resilience in cyber-physical systems. We characterize the resilience metric for linear systems and actuator-saturated linear systems, and provide methodologies for synthesizing controllers that guarantee resilience in such systems.
- We formulate a hierarchical game between the targeted cyber-physical platform and a cyber adversary, in which the value of each state of the game is equal to the resilience of the system. We propose Markovian cyber defense policies for maximizing resilience under cost constraints.
- We evaluate our proposed resilience metric and cyber assessment via power system case studies.

A. Clark was with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 – *aclark@wpi.edu*

S. Zonouz was with the Department of Electrical and Computer Engineering, Rutgers University, New Brunswick, NJ 08901 – *saman.zonouz@rutgers.edu*

The rest of the paper is organized as follows. Section II describes the related work. Section III describes the class of attacks considered in this paper. Section IV motivates the need for a definition and metric for cyber-physical intrusion resilience. Section V provides the physical system model, intrusion resilience definition and the corresponding metric. Section VI provides the resilience modeling and metric for the cyber network, and Section VII explains how the cyber and physical side resilience models are used by our framework for a hybrid cyber-physical resilience metric and assessment. Section VIII evaluates our resilience metric in a power system case study. Section II reviews the most related past work in the literature. Finally, Section IX concludes the paper.

II. Related Work

Recent work on adversary-aware control has addressed a range of topics such as models of attack and defense, risk assessment, attack detection and forensics, and secure control design. These contributions move towards development of a principled approach to cyber-physical security of power grid control systems [3].

SOCCA [4] presents a security assessment engine to identify the weaknesses of a smart grid topology against cyber attacks. For improved resiliency of microgrid operations, Che et al. [5] proposes to use a tertiary DC control. SCPSE [6] presets an online smart grid monitoring and incident detection framework to identify malicious misbehaviors on the control network of the power system and perform bad-data detection accordingly. Hossain et al. [7] proposed a resilience analysis technique in a distributed power system control setting to determine the *redundant* and *critical* controllers depending on whether the power system maintains its controllability if a particular controller is compromised. Zonouz et al. [8], [9] proposes a embedded system security monitoring solution to ensure the correct operation of the power system controller devices.

Vulnerability assessment of smart grid critical infrastructures has been studied using network interdiction formulations, e.g., sequential games [10], [11], where the operator (leader) chooses a source-destination path, and then the interdictor (follower) inspects one arc to maximize the probability with which the operator is detected. In the model by Bertsimas et al. [12], the operator chooses a feasible flow, and then the interdictor disrupts a fixed number of edges. The interdictor's goal is to minimize the maximum flow that reaches the destination node.

Bienstock [13] develops efficient mixed-integer linear network models for the power system $(N-k)$ problem. Salmeron et al. [14] solved a network interdiction problem to identify maximally disruptive cyber-physical attacks. A resource-constrained attacker (leader) targets a set of control system components, and the defender (follower) uses an optimal-flow model to implement response measures after the attack. The important work by Verma and Bienstock [13] develops network interdiction models to study the $(N-k)$ problem in power grids. State-of-the-art computational methods for solving large-scale mixed integer programs have been applied to solve these problems.

Still a major gap remains to propagate the effect of attacks on smart grids at the level of mathematical control specification to numerical solvers and optimization toolboxes, and runtime machine code executions. Our project aims to build a defense-in-depth resilient design to address this gap. Standard control-theoretic techniques such as robustness aim to ensure that a system is stable in the presence of arbitrary disturbances. The assumptions underlying these approaches are that the disturbances are bounded in energy and that the robust controller is fixed. By comparison, our resilience metric assumes that the disturbance signal can be arbitrary but is of finite duration, and that the controller can be modified to restore stability after a compromise is detected.

Furthermore, the cyber-physical smart-grid operations include close interactions between its cyber assets and physical components. Modeling the involved cyber-physical interdependencies concisely is a challenging endeavor. To that end, we leverage game-theoretic modeling and control theoretic analysis techniques to consider the cyber security interactions between the adversaries and the system, and physical dynamics of the power system, respectively. This hybrid modeling and analysis framework enables us to investigate the effects of any malicious cyber-originated misbehaviors (e.g., controller injection by a computer virus) on the operation of the power system (e.g., whether the generators are dispatched correctly).

III. Attack Model

Our proposed resilience definition and the corresponding assessment metric mainly focus on attacks that originate from the cyber network and then impact the physical components. The physical plant is assumed to be controlled by a distributed set of (possibly redundant) controllers and actuation points. The (possibly) multi-step cyber attack initiates from an attacker-resident Internet node and traverses the control network through several host compromises via vulnerability exploitations. The adversary's cyber-side goal is to compromise and gain control over controllers that are in direct contact with the physical plant actuators. Finally, the attacker will leverage the malicious access to the compromised controllers and issue unsafe control commands to drive the underlying physical plant as much away as possible from the safe states.

Once the deployed defense mechanisms detect the compromised controllers, it takes two types of response and recovery actions. As the immediate response, the untrusted controllers are contained and isolated through cyber-side actions (e.g., firewall ruleset updates and remote disconnect commands) so that the compromised controllers cannot affect the underlying physical plant actuators anyways anymore. The defense mechanisms will then take more time-consuming recovery actions (e.g., via restoring a clean state of a compromised controller) to recover normal secure operation of the controllers and connect them back to the network.

IV. Motivation and Overview

A. Motivation: Power Grid Case-Study

Traditionally, purely-cyber intrusion resilience solutions could be either model-based [10] that take advantage of system

models for their response strategy optimization, or model-free [15] that do not leverage system models and perform their strategy selection based on sensor data only. In cyber-physical settings, we believe that model-free approaches are often of limited use due to the high system complexity and sophisticated inter-dependencies among the cyber and physical components. For instance, cascading failures are widely studied in the power systems domain and occur due to high interconnectivity among the power assets. As a case in point, a *single* malicious transmission line outage could indirectly cause several subsequent line outages by forcing power redistribution to adjacent lines, causing them to overload. Using system models, an estimate of the post-outage flows can be calculated using line outage distribution factors [16]. It is noteworthy that similar cascading overload scenarios could be caused by an ill-designed intrusion resilience engine that attempts to fix a problem locally without consideration of the action's global impact on the power network. Model-based techniques for cyber-physical intrusion resilience can potentially consider such complex failure and recovery scenarios.

1) Integrated cyber-physical resilience: Cyber-based resilience represents strategies and actions that deal with cyber components and their recovery from intrusions. For instance, a firewall reconfiguration to proactively prevent an upcoming attack is a cyber-based response action. Power-side intrusion response actions support corrective manipulation of power components, e.g., generation redispatch or line status changes to tolerate a recent malicious line outage. Power-based strategies and actions support corrective manipulation of power components for resilience purposes such as power topology changes to tolerate a recent malicious line outage. When responding to and recovering from intrusions, cyber- and power-based resilience engines deal with two completely different types of system dynamics and incidents (discrete sequential logic within a computing platform vs. continuous differential dynamics governing the physical power components). The actions taken by cyber- and power-based resilience engines are also radically different. The difference arises because physical actions often occur on a continuum, e.g., a real number representing the power generation set-point, whereas cyber systems have a discrete action set, e.g., block/allow access attempts to a particular system file.

A truly comprehensive cyber-physical intrusion resilience architecture makes use of both cyber and physical resilience engines in an integrated manner such that both discrete and continuous dynamics are taken into account. Equivalently, it requires extensions to *i)* cyber-based intrusion resilience to make them power-aware so that they take into account the power system dynamics and topologies when deciding upon a cyber-based action. For instance, a cyber-based resilience engine within a CPS setting may prioritize recovery of a crashed cyber host in charge of a critical generator control over a unavailable historian logging server host because its failure leads to more severe physical impact; *ii)* power-based fault resilience to make them cyber-security-aware such that they make operating decisions on optimal response strategies considering the cyber network status. For instance, a power-based resilience engine within a CPS setting may choose to isolate a particular generator from the rest of the power system (e.g., through node-breaker reconfiguration at the substation) and compensate for its missing power through secondary generation plants after receiving a recent notification that the first generator's controller has been compromised.

Why consider physical system resilience actions as opposed to pure reliance on cyber-side capabilities? Comprehensive cyber-physical intrusion resilience requires power-side response actions because of the following reasons: *i)* A malicious attacker may break down a power component such that the system cannot be restored without physical power-side actions, e.g., by causing a generator to blow up. When cyber-only capabilities cannot fix the compromise, automated fixing via cyber-only capabilities is not possible, taking physical power-side actions is necessary, e.g., switching to a redundant component. *ii)* The consequence of a malicious attack on the power side *is* occasionally fixable through automated commands, e.g., a malicious relay opening could be reverted simply through a cyber-side close command. However, the attacker may open the relay again if the controller remains compromised and its clean state cannot be fully recovered. In those cases, cyber-side restoration is not feasible based on the cyber system's built-in capabilities and degree of redundancy, and power-side response actions may be required. if the cyber side restoration is not feasible based on the system's built-in capabilities and degree of redundancy. For instance, power-side actions may be taken to physically isolate the compromised controller through power topology reconfiguration using other non-compromised breakers in the substation.

Why consider cyber-side response actions as opposed to pure reliance on traditional control? This is the dual problem to the one discussed above. Cyber-physical intrusion resilience requires cyber-based response and recovery action execution because of the following reasons: *i)* Pure reliance on power-side fault resilience may be too costly and slow for practical deployments. Power-aware cyber-side resilience facilitates execution of corrective actions on the cyber side to restore the physical system after an attack (e.g., recover from a malicious relay opening) through timely restoration of the compromised controller. In our example attack above, once the cyber component has been recovered, the protective relay can simply re-close. Without such cyber-side resilience support, any potential malicious relay manipulation on a line would require physical power system reconfiguration and/or redispatch. *ii)* Permanent recovery from a cyber-originated cyber-physical intrusion requires cyber resilience mechanisms; otherwise, each time the physical resilience solution fixes an attack consequence, e.g., re-closure of an opened circuit breaker, the attacker could immediately cause the same consequence again, because the physical resilience engine is not aware of the compromised set of cyber assets and can only take cyber-blind control actions that are never able to "clean" the system from malicious parties or patch the cyber vulnerabilities. Consequently, without knowledge of the cyber state, any compromises and their impacts are essentially cumulative, due to the fact that the system is never cleaned. The system would only become more compromised, never less, and the physical-only resilience engine would have an increasingly

difficult time finding any feasible recovery strategy against adversaries.

B. Resilience Metric Overview

Our approach to CPS resilience is illustrated in Figure 1. The system is a hierarchy with two layers. The top (cyber) layer represents the progress of the cyber attack and is represented as a Markov decision process. The bottom (physical) layer represents the impact of the attack on the physical dynamics. For each cyber attack state, we quantify the resilience of the physical system, which characterizes the amount of control effort (cost) required to steer the system back to a stable equilibrium state, which is assumed to be at zero without loss of generality. The metric implements a sequential optimization procedure to quantify the difficulty of driving the under-attack system back to its resilient mode. The following section describes the details of the proposed metric and assessment algorithm.

V. Metric Formulation

This section presents our proposed resilience metric. We first describe the class of systems for which the metric is defined, and then formulate the metric. We analyze this metric for linear systems and linear systems with bounded actuation.

A. System Model

We consider attacks on cyber-physical systems in which the physical plant can be modeled as a continuous dynamical system with state $\mathbf{x}(t)$. The system is assumed to have control input signal $\mathbf{u}(t) \in \mathbb{R}^m$. Furthermore, the adversary is assumed to be able to introduce a disturbance signal $\mathbf{v}(t) \in \mathbb{R}^l$. The disturbance signal of the adversary may represent a physical attack on the plant, a change to the input signal via compromised control software, or a false data injection. The temporal dynamics of the state are described by the system

$$(\Omega) \begin{cases} \dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{u}(t), \mathbf{v}(t)) \\ \mathbf{y}(t) = g(\mathbf{x}(t), \mathbf{u}(t), \mathbf{v}(t)) \end{cases} \tag{1}$$

The function f describes the impact of the adversarial signal on the plant dynamics, while g describes the impact of the signal on the observed output, as in the case of false data injection attack.

A relevant special case of (1) occurs when the control input $\mathbf{u}(t)$ is an affine feedback signal and the adversary is able to compromise a set of controllers. Suppose that, in the absence of any compromise, the system dynamics are given by $\dot{\mathbf{x}}(t) = f(\mathbf{x}(t)) + B\mathbf{u}(t)$, where the i-th column of B is denoted $\mathbf{b}_i$, and that the adversary compromises a set of controllers with indices $S \subseteq \{1, \ldots, m\}$.

The impact of the attack can be described by defining matrices $B(S)$ and $E(S)$ as follows. For matrix $B(S)$, let the i-th column be given by $\mathbf{b}_i$ if $i \in \{1, \ldots, m\} \setminus S$, and 0 otherwise. For matrix $E(S)$, let the columns be given by $(\mathbf{b}_i : i \in S)$. The system dynamics for this case are given by

$$(\Omega) \begin{cases} \dot{\mathbf{x}}(t) = f(\mathbf{x}(t)) + B(S)\mathbf{u}(t) + E(S)\mathbf{v}(t) \\ \mathbf{y}(t) = g(\mathbf{x}(t)) \end{cases} \tag{2}$$

We assume that $\mathbf{x} = 0$ is an equilibrium point of the dynamics $\dot{\mathbf{x}}(t) = f(\mathbf{x}, 0, 0)$, i.e., $\mathbf{f}(0,0,0) = 0$. Our definition of resilience also assumes that all attacks are detected via cyber intrusions and not through their impact on the physical plant, and plan to integrate observer-based detection of attacks into our approach in future work.

B. Metric Definition

In order to define the metric, we first introduce the notion of basin of attraction.

Definition 1: The basin of attraction is the set of states D such that $\mathbf{x}(0) \in D$ and $\mathbf{u}(t) = \mathbf{v}(t) \equiv 0$ implies that $\lim_{t\to\infty} \mathbf{x}(t) = 0$.

Intuitively, the basin of attraction is defined as the set of initial states such that the system will return to the equilibrium point 0 if no additional input is provided. In addition to the basin D, we define the a set of safe states S. Safe states represent constraints on the basic functionality of the system, e.g., ensuring that rotor angle separations in a power system do not exceed $\pi/2$. We let $W = S \cap D$. The definition of resilience is given as follows.

Definition 2: Let T denote the time when a system compromise is detected and removed. A system (Ω) is *resilient* if, for any adversarial input $\{\mathbf{v}(t) : t \in [0, T]\}$, the resulting state $\mathbf{x}(T)$ lies in the basin of attraction when $\mathbf{x}(0) = 0$.

This definition of resilience is analogous to the definition of resilience in materials science, namely, the amount of energy that must be exerted to steer the system to a state from which it cannot recover to the stable equilibrium. We further define the *cost of recovery* as follows.

Definition 3: Let $\mathcal{R}$ denote the set of states $\mathbf{x}(T)$ that are reachable by the adversary within time T. For any state $\mathbf{x}_0 \in \mathcal{R}$, define $\mathcal{E}(\mathbf{x}_0)$ to be the cost required to steer the system state to the origin, i.e.,

$$\mathcal{E}(\mathbf{x}_0) \triangleq$$
$$\min \left\{ \int_0^\infty \mathbf{x}(t)^T Q \mathbf{x}(t) + \mathbf{u}(t)^T R \mathbf{u}(t) : \lim_{t\to\infty} \mathbf{x}(t) = 0, \mathbf{x}(0) = \mathbf{x}_0 \right\}$$

where Q and R are positive definite matrices that describe the cost of deviating from the zero state and the cost of control, respectively. The cost of recovery is defined by

$$\max \{\mathcal{E}(\mathbf{x}) : \mathbf{x} \in \mathcal{R}\}.$$

The cost of recovery captures the additional energy required to return the system to the stable state following a disturbance or malicious attack. The quadratic metric $\mathcal{E}(\mathbf{x}_0)$ is chosen for consistency with the standard cost functions from the control theory literature.

C. Resilience of Linear Systems

We first consider linear systems, which will provide initial insights towards our approach. The results of this subsection are valid for linear systems, but may also be applicable to nonlinear systems that can be approximated by linear systems, such as the linearization of a nonlinear system around a stable operating point. This approach to analysis of nonlinear systems

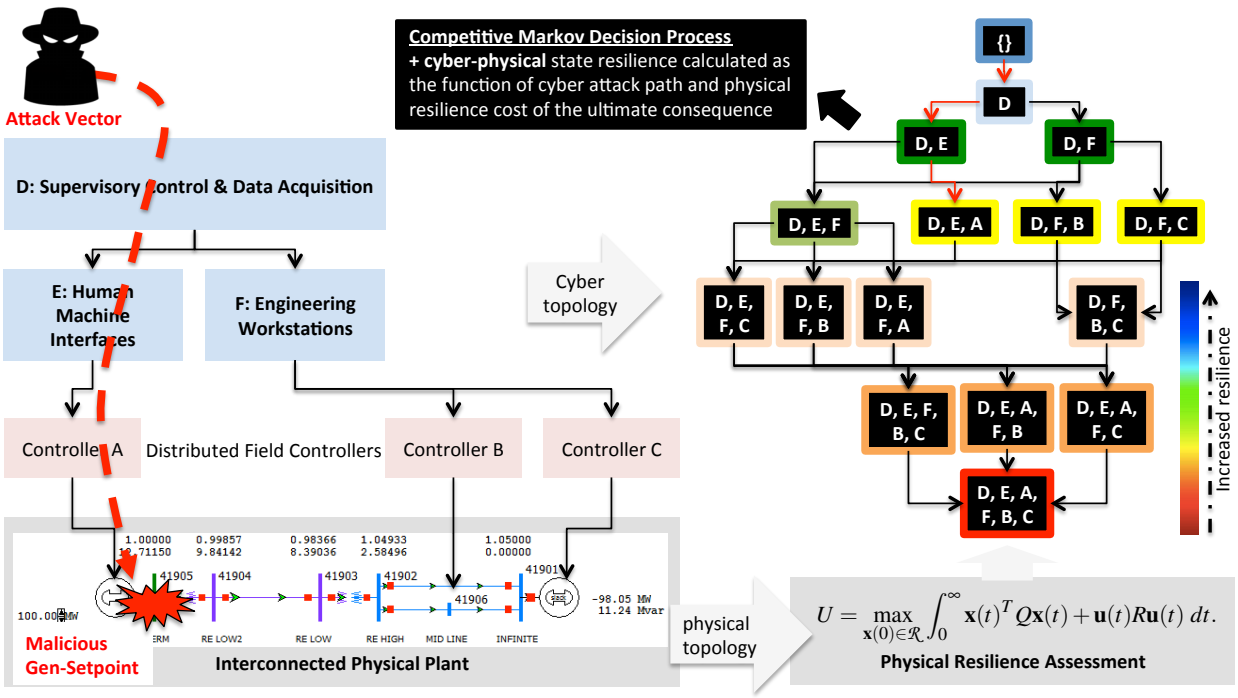


Fig. 1: Cyber-Physical Resilience Metric

is relevant to scenarios such as small-signal stability evaluation in power systems. For a linear system with dynamics

$$\begin{aligned} \dot{\mathbf{x}}(t) &= A\mathbf{x}(t) + B\mathbf{u}(t) \\ \dot{\mathbf{y}}(t) &= \mathbf{x}(t) \end{aligned} \tag{3}$$

the conditions for resilience can be described via controllability analysis of the system. Consider the controller compromised attack described by (2). As a preliminary, let $\{\mathbf{q}_1, \ldots, \mathbf{q}_l\}$ denote the set of unstable modes of A.

Proposition 1: Suppose that (A,B) is a linear system and that A is diagonalizable. The system (3) is resilient to compromise of a set of controllers S iff any unstable mode $\mathbf{q}$ of A that lies in the controllable subspace of $E(S)$ also lies in the controllable subspace of $B(S)$.

Proof: Suppose that an unstable mode $\mathbf{q}$ lies in the controllable subspace of $E(S)$ but not the controllable subspace of $B(S)$. Then there is an input $\{\mathbf{v}(t) : t \in [0,T]\}$ such that $\mathbf{x}(T) = \mathbf{q}$ when $\mathbf{u}(t) = 0$. Furthermore, by superposition and the fact that $\mathbf{q}$ is not in the controllable subspace of $B(S)$, for any input $\mathbf{u}(t)$, $\mathbf{x}(T) = \mathbf{q} + \mathbf{r}$ where $\mathbf{r}$ is linearly independent of $\mathbf{q}$. Since $\mathbf{q}$ is not in the controllable subspace of $(A,B(S))$, $\mathbf{q}$ is not in the span of the controllability Gramian for the system $(A,B(S))$, the vector $\mathbf{x}(T)$ is also not in the span, and hence there is no input $\mathbf{u}(t)$ that can steer the system to a neighborhood of the origin.

Conversely, suppose that every unstable mode that is in the controllable subspace of $(A,E(S))$ is also in the controllable subspace of $(A,B(S))$. Then $\mathbf{x}(T)$ can be decomposed as $\mathbf{x}(T) = \mathbf{r}' + \mathbf{r}''$, where $\mathbf{r}'$ is in the controllable subspace and $\mathbf{r}''$ is in the span of the stable modes, and hence will converge to $\mathbf{0}$ in the absence of any control action. Thus for any $\varepsilon > 0$, there exists a time index T' and a control signal $\{\mathbf{u}(t) : t \in [T,T']\}$ such that $||\mathbf{x}(T')|| < \varepsilon$, implying that convergence to 0 can be guaranteed. ■

Based on Proposition 1, we say that a set of controllers Z is *resilient* if the set of unstable modes, denoted $\{\mathbf{u}_1, \ldots, \mathbf{u}_l\}$, satisfy $\{\mathbf{u}_1, \ldots, u_l\} \subset \text{span}(B(Z)\ AB(Z)\ \cdots\ A^{n-1}B(Z))$. A set of controllers is denoted a *critical resilient set* if all non-trivial subsets of Z are not resilient. Equivalently, Z is a critical resilient set if for any $j \in Z$, there exists $i \in \{1, \ldots, l\}$ such that $\mathbf{u}_i \notin \text{span}(B(Z \setminus \{j\}) \cdots A^{n-1}(B(Z \setminus \{j\})))$. The problem of selecting a minimum-cardinality set of controllers satisfying this condition has been considered in, e.g., [17], and is known to be NP-hard but approximable within polynomial time up to a provable optimality bound of $O(\log m)$.

The cost of recovery for a linear system can be computed by minimizing the cost function

$$\max_{\mathbf{x}(0)} \left\{ \int_0^\infty \mathbf{x}(t)^T Q\mathbf{x}(t) + \mathbf{u}(t)^T R\mathbf{u}(t)\ dt \right\}.$$

The controller that minimizes this cost function is a feedback controller $\mathbf{u}(t) = K(S)\mathbf{x}(t)$, where $K(S)$ is obtained as $K(S) = -R^{-1}B(S)^T P$ and P is the solution to the algebraic Riccati equation

$$A^T P + PA - PB(S)R^{-1}B(S)^T P + Q = 0.$$

D. Resilience under Actuator Saturation

Another relevant case is linear systems with actuator saturation, which have dynamics defined by

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\text{sat}(\mathbf{u}(t)),$$

where $\text{sat} : \mathbb{R}^m \to \mathbb{R}^m$ is a function defined by

$$(\text{sat}(\mathbf{u}))_i = \begin{cases} -\gamma, & u_i < -\gamma \\ \gamma, & u_i > \gamma \\ u_i & \text{else} \end{cases}$$

Actuator saturation is relevant to resilience because it provides a natural scenario in which the adversary has a limited impact on the system, while the system has a limit on its ability to recover. For ease of analysis, we assume that only a single controller is compromised; our approach, however, can be extended to compromise of multiple controllers.

The resilient system design must ensure that, if the adversary is detected within time T, the remaining non-compromised controllers can still drive the system state back to $\mathbf{0}$. Our approach is to synthesize a family of resilient controllers $\mathbf{u}(t) = K\mathbf{x}(t)$ such that the system state is restricted to a region where the actuator saturation constraints are never binding, or equivalently, $||\mathbf{u}(t)||_\infty \leq \gamma$. We restrict to this set of states in order to ensure computational tractability of the controller design problem. Specifically, we synthesize a single controller matrix K and a region $\mathcal{R}$ that guarantees that the system remains in region $\mathcal{R}$ up to time T after a single controller has been compromised, as well as a set of controllers $\overline{K}_1, \ldots, \overline{K}_m$ that steer the state back to the origin after the compromise has been detected. Under this approach, the state dynamics are given by

$$\dot{\mathbf{x}}(t) = \begin{cases} A\mathbf{x}(t) + B_i \text{sat}(K\mathbf{x}(t)), & t \in [0,T] \\ (A + B_i \text{sat}(\overline{K}_i \mathbf{x}(t))), & t > T \end{cases}$$

where B_i is equal to the matrix B with the i-th column (corresponding to the compromised controller) set to 0.

Proposition 2: Suppose that there exists a set $\mathcal{R}$ and a set of controllers $\overline{K}_1, \ldots, \overline{K}_m$ and K satisfying the following conditions: (a) If node i is compromised at time 0 with $\mathbf{x}(0) = 0$, then $\{\mathbf{x}(t) : t \in [0,T]\} \subset \mathcal{R}$ when controller K is active; (b) Controller $\overline{K}_i$ guarantees asymptotic stability of the origin and positive invariance of $\mathcal{R}$; (c) $||K_i\mathbf{x}||_\infty \leq \gamma$ and $||\overline{K}_i\mathbf{x}||_\infty \leq \gamma$ for all $\mathbf{x} \in \mathcal{R}$, where K_i is the matrix obtained by removing the i-th column of K. Then the system is resilient to compromise of any single controller.

Proof: If conditions (a)–(c) hold, then the system dynamics are given by

$$\dot{\mathbf{x}}(t) = \begin{cases} (A + B_i K_i)\mathbf{x}(t) + E\text{sat}(v), & t \in [0,T] \\ (A + B_i \overline{K}_i)\mathbf{x}(t), & t > T \end{cases}$$

where $E\text{sat}(v)$ represents the impact of the malicious controller. Hence for $t > T$, the fact that $(A + B_i\overline{K}_i)$ is asymptotically stable guarantees that the system state returns to 0 and resilience is satisfied. ■

In order to satisfy the conditions of Proposition 2, we consider ellipsoidal $\mathcal{R}$ defined by

$$\mathcal{R} := \left\{ \mathbf{x} : \mathbf{x}^T P \mathbf{x} \leq \frac{1}{\alpha^2} \right\},$$

where $\alpha > 0$ and P is a positive definite matrix. We compute a candidate value of P by solving

$$A^T P + PA - \rho P = -I, \tag{4}$$

where ρ is the largest eigenvalue of A.

We choose the matrix P based on (4) so that we can apply Lyapunov theory to prove invariance of the set $\mathcal{R}$, while the goal of minimizing ρ can be interpreted as selecting the minimum-energy controller needed to stabilize A.

Remark 1: Certain types of safety constraint can also be incorporated into this choice of $\mathcal{R}$. For example, when the set of safe states is an ellipsoidal region $\{\mathbf{x}^T\Theta\mathbf{x} \leq \xi\}$, the set $\{\mathbf{x}^T P\mathbf{x} \leq \frac{1}{\alpha^2}\}$ satisfies the safety requirement iff

$$\alpha \geq \frac{1}{\sqrt{\xi}} \lambda_{max}((P^{-1/2})^T \Theta P^{-1/2}).$$

Using this definition of P, it remains to find $\mathcal{R}$ and the controller matrices. Turning to property (a) of Proposition 2, we have the following sufficient condition.

Lemma 1: Suppose that $\mathcal{R} = \{\mathbf{x} : \mathbf{x}^T P\mathbf{x} \leq \frac{1}{\alpha^2 T}\}$ and there exists $b > 0$ such that for any $\mathbf{x} \in \mathcal{R}$,

$$\mathbf{x}^T(\overline{A}_i^T P + P\overline{A}_i)\mathbf{x} + 2bE_i^T P\mathbf{x} \leq \frac{1}{\alpha^2 T}.$$

Then $\{\mathbf{x}(t) : t \in [0,T]\} \subset \mathcal{R}$ for any adversarial input signal $v(t)$.

Proof: Define a function $V(t)$ by $V(t) = \mathbf{x}(t)^T P\mathbf{x}(t)$. Since $V(0) = 0$, a sufficient condition for $\{\mathbf{x}(t) : t \in [0,T]\} \subset \mathcal{R}$ is $\dot{V}(t) \leq \frac{1}{\alpha^2 T}$ for $t \in [0,T]$. We have that

$$\begin{aligned} \dot{V}(t) &= \mathbf{x}(t)^T P\dot{\mathbf{x}}(t) + \dot{\mathbf{x}}(t)^T P\mathbf{x}(t) \\ &= \mathbf{x}^T(\overline{A}_i^T P + P\overline{A}_i)\mathbf{x}(t) + 2v(t)E_i^T P\mathbf{x} \end{aligned}$$

yielding the desired result. ■

Lemma 1 implies that

$$\max\{\mathbf{x}^T(\overline{A}^T P + PA)\mathbf{x} + 2vE_i^T P\mathbf{x} : \mathbf{x}^T P\mathbf{x} \leq \frac{1}{\alpha^2}, |v| \leq b\} \leq \frac{1}{\alpha^2 T}$$

is a sufficient condition for (a) in Proposition 2. Since the maximum value occurs at $v = b$ if $E_i^T P\mathbf{x} > 0$ and $v = -b$ otherwise, we obtain that this condition is equivalent to

$$\max\{\mathbf{x}^T(\overline{A}_i^T P + P\overline{A}_i)\mathbf{x} + 2bE_i^T P\mathbf{x} : \mathbf{x}^T P\mathbf{x} \leq \frac{1}{\alpha^2}\} \leq \frac{1}{\alpha^2 T}.$$

Finally, letting $\hat{\mathbf{x}} = \alpha\mathbf{x}$ and multiplying both sides by α^2 gives the equivalent condition

$$\max\{\hat{\mathbf{x}}^T(\overline{A}_i^T P + P\overline{A}_i)\hat{\mathbf{x}} + 2\alpha bE_i^T P\hat{\mathbf{x}} : \hat{\mathbf{x}}^T P\hat{\mathbf{x}} \leq 1\} \leq \frac{1}{T} \tag{5}$$

The left-hand side of (5) is a pointwise maximum of convex functions in $\overline{A}_i$ and α, and hence is convex, making this a convex constraint for (a).

For condition (b) of Proposition 2, a sufficient condition is that the matrix $A_i := A + B_i\overline{K}_i$ satisfies the Lyapunov equation

$$A_i^T P + PA_i < 0,$$

which is a linear matrix constraint. Finally, the condition

$$\max\{||K\mathbf{x}||_\infty : \mathbf{x}^T P\mathbf{x} \leq \frac{1}{\alpha^2}\}$$

can be made equivalent to

$$\max\{||K\hat{\mathbf{x}}||_\infty : \hat{\mathbf{x}}^T P\hat{\mathbf{x}} \leq 1\} \leq \gamma\alpha,$$

which is convex in K_i and α, by setting $\hat{\mathbf{x}} = \alpha\mathbf{x}$. Combining

these conditions together yields the convex feasibility problem

$$\begin{array}{ll} \text{variables:} & \alpha, K, \overline{K}_1, \ldots, \overline{K}_m, \overline{A}_1, \ldots, \overline{A}_m, A_1, \ldots, A_m \\ \text{constraints:} & A_i = A + B_i K,\ \overline{A}_i = A + B_i \overline{K}_i,\ i = 1, \ldots, m \\ & \max\{\hat{\mathbf{x}}^T (A_i^T P + P A_i)\hat{\mathbf{x}} + 2\alpha b E_i^T P \hat{\mathbf{x}} : \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \leq 1\} \leq \frac{1}{T} \\ & \overline{A}_i^T P + P\overline{A}_i < 0, A_i^T P + P A_i < 0,\ i = 1, \ldots, m \\ & \max\{K_i \hat{\mathbf{x}}||_\infty : \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \leq 1\} \leq \alpha\gamma \\ & \max\{||\overline{K}_i \hat{\mathbf{x}}||_\infty : \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \leq 1\} \leq \alpha\gamma \end{array} \tag{6}$$

Minimizing the cost of recovery is described as follows. Suppose the cost function is defined by

$$U = \max_{\mathbf{x}(0) \in \mathcal{R}} \int_0^\infty \mathbf{x}(t)^T Q \mathbf{x}(t) + \mathbf{u}(t) R \mathbf{u}(t)\ dt. \tag{7}$$

A bound on the cost function is given by the following lemma.

Lemma 2: Suppose that

$$\max_{i=1,\ldots,m} \sigma_{max}(P^{-1/2}(Q + \overline{K}_i^T R \overline{K}_i) P^{-1/2} \leq \sigma$$

and $\dot{V}(t) \leq -\rho V(t)$, where $V(t) = \mathbf{x}(t)^T P \mathbf{x}(t)$. Then $U \leq \frac{1}{\alpha^2}\frac{\sigma}{\rho}$.

Proof: For any $i = 1, \ldots, m$, we have that

$$\begin{aligned} U &= \max_{\mathbf{x}(0) \in \mathcal{R}} \int_0^\infty \mathbf{x}(t)^T (Q + \overline{K}_i^T R \overline{K}_i) \mathbf{x}(t)\ dt \\ &= \max_{\mathbf{x}(0) \in \mathcal{R}} \int_0^\infty \mathbf{x}(t)^T P^{1/2} P^{-1/2} (Q + \overline{K}_i^T R \overline{K}_i) P^{-1/2} P^{1/2} \mathbf{x}(t)\ dt \\ &\leq \max_{\mathbf{x}(0) \in \mathcal{R}} \int_0^\infty \mathbf{x}(t)^T P \mathbf{x}(t) \sigma_{max}(P^{-1/2}(Q + \overline{K}_i^T R \overline{K}_i) P^{-1/2})\ dt \end{aligned}$$

which follows from the definition of the singular value. Furthermore, if $\dot{V}(t) \leq -\rho V(t)$, then $\mathbf{x}(t)^T P \mathbf{x}(t) = V(t) \leq e^{-\rho t} \mathbf{x}(0)^T P \mathbf{x}(0)$. Combining these inequalities yields

$$U \leq \max_{\mathbf{x}(0) \in \mathcal{R}} \int_0^\infty e^{-\rho t} \mathbf{x}(0)^T P \mathbf{x}(0) \sigma_{max}(P^{-1/2}(Q + \overline{K}_i^T R \overline{K}_i) P^{-1/2})\ dt.$$

By definition $\mathcal{R} = \{\mathbf{x} : \mathbf{x}^T P \mathbf{x} \leq \frac{1}{\alpha^2}\}$, and thus $U \leq \frac{1}{\alpha^2}\frac{\sigma}{\rho}$. ∎

Lemma 2 implies that, in order to minimize the cost of recovery, it suffices to find the minimum value of $\beta := \frac{\sigma}{\rho}$ such that

$$\sigma_{max}(P^{-1/2}(Q + \overline{K}_i^T R \overline{K}_i) P^{-1/2}) \leq \sigma \tag{8}$$

$$\dot{V}(t) \leq -\rho V(t) \tag{9}$$

We have that (8) is equivalent to

$$P^{-1/2}(Q + \overline{K}_i^T R \overline{K}_i) P^{-1/2} - \sigma I \leq 0,$$

which is in turn equivalent to $\sigma P - Q - \overline{K}_i^T R \overline{K}_i \leq 0$. Using the Schur complement theorem, this inequality is equivalent to the linear matrix inequality

$$\begin{pmatrix} \sigma P - Q & \overline{K}_i^T \\ \overline{K}_i & R^{-1} \end{pmatrix} \geq 0.$$

For constraint (9), we have that $\dot{V}(t) \leq -\rho V(t)$ is equivalent to

$$(A + B_i \overline{K}_i)^T P + P(A + B_i \overline{K}_i) + \rho P \leq 0,$$

which is a linear matrix inequality in ρ and $\overline{K}_i$.

Combining these inequalities with (6) yields a formulation for synthesizing resilient controllers with minimum cost of recovery.

$$\begin{array}{ll} \text{minimize} & \frac{\beta}{\alpha^2} \\ \text{variables:} & \alpha, K, \overline{K}_1, \ldots, \overline{K}_m, \overline{A}_1, \ldots, \overline{A}_m, A_1, \ldots, A_m, \sigma \\ \text{constraints:} & A_i = A + B_i K,\ \overline{A}_i = A + B_i \overline{K}_i,\ i = 1, \ldots, m \\ & \max\{\hat{\mathbf{x}}^T (A_i^T P + P A_i)\hat{\mathbf{x}} + 2\alpha b E_i^T P \hat{\mathbf{x}} : \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \leq 1\} \leq \frac{1}{T} \\ & \overline{A}_i^T P + P\overline{A}_i < 0, A_i^T P + P A_i < 0,\ i = 1, \ldots, m \\ & \max\{||K_i \hat{\mathbf{x}}||_\infty : \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \leq 1\} \leq \alpha\gamma \\ & \max\{||\overline{K}_i \hat{\mathbf{x}}||_\infty : \hat{\mathbf{x}}^T P \hat{\mathbf{x}} \leq 1\} \leq \alpha\gamma \\ & \sigma \leq \rho\beta \\ & \begin{pmatrix} \sigma P - Q & \overline{K}_i^T \\ \overline{K}_i & R^{-1} \end{pmatrix} \geq 0. \\ & (A + B_i \overline{K}_i)^T P + P(A + B_i \overline{K}_i) + \rho P \leq 0 \end{array} \tag{10}$$

Eq. (10) is convex for any fixed β; hence, an optimal solution can be found in quasi-polynomial time by using a bisection algorithm to iterate over the possible values of β.

As an example, consider a single-input, single-output system with one state variable. The dynamics are given by

$$\dot{x}(t) = ax(t) + b\text{sat}(u_1(t)) + b\text{sat}(u_2(t)),$$

where a and b are positive constants. The system is resilient if the system can always be recovered to the 0 state when the attack is detected within time T. Suppose without loss of generality that the signal $u_2(t)$ is compromised first. We observe that if $x(0) > 0$, then the adversary's optimal strategy will be to choose $u_2(t) \equiv \gamma$, while the best-case for the system response will be $u_1(t) \equiv -\gamma$. The resulting dynamics are given by $\dot{x}(t) = ax(t)$, so that $x(t) = e^{aT} x(0)$.

Now, we consider the set of states x such that the system can be returned to 0 from state x after the attack is detected. We have that $\dot{x}(t) > ax(t) - b\gamma$, and therefore the system can be returned to 0 iff $ax < b\gamma$, or alternatively $x < \frac{b\gamma}{a}$. Hence, if $x(T) > \frac{b\gamma}{a}$ at the detection time T, then the system state cannot be returned to 0. Equivalently, if $x(0) > e^{-aT}\frac{b\gamma}{a}$, then the adversary can destabilize the system.

We therefore arrive at the following control strategy to ensure resilience. When $|x(t)| < \frac{e^{-aT} b\gamma}{a} - \varepsilon$ for some $\varepsilon > 0$, then the system follows a stabilizing linear control law, i.e., $u_1(t) = u_2(t) = -\frac{(a+\delta)}{b} x(t)$ for some $\delta > 0$. For $x(t)$ outside of that range, follow the law $u_1(t) = u_2(t) = \gamma$ when $x(t) < 0$ and $u_1(t) = u_2(t) = -\gamma$ when $x(t) > 0$. Following such a rule will ensure resilience provided that the system is initialized close to 0.

VI. Cyber-Side Resilience

We explain how we model cyber network security attacks using a hierarchical game scheme for resilience assessment.

A. Defense vs. Attacker Modeling

Generally, every cyber attack path consists of an escalating series of vulnerability exploitations by the adversary. The adversary initially has no access to the control network and then achieves the privilege required to reach his or her malicious goals, e.g., causing a power transmission line outage by opening the corresponding relay. In particular, a state is defined

as the compromised privilege domains in that state. Therefore, the initial state is $(\varnothing)$, in which the attacker does not yet have any privileges over the power network. Each adversarial state transition represents a privilege escalation which is achieved through a vulnerability exploitation.

Reciprocal interaction between the adversary and system operator or automated response engine is a game in which each player tries to maximize his or her own benefit. Formally, the response selection process by system operators is modeled as a sequential Stackelberg stochastic game [18] in which the operator acts as the *leader* while the attacker is the *follower*; however, in our infinite-horizon game model, their roles may change without affecting the final solution to the problem.

More specifically, the game is a finite set of security states $\mathcal{A}$ that cover all possible security conditions that the system could be in. The system is in one of the security states s at each time instant. From the system's current state, the operator, i.e., the leader, chooses and takes a response action $a_r \in \mathcal{A}$ admissible in s, which leads to a security state transition to s'. The attacker, which is the follower, observes the action selected by the leader, and then chooses and takes an adversarial action $a_a \in \mathcal{A}$ admissible in s', resulting in a state transition to s''. At each transition stage, players may receive some reward according to the reward function for each player at the destination state. The reward function value for the operator is defined as the security measure of the corresponding state. On the other hand, the reward function for an attacker is usually not known accurately, because an attacker's reward depends on his final malicious goal, which is also not always known. Therefore, assuming that the attacker takes the worst possible adversarial action, the response actions are chosen based on a security strategy called *maximin* (discussed later). It is also important to note here that although S is a finite set, it is possible for the game to revert back to some previous state; therefore, the operator-adversary game can theoretically continue forever. This stochastic game is essentially an antagonistic multi-controller Markov decision process, called a *competitive Markov decision process (CMDP)* [19].

Formally, a discrete competitive Markovian decision process Γ is defined as a tuple $(\mathcal{S},\mathcal{A},Res(.),P,\gamma)$ where $\mathcal{S}$ is the security state space, assumed to be an arbitrary non-empty set endowed with the discrete topology. A is the set of actions, which itself is partitioned into response actions and adversarial actions depending on the player. For every $s \in \mathcal{S}$, $\mathcal{A}(s) \subset \mathcal{A}$ is the set of admissible actions at state s. The measurable function $Sec : \mathcal{S} \to [0,1]$ is the security measure calculated for each state, and P is the transition probability function; that is, if the present state of the system is $s \in S$ and an action $a \in \mathcal{A}(s)$ is taken, resulting in state transition to state s' with probability $P(s'|s,a)$, an immediate reward $Res(s')$, i.e., resilience measure value of the state s', is obtained by the player taking the action. γ is the discount factor and is normalized, i.e., $0 < \gamma < 1$.

B. Optimal response selection

We explain how we model the response action selection procedure by the defense mechanism. Our solution solves the generated CMDP to find the optimal action which maximizes the expected accumulative long-run reward measure received after a sequence of response and adversarial actions. Using the *infinite-horizon discounted cost* technique [20], the solution gives more weight to nearer future rewards by recursively adding up the immediate reward, i.e., resilience measure value $Res(.)$, and the discounted expected game value from then on.

To formulate, we compute the optimal policy π^* that associates with any belief state $b \in B$ an optimal action $\pi^*(b)$. Our solution formulates the response action selection procedure as a game-theoretic *maximin* problem. In particular, every policy π is assigned a value function V_π that associates every belief state $b \in B$ with an expected global reward $V_\pi(b)$ obtained by applying π in b. For finite-horizon POMDPs, the optimal value function is piecewise-linear and convex [21], and it can be represented as a finite set of vectors. In the infinite-horizon formulation, a finite vector set can closely approximate the optimal value function V^*, whose shape remains convex. Bellman's optimality equation (Equation (11)) characterizes the unique optimal value function V^*, from which an optimal policy π^* can be easily derived:

$$V^*(b) = \max_{a_r \in A(b)} \Psi(V^*, b, a_r), \tag{11}$$

where Ψ denotes the value function given that a specific response action is taken:

$$\Psi(V^*,b,a) = \rho(b'_{b,a}) + \sqrt{\gamma} \cdot \min_{a_a \in A(b'_{b,a})} [\rho(b''_{b',a_a}) + \sqrt{\gamma} \cdot V(b''_{b',a_a})]\}, \tag{12}$$

in which $b'_{b,a}$ denotes the updated next belief state if the current state is b and action a is taken:

$$b'_{b,a}(s') = \sum_{s \in \mathcal{S}} [P(s'|s,a).b(s)], \tag{13}$$

and the ρ function computes security measure values for belief states using security levels of individual states:

$$\rho(b) = \sum_{s \in \mathcal{S}} [b(s) \cdot Res(s)]. \tag{14}$$

Briefly, to calculate V^* numerically, our solution uses the value iteration algorithm [22] that applies dynamic programming iterative updates to gradually improve on the value until it converges to the ε-optimal value function [22], i.e. $| V_t(b) - V_{t-1}(b) | < \varepsilon$. Through improvement of the value, the policy is implicitly improved as well. Once the partially observable decision process is formulated and the ε-optimal value function is calculated, the solution determines the optimal response strategy π^* at any given belief state by choosing the response action which maximizes V^*. The optimal policy π^* maps the system's current belief state b to a response action using the following equation:

$$\pi^*(b) = \arg \max_{a_r \in \mathcal{A}(b)} \Psi(V^*, b, a_r). \tag{15}$$

C. Automatic Cyber Model Generation

We discuss how one can generate the game-theoretic CMDP for the target control network given the network topology, access control policies and cyber-physical interconnections among cyber and physical components.

The control network's access control policies, such as firewall rulesets, are composed of rules about sources (IP/port addresses) that are either allowed or not allowed to reach a destination. Our implementation parses the rulesets and creates a binary network connectivity matrix that is a Cartesian product of host systems. The $[i, j]$ entry of the matrix takes on a true value if traffic from host h_i to host h_j is allowed, and a false value if it is not allowed. The connectivity matrix always includes an Internet node representing a group of hosts outside of the network where attackers are assumed to initially reside.

The implemented solution generates a comprehensive CMDP model of the control network that represents all *possible* attack paths. In particular, the generated CMDP by design, would address all system vulnerabilities including previously unknown exploitations. Additionally, the monotonicity property [23] is assumed; in other words, an attacker never backtracks, and hence does not need to relinquish privileges already gained.

To generate the CMDP model, our tool analyses the control network topology input to find out about the set of known system vulnerabilities and individual host computers, i.e., privilege domains. Given the set of system vulnerabilities, the connectivity matrix is updated accordingly to encode adversarial paths only. In particular, the tool automatically generates a CMDP by traversing the connectivity matrix and concurrently updating the CMDP. First, our solution creates the CMDP's initial state $(\varnothing)$ and starts the CMDP generation with the network's entry point (Internet) node in the connectivity matrix. Considering the connectivity matrix as a directed graph, the solution runs a depth-first search (DFS) on the graph. While DFS is recursively traversing the graph, it keeps track of the current state in the CMDP, i.e., the set of privileges already gained through the path traversed so far by DFS. When DFS meets a graph edge $[i, j]$ that crosses over privilege domains h_i to h_j, a state transition $a_a \in A$ in CMDP is created if the current state in CMDP does not include the privilege domain of the host to which the edge leads, i.e., h_j. The transition in CMDP is between the current state and the state that includes exactly the same privilege set as the current state plus the host h_j directed by the graph edge $[i, j]$. The CMDP's current state in the algorithm is then updated to the latter state, and the algorithm proceeds until no further updates to CMDP are possible according to the connectivity matrix.

In addition to the adversarial transitions, the above algorithm also updates the CMDP regarding possible response and recovery actions $a_r \in A$. In particular, host redundancies, specified by the control network topology input, help to create responsive state transitions. As a case point, consider that for a control network data historian server in the control network there exists a redundant hot spare server designated for intrusion tolerance purposes. To model such a proactive design, our solution creates a responsive state transition, denoting the *recover the historian server* action, from any state in which the historian server is compromised to states containing the same privileges except the historian server. At that point, the offline CMDP generation is complete, and by design, the CMDP includes all possible attack paths launching from remote (Internet) host systems against the network as well as response and recovery scenarios.

VII. Hybrid CPS Resilience Metric

Our cyber-physical resilience metric employs the individual resilience metrics for the physical plant (Section V) and the cyber network (Section VI) to evaluate the resilience of the whole cyber-physical platform against the malicious cyber-originated misbehaviors.

Section V presented a resilience metric that considers only the physical components given the subset of compromised controllers regardless of how those controllers get compromised. The difficulty of compromising a specific subset of controllers heavily depends on the cyber network topology and its configuration and global access control policies. Section VI-A modeled this through the state-based CMDP model generation and analysis. The model can also be enhanced through cyber security intrusion detection sensor alerts (observable incidents), and treated as a hidden Markovian model (HMM) to estimate the current state of the under-attack cyber network given the last sequence of the triggered alerts[1].

On the other hand, although the cyber-side network modeling and analysis can assess the difficulty of compromising any subset of controllers through cyber attack paths, it lacks the information regarding the impact of those compromised controllers on the resilience of the physical plant, which is measured by the resilience metric discussed in Section V. Section VI assumed the impact measure given as the function $Res : S \rightarrow \mathcal{R}$.

In particular, the impact of the compromised controllers on the physical plant is measured by the recovery cost U formulated in Equation 7. Therefore, through the following assignment, our framework's cyber-physical resilience metric considers both cyber and physical topologies:

$$Res(s) \leftarrow -U_s, \tag{16}$$

where U_s denotes the recovery cost of the physical system for the case, where the subset of the controllers defined by $s \in S$ (in CMDP) have been compromised. Using the abovementioned assignment, the cyber-based response system can leverage the measured impact of the compromised controllers defined by the CMDP's state notion (defined in Section VI-C; shown on Figure 1).

As a result, our framework can measure the resilience metric *Res* for individual states of the generated CMDP model $s_i \in S$ by computing the physical system metric U_{s_i} for each state. It is possible that, in the CMDP state s_i, none of the controllers may be compromised yet, because the adversary has not penetrated into the cyber control network sufficiently deeply. For instance, in Figure 1, the CMDP state $s_3 = \{D, E\}$ does not include a compromised controller, whereas, one of its subsequent states $s_5 = \{D, E, A\}$ includes a compromised

[1]Such a cyber security state estimation can be accomplished using conventional HMM techniques (e.g., Viterbi-based most likely path determination) and is outside of the scope of our paper.

controller A. The state transition $s_3 \rightarrow s_5$ requires compromising a software vulnerability in controller A by the adversary, whereas the state transition $s_5 \rightarrow s_3$[2] requires recovery of the compromised controller A through restoring its clean state by the response system.

For the CMDP states s with no compromised controllers, our solution assigns $Res(s) \leftarrow 0$. For the states with a nonempty subset of compromised controllers, we use Equation 16 to calculate the resilience measure for the state. Once, the *Res* function are evaluated for all the states, our solution will implement the value iteration procedures to calculate the optimal value function $V : S \rightarrow \mathcal{R}$ using Equation 11. Once the value iteration converges, the calculated values for individual CMDP model states represent the cyber-physical resilience metric for individual states:

$$CPR(s) = V^*(s) \;\; \forall s \in S. \tag{17}$$

The evaluated cyber-physical resilience metric $CPR(s)$ involves *i)* the difficulty of the cyber attack paths starting from the current state s to gain control over any subset of the controllers with actuation power on the physical plant, and *ii)* the ultimate impact of the those attacks (if the path is successfully traversed) on the physical plant's resilience (i.e., whether the physical system's safe state can be recovered, and if so, what the recovery cost would be).

VIII. Evaluation

In this section, we discuss the implementation and present experimental evaluation results. All our experiments were performed on a 32-bit system with an Intel Core 2 2.16 GHz CPU, 3.00 GB of memory, and the Windows 7 Professional operating system.

A. Cyber Resilience

Implementations. A unified XML [24] format was used to describe the power system control network topology and network access policy rules (e.g., firewall rules). During the offline phase, we use the NetAPT tool [25] to perform a comprehensive security analysis of the access policy rules and to produce the network connectivity matrix according to the control network topology input. The matrix is later translated to the corresponding CMDP model. On the power side, we used PowerWorld Simulator [26] to simulate the underlying system. In particular, we used the SimAuto toolbox to set up a real-time connection to PowerWorld.

In our experiments, we evaluated the solution on a simulated power grid infrastructure [4]. The control network models were built based on topology of a real power control network. Figure 2 shows the topology of a single control network that has 59 nodes, e.g., host systems and firewalls. The first control network monitors and controls buses $1-12$ in the power system, and the second network monitors and controls buses $13-24$. In particular, each power bus is monitored and controlled by a single host system in the corresponding control

[2]For presentation simplicity, the response and recovery transitions are not shown in Figure 1, but are discussed in Section VI-A.

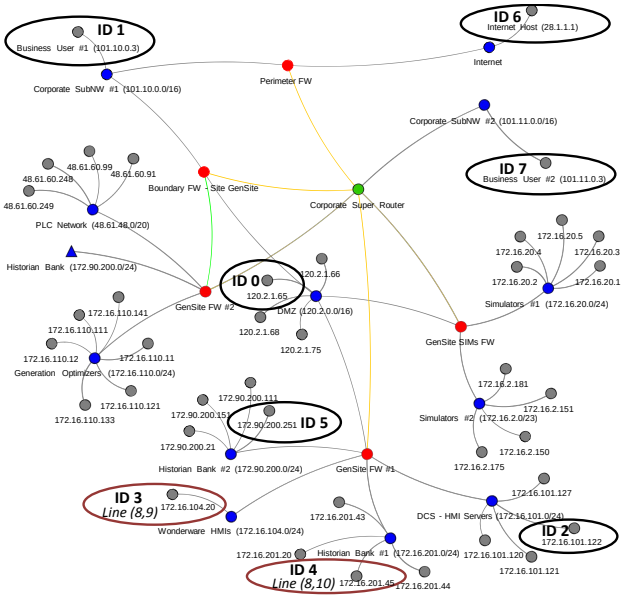


Fig. 2: Experimental Power Grid Testbed Architecture

network. Gray nodes show host systems; blue nodes are local network routers; red nodes represent firewalls; and the green node illustrates the organizational major router.

Model generation. Given the network topology and the access policy rules, i.e., about 100 firewall rules, the engine constructed the network connectivity matrix and generated the corresponding CMDP model. It is noteworthy that because the CMDP models may not be scalable specially for large-scale power-grid infrastructures, we use the envelope algorithm [27], where the CMDP is generated partially, and hence, not every individual state needs to enumerated and analyzed. More technically, given the current system state, only reachable states up to some finite horizon are explored and used for the contingency analysis. Figure 3 illustrates a simplified version of the generated CMDP in which states with incidents that are exclusively cyber are drawn in white, while states with physical consequences are in gray. The first number on each state represents its ID. Table I maps each state ID to the IDs of the compromised assets in each state.

As shown on the generated CMDP, the attacker initially resides remotely in the Internet with no privilege on the power network (CMDP's state 0) and can then traverse different attack paths to access a particular host in the power network. Each CMDP edge represents an access (i.e., possibly a vulnerability exploitation) allowed from a source to a destination host in the power network.

Metrics. In our experiments, we pessimistically assumed that all the hosts include security vulnerabilities in order to perform a worst case performance analysis. We calculated the resilience measure for individual states in the generated CMDP (i.e., shown as second and third number on each state in Figure 3, respectively). In a CMDP, there are usually many states with an identical set of physical contingencies that result in equal performance index values. To accelerate the metric calculation and minimize the number of connections to and calculations by PowerWorld, which is a time-consuming step

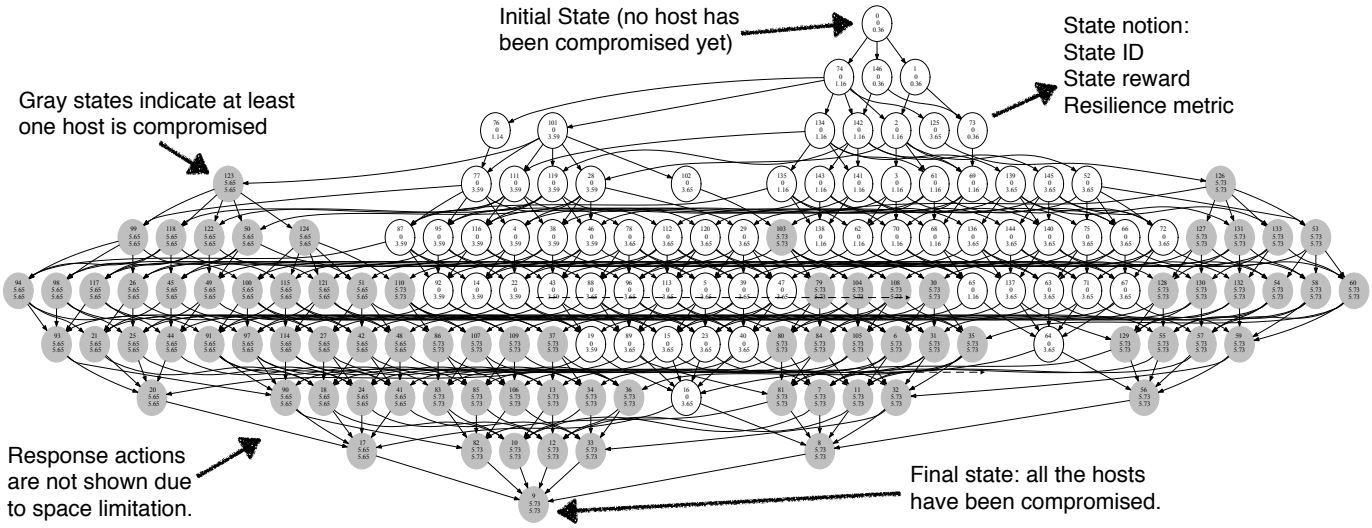


Fig. 3: Automatically Generated Model of the Power Grid for the Game-Theoretic Intrusion Resilience

TABLE I: Mappings between CMDP State IDs (Figure 3) and Compromised Asset IDs

State	Assets	State	Assets	State	Assets	State	Assets	State	Assets	State	Assets	State	Assets	State	Assets	State	Assets
0	6	1	61	2	610	3	6102	4	61023	5	610234	6	6102349	7	61023495	8	610234957
9	6102349578	10	610234958	11	61023497	12	610234978	13	61023498	14	610235	15	6102354	16	61023547	17	610235478
18	61023548	19	6102357	20	61023578	21	6102358	22	610237	23	6102374	24	61023748	25	6102378	26	610238
27	6102384	28	6103	29	61034	30	610349	31	6103495	32	61034957	33	610349578	34	61034958	35	6103497
36	61034978	37	6103498	38	61035	39	610354	40	6103547	41	61035478	42	6103548	43	610357	44	6103578
45	610358	46	61037	47	610374	48	6103748	49	610378	50	61038	51	610384	52	6104	53	61049
54	610492	55	6104925	56	61049257	57	6104927	58	610495	59	6104957	60	610497	61	6105	62	61052
63	610524	64	6105247	65	610527	66	61054	67	610547	68	61057	69	6107	70	61072	71	610724
72	61074	73	617	74	60	75	61024	76	602	77	6023	78	60234	79	602349	80	6023495
81	60234957	82	602349578	83	60234958	84	6023497	85	60234978	86	6023498	87	60235	88	602354	89	6023547
90	60235478	91	6023548	92	602357	93	6023578	94	602358	95	60237	96	602374	97	6023748	98	602378
99	60238	100	602384	101	603	102	6034	103	60349	104	603495	105	6034957	106	60349578	107	6034958
108	603497	109	6034978	110	603498	111	6035	112	60354	113	603547	114	6035478	115	603548	116	60357
117	603578	118	60358	119	6037	120	60374	121	603748	122	60378	123	6038	124	60384	125	604
126	6049	127	60492	128	604925	129	6049257	130	604927	131	60495	132	604957	133	60497	134	605
135	6052	136	60524	137	605247	138	60527	139	6054	140	60547	141	6057	142	607	143	6072
144	60724	145	6074	146	67												

due to the AC power flow solution procedures, the implementation uses a caching solution to calculate the performance index value for each physical contingency set only once.

Incident ranking. We implemented the resilience metric to rank various security incidents that could occur according to the system's current state and the generated CMDP model once the resilience indices are calculated for the power grid's corresponding CMDP model. Figure 4 shows the time requirement of the index calculations for system models with different sizes. Table II shows the ranked list of cyber-physical contingencies for each state in our case study power grid. It is important to mention that the reported results are for the case in which the attacker has not yet caused any contingency in the power grid, i.e., the current state is $s_0 = \varnothing$ with ID 0. As shown, the edge $s_0 - > s_{74}$ is ranked as the most critical contingency as it allows the attacker to get to the most impactful physical consequence with the least amount of cyber exploitation effort.

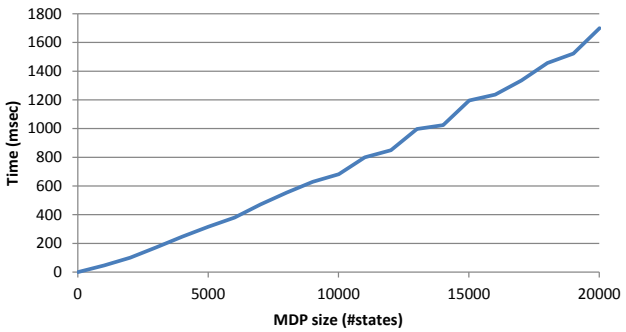


Fig. 4: Time Requirement for the Index Calculation

B. Physical Resilience

We evaluated our proposed resilience assessment metric through a numerical study using Matlab. Our study evaluated the resilience of the IEEE 57 bus power system test case [28] (Figure 5(a)) with linearized generator swing dynamics.

The states corresponded to the generator rotor angles. Since there are 7 generators in this system, the dimension of the state space is $N = 7$. In order to compute the state dynamics matrix A, we solved an optimal power flow problem to obtain an initial operating point using the Matpower utility [29]. This operating point is identical to the Matpower IEEE 57 bus test case, except with the load demands increased by 10% to create additional unstable modes (since stable linear systems are trivially resilient under our formulation). The generator dynamics were then computed by taking the Kron reduction of the admittance matrix to obtain an $N \times N$ admittance matrix Y, and then setting

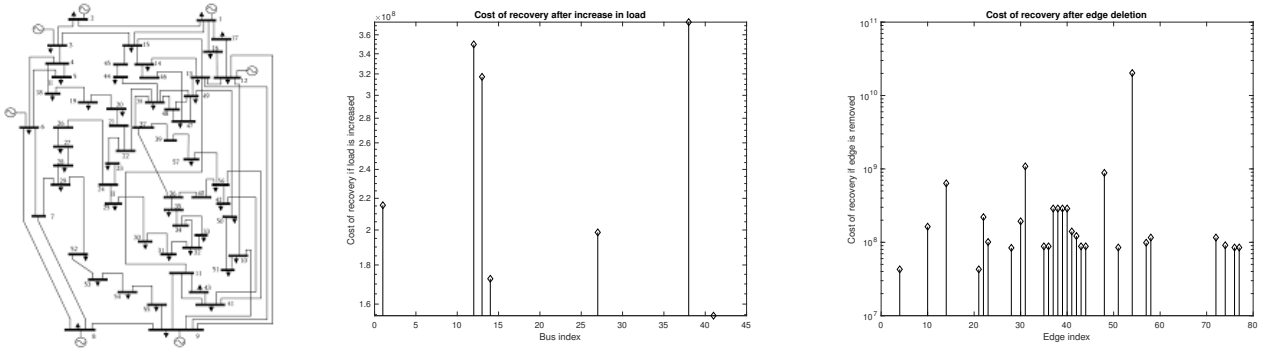
$$\dot{x}_i(t) = \sum_{j \neq i} Y_{ij} E_i E_j \cos(\theta_i - \theta_j)(x_j - x_i),$$

TABLE II: Ranked (R) List of Security Incidents (CMDP edges) using the Resilience Metric

R	Edge	R	Edge	R	Edge	R	Edge	R	Edge	R	Edge	R	Edge	R	Edge	R	Edge	R	Edge
0	0,74	1	0,1	2	0,146	3	74,125	4	74,101	5	74,2	6	74,134	7	74,142	8	74,76	9	1,2
10	1,73	11	146,142	12	146,73	13	125,126	14	101,123	15	101,102	16	101,111	17	101,119	18	101,28	19	101,77
20	2,52	21	2,28	22	2,3	23	2,61	24	2,69	25	134,139	26	134,111	27	134,61	28	134,135	29	134,141
30	142,145	31	142,119	32	142,69	33	142,143	34	142,141	35	76,77	36	73,69	37	126,53	38	126,127	39	126,103
40	126,131	41	126,133	42	123,99	43	123,124	44	123,118	45	123,122	46	123,50	47	102,103	48	111,118	49	111,112
50	111,116	51	111,38	52	111,87	53	119,122	54	119,120	55	119,46	56	119,116	57	119,95	58	28,50	59	28,29
60	28,38	61	28,46	62	28,4	63	77,99	64	77,78	65	77,95	66	77,4	67	77,87	68	52,53	69	52,75
70	52,29	71	52,66	72	52,72	73	3,75	74	3,4	75	3,62	76	3,70	77	61,66	78	61,38	79	61,62
80	61,68	81	69,72	82	69,46	83	69,70	84	69,68	85	139,131	86	139,66	87	139,136	88	139,112	89	139,140
90	135,136	91	135,87	92	135,62	93	135,138	94	141,140	95	141,116	96	141,68	97	141,138	98	145,133	99	145,72
100	145,144	101	145,120	102	145,140	103	143,144	104	143,95	105	143,70	106	143,138	107	53,54	108	53,30	109	53,58
110	53,60	111	127,79	112	127,54	113	127,128	114	127,130	115	103,79	116	103,104	117	103,108	118	103,30	119	103,110
120	131,58	121	131,128	122	131,104	123	131,132	124	133,60	125	133,130	126	133,108	127	133,132	128	99,100	129	99,94
130	99,98	131	99,26	132	124,110	133	124,100	134	124,115	135	124,121	136	124,51	137	118,94	138	118,115	139	118,117
140	118,45	141	122,98	142	122,121	143	122,117	144	122,49	145	50,26	146	50,51	147	50,45	148	50,49	149	112,104
150	112,115	151	112,113	152	112,39	153	112,88	154	116,117	155	116,113	156	116,43	157	116,92	158	38,45	159	38,39
160	38,43	161	38,14	162	87,94	163	87,88	164	87,14	165	87,92	166	120,108	167	120,121	168	120,113	169	120,47
170	120,96	171	46,49	172	46,47	173	46,43	174	46,22	175	95,98	176	95,96	177	95,92	178	95,22	179	29,30
180	29,51	181	29,39	182	29,47	183	29,5	184	4,26	185	4,5	186	4,22	187	4,14	188	78,79	189	78,100
190	78,96	191	78,5	192	78,88	193	75,54	194	75,5	195	75,63	196	75,71	197	66,58	198	66,63	199	66,39
200	66,67	201	72,60	202	72,71	203	72,47	204	72,67	205	62,63	206	62,14	207	62,65	208	70,71	209	70,22
210	70,65	211	68,67	212	68,43	213	68,65	214	136,128	215	136,63	216	136,88	217	136,137	218	140,132	219	140,137
220	140,113	221	140,67	222	138,137	223	138,92	224	138,65	225	144,130	226	144,71	227	144,96	228	144,137	229	54,6
230	54,55	231	54,57	232	30,6	233	30,31	234	30,35	235	30,37	236	58,55	237	58,31	238	58,59	239	60,57
240	60,35	241	60,59	242	79,80	243	79,84	244	79,6	245	79,86	246	128,55	247	128,80	248	128,129	249	130,57
250	130,84	251	130,129	252	104,80	253	104,105	254	104,31	255	104,107	256	108,35	257	108,84	258	108,105	259	108,109
260	110,86	261	110,107	262	110,109	263	110,37	264	132,59	265	132,129	266	132,105	267	100,86	268	100,91	269	100,97
270	100,27	271	94,91	272	94,93	273	94,21	274	98,97	275	98,93	276	98,25	277	26,27	278	26,21	279	26,25
280	115,107	281	115,114	282	115,42	283	115,91	284	121,109	285	121,114	286	121,48	287	121,97	288	51,37	289	51,27
290	51,42	291	51,48	292	117,93	293	117,114	294	117,44	295	45,21	296	45,42	297	45,44	298	49,25	299	49,48
300	49,44	301	113,105	302	113,114	303	113,40	304	113,89	305	39,31	306	39,42	307	39,40	308	39,15	309	88,80
310	88,91	311	88,15	312	88,89	313	43,44	314	43,40	315	43,19	316	92,93	317	92,89	318	92,19	319	14,21
320	14,15	321	14,19	322	47,35	323	47,48	324	47,40	325	47,23	326	96,84	327	96,97	328	96,23	329	96,89
330	22,25	331	22,23	332	22,19	333	5,6	334	5,27	335	5,23	336	5,15	337	63,55	338	63,15	339	63,64
340	71,57	341	71,23	342	71,64	343	67,59	344	67,40	345	67,64	346	65,64	347	65,19	348	137,129	349	137,89
350	137,64	351	6,7	352	6,11	353	6,13	354	55,7	355	55,56	356	57,11	357	57,56	358	31,7	359	31,32
360	31,34	361	35,11	362	35,32	363	35,36	364	37,13	365	37,34	366	37,36	367	59,56	368	59,32	369	80,81
370	80,7	371	80,83	372	84,11	373	84,81	374	84,85	375	86,83	376	86,85	377	86,13	378	129,56	379	129,81
380	105,32	381	105,81	382	105,106	383	107,83	384	107,106	385	107,34	386	109,85	387	109,106	388	109,36	389	91,83
390	91,18	391	91,90	392	97,85	393	97,24	394	97,90	395	27,13	396	27,18	397	27,24	398	93,90	399	93,20
400	21,18	401	21,20	402	25,24	403	25,20	404	114,106	405	114,41	406	114,90	407	42,34	408	42,41	409	42,18
410	48,36	411	48,41	412	48,24	413	44,20	414	44,41	415	40,32	416	40,41	417	40,16	418	89,81	419	89,90
420	89,16	421	15,7	422	15,18	423	15,16	424	19,20	425	19,16	426	23,11	427	23,24	428	23,16	429	64,56
430	64,16	431	7,8	432	7,10	433	11,8	434	11,12	435	13,10	436	13,12	437	56,8	438	32,8	439	32,33
440	34,10	441	34,33	442	36,12	443	36,33	444	81,8	445	81,82	446	83,82	447	83,10	448	85,82	449	85,12
450	106,82	451	106,33	452	18,10	453	18,17	454	90,82	455	90,17	456	24,12	457	24,17	458	20,17	459	41,33
460	41,17	461	16,8	462	16,17	463	8,9	464	10,9	465	12,9	466	33,9	467	82,9	468	17,9		

TABLE III: Evaluation of resilience metric for each possible set of compromised controllers.

Set S	**Cost**	**Set** S	**Cost**	**Set** S	**Cost**	**Set** S	**Cost**
$\emptyset$		$\{1\}$	2.72×10^7	$\{2\}$	3.01×10^7	$\{3\}$	8×10^7
$\{4\}$	1.42×10^8	$\{5\}$	1.04×10^8	$\{6\}$	2.42×10^7	$\{7\}$	2.40×10^7
$\{1,2\}$	3.58×10^7	$\{1,3\}$	1.23×10^8	$\{1,4\}$	1.39×10^8	$\{1,5\}$	1.40×10^8
$\{1,6\}$	2.75×10^7	$\{1,7\}$	2.72×10^7	$\{2,3\}$	2.10×10^8	$\{2,4\}$	1.69×10^8
$\{2,5\}$	∞	$\{2,6\}$	3.09×10^7	$\{2,7\}$	3.01×10^7	$\{3,4\}$	7.99×10^7
$\{3,5\}$	2.02×10^8	$\{3,6\}$	1.06×10^8	$\{3,7\}$	7.99×10^7	$\{4,5\}$	∞
$\{4,6\}$	3.31×10^8	$\{4,7\}$	∞	$\{5,6\}$	2.88×10^8	$\{5,7\}$	1.35×10^{10}
$\{6,7\}$	2.42×10^7						



(a) (b) (c)

Fig. 5: Numerical evaluation of proposed resilience assessment framework. (a) IEEE 57 bus network used in the numerical study. The network contains 7 generators and 80 transmission lines. (b) Effect of variations in load at the given bus on the system resilience to compromise of any single generator. The cost of recovery fluctuates as the load increases. (c) Effect of removing transmission lines on the system resilience. The impact on resilience varies between transmission lines, and in some cases causes the unstable modes to become uncontrollable, thus violating the definition of resilience.

where E_i and E_j are the excitations of generators i and j, and θ_i and θ_j are the rotor angles at the power flow solution. The control matrix B was modeled as the $N \times N$ identity matrix.

We first computed the recovery cost for this system, for each set of compromised generators S, using the matrices $Q = R = I$. The results are summarized in Table III. We observe that the cost of recovery is monotonically increasing in the set of compromised controllers, i.e., if $S \subseteq S'$ then the cost of recovery from compromise of S' exceeds the cost of recovery from S.

The resilience of the system also depends on the power system operating conditions. We analyzed two of those factors, namely, the amount of system load and the system topology. The impact of changing the system load on the worst-case cost of recovery from compromising any single generator is shown in Figure 5(b). In this figure, the load at the bus with given index is doubled and the change in resilience is observed. Increasing the load had little impact on the resilience. On the other hand, deleting edges from the network topology resulted in a large increase in the recovery cost, with significant variation between edges, in some cases causing the system to become non-resilient.

IX. Conclusions

We presented a formal definition of cyber-physical resilience, and a metric to quantify the resilience level of a given cyber-physical system. Our metric leverages the conceptual ideas from the resilience terminology used in material science, and considers the resilience in both cyber and physical components as well as their interdependencies. Our proposed metric uses discrete stochastic models (competitive Markov decision processes) to encode the dynamics and interdependencies of the cyber network along with the dynamical linear system models to capture the continuous dynamics of the underlying physical processes. We implemented a prototype of the proposed metric for case study systems, and demonstrate its capabilities for joint consideration of the cyber and physical incidents.

Acknowledgement

We would like to thank National Science Foundation (NSF) Cyber-Physical Systems program (CNS 1446471 and 1453046). Additionally, this material is partially based upon work supported by the Depart- ment of Energy under Award Number DE-OE0000780.

References

[1] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5:6, 2011.

[2] Rafiullah Khan, Peter Maynard, Kieran McLaughlin, David Laverty, and Sakir Sezer. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. 2016.

[3] Jonathan Butts and Michael Glover. How industrial control system security training is falling short. In *International Conference on Critical Infrastructure Protection*, pages 135–149. Springer, 2015.

[4] Saman Zonouz, Charles M Davis, Katherine R Davis, Robin Berthier, Rakesh B Bobba, and William H Sanders. Socca: A security-oriented cyber-physical contingency analysis in power infrastructures. *IEEE Transactions on Smart Grid*, 5(1):3–13, 2014.

[5] Liang Che and Mohammad Shahidehpour. Dc microgrids: Economic operation and enhancement of resilience by hierarchical control. *IEEE Transactions on Smart Grid*, 5(5):2517–2526, 2014.

[6] Saman Zonouz, Katherine M Rogers, Robin Berthier, Rakesh B Bobba, William H Sanders, and Thomas J Overbye. SCPSE: Security-Oriented Cyber-Physical State Estimation for Power Grid Critical Infrastructures. *IEEE Transactions on Smart Grid*, 2012.

[7] Shamina Hossain-McKenzie, Sriharsha Etigowni, Katherine Davis, and Saman Zonouz. Augmented dc power flow method with real-time measurements. In *Power Systems Computation Conference (PSCC)*, pages 1–7. IEEE, 2016.

[8] Saman Zonouz, Julian Rrushi, and Stephen McLaughlin. Automated plc code analytics for detection of industrial control malware. *IEEE Security and Privacy Magazine*, 2014.

[9] Gabriel Salles-Loustau, Vidyasagar Sadha, Dario Pompili, and Saman Zonouz. Secure mobile technologies for proactive critical infrastructure situational awareness. In *IEEE Symposium on Technologies for Homeland Security (HST)*, 2016.

[10] Saman Zonouz, Himanshu Khurana, William Sanders, and Timothy Yardley. Rre: A game-theoretic intrusion response and recovery engine. *IEEE Transactions on Parallel and Distributed Systems*, 25(2):395–406, 2014.

[11] Saman Zonouz, Amir Houmansadr, and Parisa Haghani. Elimet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior. In *Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 1–12, 2012.

[12] Dimitris Bertsimas, Ebrahim Nasrabadi, and Sebastian Stiller. Robust and adaptive network flows. *Operations Research*, 61(5):1218–1242, 2013.

[13] Daniel Bienstock and Abhinav Verma. The nk problem in power grids: New models, formulations, and numerical experiments. *SIAM Journal on Optimization*, 20(5):2352–2380, 2010.

[14] Javier Salmeron, Kevin Wood, and Ross Baldick. Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems*, 24(1):96–104, 2009.

[15] Martin Roesch et al. Snort: Lightweight intrusion detection for networks. In *LISA*, volume 99, pages 229–238, 1999.

[16] T. Guler, G. Gross, and Minghai Liu. Generalized line outage distribution factors. *Power Systems, IEEE Transactions on*, 22(2):879–881, May 2007.

[17] Vasileios Tzoumas, Ali Jadbabaie, and George J Pappas. Minimal reachability problems. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 4220–4225. IEEE, 2015.

[18] G. Owen. *Game Theory*. Academic Press, 1995.

[19] Jerzy Filar and Koos Vrieze. *Competitive Markov decision processes*. Springer Science & Business Media, 2012.

[20] L. Kaelbling, M. Littman, and A. Cassandra. Partially observable Markov decision processes for artificial intelligence. *Proceedings of the German Conference on Artificial Intelligence: Advances in Artificial Intelligence*, 981:1–17, 1995.

[21] E. Sondik. *The optimal control of partially observable Markov processes*. PhD thesis, Stanford University, 1971.

[22] R. Bellman. *Dynamic Programming*. Princeton University Press, 1957; republished 2003.

[23] Paul Ammann, Duminda Wijesekera, and Saket Kaushik. Scalable, graph-based network vulnerability analysis. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS)*, pages 217–224, 2002.

[24] *Xml: The Complete Reference*. Osborne, 2001.

[25] D. M. Nicol, W. H. Sanders, S. Singh, and M. Seri. Usable global network access policy for process control systems. *IEEE Security and Privacy*, 6:30–36, 2008.

[26] J.D. Glover, M.S. Sarma, T.J. Overbye, and T.J. Overbye. *Power system analysis and design*. Thomson, 2008.

[27] T. Dean, L. Kaelbling, J. Kirman, and A. Nicholson. Planning under time constraints in stochastic domains. *Artificial Intelligence*, 76:35–74, July 1995.

[28] IEEE 57 bus test case. https://www2.ee.washington.edu/research/pstca, 2017.

[29] Ray Daniel Zimmerman, Carlos Edmundo Murillo-Sánchez, and Robert John Thomas. Matpower: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on power systems*, 26(1):12–19, 2011.