Towards Cyber-Physical Intrusion Tolerance

Shamina Hossain, Sriharsha Etigowni*, Kate Davis, Saman Zonouz*
Electrical and Computer Engineering Department
University of Illinois, *Rutgers University
{*shossai2, krogers6*}*@illinois.edu*, {*se260, saman.zonouz*}*@rutgers.edu*

***Abstract*—While cyber-physical systems are widely deployed and known to be difficult to analyze due to their increasing complexity, the number of sophisticated attacks against them have been constantly growing. This necessitates semi-automated intrusion response and recovery capabilities for timely termination of ongoing attacks and effective recovery of the infrastructural normal and safe operations. In this paper, we present CPR, a cyber-physical response system to protect power grid critical infrastructures, and discuss major challenges in theoretical formulation and practical deployment of fully-automated tolerance capabilities in settings where continuous physical dynamics continuously interact with cyber-side discrete computation logic. Our evaluation results show that CPR leverages its hybrid cyber-physical formulation, and efficiently selects optimal joint response strategies in both physical and cyber networks.**

I. Introduction

The increasing pace and complexity of the recent sophisticated attacks against cyber-physical infrastructures necessitates not only efficient intrusion detection systems for orchestrated networks of computational procedures and physical processes but also efficient automated intrusion tolerance mechanisms. In particular, intrusion tolerance mechanisms obtain the current security state of the network/system from various security event management systems and decide upon and take appropriate (so-called optimal) response and recovery actions to respond to ongoing attacks and recover the system back to its normal and secure operational mode.

A *cyber-physical* intrusion tolerance solution needs to own three main properties (Figure 1): *i)* it has to leverage state information from both cyber and physical components, such as the set of compromised human machine interface (HMI) servers in the power control center along with the set of physical consequences already cause by the attackers, e.g., a maliciously opened circuit breaker and damaged power generator; *ii)* the engine has to select the best response strategy considering both ends of the system; This requires modeling the cyber side control network security and potential penetration/response scenarios, modeling the power system electrical response and dynamics, and modeling the potential safety-oriented recovery scenarios (e.g., optimal resource and network redispatch/reconfiguration to compensate for a failed generator); and *iii)* the tolerance framework will need distributed response and recovery actuation agents deployed in cyber and power networks such that the selection response and recovery strategies could be carried out. The actuation agents could include cyber network firewalls for rule reconfiguration and host-based management tools to delete/kill a malicious file/process as well as power automatic generation control (AGC) and relays.

While there is very little past work on cyber-physical intrusion tolerance, there have been efforts to address the purely-cyber intrusion tolerance problems from theoretical and practical angles; however, they fall short in the following aspects. The past theoretical cyber intrusion response formulations (e.g., using game-theoretic [1] and machine learning [2]) miss the system-specific details, and sometimes are based on unrealistic assumptions. Hence, their outcomes risk being too generic with very limited practical deployments. Existing practical endeavors [3] to tackle the purely-cyber intrusion tolerance problem have two major shortcomings. First, their maintenance requires a lot of manual efforts by the administrators to ensure they are updated regarding the target networks real-time configuration changes. Second, they are too system-specific and hence cannot be simply applied to various networks with different setting details and high-level business models and objectives.

Threat model. We will concentrate on cyber-originated attacks against cyber-physical platforms that can lead to physical consequences. More specifically, the adversaries launch their attacks through penetration into a cyber-side component[1], e.g., a host computer within the control center, and traverse a single- or multiple-step attack path. The attacker *will* decide to cause physical power contingencies such as a malicious transformer tap ratio change *with or without* an ultimate malicious objective, e.g., to cause transient instability in the power system. Consequently, our threat model covers neither physical attacks (e.g., adversarial physically breaking into a power substation) nor purely-cyber attacks where the adversary does not cause any physical consequence and only targets traditional cyber network security compromises such as a confidential database disclosure through cyber-based vulnerability exploitations only.

Overview. We present a cyber-physical response and recovery engine CPR that acts as a thin shim layer between the cyber and physical layers of the power grid infrastructure (Figure 1). This creates a minimal trusted computing base (TCB) [5] that minimizes the attack surface exposed to adversaries to subvert the deployed protections. The proposed solution obtains the current cyber-physical security state of the infrastructure through both cyber intrusion detector, e.g., anti-viruses, and power system sensors, e.g., current transformers[2]. Next, the engine will have to make decisions on optimal response and recovery strategies, i.e., sequence of actions, in both cyber and power system networks considering the potential impacts of the action on both ends. We define the optimality criterion to be the aggregated strategy cost before the systems secure operation mode is retrieved.

II. Cyber-Physical Intrusion Tolerance

Traditionally, purely-cyber intrusion tolerance solutions could be either model-based [7], [8] that take advantage of system models for their response strategy optimization, or model-free [9] 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

[1] Within the electronic security perimeter ESP (defined by NERC CIP [4]).

[2] The specifics of cyber-physical security state estimation is beyond the scope of this paper and interested reader is referred to SCPSE [6].

978-1-4673-8289-2/15/$31.00 ©2015 IEEE

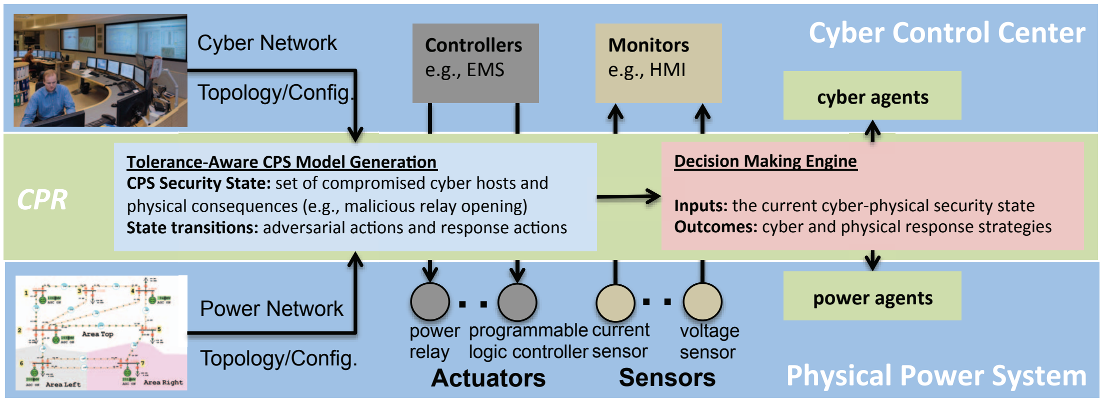

Cyber Network
Topology/Config.
Controllers
e.g., EMS
Monitors
e.g., HMI
Cyber Control Center
cyber agents
CPR
Tolerance-Aware CPS Model Generation
CPS Security State: set of compromised cyber hosts and physical consequences (e.g., malicious relay opening)
State transitions: adversarial actions and response actions
Decision Making Engine
Inputs: the current cyber-physical security state
Outcomes: cyber and physical response strategies
power agents
Power Network
Topology/Config.
Area Top
Area Left
Area Right
power relay
programmable logic controller
current sensor
voltage sensor
Actuators
Sensors
Physical Power System

Fig. 1: Cyber-Physical Intrusion Tolerance with Minimal Trusted Computing Base

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 [10]. It is noteworthy that similar cascading overload scenarios could be caused by an ill-designed intrusion tolerance 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 tolerance can potentially consider such complex failure and recovery scenarios.

A. Cyber-side vs. Power-side Intrusion Tolerance

Cyber-based tolerance 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. When responding to and recovering from intrusions, cyber- and power-based tolerance 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 tolerance 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 setpoint, 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 tolerance architecture makes use of both cyber and physical tolerance 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 tolerance 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 tolerance 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 tolerance 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 tolerance 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 power-side tolerance actions as opposed to pure reliance on cyber-side capabilities? *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 [11]. When cyber-only capabilities cannot fix the compromise, 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. 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 power system control? *i)* Pure reliance on power-side fault tolerance may be too costly and slow for practical deployments. Power-aware cyber-side tolerance 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 tolerance 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 tolerance mechanisms; otherwise, each time the power-side tolerance solution fixes a power-side attack consequence, e.g., re-closure of an opened circuit breaker, the attacker could immediately cause the same consequence again, because the power-side tolerance engine is not aware of the compromised set of cyber assets and can only take cyber-blind power-side 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 tolerance engine would have an increasingly difficult time finding any feasible recovery strategy against adversaries.

B. Control Theoretic Security Modeling

We model the reciprocal interaction between the adversary and CPR as a sequential Stackelberg stochastic game [12] where each player tries to maximize its benefit. CPR (attacker) acts as the *leader* (*follower*) [12]. The game is a finite set of *cyber-physical system security states* S where the state notion captures the set of compromised cyber hosts, e.g., HMI server, along with physical consequences, e.g., opened circuit breaker, caused by the attacker in that state. CPR chooses and takes a response action $m_s \in \mathcal{M}$ admissible in s, which leads to a security state transition to s'. The attacker observes the action selected by the leader, and then chooses and takes an adversary action $o_{s'} \in O$ admissible in s', resulting in a state transition to s''. At each transition stage, players may receive some reward according to a reward function for each player. The reward function for an attacker is usually not known to CPR, because an attacker's reward depends on his final malicious goal, which is also not known; therefore, assuming that the attacker takes the worst possible adversary action, CPR chooses its response actions based on the security strategy, i.e., *maximin*, as discussed later. Although S is a finite set, it is possible for the game to revert back to some previous state; therefore, the CPR-adversary game can theoretically continue forever. This stochastic game is essentially an antagonistic multicontroller Markov decision process, called a *competitive Markov decision process (CMDP)* [13]. A discrete CMDP Γ is defined as a tuple (S, A, r, P, γ) where S is the security state space, assumed to be an arbitrary non-empty set endowed with the discrete topology. A is set of actions, which itself is partitioned into response actions (in cyber and power components) and adversary actions, depending on the player. For every $s \in S$, $A(s) \subset A$ is the set of admissible actions at state s. The measurable function $r : K \to \Re$ is the reward where $K := \{(s,a,s')|a \in A(s); s,s' \in S\}$, and P is the transition probability function; that is, if the present state of the system is $s \in S$ and an action $a \in A(s)$ is taken, resulting in state transition to state s' with probability $P(s'|s,a)$, an immediate reward $r(s,a,s')$ is obtained by the player taking the action. γ is the discount factor, i.e., $0 < \gamma < 1$, which represents the difference in importance between future and present rewards. **What affects the response action set?** *i)* Degree of redundancy: In a cyber-physical power grid infrastructure, the amount of *possible* intrusion tolerance capabilities are heavily dependent on the degree of redundancy in the system, e.g., duplicate copies of particular sensitive system components. For instance, a malicious power generator or cyber-side application server outage could be restored through a secondary generation plant dispatch if such a plant is available, or respectively, if a secondary hot spare server is already deployed. Similarly, a malicious transmission line outage recovery may require closing circuit breakers to restore another parallel line (if available) for power flow redistribution; *ii)* Built-in topological flexibility: Given a cyber-physical platform, its built-in topological flexibility, regarding how reconfigurable the system is, could significantly improve the response action set cardinality, and hence the ultimate tolerance capability. For instance, on the power side, existing transmission-level topological flexibility can be realized through flexible energy routing. Options include coordinated FACTS device control (i.e., using Smart Wires [14]) and topology switching [15], where lines can be taken out or brought back in by the tolerance engine as needed. In general, DOE ARPA-E GENI program efforts [16] for a more flexible grid should be applied here. When constructing the response action set, we must consider that while a larger set of actions may theoretically lead to higher tolerance capabilities, it could significantly complicate the optimal solution strategy in practice. Hence, it is crucial to categorize possible actions and only employ the relevant subset in strategy optimization procedures for each system state. It is noteworthy that the existence of a larger action set for tolerance purposes also implies the existence of higher degrees of freedom for the adversaries. Hence, increased deployment of monitoring and protection solutions are warranted to combat increasing attack flexibility.

C. Optimal Response Strategy

The engine solves the CMDP for an optimal security response action from its action space, and sends an action command to its agents that are in charge of enforcing received commands. Action optimization in CPR is accomplished by trying to maximize the accumulative long-run reward measure received while taking sequential response actions. To accumulate sequential achieved rewards, here, we use the *infinite-horizon discounted cost* technique [17], which gives more weight to nearer future rewards. CMDP's solution π^* associates with each state an optimal response action. The Markovian decision process assigns to every policy π a value function V_π, which associates every state with an expected global reward obtained by applying π. For finite-horizon CMDPs, the optimal value function is piecewise-linear and convex [18], 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 equations (1) characterize in a compact way the unique optimal value function V^*, from which an optimal policy π^* can be easily derived:

$$V^*(b) = \max_{a_r \in A_r(b)} \Psi(V^*, b, a_r) \tag{1}$$

where $b \in B$ is a belief state each defined as a probability distribution (due to sensor alert uncertainties) over the system states S. $A(b) = \cup_{s \in S: b(s) \neq 0} A(s)$. $A(.)$ is partitioned into $A_r(.)$ and $A_a(.)$ for response and adversary actions, respectively. See Equation 2 for Ψ where ρ is the CMDP reward function:

$$\rho(b,a,b') = \sum_{s,s' \in S} b(s) b'(s') r(s,a,s'). \tag{3}$$

Here, $b'_{b,a,o}$ is the updated belief state if the current state is b, action a is taken, and observation o (that may indicate an adversary action if it is a true positive) is received from sensors:

$$\begin{aligned} b'_{b,a,o}(s') &= P(s'|b,a,o) \\ &= \frac{P(o|s') \sum_{s \in S} P(s'|s,a) b(s)}{\sum_{s'' \in S} P(o|s'') \sum_{s \in S} P(s''|s,a) b(s)}, \end{aligned} \tag{4}$$

where, due to the independence assumption among the alerts

$$P(o|s) = \prod_{l \in \mathcal{L}} (1_{[s_l=1]} \cdot P(o|l) + 1_{[s_l=0]} \cdot P(\bar{o}|l)). \tag{5}$$

CPR picks the optimal response via the value iteration [19]:

$$V_t(b) = \max_{a_r \in A_r(b)} \Psi(V_{t-1}, b, a_r), \tag{6}$$

that applies dynamic programming until the ε-optimal value is obtained, i.e., $| V_t(b) - V_{t-1}(b) | < \varepsilon$. Finally, optimal policy π^* maps the system's current belief state b to a response action:

$$\pi^*(b) = \arg \max_{a_r \in A_r(b)} \Psi(V^*, b, a_r), \tag{7}$$

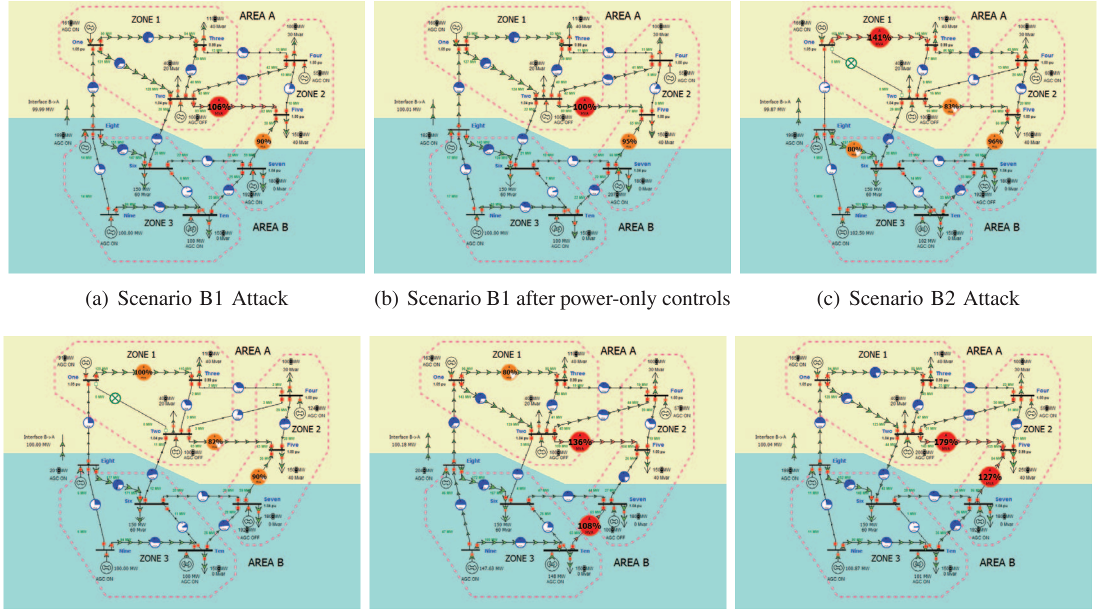
which is sent to response engine agents to carry out the selected response strategies.

III. Evaluations

We present a case study that illustrates a sample solution to cyber-physical intrusion tolerance in power systems using the optimal power flow (OPF). In power systems, OPF

$$\Psi(V,b,a) = \sum_{o\in O} P(o|b,a)\cdot\{\rho(b,a,b'_{b,a,o})+ \tag{2}$$

$$+\sqrt{\gamma}\cdot[\min_{a_a\in A_a(b'_{b,a,o})} \sum_{o'\in O} P(o'|b'_{b,a,o},a_a)\cdot(\rho(b'_{b,a,o},a_a,b''_{b',a_a,o'})+\sqrt{\gamma}\cdot V(b''_{b',a_a,o'}))]\}$$



(a) Scenario B1 Attack (b) Scenario B1 after power-only controls (c) Scenario B2 Attack

(d) Scenario B2: Power-Based Recovery (e) Scenario B3 Attack (f) Scenario B4 Attack

Fig. 2: Power Recovery Scenarios

	Power Attack Scenarios				
	B1	B2	B3	B4	B5
Solution Found	YES	YES	NO	NO	YES
Gen 1 MW	130	90.698	50	50	186.106
Gen 2 MW	**100**	**100**	**100**	**200**	50
Gen 4 MW	82.813	124.217	162.564	170.727	80
Gen 7 MW	**192.139**	**192.139**	**100**	169.003	192.139
Gen 8 MW	176.511	201.216	210	270	198.927
Gen 9 MW	100	100	141.654	150	100
Gen 10 MW	120.952	100	145.246	11.207	99.999
Line 1-2 Status	In	**Out**	In	In	In
Load 5 MW	150	150	150	**250**	150
Sol Time	0.016	0.016	0.015	0.01	0.011
Avg Bus MC	$22.23/MWh	$20.25/MWh			$19.91/MWh
Total Cost	$18662.57	$18913.82	-	-	$18563.81

TABLE I: Power-Based Intrusion Tolerance Strategies

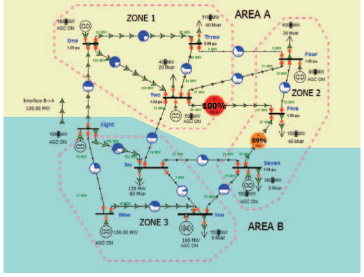


Fig. 3: Scenario B5 Attack

finds an optimal power dispatch that minimizes total cost f while meeting operating constraints; see the Federal Energy Regulatory Commission (FERC) [20]. The control variables typically include real power output of generators and as well as other controls such as parameters for voltage regulators, tap-changing transformers, phase-shifting transformers, switched capacitors and reactors, power electronics (HVDC, FACTS), and loads (demand response) [21]. The OPF's equality constraints are the power balance equations at each bus in the system. Its inequality constraints are the network operating limits, such as line flow capacities, generator real/reactive power output limits, and the maximum number of taps:

$$\begin{aligned} \min_{\mathbf{u}} \quad & f(\mathbf{x},\mathbf{u}) \\ \text{s.t.} \quad & P_i^g - P_i^l = \sum_k |V_i||V_k|(G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}) \\ & Q_i^g - Q_i^l = \sum_{k\in C} |V_i||V_k|(G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}) \\ & MVA_{ij} \le MVA_{ij}^{max} \\ & P_l^g \le P_l^{gmax} \\ & \forall i,j\in N,\ \forall l\in G,\ \forall k\in C \end{aligned} \tag{8}$$

where $\mathbf{u}$ denotes the controls (independent) variables; $\mathbf{x}$ represents dependent variables; V/θ denote the bus voltage magnitudes/angles. In our case-study, the controller of a generator is identified to be compromised (a malicious running process on its operating system), i.e., it could potentially drive the power system unsafe, e.g., unstable. CPR's two available cyber- and physical-side actions are the following. It can disable the controls for the generator and compensate by dispatching the other generators through OPF. The result is a minimal cost solution that observes our cyber constraints. Alternatively, if CPR can deploy the necessary cyber response actuation agents (e.g., to kill the malicious process on the controller), the system can be completely restored, and it will operate as normal. The costs of these actions (e.g., how long and how much effort they take to complete) are represented mathematically in CPR's overall Bellman optimization (Section II-B). We also note that the possibility to restore the system using the first option is limited; it breaks down at a certain point. A compromise could result in such severe physical consequences that the power system does not have enough built-in redundancy to compensate for it. Similarly, CPR's cyber-side recovery has limited capabilities on its own, e.g., it cannot recover a compromised controller if the adversary has root privileges. Consequently, power-aware cyber intrusion response and cyber-aware power reconfiguration capabilities complement each other, and both are essential to efficient restoration of cyber-physical system operations.

We implement our case-study using a 10-bus cyber-controlled power system with seven generators. The case is `B10Reserve.pwb`, a publicly available PowerWorld training case [22]. Table I shows a summary of the cases that CPR employed in PowerWorld to solve for optimal system recovery. Numbers in boldface on the table indicate malicious changes induced by an attacker. We considered four cyber-physical attack scenarios, **B1-4** (see below). In each scenario, the attacker compromised certain generator controllers and controllers of line circuit breakers, and these were marked as detected [3]. Rogue generator controllers maliciously changed their outputs and caused the adjacent transmission lines to be overloaded. CPR uses the remaining (non-compromised) system controls to adapt, compensate, and relieve the newly overloaded lines at least cost. In Scenarios B1 and B2, a generator redispatch suffices to fix the problem, although costs increase. In Scenarios B3 and B4, redispatch is not enough, and an acceptable system response would require additional cyber-side response and recovery controls. Scenario B5 is the system's optimal operation once cyber and power restorations have been completed.

Scenario B1: Generators (Gens) 2 and 7 are compromised. The output of Gen 2 has increased to 100 MW. This caused a line overload, but CPR redispatched the remaining controls in the system to resolve this violation, without Gens 2 and 7. See Table I for the resulting generator outputs for each scenario; **Scenario B2:** Like B1, Gens 2 and 7 are compromised, and Gen 2 output is 100 MW. Additionally, Line 1-2 has been opened. CPR was able to find a cost-optimal solution to redispatch and resolve these violations; **Scenario B3:** B3 is the same as B1, except that Gen 7's output was also maliciously set to 100 MW. CPR's power-only controls did not suffice to recover the system as no dispatch was found to satisfy the power balance equations and relieve the line overloads. The OPF solution has one unenforceable line constraint, which makes the resulting system cost and bus marginal costs invalid. CPR's cyber-side controls, coupled with its available power controls in an optimized and coordinated manner, offer a solution through cyber-side recovery of the Gen 7 controller, converting this scenario to be identical to B1; **Scenario B4:** In B4, Gen 2 is compromised and set to 200 MW. The attacker also manipulates the residential loads at bus 5 where he turns on many air conditioners at once leading to a sudden load increase to 250 MW. As in B3, no dispatch can be found to relieve the system, and there are two unenforceable line constraints. To facilitate the automated response, one could add "load shedding" to CPR's response action set. The point we emphasize here is that after a certain level of attacks, any response action set will no longer be enough to restore the system. One of the goals of this work is to find such scenarios and determine their resolution using formal mathematical modeling. **Scenario B5:** In developing this framework, we must look further ahead than just considering cyber constraints. We also consider cyber controls. That is, we examine how to use cyber controls to make suspect hosts and measurements trustworthy again. For example, there may be a certain degree of remediation that a utility is able to finance to essentially make the physical control available for action again, that is, to "fix" a compromise. Then, there will be a certain cost per cyber control to do this that can be included in mathematical formulation. Scenario B5 illustrates the best case, where both cyber and power controls are used, and the compromised controllers are fixed.

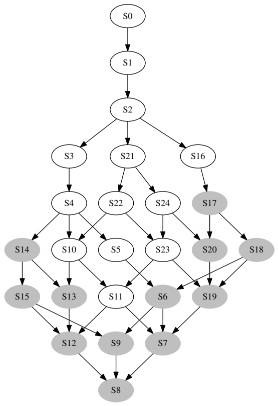
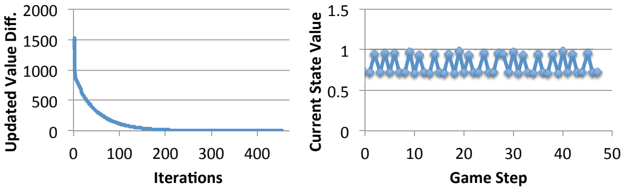


Fig. 4: Automatically Generated CMDP

For our experiments, we used the cyber control center network as described in [6]. CPR proceeds with the generation of the Markovian model (Figure 4) that the game-theoretic decision making engine makes use of for optimal response action selection purposes later. For presentation clarity, only the adversarial actions (no responses) are illustrated. The initial state s_0 (Section II-B) is the most secure state, where none of the computers within the control center have been compromised and no malicious power-side consequence has occurred. The gray states include a physical power consequence, e.g., a malicious transmission line outage. CPR's objective is to proactively prevent the power grid from entering the gray states by taking relevant response and recovery actions during the ongoing attacks within the network. Once CPR generates the CMDP model, the next step is to populate the model with the numeric security measures that will be used later for the game-theoretic intrusion tolerance. CPR goes through the generated states and calculates the corresponding power system performance index values [10] given the affected power system components. CPR implements the value function for the generated model to compute how relevant each response action is, from each given state of the network, for the restoration of the system back to its secure operational mode.

Figure 5 shows the results for CPR's response selection. For each state, the initial value was assigned to be the power system performance index [23] depending on the malicious power system damages (contingencies) caused in that state. Figure 5(a) shows how the value function (1) converges during the value iteration algorithm (6) to guarantee optimality of the chosen action by CPR. We simulated the interaction (sequence of corrective and adversarial action) between the attacker and CPR and logged the sequence of system states during the

[3] For instance, by the SCPSE's cyber-physical intrusion detection engine [6].



(a) Decision Making Convergence (b) Attack-Time State Values

Fig. 5: Optimal Response Selection

attack scenario. Figure 5(b) shows the state value sequence. It is noteworthy that the attacker is assumed to be completely rational so that he/she takes optimal actions at every state of the game. In reality, the response engine would act better as the attackers would not take optimal actions because of the computation and knowledge limitations regarding the victim networks.

IV. Related Work

Traditionally, security incident-handling [24] techniques are categorized into three broad classes. First, there are intrusion prevention methods that take actions to prevent occurrence of attacks, e.g., network flow encryption to prevent man-in-the-middle attacks. Second, there are intrusion detection systems (IDSs) such as anti-viruses. Finally, there are intrusion response techniques that take responsive actions based on received IDS alerts to stop attacks before they can cause significant damage and to ensure safety of the computing environment. So far, most research has focused on improving techniques for intrusion prevention and detection, while intrusion response usually remains a manual and time-consuming process [25] that is not suitable for real-time safety-critical infrastructures; therefore, automated intrusion response solutions are required.

During the last decade, three types of techniques aimed at enhancing automation in purely-cyber intrusion response were proposed. The majority of those techniques are based on lookup tables filled with predefined mappings, e.g., (response actions, intrusion alerts) [26]. These methods allow response systems to deal with intrusions faster. However, they suffer from a lack of 1) flexibility, mainly because these systems completely ignore the intrusion cost factor; and 2) scalability, since it is infeasible to predict all the alert combinations from IDSes in a large-scale computer network. A second group of intrusion response systems (IRSes) employs a dynamic rule-based selection procedure [27] that selects response actions based on a certain attack metric, e.g., confidence or severity of attack. Finally, there has been increasing interest in developing cost-sensitive models of response selection [7]. The main objective for applying such a model is to compare intrusion damage and response cost to ensure system recovery with minimum cost without sacrificing the normal functionality of the system under attack.

Acknowledgements

We would like to thank our research sponsor, the National Science Foundation (NSF); Award Number CNS 1446471.

V. Conclusions

We presented CPR, a practical cyber-physical intrusion tolerance architecture that makes use of a control-theoretic decision making engine to select optimal response strategies proactively through power system-based analysis of various potential upcoming system states. CPR's ultimate objective objective is to carry response strategies out through cyber- and power-based actuators and drive the system towards safe states.

References

[1] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *43rd Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2010, pp. 1–10.

[2] W. Lee, W. Fan, M. Miller, S. J. Stolfo, and E. Zadok, "Toward cost-sensitive modeling for intrusion detection and response," *Journal of Computer Security*, vol. 10, no. 1, pp. 5–22, 2002.

[3] T. S. Mule, A. S. Mahajan, S. Kamble, and O. Khatavkar, "Intrusion protection against sql injection and cross site scripting attacks using a reverse proxy," *International Journal of Computer Science & Information Technologies*, vol. 5, no. 3, 2014.

[4] R. Lepofsky, "North american energy council security standard for critical infrastructure protection (nerc cip)," in *The Managers Guide to Web Application Security:*. Springer, 2014, pp. 165–176.

[5] W. Mao, H. Chen, J. Li, and J. Zhang, "Software trusted computing base," May 8 2012, uS Patent 8,176,336.

[6] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "SCPSE: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[7] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," in *IEEE/IFIP International Conference on Dependable Systems and Networks*. IEEE, 2009, pp. 439–448.

[8] S. Zonouz, A. Houmansadr, and P. Haghani, "Elimet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior," in *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2012, pp. 1–12.

[9] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks." in *LISA*, vol. 99, no. 1, 1999, pp. 229–238.

[10] T. Guler, G. Gross, and M. Liu, "Generalized line outage distribution factors," *Power Systems, IEEE Transactions on*, vol. 22, no. 2, pp. 879–881, May 2007.

[11] J. Meserve, "Staged cyber attack reveals vulnerability in power grid; available at http://www.cnn.com/2007/US/09/26/power.at.risk/," 2007.

[12] G. Owen, *Game Theory*, 3rd ed. Academic Press, 1995.

[13] J. Filar and K. Vrieze, *Competitive Markov Decision Processes*. Springer-Verlag, 1997.

[14] Smart Wires. (2015) Smart Wires. [Online]. Available: www.smartwires.com

[15] K. Hedman, S. Oren, and R. O'Neill, "A review of transmission switching and network topology optimization," in *Power and Energy Society General Meeting, 2011 IEEE*, July 2011, pp. 1–7.

[16] DOE ARPA-E. (2015) GENI. [Online]. Available: http://arpa-e.energy.gov/?q=arpa-e-programs/geni

[17] 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*, vol. 981, pp. 1–17, 1995.

[18] E. Sondik, "The optimal control of partially observable Markov processes," Ph.D. dissertation, Stanford University, 1971.

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

[20] "Federal energy regulatory commission (ferc): Optimal power flow and formulation papers; available at http://www.ferc.gov/industries/electric/indus-act/market-planning/opf-papers.asp," 2010.

[21] H. Dommel and W. Tinney, "Optimal power flow solutions," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-87, no. 10, pp. 1866–1876, Oct 1968.

[22] PowerWorld Corp. (2015) PowerWorld Simulator. [Online]. Available: www.powerworld.com

[23] S. Zonouz, C. M. Davis, K. R. Davis, R. Berthier, R. B. Bobba, and W. H. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *Smart Grid, IEEE Transactions on*, vol. 5, no. 1, pp. 3–13, 2014.

[24] M. Agrawal, A. Campoe, and E. Pierce, *Information Security and IT Risk Management*. Wiley Publishing, 2014.

[25] M. Monshizadeh, P. Naldurg, and V. Venkatakrishnan, "Mace: Detecting privilege escalation vulnerabilities in web applications," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 690–701.

[26] A. Shameli-Sendi, M. Cheriet, and A. Hamou-Lhadj, "Taxonomy of intrusion risk assessment and response system," *Computers & Security*, vol. 45, pp. 1–16, 2014.

[27] T. Kim, X. Wang, N. Zeldovich, and M. F. Kaashoek, "Intrusion recovery using selective re-execution." in *USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2010, pp. 89–104.