A Dynamic Game-Theoretic Approach to Resilient Control System Design for Cascading Failures*

Quanyan Zhu
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
1308 W. Main St.
Urbana, IL, USA
zhu31@illinois.edu

Tamer Başar
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
1308 W. Main St.
Urbana, IL, USA
basar1@illinois.edu

ABSTRACT

The migration of many current critical infrastructures, such as power grids and transportations systems, into open public networks has posed many challenges in control systems. Modern control systems face uncertainties not only from the physical world but also from the cyber space. In this paper, we propose a hybrid game-theoretic approach to investigate the coupling between cyber security policy and robust control design. We study in detail the case of cascading failures in industrial control systems and provide a set of coupled optimality criteria in the linear-quadratic case. This approach can be further extended to more general cases of parallel cascading failures.

Categories and Subject Descriptors

C.3 [**Special-Purpose and Application-Based Systems**]: Process Control Systems; D.4.8 [**Performance**]: Stochastic analysis; I.2.8 [**Problem Solving, Control Methods, and Search**]: Control Theory

General Terms

Security, Reliability, Algorithms, Theory

Keywords

Game Theory, Differential Games, Markov Games, Cyber-Physical Systems, Nash Equilibrium

1. INTRODUCTION

Many current critical infrastructures such as power grids and transportation systems are migrating into the open public network. The technological advancement has posed many challenges on the legacy control systems. The classical design of control systems takes into account modeling uncertainties as well as physical disturbances and encompasses a multitude of control design methods such as robust control, adaptive control, and stochastic control. With the growing level of integration with new information technologies, modern control systems face uncertainties not only from the physical world but also from the cyber space. The vulnerabilities of the software deployed in the new control system infrastructure create many potential risks and threats from the attackers. Exploitation of these vulnerabilities can lead to severe damages as have been seen in [1, 2]. It has been reported in [1] that the U.S. power grid was penetrated by cyber spies and the intrusions could have damaged the power grid and other key infrastructure. In [2], it is believed that an inappropriate software update has led to a recent emergency shutdown for 48 hours of a nuclear power plant in Georgia. More recently, it is reported in [3, 4] that a computer worm, Stuxnet, has been spread to target Siemens Supervisory Control And Data Acquisition (SCADA) systems that are configured to control and monitor specific industrial processes.

In this paper, we propose a hybrid game-theoretic approach to address resilient control design issues in modern critical infrastructures. We investigate the coupling between cyber security policy at the cyber level of the system and the robust control design at the physical layer of the system. Resilience of cyber-physical systems addresses two types of disturbances. One source of disturbance comes from the physical environment, which is due to noise or uncertainty. Another source of disturbance comes from the cyber-physical system integration. The uncertainty in cyber events can trigger the system to switch from one operating state to another. Such a disturbance is usually unanticipated by the physical layer control.

2. RELATED WORK

Cascading failures have been widely studied in the literature of complex networks. In [8], authors have presented a model based on the dynamical redistribution of the flow on the network, and they have shown that the breakdown of a single node is sufficient to collapse the efficiency of the entire system if the node is among the ones with largest load. In [7], the authors have used an evolutionary algorithm to improve the resilience of complex networks to cascading failures, and have shown that clustering, modularity

*The research was partially supported by the AFOSR MURI Grant FA9550-10-1-0573, and also by an NSA Grant through the Information Trust Institute at the University of Illinois.

HiCoNS'12, April 17–18, 2012, Beijing, China.

and long path lengths all play important roles in the design of robust large-scale infrastructures. The 2003 blackout in North America has motivated the study of cascading failures in power networks. In [6], a hidden failure embedded DC model of power transmission systems has been developed to study the power law distributions observed in North American blackout data. In [5], the authors have investigated criticality in a sizable network with a fairly detailed blackout model and measure blackout size by energy unserved.

The notion of resilience has appeared in the literature of many fields such as psychology, ecology, organizational behavior, networks, and material science [9, 10]. In [11], resilience of a system is defined as the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable time and composite costs and risks. In [12], the author points out that resilience and robustness are not general properties but are relative to specific classes of perturbations. Different from the concept of robustness, resilience of a system to a class of unexpected extreme perturbations is defined as the ability of this system to (i) gracefully degrade its function by altering its structure in an agile way when it is subject to a set of perturbations of this class, and (ii) quickly recover it once the perturbations cease. The notion of resilience in [10], [11], [12] all refer to the ability of a system to withstand an unexpected event and recover after the failure. These definitions provide conceptual background for the development of quantitative methods for resilient control systems.

Metrics for resilient control systems have been studied in [14]. The authors have proposed a 3-layer system model and a resilience curve, and provided metrics for quantitative estimation of system resiliency. In [13, 15], we have introduced a hierarchical security architecture for cyber-physical systems to identify security issues at different layers of the system, and within that framework we have introduced quantitative approaches to enable the study of security issues that lie at the physical, cyber and human levels of the system. In [15, 19, 18], we have used cross-layer methods to understand the coupling between cyber and physical security. In [19], we have studied the impact of delay and packet drop rates on control system performance as a result of defense-in-depth cyber defense. In [18], we have introduced dynamic coupling between cyber defense policy-making and physical layer control design. This recently developed framework serves as the foundational basis for this paper in which we investigate the case of cascading failures in cyber-physical systems.

3. RESILIENT CONTROL SYSTEMS

Industrial control systems (ICSs) are commonly seen in many critical infrastructures such as electricity generation, transmission and distribution, water treatment and manufacturing. The main function of ICSs is to monitor and control physical and chemical processes. In the past few decades, we have seen a growing trend of integrating physical ICSs with cyber space to allow for new degrees of automation and human-machine interactions. The uncertainties and hostilities existing in the cyber environment have brought about emerging concerns for the traditional ICSs. It is of supreme importance to have a system that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature [16]. The term *resilient control system* (RCS) is used to describe systems that have these essential features.

In this section, our aim is to establish a theoretical framework for designing resilient controllers. To address this challenge, we first need to understand the architecture of industrial control systems (ICSs). Here, we adopt a layering perspective toward ICSs. This view-point has been adopted in many large scale system designs such as the Internet, power systems and nuclear power plants. For example, in smart grids, the hierarchical architecture includes economy grid, regulatory grid, electricity market grid, transmission grid and distribution grid. The seven layer OSI model for the Internet provides a set of rules and standards that allow manufacturers and developers to create software and hardware that is compatible with each other.

We hierarchically separate ICSs into 6 layers, namely, physical layer, control layer, communication layer, network layer, supervisory layer and management layer. This hierarchical structure is depicted in Fig. 1.

The physical layer comprises the physical plant to be controlled. The control layer consists of multiple control components, including observers/sensors, intrusion detection systems (IDSs), actuators and other intelligent control components. The physical layer together with the control layer can be viewed as the physical world of the system. On top of these two layers, the communication layer is where we have physical communication channels that can be in the form of wireless channels, the Internet, etc., and the network layer is where the topology and routing of the architecture live. The communication and network layers constitute the cyber world of the system. Supervisory layer coordinates all lower layers by designing and sending appropriate commands. It can be viewed as the brain of the system. Management layer is a higher level decision-making engine, where the decision-makers take an economic perspective towards the resource allocation problems in control systems. Supervisory and management layers are interfaces with humans and hence they contain many human factors and human-made decisions.

The layered architecture can facilitate the understanding of the cross-layer interactions between the physical world and the cyber world. In Fig. 2, we use $x(t)$ and $\theta(t)$ to denote the continuous physical state and the discrete cyber state of the system, which are governed by the laws f and Λ, respectively. The physical state $x(t)$ is subject to disturbances w and can be controlled by u. The cyber state $\theta(t)$ is controlled by the defense mechanism l used by the network administrator as well as the attacker's action a. The hybrid nature of the cross-layer interaction leads to adoption of the hybrid system model described later through (1), (2) and (5).

As mentioned earlier, our goal in this paper is to establish a framework for designing a resilient controller for the hybrid system model described. We view resilient control as a cross-layer control design, which takes into account the given range of deterministic uncertainties at each state as well as the random unexpected events that trigger the transition from one system state to another. Hence, it has the property of disturbance attenuation or rejection to physical uncertainties as well as damage mitigation or resilience to sudden cyber attacks. We first derive resilient control for the closed-loop perfect-state measurement information structure in a general setting with the transition law depending on the

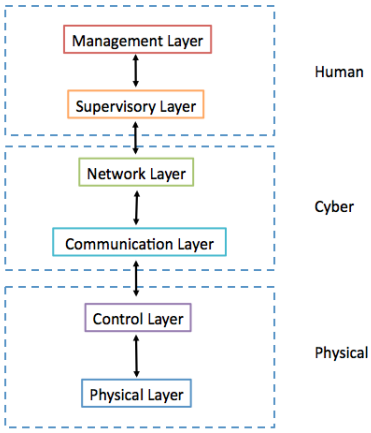

Figure 1: A hierarchical layered architecture of cyber-physical control systems.

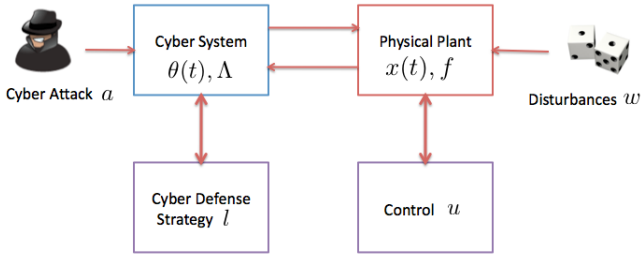

Figure 2: The interactions between the cyber and physical systems are captured by their dynamics governed by the transition law Λ and the dynamical system f. The physical system state $x(t)$ is controlled by u in the presence of disturbances and noises. The cyber state $\theta(t)$ is controlled by the defense mechanism l used by the network administrator as well as the attacker's action a.

control action, and then we simplify the result to the special case of the linear-quadratic problem.

4. SYSTEM MODEL

In this section, we consider an ICS that is subject to possible failures due to either manufacturing faults or malicious attacks. We follow the general framework that has been proposed in [18] to derive a set of coupled optimality criteria to characterize the coupling between cyber and physical systems.

In Fig. 5, we describe the cascading effects in an ICS, where the state $\theta \in \mathcal{S} := \{1, 2, \cdots, N\}$ is the failure state in the system. The dynamics of the system at each state are described by

$$\dot{x}(t) = A^\theta x + B^\theta u + D^\theta w, \quad x(t_0) = x_0. \tag{1}$$

where x_0 is the initial state of the system at time $t = t_0$. $x \in \mathbb{R}^n$, $u \in \mathbb{R}^r$ is the control input, $w \in \mathbb{R}^p$ is the disturbance. $A^\theta, B^\theta, D^\theta, \theta \in \mathcal{S}$, are matrices with real-valued entries and of appropriate dimensions, indexed by θ. By default, state $\theta = 1$ is the normal operating state and state $\theta = N$ is the terminal failure state. The states $i, 2 \leqslant i \leqslant N-1$, are intermediate compromised states in which one system component failure leads to another. We assume that the failure states are irreversible, i.e., the system cannot be fixed or brought back to its normal state immediately after faults occur. This is usually due to the fact that the time scale for critical cascading failures is much shorter than the time scale for system maintenance. The transition between the failure states follows a Markov jump process with rate matrix $\lambda = \{\lambda_{ij}\}_{i,j\in\mathcal{S}}$ such that for $i \neq j, \lambda_{ij} \geqslant 0$, $\lambda_{ii} = 1 - \sum_{j\neq i} \lambda_{ij}$, and for $i > j$, $\lambda_{ij} = 0$. For simplicity, we can use the notation $p_i = \lambda_{i,i+1}, 1 \leqslant i \leqslant N-1$, as the transition rates between adjacent states, and hence $\lambda_{ii} = 1 - p_i, 1 \leqslant i \leqslant N-1, p_N = \lambda_{NN}$. The matrices $A^\theta, B^\theta, D^\theta$ and the transition rate matrix λ are generally dependent on a given cyber policy l and attack strategy a.

4.1 Robust Control Design

At the physical control layer, our aim is to design a robust feedback controller μ to reject the worst-case disturbance w by employing an H^∞ control design using a zero-sum game-theoretic approach. We can view the controller as minimizing the following quadratic cost while the disturbance maximizing it.

$$J(\mu, \nu) = \mathbb{E}_\theta \int_{t_0}^{\infty} \left(|x(t)|^2_{Q^\theta} + |u(t)|^2_{R^\theta} - \gamma^2 |w(t)|^2 \right) dt, \tag{2}$$

where μ is a state-feedback control law, ν is a state-feedback disturbance law, and $|\cdot|$ denotes the Euclidean norm with appropriate weighting. $Q^\theta \geqslant 0$, $R^\theta > 0$, $\theta \in \mathcal{S}$, are matrices of appropriate dimensions. Under regularity conditions and for an attenuation level $\gamma > \gamma^*$, the critical attenuation level (see [17, 18] for details), the strategy that guarantees the upper value of the underlying game is in the form of linear state feedback, i.e.,

$$u(t) = \mu(t, x(t), \theta(t) = i) = -(R^i)^{-1} B^{i'} Z_i x(t), \tag{3}$$

where $Z_i, i \in \mathcal{S}$, are positive definite solutions to the following linearly coupled set of Riccati equations

$$A^{i'} Z_i + Z_i A^i - Z_i \left(B^i (R^i)^{-1} B^{i'} - \frac{1}{\gamma^2} D^i D^{i'} \right) Z_i + Q^i + \sum_{j=1}^{N} \lambda_{ij} Z_j = 0, i \in \mathcal{S}. \tag{4}$$

The value of the game when the initial mode state is $\theta = i$ is given by $V^i = x^T Z_i x$.

4.2 Cyber Policies

The cyber policy in an ICS is made by an administrator to protect the system from malicious attacks. Cyber policies are made often on a longer time scale than the physical layer control. Hence we let $k = t/\epsilon$ be the time unit at the cyber level for a sufficiently small $\epsilon > 0$. Different cyber policies can affect different aspects of physical layer control system performance. For example, intrusion detection/prevention systems (IDPSs) at the actuation side of the control can lead to packet drops in the communication channel between the actuator and the plant [22, 20, 21, 19]. Such loss of data packets can be captured by the matrix B^θ. In addition, the cyber policies at the network level can influence the

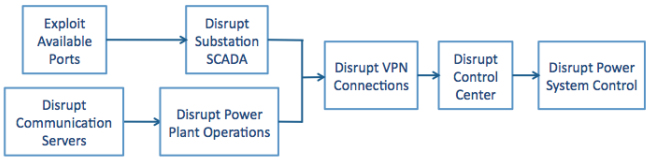

Figure 3: An illustration of sequences of attacks in system systems

```
alert tcp any any -> any 7580 (msg:"ETPRO SCADA
Siemens Tecnomatix FactoryLink CSService GetFile
path Buffer Overflow"; flow:to_server,established;
content:"LEN|00|"; depth:4; byte_test:4,>,
1028,0,little; content:"|99|"; distance:8; within:1;
content:"|99 00 00 00 08 00 00 00 02 06|"; distance:
0; byte_test:4,>,1024,0,big; classtype:attempted-
user;reference:url,digitalbond.com/tools/quickdraw/
vulnerability-rules; sid:1111675; rev:1;)
```

Figure 4: A SCADA IDS rule to detect CSService CSMSG GetFile buffer overflow in Siemens Tecnomatix FactoryLink

transition rate matrix λ because a higher level of security enforcement will lead to lower transition rates between a state i and a worse state $i+1$, $1 \leqslant i \leqslant N-1$. The rate matrix λ is determined by cyber security polices as well as reliability of physical components in the cyber-physical system. In the absence of security considerations, λ has its baseline transition rates only determined by the corresponding reliability models.

At the cyber level, we consider an attacker who uses a sequence of attacks toward achieving his goal of disrupting the services of the system. At each stage, the attacker chooses one possible attack from a set of possible actions based on the state of the system. The action set of an attacker is often characterized by attack graphs [23, 24], which consist of a multi-level hierarchy in a tree structure that captures possible ways of achieving attack goals. In Fig. 3, we illustrate a possible sequence of attacks, where each block can be associated with many different specific actions to accomplish the attack. One possible sequence starts with an exploration and exploitations of vulnerable ports and then disruption of the SCADA system at substations before launching an attack on the control center.

One way to defend a cyber system is to deploy intrusion detection systems (IDSs), which are passive devices that receive and evaluate information sent over a network against a set of signatures. IDS signatures have been developed for most published vulnerabilities and for potentially dangerous activity in common IT protocols. Configuration of IDSs is not a trivial task. The current version of the Snort IDS, for example, has approximately 10,000 signature rules located in fifty categories. Each IDS also comes with a default configuration to use when no additional information or expertise is available. It is not trivial to determine the optimal configuration of an IDS because of the need to understand the quantitative relationship between a wide range of analyzers and tuning parameters. This explains why current IDSs are configured and tuned using a trial-and-error approach. In [22], we have proposed a game-theoretic approach for dynamic configuration of IDSs and an online learning technique to search for the optimal configuration policy against an attacker.

For critical infrastructures, a set of SCADA IDS signatures that parallel Snort rules for enterprise IT systems has been designed by Digital Bond's Quickdraw which leverages the existing IDS equipment by developing signatures for control system protocols, devices and vulnerabilities [27]. In Fig. 4, we illustrate a typical SCADA IDS rule, which is used detect a buffer overflow attack. The rule is specifically designed for Siemens Tecnomatix FactoryLink software, which is used for monitoring, supervising, and controlling industrial processes. FactoryLink is commonly used to build applications such as human-machine interface (HMI) systems and SCADA systems. The logging function of FactoryLink is vulnerable to a buffer-overflow caused by the usage of `vsprintf` with a stack buffer of 1024 bytes. The vulnerability can be exploited remotely in various ways like the passing of a big path or filter string in the file related operations [27].

The goal of the network administrator is to configure an optimal set of detection rules to protect the cyber system from attackers. To model the interaction between an attacker and a defender, we use a dynamic game approach. Let $\mathcal{L}^*$ be a finite set of possible system configurations in the network and $\mathcal{A}$ be the finite action set of the attacker. Let $\mathbf{h}(k)$ denote a mixed strategy of the defender over the finite set $\mathcal{L}^*$ at time k and $\mathbf{g}(k)$ denote a mixed strategy of the attacker over the finite set $\mathcal{A}$ at time k. We focus on a class of stationary cyber policies, where mixed strategies of the defender and the attacker are only dependent on the state of the system. We let $\mathbf{H} = [\mathbf{h}_s]_{s=1}^N$ and $\mathbf{G} = [\mathbf{g}_s]_{i=1}^N$ be the stationary strategies for the defender and the attacker, where $\mathbf{h}_s$ and $\mathbf{g}_s$ are respectively mixed strategies of the defender and the attacker that correspond to state $s \in \mathcal{S}$. A defender chooses a stationary strategy to minimize the long-term cost W_β as follows while an attacker chooses one to maximize it.

$$W_\beta(\theta, \mathbf{H}, \mathbf{G}) = \int_{t_0}^{\infty} e^{-\beta k} \mathbb{E}_{\theta,\mathbf{H},\mathbf{G}} Y(Z_{s(k)}, k) dk, \qquad (5)$$

Here, $\beta > 0$ is a discount factor, $s(k)$ is the state of system at time k, $Y(\cdot)$ is a function of time k and control gain Z_s, which is related to the value of each state through the value functions obtained for (2). Note that Z_θ depends on the cyber policies $(\mathbf{H}, \mathbf{G})$.

A saddle-point equilibrium strategy pair $(\mathbf{H}^*, \mathbf{G}^*)$ is one that achieves the game value w_β^* and needs to satisfy the fixed-point optimality condition

$$\beta w_\beta^*(i) = \text{val}\left\{ Y(\mathbf{H}, \mathbf{G}, i) + \sum_{j \in \mathcal{S}} \lambda_{ij}(\mathbf{H}, \mathbf{G}) w_\beta^*(j) \right\}. \qquad (6)$$

Here, we have written $Y(\cdot)$ in terms of the strategy pair $(\mathbf{H}, \mathbf{G})$ and state i through its dependence on Z_i. w_β^* is the value function of the cost functional W_β and val is the saddle-point value operator.

4.3 Optimality Criteria for Cascading Failures

To find the robust control and saddle-point cyber policy for the cyber-physical system (1) under the physical level cost (2) and the cyber level cost (5), we need to solve the set of coupled optimality equations (4) and (6). Let

$Y = x_0^T Z_i x_0$ be the utility of each state i. For the case of cascading failure as depicted in Fig. 5 and linear quadratic robust control design, we can simplify (4) and (6) and arrive at the following set of coupled equations. The optimality criteria for the cyber system are described by

$$\begin{aligned} \beta w_\beta^*(N) &= V^N, & (7)\\ \beta w_\beta^*(i) &= \text{val}\{V^i + p_i w_\beta^*(i+1) - p_i w_\beta^*(i)\}, & (8)\\ & \quad i = 1, \cdots, N-1, \\ V^i &= x_0^T Z_i x_0. \end{aligned}$$

Here, $p_i = \lambda_{i,i+1}, 1 \leqslant i \leqslant N-1$, and V^i is dependent on p_i through Z_i in (4). Note that (8) requires solving for a saddle-point in mixed strategies. Since both players have a finite number of choice for each k, the existence of a saddle-point solution is guaranteed for the zero-sum game in (4), [25, 26].

In addition, the optimality criteria for the optimal control in the linear quadratic case can be reduced to

$$A^{N'} Z_N + Z_N A^N - Z_N \left(B^N (R^N)^{-1} B^{N'} - \frac{1}{\gamma^2} D^N D^{N'} \right) Z_N + Q^N = 0, \quad (9)$$

$$A^{i'} Z_i + Z_i A^i - Z_i \left(B^i (R^i)^{-1} B^{i'} - \frac{1}{\gamma^2} D^i D^{i'} \right) Z_i + Q^i + p_i Z_{i+1} = 0, \quad i = 1, \cdots, N-1. \quad (10)$$

Here, γ is a chosen level of attenuation. Under regularity conditions in [17], there exists a finite scalar $\gamma^\infty > 0$ such that for all $\gamma > \gamma^\infty$, solutions to (9) and (10) exist and are unique.

In (8), p_i is dependent on $\mathbf{H}$ and $\mathbf{G}$. At the same time, as a result of solving (10), the value V^i is dependent on p_i and B^i, which are in turn a function of $\mathbf{H}$ and $\mathbf{G}$. The above set of coupled equations can be solved by starting with (9) for obtaining the value of the terminal state V^N. From (7), we can calculate the value v_N^* and then in the next step use (8) and (10) for finding the stationary saddle-point equilibrium strategies $\mathbf{h}_{N-1}^*, \mathbf{g}_{N-1}^*$ at state $\theta = N-1$, their corresponding transition rate $p_{N-1}^* = \lambda_{N-1,N}(\mathbf{h}_{N-1}^*, \mathbf{g}_{N-1}^*)$ and the Riccati solution Z_{N-1}. We can iterate the process again by using Z_{N-1} in (8) for $i = N-2$, and the obtained strategy pair $(\mathbf{h}_{N-2}^*, \mathbf{g}_{N-2}^*)$ is used in (10) for solving Z_{N-2}. Hence we can use the backward induction to find Z_1 and $(\mathbf{h}_1^*, \mathbf{g}_1^*)$.

Note that the coupling between equations (9), (10) and (7), (8) demonstrates the interdependence between security at the cyber level and the robustness at the physical level. The holistic viewpoint towards these system properties is essential in addressing the resilience of cyber-physical systems. The coupling between cyber and physical levels of the system is not one-directional but rather reciprocal. The upward resilience from the physical level to the cyber level results from the function Y while the downward resilience from the cyber level to the physical level follows from the dependence of λ on the cyber policies.

5. CONCLUSIONS AND FUTURE WORK

In this paper, we have introduced a dynamic game-theoretic approach to model the interactions between the cyber level policy making and physical level robust control design. We have investigated the case of cascading failures where one unanticipated event propagates failures in the system. We have provided a set of coupled optimality conditions in the special case of linear-quadratic systems to characterize the saddle-point equilibrium of cyber defense policy and robust control design. As future work, we will generalize the cascading failure to the case as depicted in Fig. 6. In addition, we will incorporate reinforcement learning schemes such as Q-learning for learning the saddle-point cyber policy online, and study iterative methods to find solutions to the coupled set of optimality equations.

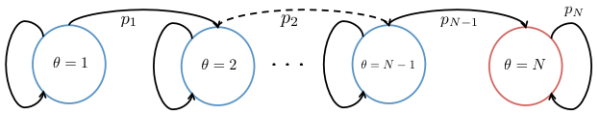

Figure 5: Cascading failures in an ICS

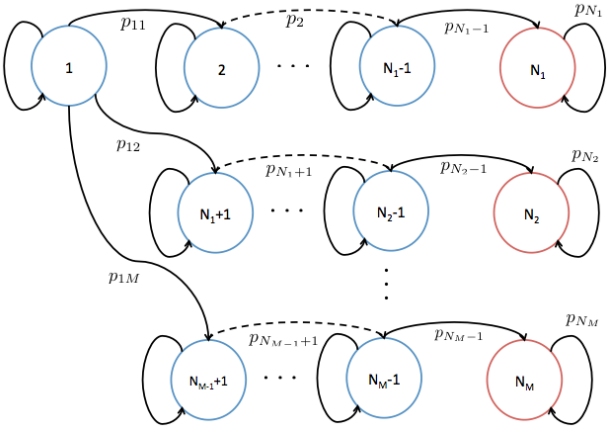

Figure 6: Generalized form of cascading failures in an ICS

6. REFERENCES

[1] S. Gorman, "Electricity Grid in U.S. Penetrated By Spies," *Wall Street Journal*, April 8, 2009, `http://online.wsj.com/article/SB123914805204099085.html`, Retrieved Aug. 16, 2011.

[2] B. Krebs, "Cyber Incident Blamed for Nuclear Power Plant Shutdown", *Washington Post*, June 5, 2008, `http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html`, Retrieved Aug. 16, 2011.

[3] S. Greengard, "The New Face of War", Communications of the ACM, Dec. 2010, vol. 53, no. 12, pp. 20–22.

[4] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computerworld*, Sept. 16, 2010, `http://www.computerworld.com/s/article/print/9185419`, Retrieved Aug. 16, 2011.

[5] D.P. Nedic, I. Dobson, D.S. Kirschen, B.A. Carreras, V.E. Lynch, "Criticality in a cascading failure blackout model," *Intl. J. of Electrical Power and Energy Systems*, vol. 28, 2006, pp. 627–633.

[6] J. Chen, J.S. Thorp, I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *Intl. J. of Electrical Power and Energy Systems*, vol. 27, no. 4, May 2005, pp. 318–326.

[7] J. Asha and D. Newth, "Optimizing complex networks for resilience against cascading failure," *Physica A*, vol. 380, pp. 673-683, 2007.

[8] P. Crucitti, V. Latora and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, 045104(R), 2004.

[9] R. Hollnagel, D. D. Woods, N. Leveson (eds.), "Resilience engineering: concepts and precepts," Ashgate Publishing Company, 2006.

[10] E. Hollnagel, J. Pariès, D. D. Woods and J. Wreathall, "Resilience Engineering in Practice," Ashgate Publishing Company, 2011.

[11] Y. Y. Haimes, "On the definition of resilience in systems," *Risk Analysis*, vol. 29, no. 4, 2009.

[12] L. Mili, "Taxonomy of the characteristics of power system operating states," 2nd NSF-VT Resilient and Sustainable Critical Infrastructures (RESIN) Workshop, Tuscon, Arizona, January 13-15, 2011.

[13] Q. Zhu, C. Rieger and T. Başar, "A hierarchical security architecture for cyber-physical systems," in Proc. of Intl. Symposium on Resilient Control Systems (ISRCS), Boise, ID, Aug. 9 - 11, 2011.

[14] D. Wei and K. Ji, "Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights," in Proc. of 3rd Intl. Symp. on Resilient Control Systems (ISRCS), 2010.

[15] Q. Zhu and Başar, "A hierarchical security architecture for smart grid," In Z. Han, E. Hossain and V. Poor (Eds.), *Smart Grid Communications and Networking*, Cambridge University Press, 2012.

[16] C.G. Rieger, D.I. Gertman, and M. A. McQueen, "Resilient control systems: next generation design research," In Proc. of the 2nd Conf. on Human System interactions, Catania, Italy, May 21-23, 2009, pp. 629–633.

[17] T. Başar and P. Bernhard, *H-infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach*, Birkhäuser, 1995.

[18] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in Proc. of 50th IEEE Conference on Decision and Control and European Control Conference, Orlando, Florida, Dec. 12-15, 2011.

[19] Q. Zhu and T. Başar, "Towards a unifying security framework for cyber-physical systems," in Proc. of Workshop on the Foundations of Dependable and Secure Cyber-Physical Systems (FDSCPS-11), CPSWeek 2011, Chicago.

[20] Q. Zhu and T. Başar, "Indices of power in optimal IDS default configuration: theory and examples," in Proc. of 2nd Conference on Decision and Game Theory (GameSec 2011), College Park, MD, USA. Nov. 14 - 15, 2011.

[21] Q. Zhu, H. Tembine and T. Başar, "Network security configuration: a nonzero-sum stochastic game approach," in Proc. of 2010 American Control Conference (ACC), June 30 -July 2, 2010, pp. 1059–1064.

[22] Q. Zhu and T. Başar, "Dynamic policy-based IDS configuration," in Proc. of 48th IEEE Conference on Decision and Control, Shanghai, China, Dec. 2009, Dec. 15-18, 2009, pp. 8600 – 8605.

[23] C.-W. Ten, C.-C. Liu and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees," Power Engineering Society General Meeting, 24-28 June 2007, pp.1–8.

[24] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. Wing, "Automated generation and analysis of attack graphs," IEEE Symposium on Security and Privacy, 2002, pp. 273–284.

[25] J. F. Nash, "Equilibrium points in n-person games PNAS," January 1, 1950 vol. 36 no. 1 pp. 48–49.

[26] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, SIAM Series in Classics in Applied Mathematics, Philadelphia, January 1999.

[27] Digital Bond, `http://www.digitalbond.com/tools/quickdraw/`, last accessed on Feb. 20, 2012.