INL/CON-11-21860
PREPRINT

A Hierarchical Security Architecture for Cyber-Physical Systems

4th International Symposium on Resilient Control Systems

Quanyan Zhu
Craig Rieger
Tamer Başar

August 2011

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

A Hierarchical Security Architecture for Cyber-Physical Systems

Quanyan Zhu, Craig Rieger and Tamer Başar

Abstract—**Security of control systems is becoming a pivotal concern in critical national infrastructures such as the power grid and nuclear plants. In this paper, we adopt a hierarchical viewpoint to these security issues, addressing security concerns at each level and emphasizing a holistic cross-layer philosophy for developing security solutions. We propose a bottom-up framework that establishes a model from the physical and control levels to the supervisory level, incorporating concerns from network and communication levels. We show that the game-theoretical approach can yield cross-layer security strategy solutions to the cyber-physical systems.**

I. Introduction

Many industry sectors are experienced with arming automation systems with modern IT technology. The integration moves the systems from an outdated, proprietary technology to more common ones such as personal computers, Microsoft Windows, TCP/IP/Ethernet, etc. It provides more efficient methods of communication, improves system interoperability and result in considerable cost and performance benefits. However, in the meantime, it poses security challenges on control systems as the integration exposes the system to public networks.

In [1], it is reported that hackers have inserted software into the US power grid, potentially allowing the grid to be disrupted at a later date from a remote location. As reported in [2], it is believed that an inappropriate software update has led to a recent emergency shutdown of a nuclear power plant in Georgia, which lasted for 48 hours. In [3], it is discovered 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. On November 29, 2010, Iran has confirmed that its nuclear program had indeed been damaged by Stuxnet [4], [5]. The infestation by this worm may have damaged Iran's nuclear facilities in Natanz and eventually delayed the start up of Iran's nuclear power plant.

Many control systems do not have built-in security functionalities and the security solutions in regular IT systems may not always apply to systems in critical infrastructures. This is because critical infrastructures have different goals, objectives and assumptions concerning what needs to be protected, and have specific applications that are not originally designed for a general IT environment. Hence, it is necessary to develop unique security solutions to fill the gap where IT solutions do not apply.

In this paper, we describe a layered architecture perspective towards secure cyber-physical systems (CPSs), which helps us to identify research problems and challenges at each layer and build models for designing security measures for control systems in critical infrastructures. We also emphasize a cross-layer viewpoint towards the security issues in cyber-physical systems in that each layer can have security dependence on the other layers. We need to understand the tradeoff between the information assurance and the physical layer system performance before designing defense strategies against potential cyber threats and attacks.

The rest of this paper is organized as follows. In Section II, we describe motivations for a hierarchical perspective towards cyber-physical systems and review related works. Section III describes the hierarchical viewpoint towards control system security and discusses security issues existing at each layer. In Section IV, we propose a theoretical cross-layer framework that allows a holistic view towards security issues in cyber-physical systems. In Section V, we conclude and discuss future work within the proposed security framework.

II. Motivations and Related Work

The concept of hierarchical structures has been adopted as solutions for the Internet and manufacturing operations. The well-known layered structure of OSI model for the Internet has influenced the integration between software and hardware [6]. The upper layers of the OSI model represent software that implements network services like encryption and management. The lower layers implement more primitive, hardware-oriented functions like routing, addressing and flow control. The layered structure introduces a practical framework for network technology development at individual layers and also allow cross-layer methods to investigate issues across these virtual boundaries between layers [8].

The integration between enterprise and control systems is guided by ISA95 standards for information exchange between enterprise and manufacturing control activities and their supporting IT systems. It defines levels within a manufacturing operation based on the Purdue Reference Model for Computer Integrated Manufacturing (CIM)[7]. PRM has formed the basis for ISA95 standards today, providing openness necessary to unify plant resource requirements.

The hierarchical viewpoint extends the notion from OSI and PRM models and integrate them for control systems in smart critical infrastructures. The cyber-physical systems we see today incorporate increasingly more smart structures and more sophisticated integrations with many complex systems. The security challenges associated with the evolving systems need to be addressed in the same spirit as in OSI and PRM models.

[†]Q. Zhu and T. Başar are with the Department of Electrical and Computer Engineering and Coordinated Science Laboratory, University of Illinois, 1308 West Main St., Urbana, IL, 61801, USA. E-mail: {zhu31,basar1}@illinois.edu. Research is supported in part by Boeing Company through the Information Trust Institute, University of Illinois at Urbana-Champaign; C. Rieger is with Idaho National Laboratory, 2525 Fremont Ave., Idaho Falls, ID 83402, USA. Email: Craig.Rieger@inl.gov.

Our research is related to resilient control systems proposed in [10], [11], [12]. The goal of a resilient control system is to maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature [10]. To achieve resilience, the control system design is divided into four parallel areas: human systems, complex networks, cyber awareness and data fusion. The hierarchical perspective shares the similar divide-and-conquer philosophy but views the system differently in a hierarchically structured way.

Our work is also related to [13], where a novel framework of security solution for power grid automation has been proposed. The integrated security framework has 3 layers, namely, power, automation & control, and security management. The automation and control system layer monitors and controls power transmission and distribution processes, while the security layer provides security features. Our approach yields a similar security framework. However, each layer has its own functions of security management instead of a centralized security management layer.

III. Control System Security: A Hierarchical Viewpoint

Industrial control systems (ICSs) are commonly seen in many critical infrastructures such as electric generation, transmission and distribution, water treatment, manufacturing, etc. 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 new degrees of automation and human-machine interactions. The uncertainties and hostilities existing in the cyber environment has brought 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. The term resilient control system (RCS) is used to describe systems that have these essential features.

Resiliency of a control system is different from the conventional properties of robustness, adaptiveness, fault-tolerance, and the like [18]. Robustness of ICSs seeks to achieve a certain level of performance with possible modeling errors in the form of parametric or nonparametric uncertainties. Adaptiveness of ICSs aims to attain performances by adjusting control parameters for given uncertain parameters of the controlled process. Fault-tolerance of ICSs focuses on overcoming control failures with identification and precaution measures. These concepts embody very specific goals that a control system needs to achieve.

In the cyber-physical world, resilience is meant to encompass all the afore-mentioned features that allow systems to attain a given level of operational normalcy [10]. It concerns issues that stand at the interface between the cyber world and the physical environment. In the physical world, the controller design can be made to be resilient by incorporating features such as robustness and reliability. In the cyber world, the control system can be protected by many cyber-security measures to ensure dependability, security, and privacy. However, the integration of optimal designs in both worlds does not necessarily ensure overall resiliency of a control system. The interaction between the two environments can create new challenges in addition to the existing ones. To address these challenges, we need to understand the architecture of ICSs. In this paper, we adopt a layering perspective towards ICSs. This view-point has been adopted in many large scale system designs such as the Internet, power systems, nuclear power plants, etc. For example, in smart grids, the hierarchical architecture includes substations, control areas, regions, and then the topological grid. 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 power grid, depicted in Fig. 2, is structured as follows. The power plant is at the physical level and the communication network and security devices are at the network and communication layers. The controller interacts with the communication layer and the physical layer. An administrator is at the supervisory layer to monitor and control the network and the system. Security management is at the highest layer where security policies are made against potential threats from attackers. SCADA is the fundamental monitoring and control architecture at the control area level. The control center of all major U.S. utilities have implemented a supporting SCADA for processing data and coordinating commands to manage power generation and delivery within the EHV and HV (bulk) portion of their own electric power system [15].

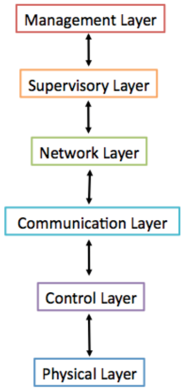

Fig. 1. The hierarchical structure of ICSs composed of 6 layers. The physical layer resides at the bottom level and the management layer at the highest echelon.

The layered structure is also commonly seen in SCADA systems [19]. In large SCADA systems, there is usually a communication network connecting individual PLCs to the operator interface equipment at the central control room. There are communication networks used at lower level in the control system architecture for communication between different PLCs in the same subsystems or facility, as well as for communication between field devices and individual PLCs. Fig. 3 describes typical SCADA network levels, where four

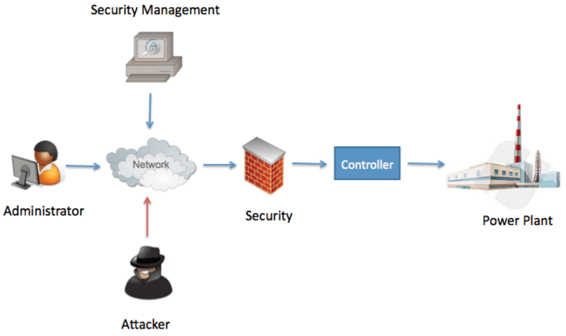

Fig. 2. The hierarchical view towards a power plant.

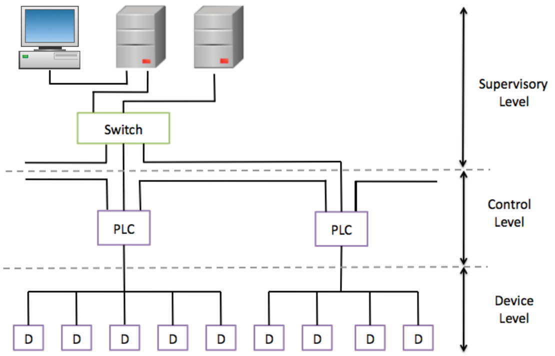

Fig. 3. Typical SCADA network levels.

layers are depicted, namely, supervisory level, communication level, control level and device/physical level.

The information structure of SCADA systems in today's power grids is highly hierarchical. Each primary controller utilizes its own local measurement only, each control area utilizes measurements in its own utility only and has its own SCADA system. Protection mechanisms are preprogrammed to protect individual pieces of equipment and rarely requires communications [16], [17].

To further describe the functions at each layer, we resort to Fig. 4, which conceptually describes a control system with a layering architecture. The lowest level is the physical layer where the physical/chemical processes we need to control or monitor reside. The control layer includes control devices that are encoded with control algorithms that have robust, reliable, secure, fault-tolerant features. The communication layer passes data between devices and different layers. The network layer includes the data packet routing and topological features of control systems. The supervisory layer offers human- machine interactions and capability of centralized decision-making. The management layer makes economic and high-level operational decisions.

A. *Six Architectural Layers*

In subsequent subsections, we identify problems and challenges at each layer and propose problems whose resolution requires a cross-layer viewpoint.

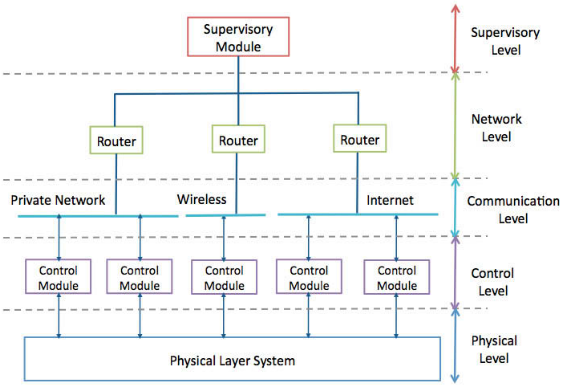

Fig. 4. A conceptual control system with layering

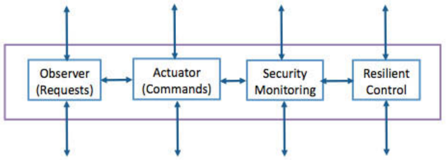

Fig. 5. Control module

1) Physical Layer: Physical layer comprises the physical plant to be controlled. It is often described by an ordinary differential equation (ODE) model from physical or chemical laws. It can also be described by difference equations, Markov models, or model-free statistics. We have the following challenges that pertain to the security and reliability of the physical infrastructure. Firstly, it is important to find appropriate measures to protect the physical infrastructure against vandalism, environmental change, unexpected events, etc. Such measures often need a cost and benefit analysis involving the value assessment of a particular infrastructure. Secondly, it is also essential for engineers to build the physical systems with more dependable components and more reliable architecture. It brings the concern on the physical maintenance of the control system infrastructures that demand a cross-layer decision-making between the management and physical levels.

2) Control Layer: Control layer consists of multiple control components, including observers/sensors, intrusion detection systems (IDSs), actuators and other intelligent control components. An observer has the sensing capability that collects data from the physical layer and may estimate the physical state of the current system. Sensors may need to have redundancies to ensure correct reading of the states. The sensor data can be fused locally or sent to the supervisor level for global fusion. A reliable architecture of sensor data fusion will be a critical concern. An IDS protects the physical layer as well as the communication layer by performing anomaly-based or signature-based intrusion detection. An anomaly-based ID is more common for physical layer whereas a signature-based ID is more common for the packets or traffic at the communication layer. If an intrusion or an anomaly occurs, an IDS raises an alert to the supervisor or work hand in hand with built-in intrusion prevention systems (related to emergency responses, e.g. control reconfiguration) to take immediate action. There lies a fundamental a trade-off between local decisions versus a centralized decision when intrusions are detected. A local decision, for example, made by a prevention system, can react in time to unanticipated events; however, it may incur a high packet drop rate if the local decision suffers high false negative rates due to incomplete information. Hence, it is an important architectural concern on whether the diagnosis and control module need to operate locally with IDS or globally with a supervisor.

3) Communication Layer: Communication layer is where we have a communication channel between control layer components or network layer routers. The communication channel can take multiple forms: wireless, physical cable, blue-tooth, etc. Communication layer handles the data communication between devices or layers. It is an important vehicle that runs between different layers and devices. It can often be vulnerable to attacks such as jamming and eavesdropping. There are also privacy concerns of the data at this layer. Such problems have been studied within the context of wireless communication networks [20]. However, the goal and objective of a critical infrastructure may distinguish themselves from the conventional studies of these issues.

4) Network Layer: Network layer concerns the topology of the architecture. We can see it comprised of two major components: one is network formation and the other is routing. We can randomize our routes to disguise or confuse the attacks so as to achieve certain security or secrecy or minimum delay. Moreover, once a route is chosen, how much data should be sent on that route has been long a concern for researchers in communications [21]. In control systems, many specifics to the data form and rates may allow us to reconsider this problem in a control domain.

5) Supervisory Layer: Supervisory layer coordinates all layers by designing and sending appropriate commands. It can be viewed as the brain of the system. Its main function is to perform critical data analysis or fusion to provide immediate and precise assessment of the situation. It is also a holistic policy maker that distributes resources in an efficient way. The resources include communication resources, maintenance budget as well as control efforts. In centralized control, we have one supervisory module that collects and stores all historical data and serves as a powerful data fusion and signal processing center.

6) Management Layer: 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. At this layer, we deal with problems such as (1) How to budget resources to different systems to accomplish a goal; and (2) How to manage patches for control systems, e.g. disclosure of vulnerabilities to vendors, development and release of patches.

B. Multi-agent Layered Architecture

Multi-agent systems provide richness in the architecture of ICSs. The decentralized agents or plans and the structure of their interactions can yield a performance level that is different from centralized supervisory control. In Fig. 6, we illustrate with an example of multi-agent system where three UAV control systems interact with each other in a networked environment. Each control system can follow its own layering architecture. The interactions between the agents reside at the network, communication and physical layers. At the network layer, the agents may assess the trustworthiness of each other and form a coalition to achieve a global goal [23]. The agents may share the same communication media. Hence, the competition and cooperation for communication resources under threats can be an important problem [22].

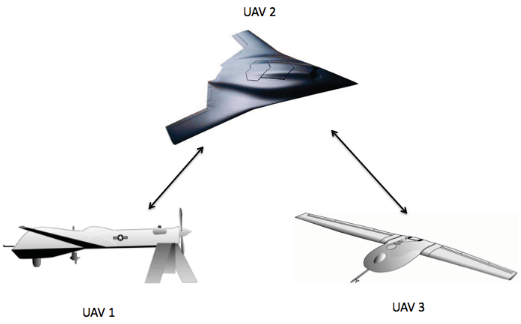

Fig. 6. A multi-agent UAV system

We are interested in addressing in several issues in the multi-agent framework; for example,

- Should agents behave in a selfish or altruist manner in the face of potential attacks?
- How the robustness or security of the entire system is affected when one agent is compromised?
- How should one agent respond, cyber-wise or physical-wise, to a malicious agent together with other agents?

IV. A Cross-Layer Framework

The layering architecture for a control system provides a basis for us to establish a holistic view point on ICS. That is essentially a starting point to consider or design secure control systems. In this section, we describe a cross-layer security model for control systems in CPS. Cyber systems include computers, intrusion detection systems, firewalls, etc. The control system is comprised of sensors, actuators, controllers and physical plants. A supervisor or computer administrator implements the controllers and enhance the security by integrating multiple cyber protection devices such as firewalls, intrusion detectors, etc. An attacker can hamper sensors and actuators through cyber systems or cause direct physical damage to them. The communication between a sensor and a controller is via RS-232, Ethernet or 802.11 wireless.

Let $\mathcal{N} = \{n_1, n_2, \cdots, n_N\}$ be a set of devices that are connected to the cyber world. It can contain a set of sensors, actuators, breakers, etc., for instance, in a power system, flight system, etc. The well-being of a device $n_i, i = 1, 2, \cdots, N$, is described by its state variable s_i which takes real values between 0 and 1. When $s_i = 0$, the device is in a corrupted state while when $s_i = 1$, the device operates as a brand new device.

Note that the state of a device extends broadly to describe the function of its physical component as well as its cyber-communication part with the controller or the plant. The definition of the state depends on the attack model we use. If we assume the goal of an attacker is to corrupt the communication channel, it is convenient to view a communication channel as a stand-alone device. However, if an attacker attempts to corrupt the performance of physical devices from the cyber world, it is more plausible to lump the physical device together with its cyber communication channel and view it as a single device. In the subsequent section, we adopt the latter viewpoint. Consider an attack which aims to compromise a physical device through cyber or physical channels.

The state evolution of the device n_i in discrete-time follows the difference equation

$$s_i(k+1) = a_i s_i(k) + b_i v_i(k) - c_i g_i(k), s_i(0) = 1, k \in \mathbb{Z}_+ \quad (1)$$

where $v_i \in [0,1]$ is the level of maintenance efforts employed by the administrator. $g_i \in [0,1]$ is the control effort used by the attacker who attempts to compromise device n_i. We will describe later the connection between the real-valued variable and the implementable actions. The scalars $b_i, c_i \in \mathbb{R}$ indicate the expertise level or the influence level of the control efforts and attacks respectively. A smaller value of b_i suggests that the device n_i is relatively hard to control and a smaller value of c_i indicates that the attacker has less direct control over the device n_i. a_i is a real-valued number close to 1 that models the lifetime of a physical device without maintenance and attacks. We assume that devices at time $k = 0$ are in excellent operation mode.

A. Security Spaces

From a cyber perspective, the available actions to the administrator to protect device n_i are chosen from a set $\mathcal{L}_i = \{l_1, l_2, \cdots, l_{L_i}\}$, where M_i is the total number of actions. An action $l_j \in \mathcal{L}_i, j = 1, 2, \cdots, L_i$, for device n_i can be, for example, "REPLACE X" ,"REPAIR X", "SHUT DOWN X" etc. If the device is non-physical, an action may suggest "LOAD DETECTION LIBRARY X", "PATCH X","UPDATE SIGNATURE X", "MONITOR X" etc. At every time instant k, an administrator is to choose a set of actions L_i as a subset of $\mathcal{L}_i$. Let $\mathcal{P}_i : \mathcal{B}(\mathcal{L}_i) \to [0,1], i \in \mathcal{N}$, be a mapping that evaluates the security level of a particular set of taken actions. $\mathcal{B}(\mathcal{L}_i)$ is the Borel set of $\mathcal{L}_i$, which is the smallest $\sigma-$algebra containing all subsets of $\mathcal{L}_i$. The mapping $\mathcal{P}_i$ needs to satisfy the following axioms:

(A1) $\mathcal{P}_i(\mathcal{L}_i) = 1$, $\mathcal{P}_i(\emptyset) = 0$.

(A2) $1 \geqslant \mathcal{P}_i(L_i^1) \geqslant \mathcal{P}_i(L_i^2) \geqslant 0$ if $L_i^2 \subseteq L_i^1, L_i^1, L_i^2 \in \mathcal{B}(\mathcal{L}_i)$.

In addition, we may also require the mapping to have the following property: for every $v_i \in [0,1]$, there is a corresponding set L_i that has the minimum size that achieves v_i, i.e.,

$$L_i := \arg \min_{L_i' \in \mathcal{B}(\mathcal{L}_i), \mathcal{P}_i(L_i') \geqslant v_i} \mathcal{P}_i(L_i') \quad (2)$$

The triple $\mathbb{L} = \langle \{\mathcal{L}_i\}_{i=1}^{i=N}, \{\mathcal{B}(\mathcal{L}_i)\}_{i=1}^{i=N}, \{\mathcal{P}_i\}_{i=1}^{i=N} \rangle$ is called a security measure space.

Likewise, an attacker can choose a set of actions A_i to attack the device n_i from a known set $\mathcal{A}_i$. A measure $\mathcal{Q}_i : \mathcal{B}(\mathcal{A}_i) \to [0,1]$ evaluates the attack strength for a set of attack actions. We can define an attack measure space as $\mathbb{A} := \langle \{\mathcal{A}_i\}_{i=1}^{i=N}, \{\mathcal{B}(\mathcal{A}_i)\}_{i=1}^{i=N}, \{\mathcal{Q}_i\}_{i=1}^{i=N} \rangle$. To generalize the model, we can consider multiple attackers and each of them has an attack space triple as above.

B. Dynamic Game Framework

The goal of an administrator is to find an optimal maintenance scheme to improve the well-being of the devices in the network. The attacker on the other hand attempts to compromise the device by his optimal control. Expressing in a mathematical framework, each device n_i encounters a dynamic game against an adversary as follows.

We can model the interaction between an attacker and a defender at device n_i by a zero-sum game. Let the finite-horizon performance index function for (1) be

$$J_i(v_i, g_i) = q_{i,f} s_i^2(K) + \sum_{k=1}^{K} q_{i,k} s_i^2(k) - v_i^2(k). \quad (3)$$

In (3), the goal of a defender is to maximize its well-being with minimum control or maintenance effort while an attacker attempts to maximize the damage to the device.

Therefore, an attacker seeks a strategy to minimize J_i while a defender seeks a policy to maximize the same quantity

$$\max_{v_i} \min_{g_i} J_i(v_i, g_i). \quad (4)$$

We can also consider a scenario where all the devices are maintained by one single administrator. Hence, an administrator needs to solve a team problem:

$$\max_{v} \min_{g} \sum_{i=1}^{N} J_i(v_i, g_i) \quad (5)$$

Note that the dynamics in (1) and the cost function in (3) are decoupled among devices. Hence, maximizing (5) is equivalent to maximizing (3) component-wise. However, we can introduce coupling by imposing a constraint on the total resources available to the administrator, i.e.,

$$\sum_{k=1}^{K} \sum_{i=1}^{N} v_i^2(k) \leqslant V_0. \quad (6)$$

If an attacker attempts to attack multiple devices, he needs to find an optimal allocation of his constrained resources to attack each device. Therefore, in addition to (3) and (5), we can introduce a constraint similar to (6), i.e., $\sum_{k=1}^{K} \sum_{i=1}^{N} g_i^2(k) \leqslant C_0$. Let the pair (v_i^*, g_i^*) be a saddle-point policy to (4) and (u^*, g^*) be a collection of saddle-point policies of all devices.

C. Control System

The well-being of each device can influence the system dynamics of the control system. Let the control system be represented in discrete time by

$$x(k+1) = \overline{A} x(k) + \overline{B} u(k), \quad x(0) = x_0 \quad (7)$$

where $x \in \mathbb{R}^n, u \in \mathbb{R}^m$ and $A \in \mathbb{R}^{n \times n}, B \in \mathbb{R}^{n \times m}$.

Matrices $\overline{A}, \overline{B}$ have dependence on the device states s. For simplicity, we can assume the dependence can be modeled by $\overline{A}(s) = A\Lambda(s)$ and $\overline{B}(s) = B\Sigma(s)$, where $\Lambda(s) \in \mathbb{R}^{n \times n}, \Sigma(s) \in \mathbb{R}^{m \times m}$. Hence, the control system is described by

$$x(k+1) = A\Lambda(s(k))x(k) + B\Sigma(s(k))u(k) \qquad (8)$$

Consider a linear quadratic optimal control problem with cost

$$J(u) = \sum_{k=1}^{K}(x^T(k)Qx(k) + u^T(k)Ru(k)) + x_K^T Q_f x_K \ . \quad (9)$$

An optimal control u^* minimizes $J(u)$ subject to system dynamics (8).

D. Multi-agent System Framework

In this subsection, we use the preceding framework to deal with multi-agent systems, for example, the consensus problem. Let $\mathcal{M}$ be a set of agents in the network. Each agent $j \in \mathcal{M}$ has a set of devices $\mathcal{N}_j = \{n_{j,1}, n_{j,2}, \cdots n_{j,N_j}\}$ and seeks to find a protection scheme $v_j = [v_{j,i}]_{i=1,2,\cdots,N_j}$ to maintain the functionalities of its devices. The interactions among agents can be described by a set of coupled difference equations:

$$\begin{aligned} x_j(k+1) &= A_j\Lambda(s_j(k))x_j(k) + B_j\Sigma(s_j(k))u_j(k) \\ &+ \sum_{m \in \mathcal{M}\backslash\{m\}} A_{mj}(s_m(k), s_j(k))x_m(k) \\ &+ \sum_{m \in \mathcal{M}\backslash\{m\}} B_{mj}(s_m(k), s_j(k))u_m(k), \end{aligned}$$

where $A_{mj}, B_{mj}, j = 1, \cdots, N$ are matrices of appropriate dimensions. Each agent can have its own security policy as a result of (4) or (5). It is interesting to note that the security polices of the agents are interdependent. A compromised agent can affect the state dynamics of other agents and hence their security policies as well. Instead of an adversarial behavior at the lower level, it is also possible to consider malicious agents at the network level within this framework where an agent can affect the overall behavior of the group through sending false information or jamming [22], [23].

V. Conclusion

In this paper, we have proposed a 6-layer security architecture for cyber-physical systems, motivated by the OSI and PRM models. We have addressed the security issues present at each layer and pinpoint a holistic viewpoint for security solutions in CPS. We proposed a game-theoretical model that builds bottom-up from the physical layer and argued that the saddle-point solution to the dynamic game gives rise to a cross-layer security policy. As future work, we intend to apply this general framework to specific power systems and battle-field management systems.

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

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

[3] R. McMillan, "Siemens: Stuxnet worm hit industrial systems," *Computerworld*, Sept. 16, 2010. URL: http://www.computerworld.com/s/article/print/9185419, retrieved Sept. 16, 2010.

[4] "Iran Confirms Stuxnet Worm Halted Centrifuges," *CBS News*, Nov. 29, 2010, URL: http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml.

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

[6] J. F. Kurose and K. W. Ross, *Computer Networking: A Top-Down Approach*, Addison Wesley, 5th edition.

[7] T. J. Williams (Ed.), "A reference model for computer integrated manufacturing (CIM): a description from the viewpoint of industrial automation," prepared by CIM Reference Model Committee International Purdue Workshop on Industrial Computer Systems.

[8] J. Wang, L. Li, S. H. Low and J. C. Doyle, "Cross-Layer optimization in TCP/IP networks," IEEE/ACM Trans. on Networking, vol. 13, no. 3, pp. 582–568, June 2005.

[9] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd edition, Classics in Applied Mathematics, SIAM, Philadelphia, 1999.

[10] 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). IEEE Press, Piscataway, NJ, 629-633.

[11] C. Rieger, "Notional examples and benchmark aspects of a resilient control systems," in Proc. of Intl. Symposium on Resilient Control Systems, 2010.

[12] K. Villez, V. Venkatasubramanian, T. Spinner, R. Rengaswamy, H. Garcia, C. Rieger, "Achieving resilience in critical infrastructures: a case study for a nuclear power plant cooling loop," in Proc. of International Symposium on Resilient Control Systems, 2010.

[13] D. Wei and K. Ji, "Resilient industrial control system (RICS): concepts, formulation, metrics, and insights", in Proc. of Intl. Symposium on Resilient Control Systems, 2010.

[14] K. Moslehi and R. Kumar, "Smart grid - a reliability perspective," in Proc. of Innovative Smart Grid Technologies (ISGT), 2010.

[15] F. F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future", Proc. IEEE, vol. 93, no. 11, pp. 1890 –1909, Nov. 2005.

[16] A. G. Phadke and J. S. Thorp, "Computer Relaying for Power Systems," New York: Wiley, 1988.

[17] M. Ilic, "From hierarchical to open access electric power systems", Proceedings of the IEEE, Vol. 95,No. 5, pp. 1060 – 1084, May 2007

[18] W. Dong, L. Yan, M. Jafari, P. Skare and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in Proc. of Intl. Symposium on Resilient Control Systems, 2010.

[19] Technical Manual, "Supervisory control and data acquisition (SCADA) systems for command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) facilities," Department of the Army, URL: http://www.army.mil/usapa/eng/DR_pubs/dr_a/pdf/tm5_601.pdf

[20] M. Manshaei, Quanyan Zhu, T. Alpcan, T. Başar and J.-P. Hubaux, "Game theory meets network security and privacy", Technical Report EPFL-REPORT-151965, EPFL, 2010.

[21] W. Saad, Quanyan Zhu, T. Başar, Z. Han and A. Hjorungnes, "Hierarchical network formation games in the uplink of multi-hop wireless networks," in Proc. of IEEE Globecom 2009.

[22] S. Bhattacharya and T. Başar, "Graph-theoretic approach for connectivity maintenance in dynamic networks in the presence of a jammer," in Proc. of IEEE Conf. on Decision and Control, Atlanta, Georgia, 2010.

[23] S. Bhattacharya and T. Başar, "Differential game-theoretic approach to a spatial jamming problem," in Proc. of Intl. Symposium on Dynamic Games and Applications 2010.