A New Multilevel Framework for Cyber-Physical System Security

Tianbo Lu[1,2], Bing Xu[1], Xiaobo Guo[1], Lingling Zhao[1], Feng Xie[2]
[1]School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]China Information Technology Security Evaluation Center, Beijing, 100085, China
lutb@bupt.edu.cn

***Abstract*—Cyber-Physical System (CPS) is a system of system which integrates physical system with cyber capability in order to improve the physical performance. It is being widely used in areas closely related to national economy and people's livelihood, therefore CPS security problems have drawn a global attention and an appropriate risk assessment for CPS is in urgent need. In this paper, a security framework for CPS is proposed. Then this paper analyzes the risk assessment on CPS these parts: assets, threat and vulnerability. At last this paper proposes a method of CPS simulation using Matlab, PLC and Emulab.**

Keywords-component; CPS; security; risk assessment; simulation

I. INTRODUCTION

Cyber-physical system (CPS) is a kind of swarm system which combines physical systems with cyber systems. CPS integrates networked computational resources into physical processes in order to add new capabilities into the original system and realize real-time perception, dynamic control, information services in large-scale projects. In the contemporary time, CPS is being applied in nuclear facilities, steel industries, chemical engineering, electric power and many other areas closely related to national economy and people's livelihood. In 2007, U.S. President's Council of Advisors on Science and Technology (PCAST) ranked CPS as a national priority for Federal R&D [1].As with all communication and computer networks, information, security is a big problem which can't be ignored during CPS network development process. CPS system inherits the advantage of wireless sensor networks, next-generation networks and network control system. However, it brings the defect into the network at the same time. CPS is being faced with a series of new security issues, such as security protocols seamless, global trust assessment, collaborative process of privacy protection, etc.

This paper comes up with a security framework on CPS based on the threat analysis, which takes consideration of risk assessment from four angles: assets, threat, vulnerability and damage. At last this paper proposes an idea on CPS simulation using Matlab, PLC and Emulab.

II. CPS SECURITY FRAMEWORK

A. Security Framework

Now the research safety of CPS is focused on the security of information and controlling. Information security solves the problems of information collection, processing and sharing nondestructively in large-scale, high-mix, collaborative autonomous network environment. Its key point is enhancing existing security mechanisms, user privacy protection, efficient processing of massive data encryption, etc. The controlling security solves the controlling problems in the networked systems with open interconnection and loosely-coupled architecture. It focuses on overcoming the influence from attacks on system estimation and control algorithms.

As shown in Figure1, it is a CPS security architecture proposed by this paper. In the cyber filed, multiple security mechanisms for a same security problem is set to realize the defense in depth, using hierarchical network structure and from and starting from each logical hierarchy. In the control field, security threats is analyzed by means of traditional delay, interference, and fault model and security control can be achieved with the use of tolerant control, distributed estimation, robust estimation and etc.

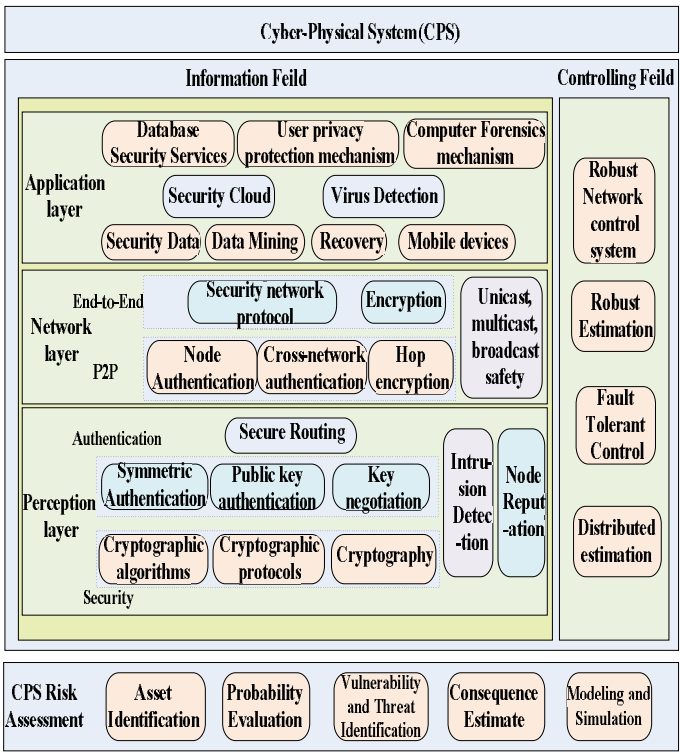

Figure 1. Security framework for CPS

B. Security Structure in the Framework

(1) Security architecture in perception layer

In perception layer of CPS, a closed system composed of sensor network, whose all communication with external networks must depends on the gateway node, the security issues of the sensor network itself is the unique factor to be considered in the design of security architecture. In CPS environment, perception layer is more vulnerable to external cyber-attacks, so establishing intrusion detection and intrusion recovery mechanisms and improving the system robustness is another important issue in perception layer. And establishing a

credibility model, making a behavioral assessment on suspicious nodes and reducing the impact of malicious behavior are important tasks in perception layer. In addition, a mutual trust mechanism between sensor nodes and external networks to ensure the secure transmission of sensory information should be taken into consideration.

(2)Security architecture in network layer

In network layer, both the sensory data and controlling commands are time sensitive, and a large number of heterogeneous networks with different performance and defense capability against cyber-attacks make special security protocols aiming at network specificity an urgent demand. Security architecture can be divided into two sub-layers: point-to-point security sub-layer and end-to-end security sub-layer. The point-to-point security sub-layer could ensure the data security during the hop transmission. Its corresponding security mechanisms include: mutual authentication between nodes, hop encryption and across-network certification. The end-to-end security sub-layer could ensure the end-to-end confidentiality and protect the network availability. Its corresponding security mechanisms include: the end-to-end authentication and key agreement, the key management and cryptographic algorithm selection, the detection and prevention of Dos and DDoS attacks. Further, special security mechanism for unicast, broadcast and multicast should be designed according to the different network communication modes.

(3)Security architecture in application layer

The design of security architecture in application layer must follow the principle of differentiated services. As there is a wide variety of applications of CPS, security requirements are different. Even for the same security service, there may be completely different definition for different users. Therefore, providing targeted security services according to the users' needs is the core idea of the design. The main challenges in the application layer include: hierarchical access to the sensory data and the privacy protection in the user authentication process.

C. Risk Assessment for CPS

CPS is being exposed to various kinds of risks and a well-designed risk assessment for CPS will provide an overall view of CPS security status and support efficient allocations of safeguard resources. When making risk assessment for CPS, 4 elements should be taken into consideration: asset, threat, vulnerability and damage. Asset and damage is positively related and they should be banded together. The final risk value is positively related to the four elements.

Assets are tangible or intangible presence, which have a direct value for business or organization and need to be protected. Assets quantization can be considered from three aspects: direct economic losses, indirect economic losses and casualties. Threat is factors or events that can be a likelihood of potentially damaging from the outside for the assets of enterprises or institutions. The quantification of threat can be conducted through the threat matrix, which have seven angles includes intense, stealth, time, technical personal, information knowledge, physical knowledge and access, proposed by US Sandia Lab [2]. Vulnerability is a kind of condition or environment which exists as corporate or institutional assets and can be utilized by threat to cause a loss to the assets. Vulnerability quantification can be quantified through expert evaluation method or comparison with best practices in industries. Methods can be adopted to simulate the real components, data stream and entity stream of CPS to anticipate what will happen to the whole system and to obtain the possible damage [3].

III. MODELING AND SIMULATION

In CPS simulation, a combination of physical real components and software simulation components can be adapted. Our proposed framework can use simulation for the physical components and an emulation testbed based on Emulab to recreate the cyber components of networked industrial control systems such as SCADA servers and corporate networks. The models of the physical systems are developed using Matlab Simulink, from which the corresponding C code can be generated using Matlab Real Time Workshop. The generated code is executed in real time and can interact with the real components in the emulation testbed. PLC can be a good representative for interaction. From an operational point of view, PLCs receive data from the physical layer, elaborate a "local actuation strategy", and send back commands to the actuators. PLCs execute also the commands that they receive from the SCADA servers (Masters) and additionally provide, whenever requested, detailed physical layer data [3].

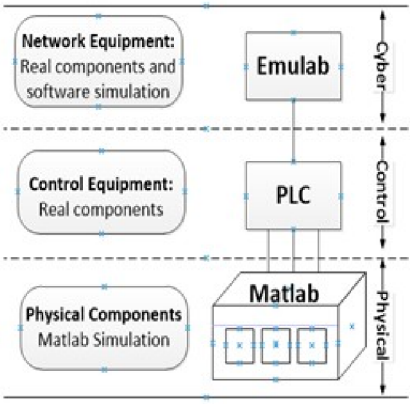

Figure 2. Hierarchical simulation framework for CPS

REFERENCES

[1] Natioanl Institute of Standards and Technology, Cyber-Physical Systems: Situation Analysis of Current Trends,Technologies and Chanllenges, 2012.

[2] Feng Xie and Tianbo Lu, Security Analysis on Cyber-Physical System Using Attack Tree, The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013.

[3] Yong Peng and Tianbo Lu, Cyber-Physical System Risk Assessment, The Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013.