International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.1-16
http://dx.doi.org/10.14257/ijsia.2015.9.7.01

A Security Architecture in Cyber-Physical Systems: Security Theories, Analysis, Simulation and Application Fields

Tianbo Lu[1,3], Jiaxi Lin[1], Lingling Zhao[1], Yang Li[1] and Yong Peng[1,3]

[1]*School of Software Engineering, Beijing University of Posts and Telecommunications, 100876, Beijing, China*
[2]*Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada*
[3]*China Information Technology Security Evaluation Center, 100085, Beijing, China*
lutb@bupt.edu.cn, linjx0515@gmail.com

Abstract

Governments, companies, universities and research institutes are pushing the research and development of cyber-physical systems (CPS). However, the development of cyber-physical systems is constrained by security factors. According to this situation, this paper put forward a CPS security model, which contains security objectives, basic theories, simulation, and CPS framework, summarizes security attacks to cyber-physical systems as a theoretical reference for the study of cyber–physical systems and to provide useful security defense. Based on the cyber-physical systems framework, the paper classifies attacks for the execution layer, transport layer and control layer. The execution layer attacks include security attacks for nodes such as sensors and actuators. Transport layer attacks include data leakage or damage and security issues during massive data integration. Control layer attacks include the loss of user privacy, incorrect access control policies and inadequate security standards. This paper gives security defenses and recommendations for all types of security attacks. Finally, this paper introduces categorizations of CPS application fields and explores their relationships.

Keywords: *Cyber-physical systems (CPS), architecture, security theories, attack analysis, defense analysis, application fields*

1. Introduction

In recent years, the development of computer technology and network technology brought a great convenience to people's lives. With the continuous improvement of computer data handling capacity and the rapid development of data communications capability, people for a variety of computing systems and engineering equipment demand has not only limited expansion capabilities, but more focused on the integration between information systems and physical devices, rational allocation of system resources, system performance optimization, etc. In these conditions, cyber-physical systems came into being, which attract a great attention of governments, companies, universities and research institutes.

Cyber-physical systems are integrations of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computation and vice versa [1]. Cyber-physical systems performance optimization is taken into main consideration on function, which is the collection of computation, communication, control (3C) in the integration of smart technology. Through the combination of 3C technology, real-time perception, dynamic control and information services are

ISSN: 1738-9976 IJSIA

realized in large engineering systems. At the same time, the systems also have many characters, such as real-time, safe, reliable, high-performance and etc. Cyber-physical systems not only have become an important direction in academic research at home and abroad, but also is an advance field in industry.

However, some security factors constrain the development of cyber-physical systems. If the security factors are not taken into consideration, cyber-physical systems cannot operate healthily and stably. First of all, this paper presents a systematic CPS security model, which includes security theories, CPS architecture, attacks and defenses analysis, application fields. Secondly, security objectives and basic theories are introduced in the view of security theory. Thirdly, based on the three layers of CPS architecture, attacks which three layers are facing are summarized in detail. Meanwhile, defenses against attacks are also concluded. Finally, this paper presents a literature map of application fields, in which application fields are clearly classified.

2. CPS Security Architecture

In recent years, academic researches about cyber-physical systems have paid much attention to some security issues, such as safety, security, reliability, resilience, dependability, etc. So do the other theoretical knowledge. They also put forward their own CPS architectures. Few of them combined security theories with the attacks which cyber-physical systems are facing, and provide recommendations and defenses. The CPS security architecture we put forward successfully addresses these issues. At the same time, a literature map of application fields is presented, and in which they are systematically classified.

This paper describes our CPS security architecture from three aspects (Figure 1). One of them is CPS security theories, which contains security objectives and basic theories. Security objectives provide a sort of goals which CPS should achieve. Without security objectives, such as safety, security, reliability and resilience, we could not know in which conditions CPS cannot operate healthily and stably. Basic theories usually contain information theory, control theory and game theory, which provide theoretical support for CPS research.

The other one is the analysis of attacks and defenses from the three layers of CPS architecture. We propose a three-layer CPS architecture, which consists of execution layer, transport layer and control layer. Based on the CPS architecture, the paper analyzes attacks and defenses in the view of the three layers.

Another is simulation and application. From different technical means in CPS, we divide simulation into three categories, physical simulation, mathematical simulation and hardware-in-the-loop simulation. Then we summarize and arrange the existing literatures in the application fields of CPS, such as smart grid, medical device, automobile and aircraft, and present a literature map.

We will discuss the several aspects detailedly in the following content.

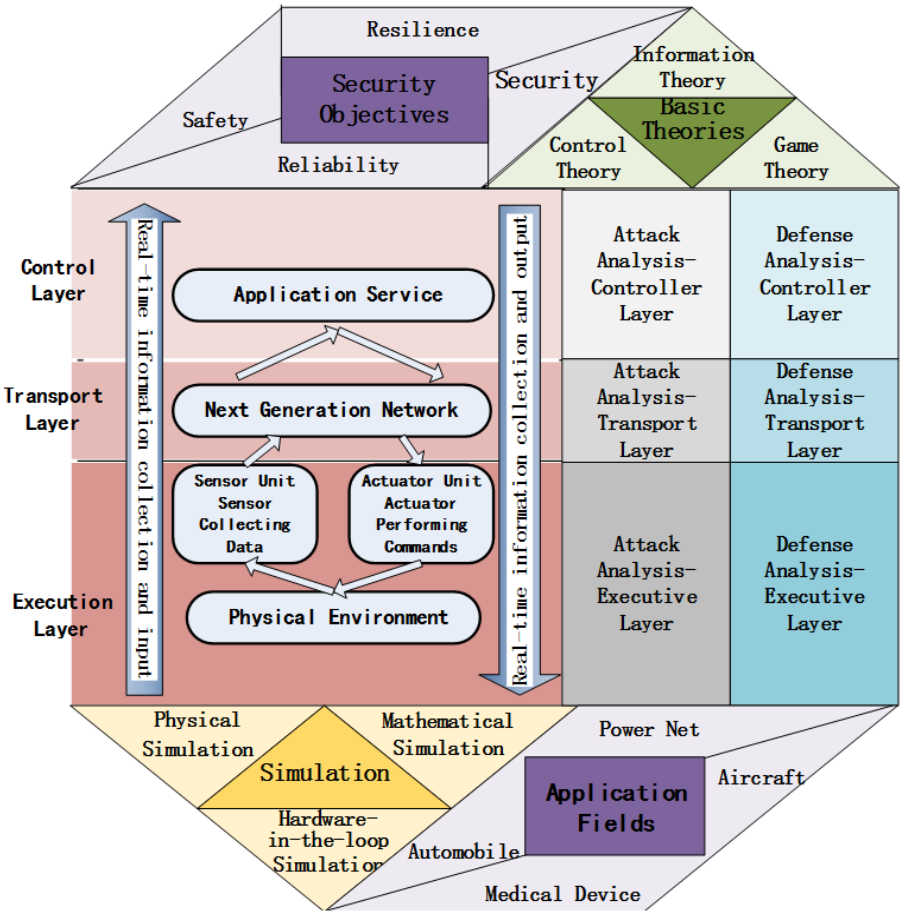

Figure 1. CPS Security Architecture

3. CPS Security Theories

In this section, combining the security requirement of the cyber-physical system and the important literature which research the security of CPS in the academe, we summarize the security objectives the CPS should achieve. Besides, we present three basic theories which are widely used in cyber-physical systems. Figure 2 shows the literature map of the CPS security theories using in this paper.

3.1 Security Objectives

3.1.1 Safety: In industrial applications, with a control system in charge of the technological process, typically safety was considered a critical property. Computer systems were designed such that the behavior of computer software or hardware would not endanger the environment in a sense that equipment's failure would cause death, loss of limbs or large financial losses [2].

In the ISO 60601 standard for safety of medical electrical equipment, we can find the most generic definition of safety for cyber-physical systems. In this standard, safety is defined as the avoidance of hazards due to the operation of a medical device under normal or single fault condition [3]. This definition can also be applied to cyber-physical systems in general non-medical domains by broadening the scope of hazards considered.

Safety is a property of any system by virtue of which it can be guaranteed that there will be no harm to the infrastructure and to the physical environment during normal or faulty operation of the system [4].

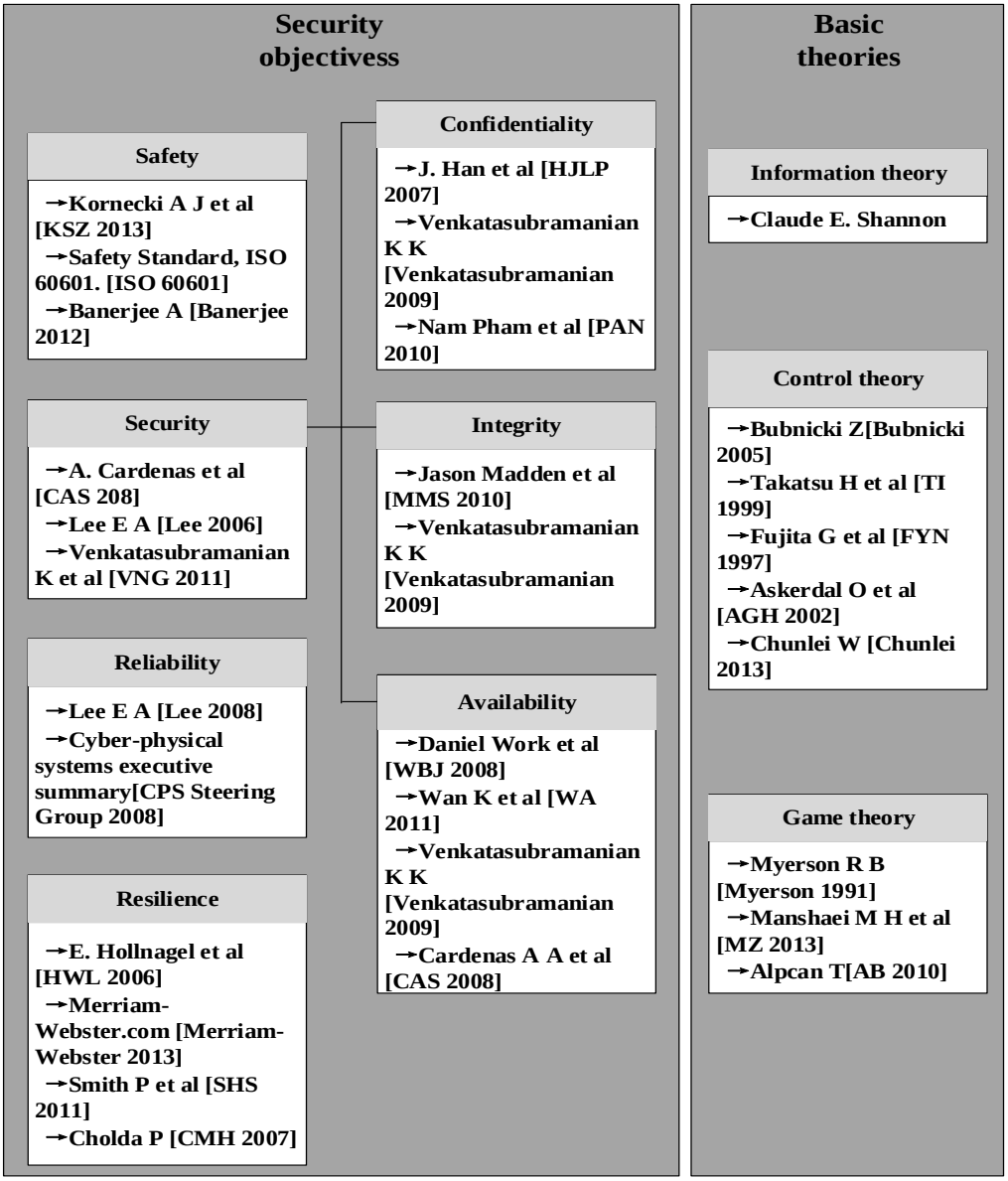

Figure 2. Literature Map of CPS Security Theories

3.1.2 Security: In cyber-physical systems, security can be categorized into two classes: information security which is mainly focused on encryption and data security, and secure control theory which studies how cyber attacks affect the control systems' physical dynamics [5].

Lee considered security as the ability to deliver service under given conditions for a given time without unauthorized disclosure or alteration of sensitive information [6].

Security is defined as the ability to ensure that both data and the operational capabilities of the system can only be accessed when authorized in cyber-physical systems,. For cyber-physical systems, security is a relatively new area. As with any new field most of the effort seems to be focused on efficiently mapping solutions

from existing domains [7]. The need for security in cyber-physical systems is manifold. Some of main factors are as follows.

- Confidentiality—Confidentiality refers to the capability to prevent the disclosure of information to unauthorized individuals or systems [8]. In [9], confidentiality is also defined as the ability to hide data.

[10] considered that confidentiality is necessary (but not sufficient) for maintaining the users' privacy in Cyber Physical Systems.

Realizing Confidentiality in CPS must prevent an adversary from inferring the state of the physical system by eavesdropping on the communication channels between the sensors and the controller, as well as between the controller and the actuator.

- Integrity—Integrity refers to data or resources cannot be modified without authorization. Integrity is violated when an adversary accidentally or with malicious intent modifies or deletes important data; and then the receivers receive false data and believe it to be true. Integrity in CPS could be the capability to achieve the physical goals by preventing, detecting, or blocking deception attacks on the information sent and received by the sensors and the actuators or controllers [11].

Ensuring data integrity requires the ability to detect any changes introduced (maliciously or otherwise) in the message being communicated. This is usually done using a message digest – a one way (hash) function which takes as input the data whose integrity is being protected and produces a fix length random value called a digest. As the function is one-way in nature, given the digest it is computationally infeasible to re-create the input, further even a on-bit change in the input produces a drastically different output [9].

- Availability—For any system to serve its purpose, the service must be available when it is needed. It means that the cyber systems used to store and process the information, the physical controls used to perform physical process, and the communication channels used to access it must be functioning correctly. High availability [12] of CPS aims to always provide service by preventing computing, controls, communication corruptions due to hardware failures, system upgrades, power outages or denial-of-service attacks.

Ensuring that any entity which uses the data and services and resources of the system able to do when required. Critical processes, physical devices and their services must be available with least interruption [9]. In case of denial of service, some entity must be responsible to explain why it happened and ensure it does not happen again [13].

A lack of confidentiality results in disclosure, when an unauthorized entity gains access to data. A lack of integrity leads to deception – when an authorized party receives false data and believes it is true. While a lack of availability results in denial of service (DoS) when an authorized entity cannot receive commands or data. Deception, disclosure and DoS are three basic types of cyber-attacks on CPS [5].

3.1.3 Reliability: Reliability has been recognized as a critical requirement for cyber-physical systems. In Lee's paper "Cyber Physical Systems: Design Challenges", he pointed out that the expectation of reliability in cyber-physical systems will only increase, and cyber-physical systems will not be deployed into some mission critical applications as traffic control, automotive safety, and health care without improved reliability and predictability [14]. CPS steering group stated in its executive summary that architectures and tools are needed in order to build reliable and resilient cyber-physical systems [15]. The report also described software reliability affects the overall system reliability because replicated software can cause systematic failures that are not common in purely physical systems and

todays computer systems do not allow us to distribute computer-based control in ways that preserve reliability.

3.1.4 Resilience: In control systems, resilience is an important property, since the system must remain stable in presence of unexpected conditions and threats, including the prevention or mitigation of unsafe, hazardous or compromising conditions that threaten its operation [22]. By definition, resilience is an ability to recover from or easily adjust to misfortune or change [23], which is viewed today, more than ever before, as a major requirement and design objective.

[24] presents fundamental elements of resilience such as metrics, policies, and information sensing mechanisms, which drives the design of a distribute multilevel architecture that lets the network defend itself against, detect, and dynamically respond to challenges.

[CMH 2007] presents a comprehensive survey of research efforts related to resilience differentiation in the Internet and telecommunications networks. The article also presents a general framework classification which is used as the basis for the subsequent review of the relevant literature.

3.2 Basic Theories

3.2.1 Information Theory: Information theory is a branch of applied mathematics, electrical engineering, and computer science involving the quantification of information. Information theory was developed by Claude E. Shannon to find fundamental limits on signal processing operations such as compressing data and on reliably storing and communicating data.

3.2.2 Control Theory: Control theory is an interdisciplinary branch of engineering and mathematics that deals with the behavior of dynamical systems. With the deepening of the research, modern control theory has a little different from classical control theory. [16] defined modern control theory as a discipline dealing with formal foundations of the analysis and design of computer control and management systems.

Control theory can be widely applied in industrial control system. [17] reported the situation and directions of control theory which had been practically applied to Japanese industries. [18] applied H^{∞} control theory to the power system stabilization control. Adopted from control theory, [19] developed a composite methodology for analyzing the effect of data errors on control systems dependability. [20] propose a unified modeling framework for cyber-physical systems, monitors, and attacks, in which monitors leverage on tools from control theory and distributed computing, and attack design method relies upon the control-theoretic notion of controlled invariant subspace. [21] proposed a network security validation model based on adaptive control theory to validate network security in dynamic network environment.

3.2.3 Game Theory: Game theory is a study of strategic decision making. In [26], it is defined as the study of mathematical models of conflict and cooperation between intelligent rational decision-makers. It is widely used in economics, political science, and psychology, as well as logic, computer science, and biology.

Game theory can also be applied to the security of cyber-physical systems. Recently, it has been used as a quantitative method for analyzing security policies and designing defense mechanisms. [27] summarized equilibrium analysis and security mechanism designs by using game-theoretic approaches. [28] applied game theory to understanding diverse network security problems. [29] develops new

game-theoretic frameworks for addressing security and resilience problems residing at multiple layers of the cyber-physical systems including robust and resilient control, secure network routing and management of information security and smart grid energy systems.

4. CPS Architecture

In the early stage, CPS architecture had a two-layer structure inherently, the physical part and the cyber part. The physical part senses physical environment, collects data, performs commands from the cyber part. The cyber part analyzes and processes the data from the physical part and rise commands.

In some literatures [30, 31, 32], a few of new CPS architectures were put forward, some of which were not hierarchical. Although [32] put forward a three-tiers of CPS architecture, the description of which was also vague.

In this paper, we propose a three-layer CPS architecture, as shown in Figure 3, which consists of execution layer, transport layer and control layer.

- Execution layer—Besides a target environment, execution layer consists of various physical devices, such as sensor, actuator, RFID (radio frequency identification) tags, RFID readers, mobile intelligent terminal and etc., which is in charge of collecting data from physical environment and performing commands.

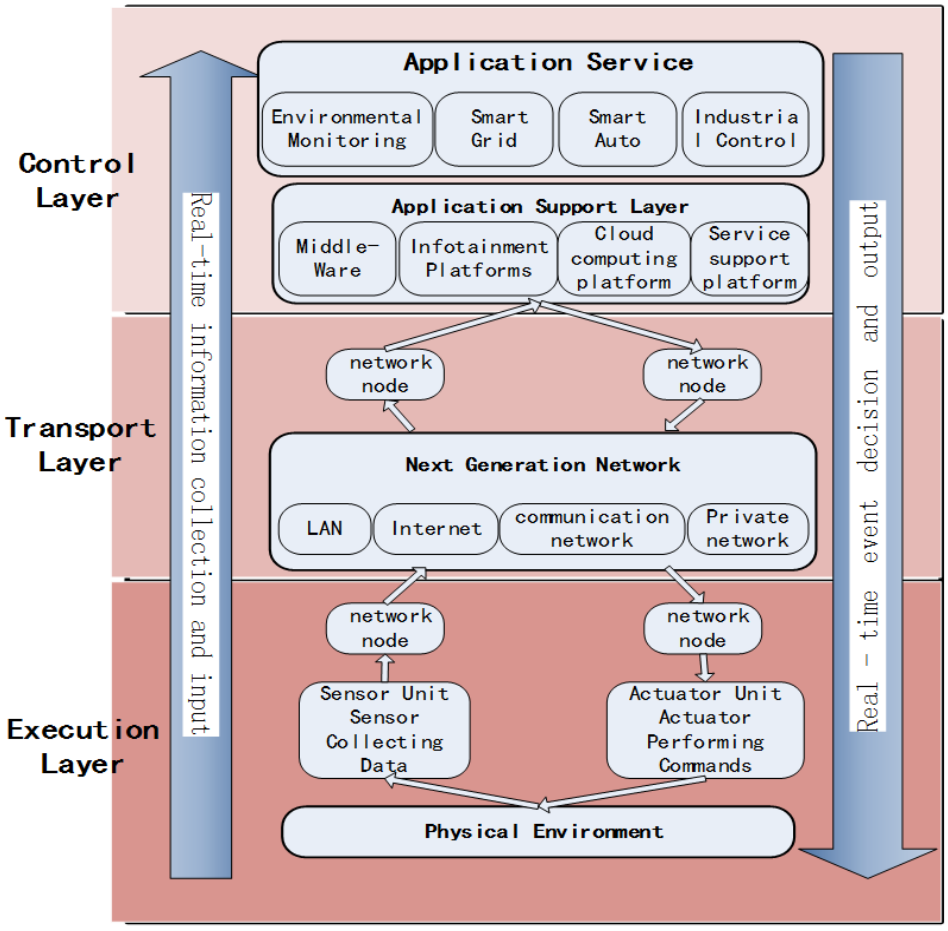

Figure 3. CPS Architecture

- Transport layer—The next generation network supports transport layer, the main technical methods of which contain LAN, Internet, communication network

and private network. Transport layer not only realizes real-time transmission, but also has the ability to process and manage amounts of data.

- Control layer—Control layer is the key part of the interaction between the cyber part and the physical part. Control layer process the data which is collected from sensors and generate commands which will feedback to actuator in execute layer through transport layer. As a part of control layer, application support layer makes use of middle-ware, infotainment platform, cloud computing platform, service support platform and etc. Combining control layer with various industries, environmental monitoring, smart grid, smart auto, and industry control come into being.

Based on the CPS architecture, the paper classifies attacks for the execution layer, transport layer and control layer, as shown in Figure 4. The execution layer attacks include security attacks for nodes such as sensors and actuators. Transport layer attacks include data leakage or damage and security issues during massive data integration. Control layer attacks include the loss of user privacy, incorrect access control policies and inadequate security standards.

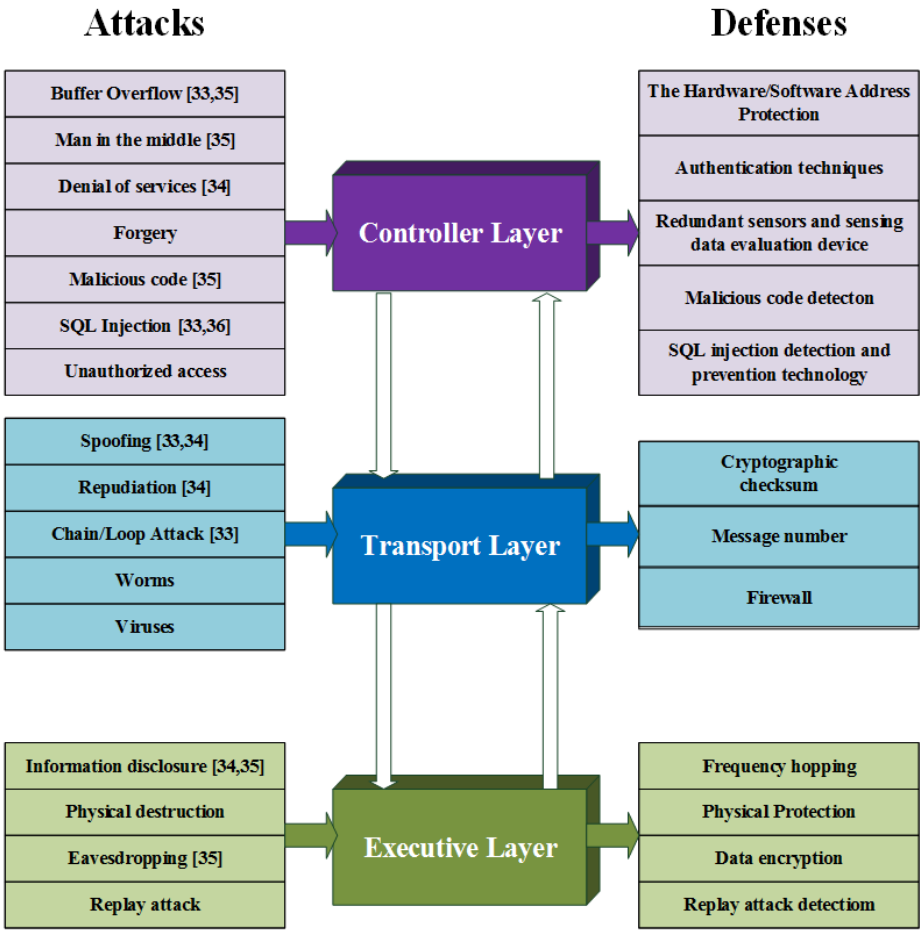

Figure 4. Layer Attacks and Defenses on CPS

The British Columbia Institute of Technology (BCIT) maintains an industrial cyber security incident database, which includes deliberate events such as external hacks, Denial of Service (DoS) attacks, and virus/worms infiltrations. Zhu B et al [33] focus on systematically identifying and classifying likely cyber attacks including cyber-induced cyber-physical attacks on SCADA systems, such as database attacks, man in the middle attacks, buffer overflow and SQL injection in

control layer, spoofing, Chain/Loop Attack and flood in transport layer. Yampolskiy M *et al*. [34] analyze cyber-attacks, such as information disclosure in executive layer, spoofing, repudiation in transport layer, denial of service in control layer. They [35] propose a taxonomy for description of attacks on CPS. Each taxonomy of attacks, such as buffer overflow attack, information disclosure, malicious code, eavesdropping and et al, is defined as influenced element, influence, victim element, impact on victim, attack means and preconditions. Kindy D A *et al*. [36] present a detailed review on various types of SQL injection attacks, vulnerabilities, and prevention techniques. Tran T T *et al*. [37] focus on replay attacks and propose a new detection scheme for replay attacks based on a solution originally developed for a control system.

5. Simulation and Application Fields

5.1 Simulation

From different technical means in CPS, simulation can be divided into three categories, physical simulation, mathematical simulation and hardware-in-the-loop simulation. In recent years, among them, hardware-in-the-loop simulation is the most popular in academe.

5.1.1 Physical Simulation: A physical simulation is defined as simulation in which physical objects are substituted for the thing in physical environment. These physical objects are often chosen for the reason that they are smaller or cheaper than the actual object or system.

However, physical simulation is different from physical testing. While all physical simulation contains physical testing, the key difference is that the former attempts to replicate the precise physical parameters actual object on a laboratory scale in a way that the resultant data can be used to solve real-world problems.

5.1.2 Mathematical Simulation: A mathematical simulation is a simulation, run on a single computer, or a network of computer, to reproduce behavior of a system via a mathematical model, which is described by using mathematical concepts and language.

Mathematical simulations have been widely modeling many natural systems not only in physics, chemistry and biology, and human systems in economics and social science but also in engineering to gain insight into the operation of those systems. Zufia A et al [38] build up a Mathematical model, working on a PC, able to simulate the controlled cooling of wire rods in an EDC conveyor.

5.1.3 Hardware-in-the-loop Simulation: Ledin J A [39] defines hardware-in-the-loop simulation as a technique for performing system-level testing of embedded systems in a comprehensive, cost-effective, and repeatable manner.

A wide variety of systems apply the HIL simulation test concept from relatively simple devices to complex systems. Isermann R *et al*. [40] give an overview of the various kinds of real-time and HIL simulation, discuss HIL simulation for relatively slow processes, and show the HIL simulation of combustion engines in detail. Bouscayrol A [41] suggests three different kinds of HIL simulation: signal level, power level, and mechanical level. Steurer M *et al*. [42] apply a 5-MW variable voltage source amplifier converter in power hardware-in-the-loop experiments with megawatt-scale motor drives.

5.2 Application Fields

In application fields of cyber-physical systems, researchers usually focus on the fields of smart grid, medical device, automobile and aircraft. Based on the exiting literatures, especially what has been publish in recent year, we summarize and arrange them, as shown in figure 5. In Figure 5, solid arrows demote an explicit inheritance, *i.e.*, actual usage of a previously publish idea; dotted lines denote they have the same authors.

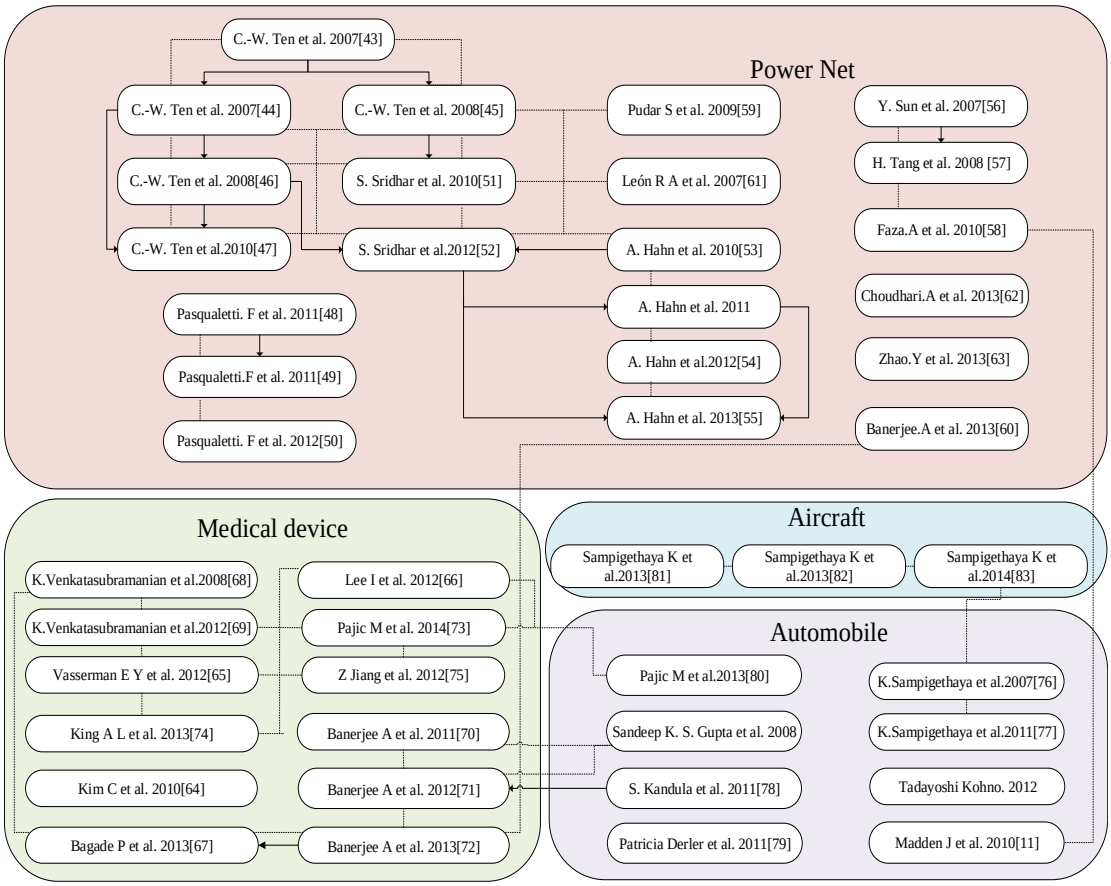

Figure 5 Literature map of application fields

5.2.1 Power Net: C.-W. Ten *et al.* [43-47] proposes a vulnerability assessment methodology to systematically evaluate the vulnerabilities of systems at three levels: system, scenarios, and access points using attack tress. Pudar S *et al.* [59] propose Petri Net Attack Modeling by extending the attack trees with new modeling contructs and analysis approaches. Pasqualetti. F *et al.* [48] provide a necessary and sufficient graph theoretic condition for the existence of vulnerabilities that are inherent to the power network interconnection structure and [49, 50] proposes a unified framework and a distribute method to monitor the operating condition of a power network. S. Sridhar *et al.* [51] extend cyber security attack concepts to control systems in an electric power system and [52] introduce a layered approach to evaluating risk based on the security of both the physical power applications and the supporting cyber infrastructure. A. Hahn *et al.* [31, 53-55] introduce current vulnerability disclosure methods, design and implement a testbed while proposing cyber attack scenarios which will negatively affect grid operations, and provide an overview of a smart grid security testbed which required to provide an accurate cyber-physical environment. Y.Sun *et al.* [56], H.Tang *et al.* [57], Faza.A *et al.* [58]

study noninterference, security and quantitative reliability in smart grid. Banerjee A et al [60] propose an error-bound hybrid simulator that simulates energy interactions in a cyber-physical energy system and evaluate the accuracy of the simulator. León R A *et al.* [61] propose a novel conceptual design for an application of wireless sensor technology for assessing the structural health of transmission lines and their implementation to improve the observability and reliability of power systems. Choudhari A *et al*. [62] present a distributed algorithm to adaptively schedule power transfers between nodes in a smart power grid in such a way that the stability of both the computer network and the physical system are maintained. Y Zhao *et al*. [63] put forward a solution of the entire set of the sparsest unobservable attacks in polynomial time.

5.2.2 Medical Device: Kim C *et al.* [64] introduce the Network-Aware Supervisory System to integrate medical devices into such a clinical interoperability system that uses real networks. Vasserman E Y *et al.* 2012 [65] define a failure model, or the specific ways in which IMD (Interoperable medical device) environments might fail when attacked. Lee I *et al*. [66] and Bagade P *et al*. [67] discuss the challenges in developing MCPS (Medical cyber-physical systems). Venkatasubramanian K *et al*. [68, 69] provide an overview of the IMD (Interoperable medical device) environment and the attacks, and present Ayushman system. [70, 71, 72] propose CPS-MAS, a cyber-physical medical system modeling and analysis framework, and a time and space bound LlSTHA reachability analysis algorithm for safety verification. Pajic M *et al*. [73] and King A L [74] both present a verification approach to establish the safety properties of medical cyber-physical systems. Jiang Z *et al*. [75] present a methodology to construct a timed-automata model for functional and formal testing and verification of the closed-loop system.

5.2.3 Automobile: Base on the characteristics of vehicular ad hoc networks, Sampigethaya K *et al*. [76, 77] propose a scheme called AMOEBA, which provides location privacy by utilizing the group navigation of vehicles. Kandula S *et al.* [78] propose modeling abstractions by using AVs (Autonomous Vehicles) and enable safety analysis without requiring any expertise on formal methods. Derler P *et al*. [79] use a portion of aircraft vehicle management systems to illustrate the challenges of the intrinsic heterogeneity, concurrency, and sensitivity to timing. Pajic M *et al.* [80] introduce a design framework for development of high-confidence vehicular control systems that can be used in adversarial environments. Madden J *et al*. [11] describe that a vehicle composed of an embedded computer system, its operator, and its environment show how information is disclosed to an observer that is watching from the outside to illustrate new security challenges in CPS. Gupta [84] present a critical modeling framework and depict its applicability to various of crises management.

5.2.4 Aircraft: Sampigethaya K *et al*. [81, 82, 83] present CPS challenges and solutions aircraft, and propose a novel CPS framework to understand the cyber layer and cyber-physical interactions in aviation.

6. Conclusion

Cyber-physical systems are supposed to play an important role in the design of future engineering systems. Meanwhile, its security issues attract more and more attention not only in academe research at home and aboard but also in an advance field of industry. In this paper, we present a novel CPS security architecture, and describe it in three aspects in detail. One of the aspects is security theories, which

contain security objectives and basic theories. Security objectives include safety, security, reliability and resilience, and basic theories consist of information theory, control theory and game theory. The other aspect is CPS three-layer architecture (control layer, transport layer and executive layer) which we propose and the analysis of attacks and defenses in three layers. Another aspect is simulation and application fields. Based on different technical means in CPS, we divide simulation into three categories, physical simulation, mathematical simulation and hardware-in-the-loop simulation. We also present a literature map of application fields, which contains the exiting literatures, especially what has been publish in recent year. This is unsatisfactory, and hopefully, by providing a novel CPS security architecture and a literature map of application field, this paper will contribute in CPS security researches, and help researchers, operators and others to target their effort efficiently.

Acknowledgments

This work is supported by the following programs: the National Natural Science Foundation of China under Grant No.61170273; the China Scholarship Council under Grant No.[2013]3050; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (NO. CAAC-ITRB-201201);2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software".

References

[1] E. Lee, "Computing foundations and practice for cyber-physical systems: A preliminary report", technical report, UCB/EECS2007-72 [R]. Berkeley, USA: University of California at Berkeley, **(2007).**
[2] A J. Kornecki, N. Subramanian and J. Zalewski, "Studying interrelationships of safety and security for software assurance in cyber-physical systems: Approach based on bayesian belief networks[C]", Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on. IEEE, **(2013)**, pp. 1393-1399.
[3] Safety Standard, ISO 60601. [Online].Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=.
[4] A. Banerjee, "Model Based Safety Analysis and Verification of Cyber-Physical Systems [D]", Arizona State University, **(2012)**.
[5] A. A. Cardenas, S. Amin and S. Sastry, "Secure control: Towards survivable cyber-physical systems [J]", System, **(2008)**, 1(a2): a3.
[6] E A. Lee, "Cyber-physical systems-are computing foundations adequate[C]", Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, **(2006)**.
[7] K. Venkatasubramanian, S. Nabar, S. K. Gupta and R. Poovendran, "Cyber physical security solutions for pervasive health monitoring systems [J]", Watfa, Ed. IGI Global, (**2011**).
[8] J. Han, A. Jain, M. Luk, and A. Perrig, "Don't sweat your privacy: Using humidity to detect human presence", In Proceedings of 5th International Workshop on Privacy in UbiComp (UbiPriv'07), September **(2007)**.
[9] K K. Venkatasubramanian, "Security solutions for cyber-physical systems [D]", Arizona State University, **(2009)**.
[10] N. Pham, T. Abdelzaher and S. Nath, "On Bounding Data Stream Privacy in Distributed Cyber-physical Systems", 2010 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, **(2010)**.
[11] J. Madden, B. McMillin, and A. Sinha, "Environmental Obfuscation of a Cyber Physical System - Vehicle Example", Workshop On 34th Annual IEEE Computer Software and Applications Conference, **(2010)**.
[12] D. Work, A. Bayen and Q. Jacobson, "Automotive Cyber Physical Systems in the Context of Human Mobility", National Workshop on High-Confidence Automotive Cyber-Physical Systems, Troy, MI, **(2008)**.
[13] K. Wan and V. Alagar, "Dependable Context-Sensitive Services in Cyber Physical Systems[C]", Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on. IEEE, **(2011)**, pp. 687-694.
[14] E A. Lee, "Cyber physical systems: Design challenges [C]", Object Oriented Real-Time Distributed Computing (ISORC), 2008 11th IEEE International Symposium on. IEEE, **(2008)**, pp. 363-369.

[15] CPS Steering Group, "Cyber-physical systems executive summary [J]", CPS Summit, **(2008)**.
[16] Z. Bubnicki, "Modern control theory [M]", Berlin: Springer, (**2005**).
[17] H. Takatsu and T. Itoh, "Future needs for control theory in industry-report of the control technology survey in Japanese industry [J]", Control Systems Technology, IEEE Transactions on, (**1999**), vol. 7, no. 3, pp. 298-305.
[18] G. Fujita, R. Yokoyama, T. Niimura, D. Makita, S. Takeuchi and G. Shirai, "Power system stabilizing control using variable series capacitor based on H∞ control theory considering AVR and governor[C]", Electrical and Computer Engineering, 1997, Engineering Innovation: Voyage of Discovery. IEEE 1997 Canadian Conference on. IEEE, vol. 1, **(1997)**, pp. 43-46.
[19] O. Askerdal, M. Gafvert, M. Hiller and N. Suri, "A control theory approach for analyzing the effects of data errors in safety-critical control systems [C]", Dependable Computing, 2002. Proceedings. 2002 Pacific Rim International Symposium on. IEEE, **(2002**), pp. 105-114.
[20] F. Pasqualetti, "Secure control systems: A control-theoretic approach to cyber-physical security [D]", UNIVERSITY OF CALIFORNIA Santa Barbara, **(2012)**.
[21] W. Chunlei, "Dynamically validate network security based on adaptive control theory [C]", Information and Network Security (ICINS 2013), 2013 International Conference on. IET, **(2013),** pp. 1-6.
[22] E. Hollnagel, D. D. Woods and N. Leveson, "Resilience Engineering: Concepts and Precepts", Ashgate Publishing, **(2006)**.
[23] Merriam-Webster.com. Merriam-Webster, n.d. Web. http://www.merriam-webster.com/dictionary/resilience. Accessed 9 Oct **(2013)**
[24] P. Smith, D. Hutchison, J. P. Sterbenz, M. Scholler, A. Fessi, M. Karaliopoulos and B. Plattner, "Network resilience: a systematic approach [J]", Communications Magazine, IEEE, vol. 49, no. 7, **(2011)**, pp. 88-97.
[25] P. Cholda, A. Mykkeltveit, B. E. Helvik, O. J. Wittner and A. Jajszczyk, "A survey of resilience differentiation frameworks in communication networks [J]", Communications Surveys & Tutorials, IEEE, vol. 9, no. 4, **(2007)**, pp. 32-55.
[26] R B. Myerson, "Game theory: analysis of conflict [J]", Harvard University, **(1991)**.
[27] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar and J. P. Hubaux, "Game theory meets network security and privacy [J]", ACM Computing Surveys (CSUR), vol. 45, no. 3, **(2013)**, p. 25.
[28] T. Alpcan and T. Baar, "Network security: A decision and game-theoretic approach [M]", Cambridge University Press, **(2010)**.
[29] Q. Zhu, "Game-theoretic methods for security and resilience in cyber-physical systems [D]", University of Illinois at Urbana-Champaign, **(2013)**.
[30] L. Miclea and T. Sanislav, "About dependability in cyber-physical systems [C]", Design & Test Symposium (EWDTS), 2011 9th East-West. IEEE, **(2011),** pp. 17-21.
[31] A. Ashok, A. Hahn and M. Govindarasu, "A cyber-physical security testbed for smart grid: System architecture and studies [C]", Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, ACM, **(2011)**, p. 20.
[32] H J. La and S D. Kim, "A service-based approach to designing cyber physical systems[C]", Computer and Information Science (ICIS), 2010 IEEE/ACIS 9th International Conference on. IEEE, **(2010)**, pp. 895-900.
[33] B. Zhu, A. Joseph and S. Sastry, "A taxonomy of cyber attacks on SCADA systems[C]", Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, IEEE, **(2011)**, pp. 380-388.
[34] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, "Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach[C]", Resilient Control Systems (ISRCS), 2012 5th International Symposium on. IEEE, **(2012),** pp. 55-62.
[35] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on CPS[C]", Proceedings of the 2nd ACM international conference on High confidence networked systems, ACM, **(2013)**, pp. 135-142.
[36] D A. Kindy and A S K. Pathan, "A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques [J]", **(2011)**.
[37] T T. Tran, O S. Shin and J H. Lee, "Detection of replay attacks in smart grid systems[C]", Computing, Management and Telecommunications (ComManTel), 2013 International Conference on. IEEE, **(2013)**: 298-302.
[38] A. Zufia and J M. Llanos, "Mathematical simulation and controlled cooling in an EDC conveyor of a wire rod rolling mill [J]", ISIJ international, vol. 41, no. 10, **(2001)**, pp. 1282-1288.
[39] J A. Ledin, "Hardware-in-the-loop simulation [J]", Embedded Systems Programming, vol. 12, **(1999)**, pp. 42-62.
[40] R. Isermann, J. Schaffnit and S. Sinsel, "Hardware-in-the-loop simulation for the design and testing of engine-control systems [J]", Control Engineering Practice, vol. 7, no. 5, **(1999)**, pp. 643-653.
[41] A. Bouscayrol, "Different types of hardware-in-the-loop simulation for electric drives[C]", Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on. IEEE, **(2008),** pp. 2146-2151.

[42] M. Steurer, C. S. Edrington, M. Sloderbeck, W. Ren and J. Langston, "A megawatt-scale power hardware-in-the-loop simulation setup for motor drives [J]", Industrial Electronics, IEEE Transactions on, vol. 57, no. 4, **(2010)**, pp. 1254-1260.
[43] C W. Ten, C C. Liu and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees [C]", Power Engineering Society General Meeting, 2007. IEEE. IEEE, **(2007)**, pp. 1-8.
[44] C W. Ten, M. Govindarasu and C C. Liu, "Cybersecurity for electric power control and automation systems [C]", Systems, Man and Cybernetics, 2007. ISIC. IEEE International Conference on. IEEE, **(2007**), pp. 29-34.
[45] C W. Ten, C C. Liu and M. Govindarasu, "Cyber-vulnerability of power grid monitoring and control systems [C]", Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, ACM, **(2008)**, p. 43.
[46] C W. Ten, C C. Liu and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems [J]", Power Systems, IEEE Transactions on, vol. 23, no. 4, **(2008)**, pp. 1836-1846.
[47] C W. Ten, G. Manimaran and C C. Liu, "Cybersecurity for critical infrastructures: attack and defense modeling [J]", Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, vol. 40, no. 4, **(2010)**, pp. 853-865.
[48] F. Pasqualetti, A. Bicchi and F. Bullo, "A graph-theoretical characterization of power network vulnerabilities[C]", American Control Conference (ACC), 2011. IEEE, **(2011)**, pp. 3918-3923.
[49] F. Pasqualetti, F. Dorfler and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design [C]", Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on. IEEE, **(2011),** pp. 2195-2201.
[50] F. Pasqualetti, R. Carli and F. Bullo, "Distributed estimation via iterative projections with application to power network monitoring [J]", Automatica, vol. 48, no. 5, **(2012)**, pp. 747-758.
[51] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system [C]", Power and Energy Society General Meeting, 2010 IEEE. IEEE, **(2010),** pp. 1-6.
[52] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–physical system security for the electric power grid [J]", Proceedings of the IEEE, vol. 100, no. 1, **(2012)**, pp. 210-224.
[53] A. Hahn, B. Kregel, M. Govindarasu, J. Fitzpatrick, R. Adnan, S. Sridhar and M. Higdon, " Development of the PowerCyber SCADA security testbed[C]", Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. ACM, **(2010)**: 21.
[54] A. Hahn and M. Govindarasu, "Cyber vulnerability disclosure policies for the smart grid[C]", Power and Energy Society General Meeting, 2012 IEEE, IEEE, **(2012),** pp. 1-5.
[55] A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid [J]", Smart Grid, IEEE Transactions on, vol. 4, no. 2, **(2013)**, pp. 847-855.
[56] Y. Sun, B. McMillin, X. F. Liu and D. Cape, " Verifying noninterference in a cyber-physical system the advanced electric power grid [C]", Quality Software, 2007, QSIC'07. Seventh International Conference on. IEEE, **(2007),** pp. 363-369.
[57] H. Tang and B M. McMillin, "Security property violation in CPS through timing [C]", Distributed Computing Systems Workshops, 2008. ICDCS'08, 28th International Conference on. IEEE, **(2008),** pp. 519-524.
[58] A. Faza, S. Sedigh and B. McMillin, "Integrated cyber-physical fault injection for reliability analysis of the smart grid [M]", Springer Berlin Heidelberg, **(2010)**.
[59] S. Pudar, G. Manimaran and C C. Liu, "PENET: A practical method and tool for integrated modeling of security attacks and countermeasures [J]", Computers & Security, vol. 28, no. 8, **(2009)**, pp. 754-771.
[60] A. Banerjee, J. Banerjee, G. Varsamopoulos, Z. Abbasi and S. K. Gupta, "Hybrid simulator for cyber-physical energy systems [C]", Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), 2013 Workshop on. IEEE, **(2013)**, pp. 1-6.
[61] R A. León, V. Vittal and G. Manimaran, "Application of sensor network for secure electric energy infrastructure [J]", Power Delivery, IEEE Transactions on, vol. 22, no. 2, **(2007)**, pp. 1021-1028.
[62] A. Choudhari, H. Ramaprasad, T. Paul, J. W. Kimball, M. J. Zawodniok, B. M. McMillin and S. Chellappan, "Stability of a Cyber-Physical Smart Grid System using Cooperating Invariants [C]", COMPSAC, **(2013)**, pp. 760-769.
[63] Y. Zhao, A. Goldsmith and H V. Poor, "Fundamental limits of cyber-physical security in smart power grids[C]", Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on. IEEE, **(2013)**, pp. 200-205.
[64] C. Kim, M. Sun, S. Mohan, H. Yun, L. Sha and T. F. Abdelzaher, "A framework for the safe interoperability of medical devices in the presence of network failures[C]", Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems. ACM, **(2010)**, pp. 149-158.
[65] E. Y. Vasserman, K. K. Venkatasubramanian, O. Sokolsky and I. Lee, "Security and interoperable-medical-device systems, part 2: Failures, consequences, and classification [J]", Security & Privacy, IEEE, vol. 10, no. 6, **(2012)**, pp. 70-73.

[66] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim and K. K. Venkatasubramanian, "Challenges and research directions in medical cyber–physical systems [J]", Proceedings of the IEEE, vol. 100, no. 1, **(2012)**, pp. 75-90.
[67] P. Bagade, A. Banerjee and S K S. Gupta, "Safety Assurance of Medical Cyber-Physical Systems using Hybrid Automata: A Case Study on Analgesic Infusion Pump [J]",
[68] K. Venkatasubramanian, S K. Gupta and Ayushman, "a secure, usable pervasive health monitoring system[C]", Proceedings of the 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, ACM, **(2008),** p. 12.
[69] K. K. Venkatasubramanian, E. Y. Vasserman, O. Sokolsky and I. Lee, **"**Security and Interoperable Medical Device Systems: Part 1", IEEE security & privacy, vol. 10, no. 5, **(2012)**, p. 61.
[70] A. Banerjee, S. K. Gupta, G., Fainekos and G. Varsamopoulos, "Towards modeling and analysis of cyber-physical medical systems [C]", Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies, ACM, **(2011),** p. 154.
[71] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee and S. K. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber–physical systems [J]", Proceedings of the IEEE, vol. 100, no. 1, **(2012)**, pp. 283-299.
[72] A. Banerjee, S K S. Gupta, "Spatio-temporal hybrid automata for safe cyber-physical systems: A medical case study[C]", Cyber-Physical Systems (ICCPS), 2013 ACM/IEEE International Conference on. IEEE, **(2013**), pp. 71-80.
[73] M. Pajic, R. Mangharam, O. Sokolsky, D. Arney, J. Goldman and I. Lee, "Model-driven safety analysis of closed-loop medical systems [J]", **(2012)**.
[74] A. L. King, L. Feng, O. Sokolsky and I. Lee, "Assuring the safety of on-demand medical cyber-physical systems [J]", **(2013)**.
[75] Z. Jiang, M. Pajic and R. Mangharam, "Cyber–physical modeling of implantable cardiac medical devices [J]", Proceedings of the IEEE, vol. 100, no. 1, **(2012)**, pp. 122-137.
[76] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet [J]", Selected Areas in Communications, IEEE Journal on, vol. 25, no. 8, **(2007)**, pp. 1569-1589.
[77] K. Sampigethaya, W. Beck, K. Lane, S. Lintelman and R. Poovendran, "Bridging Aero and Auto CPS: Secure Software and Data Distribution", NIST/NSF/USCAR Workshop on Developing Dependable and Secure Automotive Cyber-Physical Systems from Components, March **(2011)**.
[78] S. Kandula, T. Mukherjee and S K S. Gupta, "Toward autonomous vehicle safety verification from mobile cyber-physical systems perspective [J]", ACM SIGBED Review, vol. 8, no. 2, **(2011)**, pp. 19-22.
[79] P. Derler, E A. Lee and A L. Sangiovanni-Vincentelli, "Addressing modeling challenges in cyber-physical systems [R]", CALIFORNIA UNIV BERKELEY DEPT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, **(2011)**.
[80] M. Pajic, N. Bezzo, J. Weimer, R. Alur, R. Mangharam, N. Michael and I. Lee, "Towards synthesis of platform-aware attack-resilient control systems[C]", Proceedings of the 2nd ACM international conference on High confidence networked systems, ACM, **(2013)**, pp. 75-76.
[81] K. Sampigethaya and R. Poovendran, "Cyber-physical integration in future aviation information systems[C]", Digital Avionics Systems Conference (DASC), 2012 IEEE/AIAA 31st. IEEE, **(2012)**, pp. 7C2-1-7C2-12.
[82] K. Sampigethaya and R. Poovendran, "Aviation cyber–physical systems: foundations for future aircraft and air transport [J]", Proceedings of the IEEE, vol. 101, no. 8, **(2013)**, pp. 1834-1855.
[83] K. Sampigethaya and R. Poovendran, "Transportation CPS: Insights from Aviation on Major Challenges and Directions", invited (position paper), NSF Transportation CPS Workshop, 23-24 January **(2014)**.
[84] S K S. Gupta, "Towards Human-Centric Middleware for Future Automotive CPS: A White Paper [J]", High-Confidence Automotive Cyber-Physical Systems, pp. 1-3.

Authors

Tian-Bo Lu, he was born in Guizhou Province, China, 1977. He is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information security and computer network.

Jia-Xi Lin, he was born in Inner Mongolia Province, China, 1989. He is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. His technical interests include information and network security, anonymous communication.

Ling-Ling Zhao, she is a graduate student in School of Software Engineering, Beijing University of Posts and Telecommunications, China. Her technical interests include Cyber-Physical System and P2P network.

Yang Li, he was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.

Yong Peng, he was born in Hunan province, China, 1974. His current research interests include information security and cyber-physical system.

