International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 25-40
http://dx.doi.org/10.14257/ijsia.2015.9.3.04

Towards a Framework for Assuring Cyber Physical System Security

Tianbo Lu[1,2], Jinyang Zhao[1], Lingling Zhao[1], Yang Li[1] and Xiaoyan Zhang[1]

[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*
lutb@bupt.edu.cn, zhaojinyang@sina.cn, wodepengyouzhao@163.com

Abstract

Today, cyber physical systems (CPS) are becoming popular in power networks, healthcare devices, transportation networks, industrial process and infrastructures. As cyber physical systems are used more and more extensively and thoroughly, security of cyber physical systems has become the utmost important concern in system design, implementation and research. Many kinds of attacks arise (e.g. the Stuxnet worm), causing heavy losses and serious potential security risks. For the past few years, researchers are focusing their researches on different aspects of security of cyber physical systems. In this paper, we propose a security framework assuring the security of cyber physical systems and analyze main universities and institutes studying CPS security and their relations in three levels: CPS security objectives, CPS security approaches and security in specific CPS applications. Finally, a conclusion of this article is given.

Keywords: *Cyber Physical Systems, Security, Cyber-Physical Attack*

1. Introduction

Cyber physical systems can be described as smart systems that encompass computational (*i.e.,* hardware and software) and physical components, seamlessly integrated and closely interacting to sense the changing state of the real world [1]. Unlike more traditional embedded systems, a full-fledged CPS is typically designed as a network of interacting elements with physical input and output instead of as standalone devices [2, 3].

Cyber physical systems are becoming prevalent in many application areas: power networks, aerospace, automotive, manufacture, healthcare, critical infrastructure, and so on. However, with its prevalence and extensive use in critical and important applications, cyber physical system becomes increasingly more susceptible to the security vulnerabilities and targets for cyber physical attacks [4]. Hackers can launch malicious attacks on power networks and transportation systems [5] and be able to hack medical devices implanted in human body which have wireless communications [6]. More and more security vulnerabilities are being found in all kinds of cyber physical systems [7]. Security of cyber physical systems has arisen as the concern of utmost importance in research and system design of cyber physical systems.

In this paper, we make the following contributions: We first give a literature review of research on security of cyber physical system in different countries and universities. We present a security framework assuring cyber physical system security and give comprehensive review on CPS security objectives, CPS security approaches and CPS security in specific applications.

ISSN: 1738-9976 IJSIA

2. Literature Review

The prevalence and vulnerabilities of cyber physical systems draw the attention of both researchers and attackers. Many university labs and institutes are founded to do the research related to security of cyber physical systems in recent years. The following Figure the main university laboratories and institutes studying security of cyber physical systems and the relations between different labs and institutes.

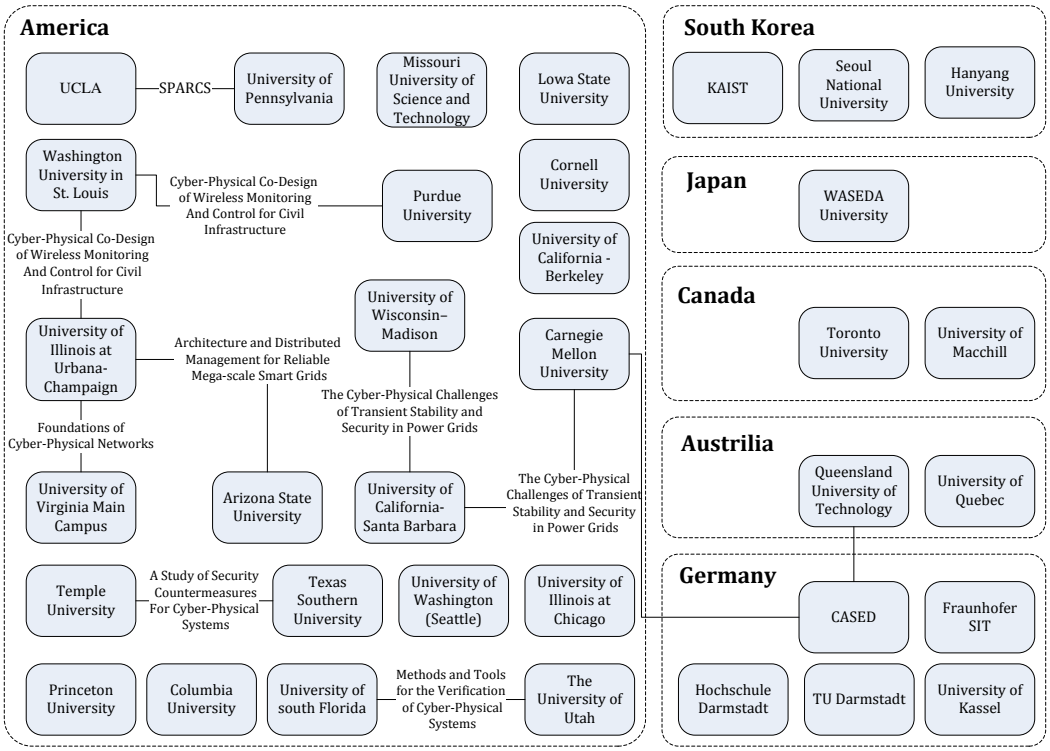


Figure 1. Main Universities and Institutes Studying Security of Cyber Physical Systems and their Relations

In general, American universities are leading the research of CPS security. PowerCyber testbed, a testbed for electric power grid, is built in Iowa State University, which provide an accurate environment for simulation and security evaluation of current issues and future ideas [8, 9]. Similar testbeds are built as Virtual Power System Testbed in University of Illinois [10], Virtual Control System Environment in Sandia National Laboratory [11] and the Testbed for Analyzing Security of SCADA Control Systems in University of Arizona [12]. And researchers of Iowa State University and Cylab of Carnegie Mellon University mainly focus their research on electric power grid security [13-19]. University of California at Los Angeles and University of Pennsylvania make their contribution on promoting robustness of cyber physical systems. Also, University of Pennsylvania and Arizona State University leading the research of medical CPS security from diverse aspects: modeling, attack detection, security solutions, and so on [92-93]. University of California at Berkeley and University of California University at Santa Barbara make contributions on attack modeling and detection in CPS [88].

In Asia, Seoul National University, Hanyang University WASEDA University and HongKong Polytechnic University and so on also make their contribution on security of cyber physical systems [49, 84, 87]. Toronto University and University of McGill in Canada, University of Quebec in Australia, TU Darmstadt and CASED in Germany and so on have done a lot of contribution on assuring security of cyber physical systems [41, 85, 90].

We present a security framework acting as guidance of the thesis. We first talk about several security objectives, confidentiality, integrity, availability, reliability and trustworthiness. Second, we study the main security approaches assuring the security objectives. Finally, we discuss security in specific applications. The following figure shows the security framework.

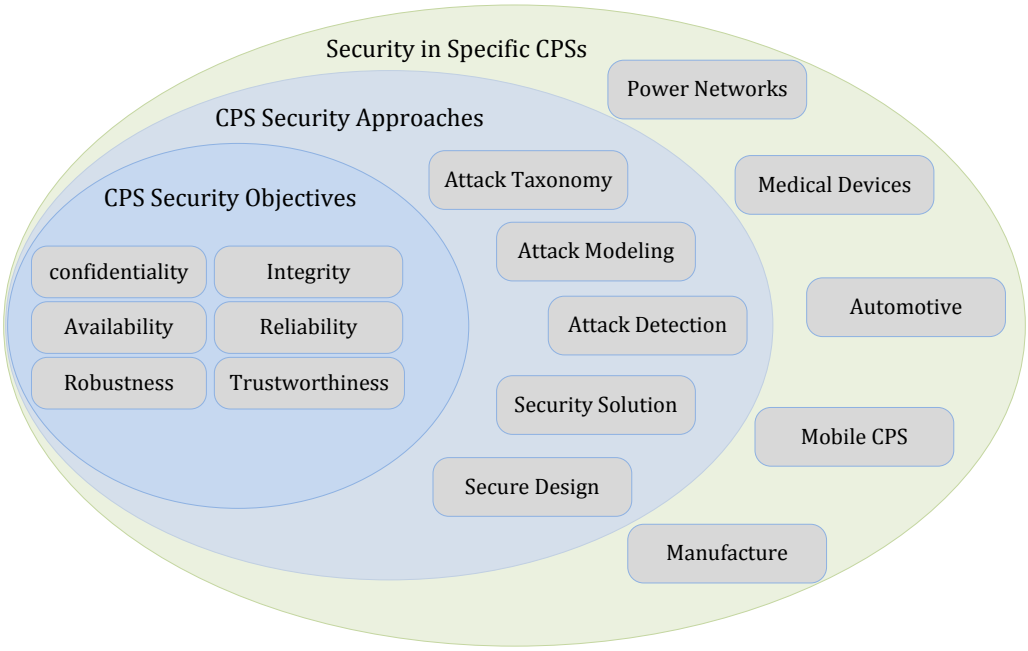


Figure 2. The Framework of Cyber Physical System Security

3. CPS Security Objectives

In assuring the security of cyber physical systems, there are several security objectives to achieve. In the following figure, we show the six security objectives and their related references: confidentiality, integrity, availability, robustness, reliability and trustworthiness.

3.1 Confidentiality

Confidentiality means that cyber physical systems should have the capacity to prevent the disclosure to unauthorized individuals or systems [20-22]. For example, in a healthcare CPS, patients' personal health record may transmit from local record system or devices to the clinician or analyze center. The healthcare CPS should enforce confidentiality by encrypting the transmitted data, limiting the places storing patients' personal health record, restricting access to these storing places, and so on. Disclosure of patients' personal health data in any way results in a breach of the system's confidentiality.

To realize confidentiality, a cyber-physical system should protect the communication channels between sensors and controllers and between the controllers and actuators from eavesdropping [23-25].

Thoshitha T. Gamage, *et al.,* in [22] addresses the security vulnerability of confidential violation due to external observation. They first develop a basis for a CPS security model by composing simple building blocks into a more complex system, and then examine the information security specifically geared towards preserving the event confidentiality in CPS.

Wei Jiang, *et al.,* in [27] investigate the problem of scheduling periodic messages with both time-critical and security-critical requirements and build a risk-based security profit model measuring the security quality of messages, trying to incorporate confidentiality improvement into message scheduling which expose critical messages to security threats, especially by confidentiality attacks.

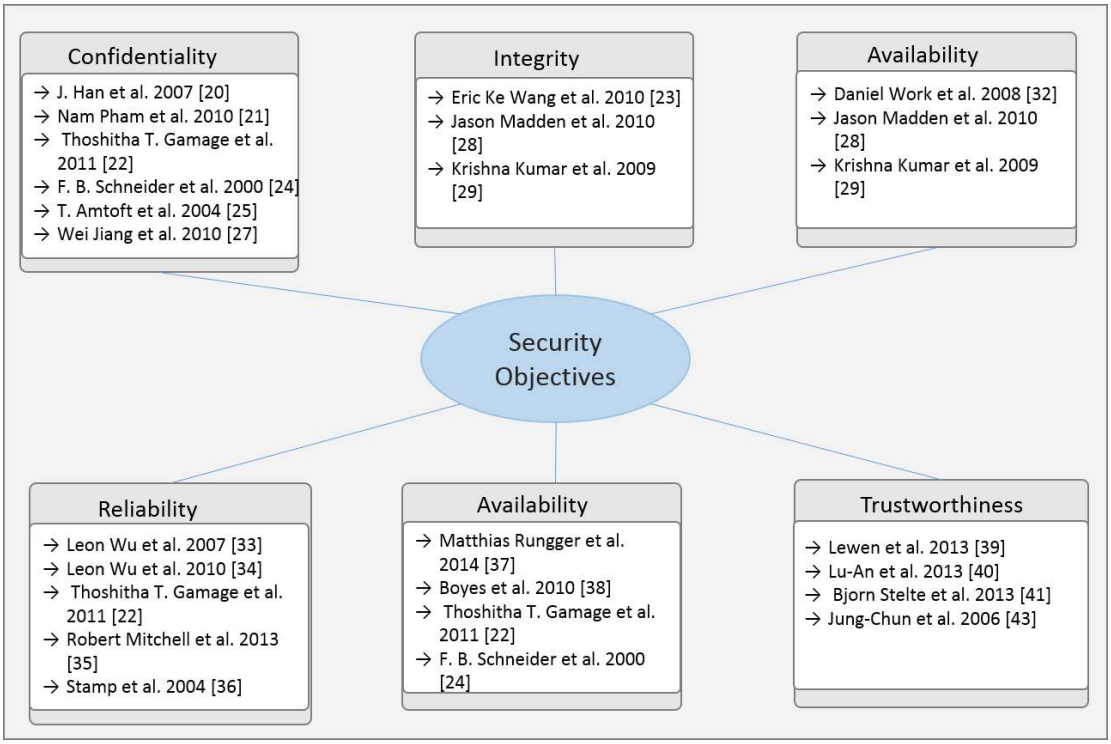


Figure 3. Security Objectives of Cyber Physical Systems

3.2 Integrity

Integrity refers to data or resources cannot be modified without authorization [23]. To ensure the integrity, cyber physical systems should have the capacity to achieve the physical goals by preserving, detecting, or blocking deception attacks on the information attacks on the information sent and received by the sensors and actuators or controllers [28].

Ensuring data integrity requires the ability to detect any changes introduced (maliciously or otherwise) in the massage being communicated [29]. Omar Al Ibrahim, *et al.,* in [30] present some thoughts to utilize the physical unclonable functions technology to build secure coupling between cyber and physical substrates based on intrinsic physical material to achieve integrity of CPS.

3.3 Availability

High availability [32] of cyber physical system aims to always provide service by preventing computing, controls, communication corruptions due to hardware failures, system

upgrades, power outages or denial-of-service attacks. Sazia Parvin, et al., proposes a multi-cyber framework to improve the availability of CPS based on Markov model in [31].

3.4 Reliability

An unreliable CPS often leads to system malfunctions, service disruptions, financial losses and even human life [36]. Leon Wu, *et al.,* in [33] describes a framework for benchmarking reliability of cyber physical systems.

Leon Wu, *et al.,* in [34] describe a data-centric runtime monitoring system for improving the reliability of these types of cyber physical systems, which employs automated online evaluation, working in parallel with cyber physical system to continuously conduct automated evaluation at multiple stages in the system workflow and provide real-time feedback for reliability improvement.

Robert Mitchell, *et al.,* in [35] analyze the effect of intrusion detection and response on the reliability of cyber physical systems and develop a probability model based on stochastic Petri nets to describe the behavior of the CPS in the presence of both malicious nodes exhibiting a range of attacker behaviors, and an intrusion detection and response system for detecting and responding to malicious events at runtime.

3.5 Robustness

Robustness as a system property describes the degree to which a system is able to function correctly in the presence of disturbance, i.e. unforeseen or erroneous inputs. Matthis Rungger, *et al.,* in [37] introduce a notion of robustness termed input-output dynamical stability for cyber physical systems, which captures two intuitive aims of robustness: bounded disturbances have bounded effects and the consequences of a sporadic disturbance disappear over time.

3.6 Trustworthy

Trustworthiness of cyber physical systems refers to the extent to which the system can be relied upon to perform exclusively and correctly the system tasks under defined operational and environment conditions over a defined period of time, or at a given instant in time [38, 39].

Lu-An Tang, *et al.,* in [40] propose a method estimating the locations of objectives causing alarms, constructs an objective-alarm graph and carrying out trustworthy inferences, to find out trustworthy alarms and increase the feasibility of CPS. Bjorn Stelte, *et al.,* in [41] propose an idea to us device redundancy in WSN (Wireless Sensor Network) to detect and isolate malicious nodes, and with this efficiently protect off-the-shelf WSN as well as assure the trustworthiness of sensor data.

4. CPS Security Approaches

Compared to Internet attacks, attacks on CPS are more difficult to detect and prevent. To evade detection, hacks may apply multiple attack stages to gain the access to a cyber-physical system.

In this chapter, we present several security approaches to address attacks on cyber physical system. The following figure shows the CPS security approaches and their related references.

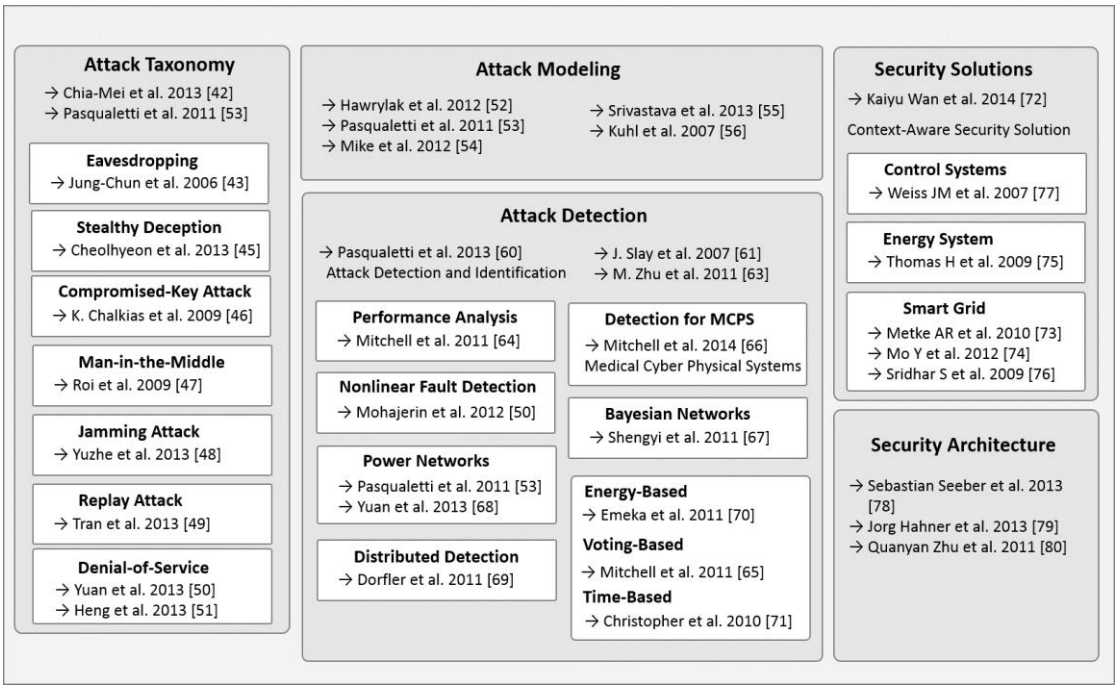


Figure 4. Security Approaches of Cyber Physical Systems

4.1 Attack Taxonomy

Attacks on CPS include not only the cyber attacks from traditional IT area but also the attacks specifically for cyber physical systems, which are capable to across the cyber-physical domain boundary [42]. We present taxonomy of attacks on CPS as follows.

4.1.1 Eavesdropping: Eavesdropping in CPS means that an attacker may intercept any information communicated by the cyber physical system [43]. When launching an eavesdropping attack, attacker doesn't interfere with the working of CPS and just observes its operation. Eavesdropping also violate users' privacy such as patients' personal health data in a medical cyber physical system [6].

4.1.2 Stealthy Deception Attack: Stealthy deception attack means that attacks may tamper with system components or data and don't concern whether they can be detected by the systems detection system. Cheolhyeon Kwon, *et al.,* in [45] study the performance of stealthy deception attacks according to the attackers' ability to compromise the system from a system's perspective.

4.1.3 Compromised-Key Attack: A compromised key refers to a secret code obtained by an attacker to interpret secure information [46]. Using a compromised key attacker can stealthily gain the access to a secured communication, decrypt or modify data and try to use the compromised key to compute additional compromised keys.

4.1.4 Man-in-the-Middle Attack: In man-in-the-middle attack [47], false messages are sent to the operator, and can take the form of a false negative or a false positive. This may cause the operator to take an action, such as flipping a breaker, when it is not required, or it

may cause the operator to think everything is fine and not take an action when an action is required.

4.1.5 Jamming Attack: An external attacker may jam the wireless channel between sensor nodes and the remote estimator in a cyber physical system. Yuzhe Li, *et al.,* study the interactive decision making process of when to send and when to attack, with energy constraints for both the sensor and the attack, and formulate a game-theoretical framework to study jamming attacks [48].

4.1.6 Replay Attack: Cyber physical systems may be vulnerable to replay attacks, especially for smart grid systems whose security protocol that cover the whole system are still not complete. Thien-Toan Tran, *et al.,* in [49] study the replay attacks and propose a new detection scheme for replay attacks based on a solution originally developed for a control system.

4.1.7 Denial-of-Service Attack: Gaining the access to networks of cyber physical systems, attacker may flood a controller or entire sensor network, send invalid data to controllers or block the traffic of cyber physical systems. Yuan Yuan, *et al.,* in [50] design resilient controllers for cyber physical control systems under Dos attacks and design a coupled framework incorporating the cyber configuration policy of IDS and robust control of dynamical system to study Dos attacks on cyber physical systems. Meanwhile, Heng Zhang, *et al.,* investigate how the attacker should design its Dos attacking policy to make the system performance deteriorated as much as possible [51].

4.2 Attack Modeling

Due to all kinds of constraints, research on attacks on cyber physical systems are usually taken out by simulation and modeling. Modeling attacks on real systems has great significance [55]. Peter J. Hawrylak, *et al.,* provide a novel method to model cyber-physical attacks in smart grid with hybrid attack graphs [52].

Fabio Pasqualetti, *et al.,* propose an attack model, which generalizes the prototypical stealth, false data injection and replay attacks, to form a unified framework and advanced monitoring procedures for malfunction and attack detection [53].

Mike Burmester, *et al.,* in [54] describe a framework for modeling the security of a cyber physical system in which the behavior of the adversary is controlled by a threat model that captures the cyber aspects and the physical aspects in a unified way.

For testing security methods, Michael E. Kuhl, *et al.,* provide a cost-efficient and time-saving simulation method to represent computer net-works and intrusion detection systems to simulate cyber attack scenarios [56].

4.3 Attack Detection

Numerous papers concerns on system fault detection, isolation and recovery of control systems [58-59, 63]. However, cyber physical systems suffer from specific vulnerabilities which do not affect classical control systems, and for which appropriate detection and identification techniques need to be developed [60]. The security methods do not exploit the compatibility of measurements with the underlying physical process or the control mechanism, and they are therefore ineffective against insider attacks targeting the physical dynamics [61].

Robert Mitchell, *et al.,* in [64] develop a generic hierarchical model for performance analysis of intrusion detection techniques as applied to a cyber physical system. They develop two intrusion detection techniques for intrusion detection of malicious attacks in a CPS and utilize the hierarchical model developed to analyze the performance characteristics of these two techniques and identify optimal design settings maximizing the reliability of the CPS.

In [65], P. Mohajerin Esfahani, *et al.,* propose a novel methodology make a linear generator robust for a nonlinear system in the presence of certain disturbance signature and provide description of a multi-machine power system that represent a two-area power system and model a cyber-physical attack emanating from the vulnerabilities introduced by the interaction between IT infrastructure and power system.

In [66] Robert Mitchell, *et al.,* propose and analyze a behavior-rule specification-based technique for intrusion detection of medical devices embedded in medical cyber physical systems. Bayesian Networks and casual event graphs are applied in [67] to model the causal relationship between devices in a cyber-physical system.

Because of the large dimensionality and the difficulty in calibrating dynamical network models, centralized attack detection algorithm can't be used in attack detection in power networks [70]. Florian Dorfler, *et al.,* in [69] propose a unified modeling framework and an advanced detection procedure to model a power network and attack on power networks. They design an entirely distributed detection filter based on a sparse residual filter in descriptor form.

Christopher Zimmer, *et al.,* in [71] present three mechanisms for time-based intrusion detection to detect the execution of unauthorized instructions in real-time CPS environments and develop techniques to detect intrusions in a self-checking manner by application and through the operating system scheduler.

4.4 Security Solutions

Cyber physical systems are usually large networked systems, in which a component may itself be a system. Kaiyu Wan, *et al.,* in [72] trying to improve security solutions for cyber physical systems by investigate the CPS security and extent to which the context information may be used to improve the security. Security challenges, loopholes existing in current security architecture, and some solutions to strengthen security in electric power grids are discussed in [73-77]. In the report [77] security threats faced by water distribution systems and the necessity to develop risk models and management roles in security administration have been outlined.

4.5 Security Architecture & Design

Cyber physical systems are widely expected to be formed of networked resource contained devices. To suit the constraints of such networks, the IETF developed the RPL routing protocol for Low-power and Lossy Networks. Security in CPS is important for maintaining the integrity and privacy of data, while also improving network resiliency to attacks. Sebastian Seeber, *et al.,* in [78] present how it would be possible to use the security the communication in RPL network.

Cyber physical system would be targets for new security threats, *e.g.,* manipulating the system both at IT system level and within its surroundings. Jorg Hahner, *et al.,* in [79] discuss these new types of security threats and present a novel system architecture that extends ideas from the domain of Organic Computing and a research agenda towards building future secure CPS.

Quanyan Zhu, *et al.,* in [80] adopts a hierarchical viewpoint to these security issues, addressing security concerns at each level and emphasizing a holistic cross-layer philosophy for developing security solutions.

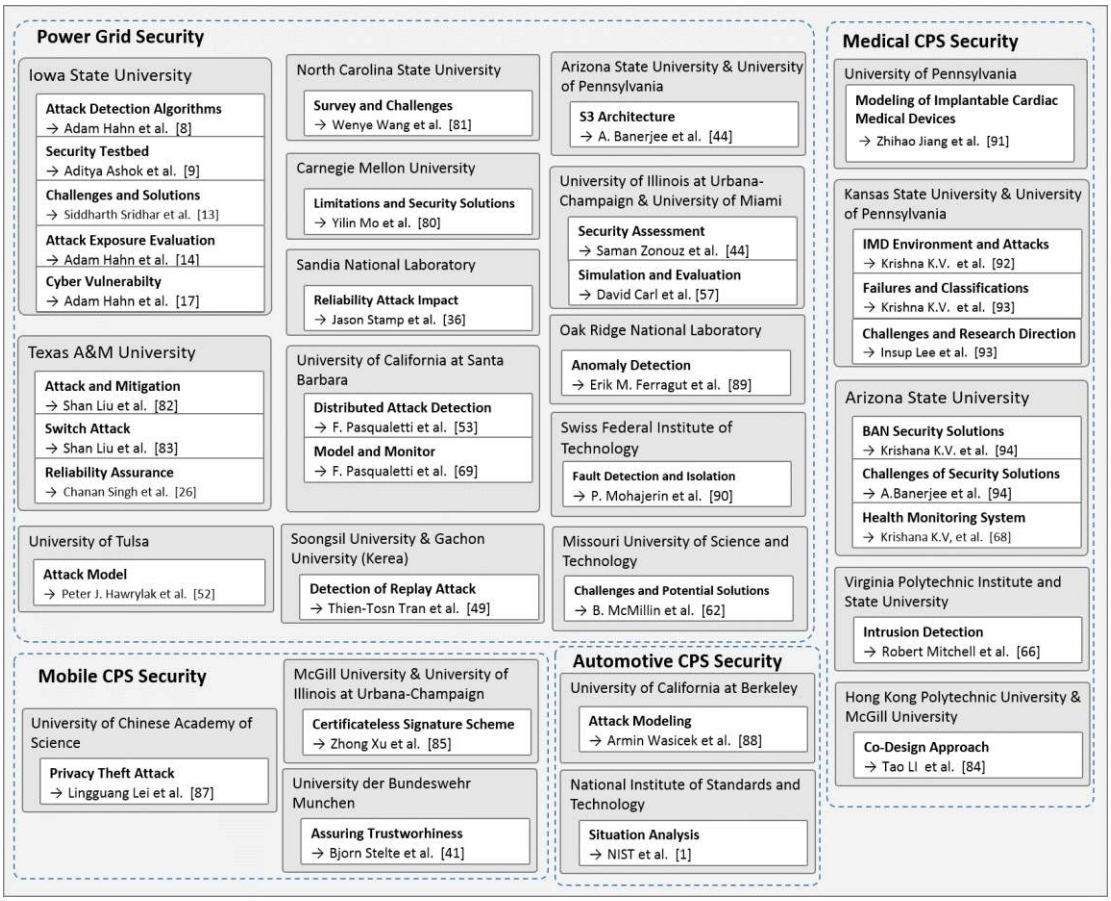


Figure 5. Institutes and Universities Studying CPS Security in Diverse Application Areas and their Main Research Directions

5. Security in Specific CPS

In this chapter, we analyze security issues in specific cyber physical systems especially security issues in power networks and give a comprehensive analysis on institutes, universities, and researchers contributing to security research of power networks, as well as their relations. The following figure show main security research institutes and universities in diverse cyber physical system application areas.

5.1 Power Network Security

Today's electric grid is a large-scale, computer-mediated physical distributed complex system of systems, on which cyber physical system (CPS) stand to have a significant impact [1]. With the integration of advanced computing and communication technologies, the smart grid is expected to greatly enhance efficiency and distributed intelligence [81].

The smart grid brings with it many new data collection, communication, and information sharing capacities in the power system along with new security threats,

vulnerabilities and associated cyber-physical attacks. For modeling and accurate security evaluation of smart grid, Aditya Ashok, *et al.,* in [9] present the testbed architecture implemented at Iowa State University.

The tight coupling of cyber communication networks and physical control systems in smart grid brings in a number of new security risks. Diverse cyber-physical attacks on smart grid and mitigations are discussed in [81-84, 52-53]. Attack Detection in smart grid is focused and studied in [49, 18, 69]. Adam Hahn, *et al.,* in [18] discuss the attack exposure and detection algorithms in smart grid and introduce a model-based intrusion detection system to identify attacks against electric grid substation. Florian Dorfler, *et al.,* in [69] present a distributed detection method to detect cyber-physical attacks in power networks. Anomaly Detection and Fault Detection for smart grid are discussed respectively in [89, 90].

5.2 Medical CPS Security

Medical cyber physical systems are life-critical, context-aware, networked systems of medical devices. The past decades has witness a technological revolution in healthcare domain. New materials replace metals and devices and systems based on information technology replace analog devices to be used in diagnosis, monitoring, and treatment. Computing, sensing, modeling, and communications technologies deeply integrated in physical elements allow medical cyber physical systems to achieve new levels of performance with unprecedented functionality [1].

Zhihao Jiang et al. from University of Pennsylvania in [91] develop a real-time virtual heart model (VMH) to model the electrophysiological operation of functioning and malfunctioning heart, working towards a testing and verification approach for medical cyber-physical systems with patient-in-the-loop.

Interoperable medical devices, due to its networking and coordination functionalities and increased attack surface, face threats to systems' security. Eugene Vasserman, *et al.,* from University of Pennsylvania give an overview of IMD environment and analyze the attacks in [92]. In [93], they define a failure model and consequences model to express the combination of failures experienced by IMD environment for each attack vector.

Recent years have seen the emergence of a new class of security solutions for body area networks, cyber physical security solutions enabling plug-n-play secure communication within a BAN using environment derived features. K. K. Venkatasubramanian, *et al.,* in [94] characterize the energy footprint of a cyber physical security solution to compute PKA's energy consumption and determine whether prominent energy scavenging technique can be used to meet its requirements.

Robert Mitchell, *et al.,* in [66] propose and analyze a behavior-rule specification-based technique for intrusion detection of medical devices embedded in a medical cyber physical system. They propose a methodology to transform behavior rules to a state machine, so that a device being monitored can easily be checked against the transformed state machine for deviation from its behavior specification.

5.3 Mobile CPS Security

Many cyber physical system applications will be implemented on computing devices using mobile ad hoc networks. Before these systems can be used in multifarious environments, the security properties of mobile cyber physical systems must be fully understood.

Guanzhong Dai, *et al.,* in [86] propose an efficient certificateless signature scheme for mobile cyber physical systems based on bilinear Diffie-Hellman assumption.

The powerful processors and variety of sensors on nowadays smartphones makes them being ideal mobile cyber-physical systems. These advantages can also be used to launch serious sensor-based privacy theft attacks through sensors abusing. Lingguang Lei, *et al.,* in [87] presented a sensor-based voice privacy theft attack named CPVT and introduce two measures in CPTV to resolve the problems.

5.4 Automotive CPS Security

Automotive CPS is a kind of safety-critical cyber physical system in which the protection against malicious design and interaction faults is paramount to guaranteeing correctness and reliable operation. Armin Wasicek, *et al.,* in [88] introduce aspect-oriented modeling as a powerful, model-based design technique to access the security of automotive cyber-physical systems.

5.5 Smart Manufacturing Security

Smart manufacture combines technology, knowledge, information, and human ingenuity to develop and apply "manufacturing intelligence" [1]. Smart manufacturing allows for the complete optimization of a manufacturing plant, where information can be communicated among industrial machines in real-time.

As technology progresses, cyber-physical systems are becoming susceptible to a wider range of attacks. In manufacturing, these attacks pose a significant threat to ensuring products conform to their original design intent and to maintaining the safety of equipment, employees, and consumers. Lee J. Wells, *et al.,* in [95] discuss the importance of research and development of cyber-security tools specifically designed for manufacturing.

6. Conclusion

This article gives a comprehensive review on CPS security following the security framework from diverse perspectives. With the increasing prevalent use and vulnerabilities of CPS to cyber-physical attacks, CPS security is playing a critically important role in the research of CPS. We survey the main universities and institutes leading the research of CPS security and analyze their research focuses and the relations between them. The objectives for achieving security of CPS in different aspects are introduced with related literature efforts. Then the main security approaches on detecting cyber-physical attacks and assuring CPS security are listed and analyzed. Finally, we summary security in specific applications with the dominant research groups presented.

As a result of our efforts, it is seen that security research is far from mature for the newly-emerged cyber physical systems and there are still many challenges facing designers, operators and researchers. This is unsatisfactory, and hopefully, by providing an overview of the literature efforts done, the overview will contribute in providing reference for researcher in the area of CPS security.

ACKNOWLEDGEMENTS

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] "Foundations for Innovation in Cyber-Physical Systems Workshop Summary Report", **(2013)** January, http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf.
[2] "Electrical Engineering and Computer Sciences, University of California at Berkeley", Technical Report No., **(2008)**, UCB/EECS-2008-8, http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html.
[3] Q. Shafi, "Cyber Physical Systems Security: A Brief Survey," Computational Science and Its Applications (ICCSA)", 2012 12th International Conference on, **(2012)**, pp. 146-150.
[4] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui and K. P. Chow, "Security Issues and Challenges for Cyber Physical System," 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, **(2010)**, pp. 733-738.
[5] E. Mills, "Hackers broke into FAA air traffic control system", The Wall Street Journal, **(2009)**, pp. A6.
[6] N. Leavitt, "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers", Computer, vol. 43, **(2013)**, pp. 11-14.
[7] K. K. Fletcher and X. F. Liu, "Security Requirements Analysis, Specification, Prioritization and Policy Development in Cyber-Physical Systems," Secure Software Integration & Reliability Improvement Companion (SSIRI-C), 2011 5th International Conference on, **(2011)**, pp. 106-113.
[8] A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," Smart Grid, IEEE Transactions on, **(2013)**, pp. 847-855.
[9] A. Ashok, A. Hahn and M. Govindarasu, "A Cyber-Physical Security testbed for Smart Grid: System Architecture and Studies," Department of Electrical and Computer Engineering, **(2011)**.
[10] D. C. Bergman, D. Jin, D. M. Nicol and T. Yardley, "The virtual power system testbed and inter-testbed integration," in Proc. 2nd Workshop Cyber Security Exp. Test, **(2009)**.
[11] M. J. McDonald, *et al.,* "Modeling and simulation for cyber-physical system security research," Development and Applications, Sandia National Laboratories, SAND2010-0568, **(2010)** February.
[12] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga and S. Hariri, "A testbed for analyzing security of SCADA control systems (TASSCS)," inProc. IEEE PES Innov. SmartGrid Technol., (ISGT), **(2011)**, pp.1–7,
[13] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," Proceedings of the IEEE, **(2012)**, pp. 210-224.
[14] A. Hahn and M. Govindarasu, "Cyber Attack Exposure Evaluation Framework for the Smart Grid," Smart Grid, IEEE Transactions on, **(2011)**, pp. 835-843.
[15] C.-W. Ten, G. Manimaran and C.-C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling, Systems, Man and Cybernetics", Part A: Systems and Humans, IEEE Transactions on, **(2010)**, pp. 853-865.
[16] S. Pudar, G. Manimaran and C.-C. Liu, "PENET: A practical method and tool for integrated modeling of security attacks and countermeasures, Computers & Security, vol. 28, Issue 8, **(2009)**, pp. 54–771.
[17] A. Hahn and M. Govindarasu, "Cyber vulnerability disclosure policies for the smart grid", Power and Energy Society General Meeting, IEEE, **(2012)**, pp. 1-5.
[18] A. Hahn, "Cyber securit y of the smart grid: Attack exposure analysis, detection algorithms, and testbed evaluation," Graduate Theses and Dissertations, Iowa State University, **(2013)**.
[19] Y. Mo, T. H. H. Kim, K. Brancik and D. Dickinson, "Cyber–Physical Security of a Smart Grid Infrastructure," Proceedings of the IEEE, **(2011)**, pp. 195-209.
[20] 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), **(2007)**.
[21] 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)**.
[22] T. T. Gamage, T. P. Roth and B. M. McMillin, "Confidentiality Preserving Security Properties for Cyber-Physical Systems," 2011 35th IEEE Annual Computer Software and Applications Conference, **(2011)**, pp. 28-37.
[23] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L .C. K. Hui and K. P. Chow, "Security Issues and Challenges for Cyber Physical System," 2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing, **(2010)**, pp. 733-738.
[24] F. B. Schneider, "Enforceable Security Policies," ACM Transactions on Information and System Security TISSEC, vol. 3, no. 1, **(2000)**, pp. 30–50.
[25] T. Amtoft and A. Banerjee, "A Logic for Information Flow Analysis with an Application to Forward Slicing of Simple Imperative Programs," Science of Computer Programming, vol. 64, **(2004)**, pp. 3–28.

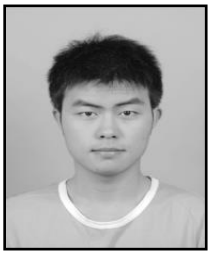
[26] C. Singh and A. Sprintson, "Reliability Assurance of Cyber-Physical Power Systems," Power and Energy Society General Meeting, **(2010)**, pp. 1-6.
[27] W. Jiang, W. Guo and N. Sang, "Periodic Real-Time Message Scheduling for Confidentiality-Aware CyberPhysical System in Wireless Networks," 2010 Fifth International Conference on Frontier of Computer Science and Technology, **(2010)**, pp. 355-360.
[28] 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)**, pp. 176-181.
[29] K. K. Venkatasubramanian, "Security solutions for cyber-physical systems," A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy, **(2009)**.
[30] O. Al Ibrahim and S. Nair, "Cyber-Physical Security Using System-Level PUFs," Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, **(2011)**, pp. 1672-1676.
[31] S. Parvin, F. K. Hussain, O. K. Hussain, T. Thein and J. S. Park, "Multi-cyber framework for availability enhancement of cyber physical systems," vol. 95, **(2013)**, pp. 927-948.
[32] 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)**.
[33] L. Wu and G. Kaiser, "FARE: A Framework for Benchmarking Reliability of Cyber-Physical Systems," Columbia University Computer Science Technical Reports, Columbia University, **(2013)**.
[34] L. Wu and G. Kaiser, "An Autonomic Reliability Improvement System for Cyber-Physical Systems," Columbia University Computer Science Technical Reports, **(2012)**.
[35] R. Mitchell and I.-R. Chen, "Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems," IEEE Transactions on Reliability, vol. 62, no. 1, **(2013)** March.
[36] J. Stamp, A. McIntyre and B. Ricardson, "Reliability impacts from cyber attack on electric power systems," Power Systems Conference and Exposition, **(2009)**, pp.1-8, 15-18.
[37] M. Rungger and P. Tabuada, "A Notion of Robustness for Cyber-Physical Systems," Cornell University Library, **(2014)**.
[38] H. A. Boyes, "Trustworthy cyber-physical systems: A review," System Safety Conference incorporating the Cyber Security Conference 2013, 8th IET International, **(2013)**, pp. 1-8.
[39] Z. Lewen, Z. Yong, C. Yixiang, Z. Min and Z. Juyang, "Stability of Software Trustworthiness Measurements Models," Software Security and Reliability-Companion (SERE-C), 2013 IEEE 7th International Conference on, **(2013)**, pp. 219-224.
[40] T. Lu-An, Y. Xiao, K. Sangkyum and H. Jiawei, "Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems," Data Mining (ICDM), 2010 IEEE 10th International Conference on, **(2010)**, pp. 1079-1084.
[41] B. Stelte and G. D. Rodosek, "Assuring Trustworthiness of Sensor Data for Cyber-Physical Systems," 2013 IFIP/IEEE International Symposium on Integrated Network Management (IM2013), **(2013)**, pp. 395-402.
[42] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue and J. Sztipanovits, "Taxonomy for Description of Cross-Domain Attacks on CPS," Vanderbilt University, Institute for Software Integrated Systems, **(2013)**, pp. 135-143.
[43] J.-C. Kao and R. Marculescu, "Eavesdropping Minimization via Transmission Power Control in Ad-Hoc Wireless Networks", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, **(2006)**, pp. 707-714.
[44] S. Zonouz and P. Haghani, "Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior," Computers & Security, vol. 39, **(2013)**, pp. 190-200.
[45] K. Cheolhyeon, L. Weiyi and H. Inseok, "Security analysis for Cyber-Physical Systems against stealthy deception attacks," American Control Conference (ACC), **(2013)**, pp. 3344-3349.
[46] K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis and G. Stephanides, "Two Types of Key-Compromise Impersonation Attacks against One-Pass Key Establishment Protocols", Communications in Computer and Information Science, vol. 23, **(2009)**, pp. 227-238.
[47] R. Saltzman and A. Sharabani, "Active Man in the Middle Attacks, A Security Advisory", A whitepaper from IBM Rational Application Security Group, **(2009)** February 27.
[48] L. Yuzhe, S. Ling, C. Peng, C. Jiming and D. E. Quevedo, "Jamming attack on Cyber-Physical Systems: A game-theoretic approach," Cyber Technology in Automation, Control and Intelligent Systems (CYBER), 2013 IEEE 3rd Annual International Conference on, **(2013)**, pp. 252-257.
[49] T.-T. Tran, O.-S. Shin and J.-H. Lee, "Detection of replay attacks in smart grid systems," Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, **(2013)**, pp. 298-302.
[50] Y. Yuan, Z. Quanyan, S. Fuchun, W. Qinyi and T. Basar, "Resilient control of cyber-physical systems against Denial-of-Service attacks," Resilient Control Systems (ISRCS), 2013 6th International Symposium on, **(2013)**, pp. 54-59.

[51] Z. Heng, C. Peng, S. Ling and C. Jiming, "Optimal DoS attack policy against remote state estimation," Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on, **(2013)**, pp. 5444-5449.
[52] P. J. Hawrylak, M. Haney and M. H. Papa, "Using hybrid attack graphs to model cyber-physical attacks in the Smart Grid" Resilient Control Systems (ISRCS), 2012 5th International Symposium on, **(2012)**, pp. 161-164.
[53] F. Pasqualetti, F. Dorfler and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on, **(2011)**, pp. 2195-2201.
[54] M. Burmestera, E. Magkos and V. Chrissikopoulos, "Modeling security in cyber-physical systems," international journal of critical infrastructure protection, vol. 5, **(2012)**, pp. 118-126.
[55] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, P. Shengyi and U. Adhikari, "Modeling Cyber-Physical Vulnerability of the Smart Grid with Incomplete Information," Smart Grid, IEEE Transactions on, **(2013)**, pp. 235-244.
[56] M. E. Kuhl, J. Kistner, K. C. Antini and M. Sudit, "Cyber attack modeling and simulation for network security analysis," Simulation Conference, **(2007)**, pp. 1180-1188.
[57] D. C. Bergman, "Power grid simulation, evaluation, and test framework," University of Illinois at Urbana-Champaign, **(2010)**, https://www.ideals.illinois.edu/handle/2142/16156?show=full.
[58] M.-A. Massoumnia, G. C. Verghese and A. S. Willsky, "Failure detection and identification,"IEEE Trans. Autom. Control, vol. 34, **(1989)**, pp. 316–321.
[59] M. Basseville and I. V. Nikiforov, "Detection of Abrupt Changes: Theory and Application. Englewood Cliffs", NJ, USA: Prentice-Hall, **(1993)**.
[60] F. Pasqualetti, F. Dorfler and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," Automatic Control, IEEE Transactions on, **(2013)**, pp. 2715-2729.
[61] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," Critical Infrastructure Protection, vol. 253, **(2007)**, pp.73–82.
[62] B. McMillin, "Privacy and Confidentiality in Cyber-Physical Power Systems," Power and Energy Society General Meeting, **(2012)**, pp. 1-3.
[63] M. Zhu and S. Martínez, "Stackelberg-game analysis of correlated attacks in cyber-physical systems," in Proc. Amer. Control Conf., San Francisco, CA, USA, **(2011)**, pp. 4063–4068.
[64] R. Mitchell and I. R. Chen, "A hierarchical performance model for intrusion detection in cyber-physical systems," Wireless Communications and Networking Conference (WCNC), **(2011)**, pp. 2095-2100.
[65] R. Mitchell and I.-R. Chen, "Survivability analysis of mobile cyber physical systems with voting-based intrusion detection," Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, **(2011)**, pp. 2256-2261.
[66] R. Mitchell and I. R. Chen, "Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems," Dependable and Secure Computing, IEEE Transactions on, **(2014)**.
[67] S. Pan, T. H. Morris, U. Adhikari and V. Madani, "Causal Event Graphs Cyber-physical System Intrusion Detection System," Mississippi State University, **(2011)**.
[68] K. Venkatasubramanian and S. K. Gupta, "AYUSHMAN: A Secure, Usable Pervasive Health Monitoring System," Proceedings of the 2nd International Workshop on Systems and Networking Support for Health Care and Assisted Living Environments, Article, no. 12, **(2008)**.
[69] F. Dorfler, F. Pasqualetti and F. Bullo, "Distributed detection of cyber-physical attacks in power networks: A waveform relaxation approach," Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on, **(2011)**, pp. 1486-1491.
[70] E. Eyisi and X. Koutsoukos, "Energy-Based Attack Detection in Networked Control Systems," United Technologies Research Center, **(2011)**, pp. 115-124.
[71] C. Zimmer, B. Bhat, F. Mueller and S. Mohan, "Time-Based Intrusion Detection in Cyber-Physical Systems," ICCPS '10 Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, **(2010)**, pp. 109-118.
[72] K. Wan and V. Alagar, "Context-Aware Sec urity Solutions for Cyber-Physical Systems" Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 109, **(2013)**, pp. 18-29.
[73] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks", IEEE Trans Smart Grid, vol. 1, no. 1, **(2010)**, pp. 99–107.
[74] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, "Cyber Physical security of a smart grid infrastructure. Proc IEEE, vol. 100, no. 1, **(2012)**, pp. 195,209.
[75] T. H. Morris, A. K. Srivastava, B. Reaves, K. Pavurapu, S. Abdelwahed, R. Vaughn, W. McGrew and Y. Dandass, "Engineering future cyber-physical energy systems: challenges, research needs, and roadmap", North American Power Symposium (NAPS), Starkville, **(2009)**, pp. 1–6.

[76] S. Sridhar, A. Hahn and M. Govindarasu, "Cyber Physical system security for the electric power grid. Proc IEEE, vol. 100, no. 1, **(2012)**, pp. 210,224.
[77] J. M. Weiss, "Control systems cyber security - the need for appropriate regulations to assure cyber security of the electric grid", Testimony (Report) to Homeland Security's Subcommittee on Emerging Threats, Cyber-security, and Science and Technology, **(2007)**, http://chsdemocrats.house.gov/SiteDocuments/SiteDocuments/20071017164638-60716.pdf**.**
[78] S. Seeber, A. Sehgal, B. Stelte, G. D. Rodosek and J. Schönwälder, "Towards A Trust Computing Architecture for RPL in Cyber Physical Systems," In proceeding of: 2013 IFIP/IEEE International Conference on Network and Service Management (CNSM 2013), **(2013)**, pp. 134-137.
[79] J. Haehner, S. Rudolph, S. Tomforde and D. Fisch, "A Concept for Securing Cyber-Physical Systems with Organic Computing Techniques," **(2013)**, pp. 1-13.
[80] Q. Zhu, C. Rieger and T. Basar, "A hierarchical security architecture for cyber-physical systems," Resilient Control Systems (ISRCS), 2011 4th International Symposium on, **(2014)**, pp. 15-20.
[81] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol. 57, Issue 5, **(2013)**, pp. 1344–1371.
[82] S. Liu, D. Kundur, T. Zourntos and K. Butler-Purry, "Coordinated Variable Structure Switching in Smart Power Systems: Attacks and Mitigation," Proceedings of the 1st international conference on High Confidence Networked Systems, **(2012)**, pp. 21-30.
[83] S. Liu, X. Feng, D. Kundur, T. Zourntos and K. L. Butler-Purry, "A class of cyber-physical switching attacks for power system disruption," Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Article no. 16, **(2011)**.
[84] T. Li, F. Tan, Q. Wang, L. Bu, J.-N. Cao and X. Liu, "From Offline toward Real-Time: A Hybrid Systems Model Checking and CPS Co-Design Approach for Medical Device Plug-and-Play (MDPnP)," ICCPS '12 Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, **(2012)**, pp. 13-22.
[85] Z. Xu, X. Liu, G. Zhang and W. He, "A Certificateless Signature Scheme for Mobile Wireless Cyber-Physical Systems," Distributed Computing Systems Workshops, 2008. ICDCS '08. 28th International Conference on, **(2008)**, pp. 17-20.
[86] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai and W. Shu, "A Certificateless Signature Scheme for Mobile Wireless Cyber-Physical Systems," 2008 The 28th International Conference on Distributed Computing Systems Workshops, **(2008)**, pp. 489-494.
[87] L. Lei, Y. Wang, J. Zhou, D. Zha and Z. Zhang, "A Threat to Mobile Cyber-Physical Systems: Sensor-Based Privacy Theft Attacks on Android Smartphones," trustcom, 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), **(2013)**, pp. 126-133.
[88] A. Wasicek, P. Derler and E. A. Lee, "Aspect-oriented Modeling of Attacks in Automotive Cyber-Physical Systems," Proceedings of the The 51st Annual Design Automation Conference on Design Automation Conference, **(2014)**, pp. 1-6.
[89] E. M. Ferragut, J. Laska, B. Czejdo and A. Melin, "Addressing the Challenges of Anomaly Detection for Cyber Physical Energy Grid Systems," Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, Article no. 3.
[90] P. M. Esfahani, M. Vrakopoulou, G. Andersson and J. Lygeros, "A Tractable Nonlinear Fault Detection and Isolation Technique with Application to the Cyber-Physical Security of Power Systems," 51st IEEE Conference on Decision and Control, **(2012)**, pp. 3433-3438.
[91] Z. Jiang, M. Pajic and R. Mangharam, "Cyber-Physical Modeling of Implantable Cardiac Medical Devices," University of Pennsylvania, http://repository .upenn.edu/mlabpapers/21, **(2012)**.
[92] 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)**, pp. 61-63.
[93] K. K. Venkatasubramanian, E. Y. Vasserman, O. Sokolsky and I. Lee, "Security and Interoperable-Medical-Device Systems, Part 2," IEEE Security & Privacy, vol. 10, no. 5, **(2012)**, pp. 61-63.
[94] K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta, "Green and Sustainable Cyber-Physical Security Solutions for Body Area Networks," 2009 Sixth International Workshop on Wearable and Implantable Body Sensor Networks, **(2009)**, pp. 240-245.
[95] L. J. Wells, J. A. Camelio, C. B. Williams and J. White, "Cyber-physical security challenges in manufacturing systems," Manufacturing Letters, vol. 2, Issue 2, **(2014)**, pp. 74–77.

Authors

Tian-Bo Lu 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.



Jin-Yang Zhao was born in Hebei Province, China, 1991. 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 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 was born in Hunan Province, China, 1978. He is a PhD and his technical interests include information security, distributed computing and P2P network.

Xiao-Yan Zhang was born in Shandong Province, China, 1973. She is an Associate professor in School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing, China. Her technical interests include software cost estimation and software process improvement.