THE UNIVERSITY OF AUCKLAND
FACULTY OF ENGINEERING

RESEARCH PROPOSAL FOR PhD Advisory Committee

Cyber Physical System(CPS) Security : smart grid a case study

Kelvin Anto
Student ID: 648009640

Faculty of Electrical and Computer Engineering
University of Auckland

Supervisors: Dr. Akshaya Swain & Dr. Partha Roop
February 4, 2020

Contents

1 Introduction

Cyber Physical Systems (CPS) is defined as developmental technologies for managing interconnected systems between its physical assets and information and computational capabilities [1]. Predominantly, a cyber physical system (CPS) consists of two major components, a physical process and a cyber system [2]. Cyber physical system (CPS) aims at monitoring the behaviour of physical processes, and actuating actions to alter its behaviour in order to make the physical environment work accurately and better [2]. Cyber physical systems will empower our critical infrastructure and have the potential to significantly impact our day-to-day lives as they form the basis for emerging and future smart technology. General workflow of CPS can be categorized into four important steps:

- **Monitoring of physical processes and environment** - This is the fundamental step and also used to provide feedback based on past actions.
- **Networking** - Data aggression and diffusion is performed in this step.
- **Computing** - Data collected during monitoring is analysed to check whether the physical process satisfies certain pre-defined criteria.
- **Actuation** - The actions determined during computing phase are pre-dominantly executed in this phase [2].

Cyber physical systems has numerous opportunities in vivid engineering and medical fields. Some of the mind-blowing applications in bio-medical and health care systems include intelligent operating rooms and hospitals, image-guided surgery and therapy, fluid flow control for medicine and biological assays, and the development of physical and neural prostheses [1]. Cyber physical systems has also many applications the design of future aircraft and air traffic management systems, as well as on aviation safety. Another important application of cyber physical system is the smart grid. This has always been in the forefront of public interest and is therefore of utmost importance for policy makers [1]. With recent developments in engineering and information technology that have resulted in greater availability and cost-effectiveness of sensors, data acquisition systems and computer networks, there has been a rapid rise in the implementation of CPS approach among factories [3].

However, the increased use of CPS brings more threats that could have considerable consequences for users [4]. As the interaction between the physical and cyber systems increases, the physical systems become increasingly more vulnerable to the security risks in the cyber system[2]. The number of threats is increasing daily, and cyber attacks have been rising both in number and complexity [5]. For instance, 2013 reports state that Stuxnet virus is a reasonable explanation for the cyber attack launched on an Iranian nuclear facility in Natanz in 2008. The attacks were designed to induce rapid changes in the centrifuge's rotor speed, initially by increasing the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would ultimately destroy the centrifuge [6]. Another incident where hackers broke into the air

traffic control mission-support systems of the U.S. Federal Aviation Administration several times in recent years also received widespread attention [7]. According to a CIA report, some hackers have penetrated power systems in several regions outside the United States, and in at least one case caused a massive power outage affecting multiple cities [8]. The main targets for cyber-attacks are the smart grids, government websites, financial systems, biomedical and health care systems, military networks, as well as public infrastructure systems. The motives of attack range from theft of identity, theft of intellectual property, financial fraud, damage to critical infrastructure and disruption of a nation's economy [5]. The major types of attacks to CPS can be summarized as follows:-

- **Key-Compromise personation attacks** - Key is the secret code that is mandatory for the interpretation of secure information. Once the attacker obtains the private key, it becomes "compromised key" and attacker can decrypt or modify data using this key [9].
- **Eavesdropping risk** - The interception in the transmission of data packets by an adversary node located within the transmission range of the sending node is often termed as *Eavesdropping risk or hear-and-fire attacks*[10].
- **Active Man in the middle** - In this type of attack, usually the attacker sends false negative or false positive messages which lead the operator or user to take an action when it is not required [11].
- **Denial of service (DoS)** - In this type of attack, the network is overloaded with the traffic sent by adversary such that it prevents the legitimate traffics or requests for network resources from being processed or responded by the system. Recent studies demonstrate that the shared nature of the medium in wireless networks makes it effortless for an attacker to launch a Wireless Denial of Service (WDoS) attack [12].

Protecting such CPSes from these kind of attacks requires an in-depth understanding of the system and its response, not just the typical computer security defense mechanisms [13]. Cyber physical systems have supplementary security requirements because of the addition of physical control and communication channels, real time requirements, and their common application to critical infrastructure.

Cyber physical system security issues have been most widely observed in the smart grid infrastructure. Smart grids emphasize on the integration of the physical systems (power network infrastructure) and cyber systems (sensors, ICT, and advanced technologies such as IoT, LoRAWAN etc) and exhibit characteristics typical of cyber physical systems [14]. The electrical power grid is a massive interconnected network which delivers electricity from source to consumers and has been a vital energy supply [15]. Most of the world relies on electrical network which is built 50 or 60 years ago. These are inefficient and cannot offer prompt response to the today's urgent global challenges. This poses an imminent need for a low carbon, clean and efficient system. Smart grid will be a necessary enabler for this transition. Smart grid is an intelligent, digitized electrical infrastructure that delivers power to our homes and businesses. The modernization of the existing electrical system has enhanced customers' and utilities' ability to monitor, control, and predict energy use [16]. It also comes with additional functionalities such as self-healing, motivates and

includes the consumer, resists attack, increases power quality, accommodates all generation and storage options, enables electrical markets, optimizes assets and operates efficiently[17].

The smart grid concept aims to enhance the electric power grid's security, reliability and efficiency through two-way communication of consumption data and dynamic optimization of electric-system operations, network maintenance, and network planning[18]. The smart grid allows close interaction and inter-operation of the transmission and distribution grid through digital and information technology. Because of this, there is an increased possibility of cyberattacks and cascade failures propagating from one system to another[18]. Various cyber security challenges in the smart grid can be summarized as

- **Connectivity** - The power grid has new communication requirements in terms of communication protocols, delay, bandwidth, and cost. It is mandatory to keep up-to-date with technologies in the smart grid security development. There are large number of devices that interoperate in the smart grid. Since the nature of the smart grid environment is decentralized, the systems require a greater level of protection against attacks and vulnerabilities. [19][20]
- **Trust** - There exist some customers are non-compliant to the policies and agreements and might intentionally damage smart meters to report false data and thereby save money on bills. [20]
- **Heterogeneity** - Networking in the latest power grid uses heterogeneous technologies and communication protocols such as ProfiBus(Process Field Bus, ModBus, ModBus+, ICCP (Inter-control Center Communication Protocol), DNP3 and so on. Lion's share of them were designed for connectivity without cyber security. [20]
- **Software Vulnerabilities** - A greater risk of malwares and viruses are introduced by the general purpose technology used in the Supervisory control and data acquisition (SCADA) systems.[20]

The past decade has witnessed several cyber-related attacks on the electrical power grid which have raised the question regarding the security vulnerabilities and its significant impact on the critical power system infrastructure[17].Some significant issues related to cyber-attack on the power grid are :-

- *On August 14, 2003, a complete power blackout was experienced in large portions of the Midwest and Northeast United States and Ontario, Canada, and lasted for up to 4 days in some parts by affecting more than 50 million people and 61,800 megawatts (MW) of load in some parts of the United States. The root cause for the failure was found to be the failure of the software in the cyber system.* [17]
- *During 2010, a computer worm 'Stuxnet' was discovered which spreads using 'Windows' operating system and targeted Siemens industrial software and equipment to interrupt the operation of power system operation.*[17]

Smart grid security is of utmost importance to maintain stable and reliable power system operation during the contingency situation when any critical power system component fails [17]. Ensuring a secured smart grid involves with a less possibility of power grid collapse or equipment malfunction. The lack of the proper 'security measures' could lead to a major blackout may occur which can even lead to a cascading failure [17].

In the literature there are some existing solutions and methods that address the cyber security issues in the smart grid.

- **Network Security** - Denial of Service(DoS) has received widespread attention among the types of cyber attacks on the smart grid. DoS Detection and DoS Mitigation are the two solutions to handle this type of attacks [20].
- **Data Security** - Cryptography methods and algorithms are used to encrypt the data, provide additional protection and security [20].
- **Key management** - Key management plays a pivotal role in authentication and encryption for achieving a secure system. This is categorized into public key infrastructure (PKI) and symmetric key management [20].
- **Network Security Protocols** - Designing secure communications protocols in smart grid infrastructure is also important to achieve a greater level of cyber security[20].
- **Compliance Checks** - Compliance checks is done via automated tools that run-checks across all components in the system to ensure that configurations of each component are up to standards of secure mitigation and protection[20].

Over the past couple of years, run-time enforcement and machine learning are also gaining widespread interest in enhancing the smart-grid cyber security. Run-time enforcement basically adds an additional layer of execution which constantly monitors the inputs and outputs of a given system, and if they deviate from expected or acceptable values, it pre-emptively corrects them [21]. Runtime verifiers are widely used in commercial and industrial applications for monitoring system accuracy [22]. For instance, a closed-loop Run-time Enforcement (RE) of the heart-pacemaker system, where they interact through an "enforcer" was proposed in [23]. This provides an additional layer of safety. Another instance where the run-time enforcers were proposed in [24], to improve the safety of critical CPS which takes Toyota car as an illustrative example. A novel application of bi-directional runtime enforcement was proposed in [22] where enforcers were synthesized to a new hardware architecture within PLC input/output modules to act as an effective line of defence between the cyber and the physical domains.

2 Objectives

In recent years, smart grid security is gaining widespread interest due to its need for smooth and efficient functioning of the smart grid. Run-time enforcement is a subject undergoing intense study in the field of smart grid cyber security.

The prime goal of this research work is to propose a novel approach which emphasizes on a combination of run-time enforcement with non-linear system identification to solve smart grid security issues. The main objectives are as follows:-

- To investigate into the major applications of run-time enforcement in CPS security.
- Develop a run-time enforcement approach to improve network security and enhance compliance checks.
- Delve into the possibilities of combining machine learning and run-time enforcement to enhance the smart grid cyber security concerns.
- Validate the efficacy of proposed approach in a device in the smart grid infrastructure.

3 Methodology

The primary research method for this study is literature review and learning applications of run-time enforcement, machine learning to mitigate cyber-physical attacks on smart grid. Furthermore, the mathematical understanding of the run-time enforcement and machine learning gives an initial start. Choosing a suitable platform or compiler such as *SCChart* for compiling the run-time enforcement algorithm is also a part of primary stage of research.

In the second stage of this study, we intend to extend the concept to a device in the smart grid and validate the efficacy with the existing approaches.

Bibliography

[1] R. Baheti and H. Gill, "Cyber-physical systems," *The impact of control technology*, vol. 12, no. 1, pp. 161–166, 2011.

[2] 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," in *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, IEEE, 2010, pp. 733–738.

[3] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing letters*, vol. 3, pp. 18–23, 2015.

[4] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97, 2017.

[5] M. Abomhara *et al.*, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.

[6] B. Insider, *The stuxnet attack on iran's nuclear plant was 'far more dangerous' than previously thought*, 2013.

[7] E. Mills, "Hackers broke into faa air traffic control system," *The Wall Street Journal, page A*, vol. 6, p. 2009, 2009.

[8] K. O'Connell, "Cia report: Cyber extortionists attacked foreign power grid, disrupting delivery," *Internet Business Law Services*, 2008.

[9] K. Chalkias, F. Baldimtsi, D. Hristu-Varsakelis, and G. Stephanides, "Two types of key-compromise impersonation attacks against one-pass key establishment protocols," in *International Conference on E-Business and Telecommunications*, Springer, 2007, pp. 227–238.

[10] J.-C. Kao and R. Marculescu, "Eavesdropping minimization via transmission power control in ad-hoc wireless networks," in *2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, IEEE, vol. 2, 2006, pp. 707–714.

[11] R. Saltzman and A. Sharabani, "Active man in the middle attacks," *OWASP AU*, 2009.

[12] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[13] C. Neuman, "Challenges in security for cyber-physical systems," in *DHS workshop on future directions in cyber-physical systems security*, Citeseer, 2009, pp. 22–24.

[14] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, 2016.

[15] K. Moslehi, R. Kumar, *et al.*, "A reliability perspective of the smart grid.," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 57–64, 2010.

[16] H. Farhangi, "The path of the smart grid," *IEEE power and energy magazine*, vol. 8, no. 1, pp. 18–28, 2009.

[17] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," *arXiv preprint arXiv:1401.3936*, 2014.

[18] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[19] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[20] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali, "Smart grid cyber security: Challenges and solutions," in *2015 international conference on smart grid and clean energy technologies (ICSGCE)*, IEEE, 2015, pp. 170–175.

[21] J. Ligatti, L. Bauer, and D. Walker, "Edit automata: Enforcement mechanisms for run-time security policies," *International Journal of Information Security*, vol. 4, no. 1-2, pp. 2–16, 2005.

[22] H. Pearce, S. Pinisetty, P. S. Roop, M. M. Kuo, and A. Ukil, "Smart i/o modules for mitigating cyber-physical attacks on industrial control systems," *IEEE Transactions on Industrial Informatics*, 2019.

[23] S. Pinisetty, P. S. Roop, S. Smyth, N. Allen, S. Tripakis, and R. V. Hanxleden, "Runtime enforcement of cyber-physical systems," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 5s, pp. 1–25, 2017.

[24] M. Wu, H. Zeng, C. Wang, and H. Yu, "Safety guard: Runtime enforcement for safety-critical cyber-physical systems," in *2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC)*, IEEE, 2017, pp. 1–6.