Key Security Challenges and Threats to Cyber-Physical Systems and Their Applications

Raja W. Anwar[1,*], Anazida Zainal[1], Saleem Iqbal[2], Mahmood Bashir[2]

[1]Faculty of Computing, UTM, Malaysia.
[2]Department of Information Technology, PMAS-ARID Agriculture University Rawalpindi, Pakistan.
[*]Corresponding author:waraja2@live.utm.my

Abstract

There is a rapid emergence in the field of future technologies and next generation networks (NGN) such as cyber-physical systems (CPS), which are equipped with embedded sensors for monitoring the physical phenomenon and process further for decision making. However, such systems are at constant threat due to inherent uncertainty, context-dependencies, and loss of data packets due to malicious attacks which are causing severe damage to networks. The security of transferred information among different components in cyber-physical systems is vulnerable to the attacks of adversaries who can hijack a physical node to steal all the information. Thus, ensuring the security and early identification of attacks is crucial for cyber-physical systems security. In this paper, we highlight various kinds of security attacks and threats to cyber-physical systems which must be considered while designing a network based on a secure cyber-physical system along with its applications.

Keywords—Cyber-physical systems, security, threats, IoT.

1 Introduction

Cyber-physical systems (CPS) are integration of communication, control and computational components together which form and connect a network between cyber and physical world. The systematic and seamless integration of sensors and actuators make it possible to monitor the physical phenomena from the deployed environment and communicate back to the centralized authority for decision making [1]. The use of Wireless Sensor Networks (WSNs) in the design of cyber-physical systems plays an important role more specifically in the information disseminating stage since secure communication is vital and any breach of data could threaten the whole process of decision making. In addition, the use of cyber-physical systems into various domains, critical infrastructures and applications such as heal-thcare, body area networks, Intelligent Transport System (ITS), security and surveillance systems could have equally catastrophic consequences if security is ignored and there is a lack of appropriate countermeasures. The sensors are small devices with simple deployment scenarios usually in difficult areas where human interaction is hard, thus making them vulnerable to different types of attacks. In addition, the potential use of the cyber-physical sys-tems is also proved by the fact that huge investments are being made by developed nations like the United States and European Union towards the research and development of the CPS [2]- [6]. Moreover, various research initiatives are in progress related to CPS system design, modelling and implementation. Cyber-physical systems applications are used in many disciplines including, energy-sector, Health-care, home appliances, SCADA, manufacturing, intelligent transportation and in environment monitoring. Figure 1 summarizes various applications of cyber-physical systems. Because of the rapid growth in world's population, the security in cyber-physical system becomes a major concern to oversee and steering the individuals in this world. Nowadays, there are a number of technology modes that may have remarkable collision when scheming and executing solutions on cyber-physical infrastructures. One of these impacts is security which is still a big challenge. Cyber-physical systems are the multi-channel, multiplex methodology of a joined-up computing, networks and substantial domain. A Cyber-physical system upgrades the capacity of the system in many facets such as communication in real-time environment, processing of information, self-

ISSN: 2523-0379 (Online), ISSN: 1605-8607 (Print)

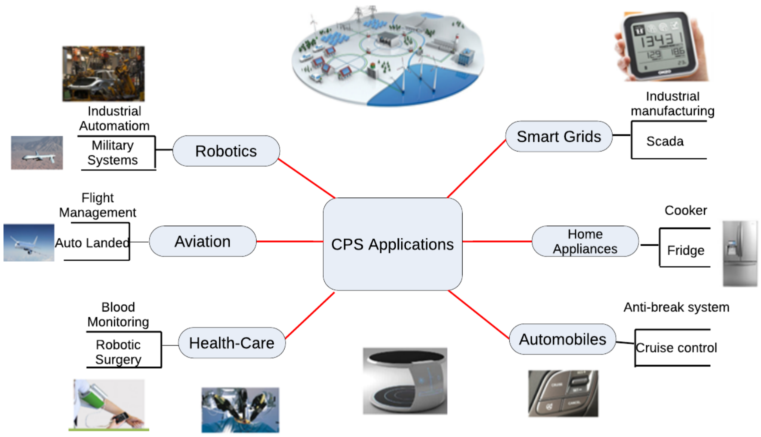

Fig. 1: Applications of cyber-physical systems

supporting of building blocks coordination unit and tangible entities in greatly integrated network domains by mean of string of computation [7]. To provide a secure and trustworthy environment, it is important to detect the attacks early and proper countermeasures must be in in place. In this paper, we analyze various threats and attacks which are aimed to disrupts the operation of cyber-physical system.

The rest of the paper is organized as follows. Section 2 provides various security aspects related to Cyber-physical systems. Sections 3 discusses different attacks related to CPS, while Section 4 describes the security countermeasures and Section 5 discusses the new era of CPS. Finally, Section 6 concludes the paper.

2 Security Aspects In CPS

The basic overflow of any CPS is the monitoring, networking, computing and actuating [8]. Security is one of the issues that is present in all of these processes of Cyber-physical systems. False data may be fed into the system during the monitoring process, the information may be corrupted or blocked at the networking level, the computation process may be attacked to perform malicious controls and calculations and the actuation may be hindered by vandalism of the physical components or the actuators themselves may be physically attacked, as shown in Figure 2. In recent times, there has been a significant increase in attacks against Cyber-physical system. These attacks can massively affect the government, business and other public and private entities as the Cyber-physical system has already started to flourish into every possible field. The reasons behind these attacks may vary, however, some of the major categories of attackers are listed below [9].

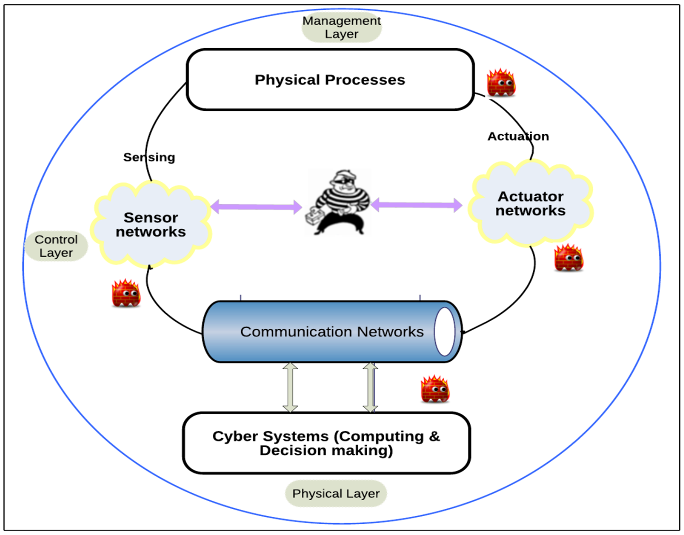

Fig. 2: Security attacks at various layers

1) **Disgruntled employees:** People are the weakest links in the security. More specifically, the unhappy employees can penetrate into the vulnerable parts of the network within the organization and manipulate the processes by misusing the trust and power given to them. This forms one of the most fatal and violated security issues of the current times.
2) **Hackers / Cyber-criminals:** These attackers may not be attacking for any specific purpose of harming the system, but only for gaining other insignificant benefits.
3) **Rival governments:** Governments may try to attack other government organizations to gain intelligence, hamper the economic growth, and/or harm the infrastructure, etc.
4) **Other organizations:** Organizations like various groups of terrorists, activists, or criminal gangs can organize a cyber-attack against other organizations for their own respective

reasons.

Some of the consequences of these attacks are data damaging, denial of access, stealing of data, manipulation of data, and manipulation in the sensing and actuating process. Whereas, the other challenges in the cyber-physical systems are inter-operability, efficiency, safety, dependability, sustainability, reliability and predictability [10].

3 Attacks In CPS

Due to the sensing and communication nature of cyber-physical systems (CPS), they are always a target for adversaries which launch different attacks on these systems. Some of these attacks are mentioned as follows.

1) **Denial of Service (DoS):** In this kind of attack, the attacker floods the communication network or the server with huge volumes of traffic or spurious workloads, thus denying service to legitimate users [11] [12].
2) **Man-in-the-Middle (MITM):** This type of attack is classified as active eavesdropping where an attacker initiates and establish a connection with a victim and relays messages. Moreover, the attacker gains the complete control over the victim's conversation.
3) **Time Synchronization Attack (TSA):** The timing information target of a real-time system may be attacked [13].
4) **Routing attacks:** A malicious node in the network can block the network communication path between source to destination and even consume excessive energy.
5) **Malware:** It is a specially created software which exploits the known vulnerabilities in the operating system, hardware and in the protocol. Moreover, a malware enables an automatic and remote management.
6) **Network-based intrusion:** An adversary can penetrate into the existing networks and firewalls through hardware back-doors and exploit the open ports in the software and hardware and even inject the malicious code.
7) **Eavesdropping:** Through some monitoring tools, an adversary can obtain sensitive information or even gain control of the deployed sensor nodes.
8) **Clone attacks:** In a deployed network, an adversary can hijack the physical nodes and replicate the hijacked nodes and then re-deploy them back into the existing network. Such attacks are known as clone attacks.

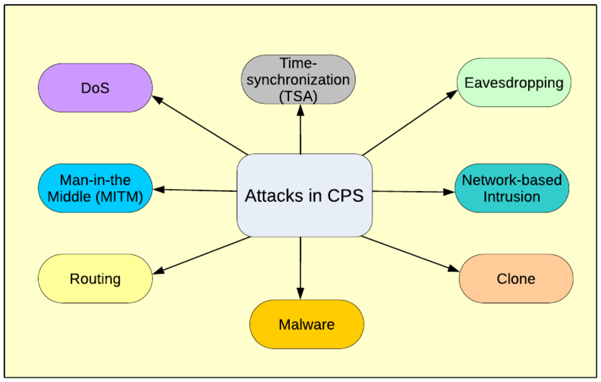

Fig. 3: The taxonomy of CPS attacks

Figure 4 summarizes the taxonomy of the CPS attacks. 2. In addition to the attacks in cyber-physical systems, the following security services are requisite.

1) **Integrity:** The integrity ensures that the message or data is not altered while it is in transit or deliberately tampered by an adversary or through malicious node attacks [14].
2) **Confidentiality:** The confidentiality of the data ensures that the information remain secure from the unauthorized access [14].
3) **Availability:** In an unreliable operating environment, the availability affects the network performance, especially if the network is under a Denial of service (DoS) attack.
4) **Authenticity:** Authenticity validates the participating entities through validation since unauthorized entities affect the network performance.

4 Security Countermeasures

By the discussions in the earlier sections, it is well under-stood that managing the security of cyber-physical systems is not trivial and requires a careful design and countermeasures against well-known threats. Moreover, the implemented countermeasures should have an ability to not only resist the attacks, but also to bring the system back into operational state. The security measures in cyber-physical system can broadly be divided into following categories.

4.1 Prevention

Prevention is based on the manufacturers' understanding of the vulnerabilities within the design of cyber-physical systems and the hardware which includes the various precautionary measures taken to prevent any attack. Similarly, the specific software which is designed only for underlying Cyber-physical system (CPS) also falls in this category.

4.2 Detection

None of the systems are perfectly secure and thus there is always a chance of attack on a deployed cyber-physical system. Therefore, an early detection of attack limits the impact of a damage. In addition, once an attack is detected, appropriate countermeasures must be in place to ensures the system resilience. Some of the countermeasures implemented in the cyber-physical system to obtain better security include the following.

1) **Cryptography:** It is one of the oldest and most implemented methods of securing a system. It involves authentication through security passwords, keys etc.
2) **Remote attestation:** In this technique, a remote device is attested for verifying a node [15]. Attestation can be for both soft-ware and hardware.
3) **Prediction Mechanisms:** The system uses certain algorithms to predict potential attacks, failures or malicious activities and warns accordingly [16].
4) **Trust and reputation:** Using trust and reputation as security measures is a new method which involves lower overhead and computational complexity as compared to the traditional cryptographic security measures. It is a degree of trust which one node has for another. Trust and reputation increases the confidence level of nodes while communicating with other nodes for sharing the data [20].

5 New Era for Cyber-Physical Systems

Internet of things (IoT), is a network of physical objects, usually sensors and actuators, which have sensing and communication capabilities where sensors provide the captured data directly to the application.

5.1 Internet of Thing (IoT)

IoT is a framework which provides distinctive identifiers to individuals or objects and connects them using Internet, enabling data transmission without human interaction. The key challenge for IoT is to create a better world for humans in which entities around us understand our needs and likes [17]. Just like cyber-physical systems, several aspects such as anti- eavesdropping, privacy, encryption, secure point to point connection with authentication request of access control, and approaches which supports security and privacy issues by means of identification and authentication are required to achieve security in a network. The diverse issues are presented in Figure 3. For a secure storage, an instrument is needed which is based on encryption algorithms and which enables the protection of information [18]. Authentication, data integrate, device availability, data secrecy and confidentiality are some of the notable features for effective and secure communication among devices in IoT.

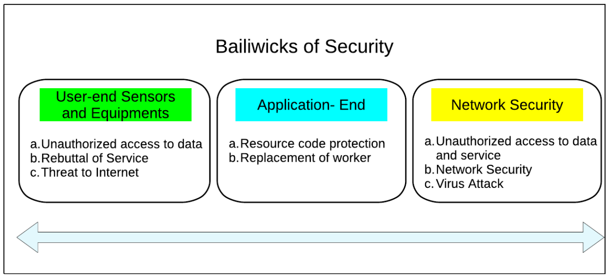

Fig. 4: Security issues in IoT

5.2 Big Data

Big data is a set of huge amount of data which cannot be managed and processed by traditional software tools within an acceptable processing time. Big data refers to all the data which is present in a serverâĂŹs data-base. Nowadays social networks, cloud systems, and smart mobiles are able to process big amount of data which refers to the term Big data [19]. Big data represents a Multi-V mechanism which refers to a huge amount of data (minimum in Terabytes), variety of data by means of different formats, velocity by means of data arrival at a high frequency, and huge number of data source. Because of the low cost, and far-reaching technology, the big data enables new and seamless provocation and possibilities in the area of cyber-physical systems. In cyber physical applications, environment sensors collects data from the physical environment and reports it back to a centralized authority which generates real-time response [20]. Real-time processing of big data has now become a challenge for the applications of cyber-physical systems.

5.3 Cloud Computing

A group of servers and network software that allows centralized database for data storage and online access to online services or resources such as Facebook, Google constitute cloud computing. The terminology of evolution of on-demand information technology services and products refers to the recently introduced technology of cloud computing. Cloud computing provides real-time services, security and protection, solidity, and reliability requirement in cyber physical system. Cyber physical systems require resilience and auto-scaling capabilities of the cloud platforms as change in the amount of work in done. The use of Smart Networked System (SNS) bridge the gap between the physical and virtual world which interlinks the network of sensors, actuators and processing devices. The SNS concept is based on five technologies including networked system, wireless sensor network, real-time processing systems, social networks and cloud computing [21]. Following are some of the technical challenges for cloud based cyber-physical systems.

- System-wide auto-scaling
- To balance the real-time curb with a cost and other goals, a versatile optimized algorithm is needed.
- To support real-time demand, improve the fail-over or fault-tolerance.
- An algorithm that depends on the physical properties of the computations is the need for data provisioning and load balancing.

6 Conclusion

Cyber-physical systems are the composition of cyber and physical components which are integrated deeply into all the applications with an ability to process and hold a huge amount of data. Cyber-physical systems are expected to connect possibly everything within a network and use the individual components which not only generate voluminous amount of data, but also require trustworthy transmission and storage. Since the physical components of IoT and the big data requires interconnection and access between each other, it leads to a demand of cloud computing which enables the access to a network. The integration of these three individual fields of information technology further leads to a much more efficient, effective and powerful rise of cyber-physical systems which can have more influence on every field of pervasive computing. In addition, these devices are highly vulnerable to various attacks and threats. Therefore, the design of security countermeasures must be robust against these attacks to make the system highly secure and trustworthy.

References

[1] Tang, Lu-An, et al. "Trustworthiness analysis of sensor data in cyber-physical systems". Journal of Computer and System Sciences, vol. 79, no. 3, pp.383–401, 2013.

[2] Available at https://www.ece.ncsu.edu/2013/08/chakrabortty-receives-nsf-funding-for-cyber-physical-systems/. Visited on 23 September, 2018.

[3] Available at http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ict-01-2014.html. Visited on 23 September, 2018.

[4] Available at http://www.aaas.org/sites/default/files/15pch24.pdf. Visited on 23 September, 2018.

[5] Shi, J., Wan, J., Yan, H. and Suo, H. "A survey of cyber-physical systems". IEEE International Conference on Wireless Communications and Signal Processing, pp.1–6, 2011.

[6] Chen, Hong. "Applications of cyber-physical system: a literature review". Journal of Industrial Integration and Management, vol. 2, no. 03, 2017.

[7] Zhang, Li, et al. "Security threats and measures for the cyber-physical systems". Journal of China Universities of Posts and Telecommunications, vol. 20, pp.25–29, 2013.

[8] Wang, Eric Ke, Yunming Ye, Xiaofei Xu, Siu-Ming Yiu. "Security issues and challenges for cyber physical system". IEEE Green Computing and Communications (GreenCom), ACM Int'lst International Conference on Cyber, Physical and Social Computing (CPSCom), pp.733–738, 2010.

[9] Cardenas, Alvaro, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, and Shankar Sastry. "Challenges for securing cyber physical systems". In Workshop on future directions in cyber-physical systems security, vol. 5, 2009.

[10] Gunes, Volkan, Steffen Peter, Tony Givargis, and Frank Vahid. "A survey on concepts, applications, and challenges in cyber-physical systems". KSII Transactions on Internet & Information Systems, vol. 8, no. 12, 2014.

[11] Habash, Riadh WY, et al. "Risk management framework for the power grid cyber-physical security". British journal of applied science & technology 3, no. 4, pp.1070, 2013.

[12] Govindarasu, Manimaran, Adam Hann, and Peter Sauer. "Cyber-physical systems security for smart grid". Future Grid Initiative White Paper, PSERC, Feb, 2012.

[13] Aloul, Fadi, A. R. Al-Ali, Rami Al-Dalky, Mamoun Al-Mardini. "Smart grid security: Threats, vulnerabilities and solutions". International Journal of Smart Grid and Clean Energy, vol. 1, no. 1, pp.1–6, 2012.

[14] Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry. "Secure control: Towards survivable cyber-physical systems". IEEE 28th International Conference on Distributed Computing Systems Workshops, pp.495–500, 2008.

[15] Sridhar, Siddharth, et al. "Cyber-Physical System Security for the Electric Power Grid". Proceedings of the IEEE 100, no. 1, pp.210–224, 2012.

[16] Fadlullah, Zubair Md, Mostafa M. Fouda, Nei Kato, Xuemin Shen, and Yousuke Nozaki. "An early warning system against malicious activities for smart grid communications". IEEE Network, vol. 25, no. 5, 2011.

[17] Perera, Charith, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. "Context aware computing for the internet of things: A survey". IEEE communications surveys & tutorials, vol. 16, no. 1, pp.414–454, 2014.

[18] Skarmeta, Antonio, and M. Victoria Moreno. "Internet of things". In Workshop on Secure Data Management, Springer, Cham, pp.48–53, 2013.

[19] Bertino, Elisa. 'data-opportunities and challenges". In Proceedings of the IEEE 37th Annual Computer Software and Applications Conference, pp.479–480, 2013.

[20] Zhang, Lichen. "An approach to model complex big data driven cyber physical systems". In International Conference on Algorithms and Architectures for Parallel Processing, Springer, Cham, pp.740–754, 2014.

[21] Saqib, A., et al. "Cyber security for cyber physcial systems: A trust-based approach". J Theor Appl Inf Technol, vol. 71, no. 2, pp.144–152, 2015.