Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.401 – 405

REVIEW ARTICLE

Review of Attack Detection Scheme for Cyber Physical Security System

Preety T. Gunjal[1], Sunil G. Tamhankar[2]

[1]Department of Information Technology, Walchand College of Engineering, Sangli, India
[2]Department of Electronics Engineering, Walchand College of Engineering, Sangli, India
[1] preeti.gunjal27@gmail.com; [2] sunil.tam@gmail.com

Abstract

Cyber-Physical Systems (CPSs) are characterized by integrating computation and physical processes. The theories and applications of CPSs face the enormous challenges that are (1) general workflow of cyber physical systems, (2) identifying the unique properties of cyber-physical systems and (3) dis-cussing security mechanisms applicable to cyber physical systems. In particular, we analyze and we propose a mathematical framework for security mechanisms for: prevention, detection, resilience of attacks cyber-physical systems, attacks, and monitors.

Keywords- Cyber Physical System (CPS); security mechanism; attacks

I. INTRODUCTION

Cyber-physical systems, however, suffer from specific vulnerabilities which do not affect classical control systems, and for which appropriate detection and identification techniques need to be developed. The principal goal of CPS is to monitor the behavior of physical process1 they are a part of, and actuate actions to change its behavior, if needed. CPS platforms are usually designed as an amalgamation of electro-mechanical sensors and actuators, a communication stack, memory and a processing unit [3],[5]. However, as the interaction between the physical and cyber systems increases, the physical systems become increasingly more susceptible to the security vulnerabilities in the cyber system.For example, some hackers have broken into the air traffic control mission-support systems of the U.S. Federal Aviation Administration several times in recent years,to an Inspector General report sent to the FAA in 2009 [1].Actually, the security vulnerabilities are being found in more and more cyber-physical systems like electronic power grid, smart transportation systems, and medical systems, and so on.

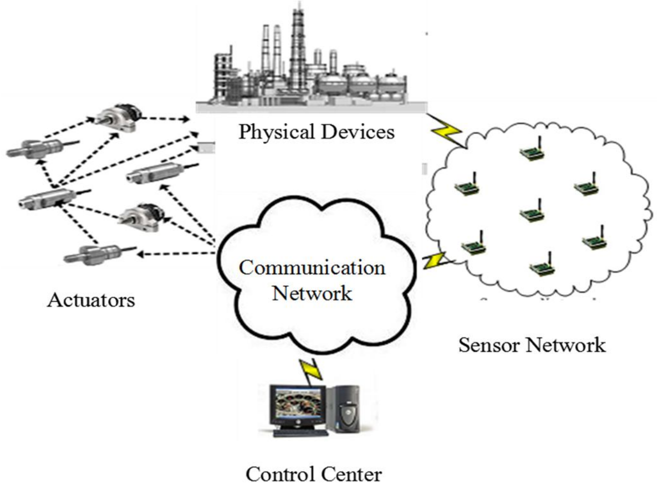

Fig. 1 Cyber Physical System [1]

Irrespective of the domain, a CPS has three principal characteristics are (1) Environment Coupling: CPSs are very tightly coupled with their environment (physical process) – any change in the behavior of the environment results in a change in the CPS' behavior and vice-versa. Prominent examples include medical devices such as ICDs. (2)Diverse Capabilities: CPSs are usually made up of diverse heterogeneous entities with order of magnitude difference in capabilities. Sensors deeply embedded in physical processes for monitoring purposes have limited capabilities, while those entities which manage them are much more capable. For example, a health monitoring CPS is usually made up of limited size medical sensors for usability reasons, but the base station managing the sensors is usually a hand-held computer. A direct consequence of this heterogeneity is potential bottleneck in terms of computation, communication and memory in the workflow. (3) Networked: CPSs, unlike traditional stand-alone embedded systems, usually require a communication channel between its components, either embedded within the physical processes or external to it, in order to provide its (usually coordinated) services [4]. For example, in an automobile CPS, a sensor monitoring the car transmission communicates with the car radio in order to enable it to increase the volume automatically as the speed increases, thus compensating for the extra noise.

II. GENERALWORKFLOW OF CPS

A general workflow of CPS can be categorized into four main steps:

1) **Monitoring**: Monitoring of physical processes and environment is a fundamental function of CPS. It also used to give feedback on any past actions which are taken by the CPS and ensure correct operations in the future. The physical process is to achieve the original physical goal of the CPS.

2) **Networking**: This step deals with the data aggregation, diffusion. There can be much more than one sensor in CPS. These sensors can generate data in real-time, various sensors could generate much data which is to be aggregated or diffused for analyzers to process further. At the same time, different applications need to be interacted with networking communication.

3) **Computing**: This step is for reasoning and analyzing the data collected during monitoring to check whether the physical process satisfies certain pre-defined criteria. If the criteria are not being satisfied, the corrective actions are proposed to be executed in order to ensure meeting the criteria. For instance, a datacenter CPS can have a model to predict the temperature rise with respect to various scheduling algorithms, which can be used to determine future operations [11].

4) **Actuation**: This step executes the actions determined during the computing phase. Actuation can actuate various forms of actions such as correcting the cyber behavior of the CPS, changing the physical process. For instance, the action can be the delivery of some type of medicine in a medical CPS.

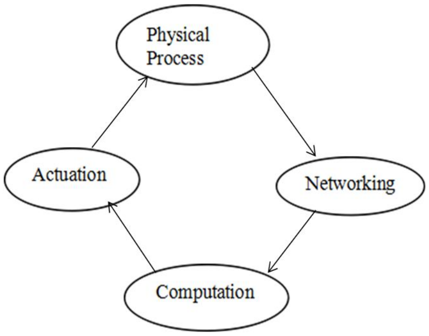

Fig. 2Abstraction of CPS

III. CPS SECRITY OBJECTIVES AND THREATS

A. Security Objectives

Confidentiality: Confidentiality refers to the capability to prevent the disclosure of information to unauthorized individuals or systems. Also defined a set of rules or a promise that limits access or places restrictions on certain types of information. For example, a Healthcare CPS on the Internet requires the personal health records to be transmitted from the Personal Health Record system to the doctor or front medical devices. The system attempts to enforce confidentiality by encrypting the personal health record during transmission, by limiting the places where it might appear (in databases, log files, backups, and so on), and by restricting access to the places where it is stored [2].If an unauthorized party obtains the personal health care in any way, a breach of confidentiality has occurred.

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.

Availability: 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 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.

Authenticity: In computing and communication process it is necessary to ensure that the data, transactions, communications are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are. In CPS, the authenticity aims to realize authentication in all the related process such as sensing, communications, actuations.

IV. MAJOR TYPES OF ATTACKS TO CPS

Compromised-Key Attack:

A key is a secret code which is necessary to interpret secure information. Once an attacker obtains a key, then the key is considered a compromised key [2]. An attacker can gain access to a secured communication without the perception of sender or receiver by using the compromised key. The attacker can decrypt or modify data by the compromising key, and try to use the compromised key to compute additional keys, which could allow the attacker access to other secured communications or resources.

Eavesdropping:

Eavesdropping refers to the attack that adversary can intercept any information communicated by the system. It is called passive attack that the attacker does not interfere with the working of the system and simply observes its operation. CPS is particularly susceptible to eavesdropping through traffic analysis such as intercepting the monitoring data transferred in sensor networks collected through monitoring.

Man-in-Middle attack:

In man-in-the-middle attack, false messages are sent to the operator, and can take the form of a false negative or a false positive [2]. 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.

Denial-of-Service attack:

Denial of Service (DoS) attack is one of the network attacks that prevent the legitimate traffics or requests for network resources from being processed or responded by the system. This type of attacks usually transmits a huge amount of data to the network to make busy handling the data so that normal services cannot be provided [2].

V. SYSTEM ARCHITECTURE

One motivation is about the availability of mobile network such as WiFi and 3G. Utilizing mobile internet, deployment of CPS which requires a good level of network connectivity becomes feasible and widely available [7]. There is a general consensus on what CPS is, what it can do, and how it can be used. However, there is a lack of consensus on key elements of CPS, their relationships, and communication models of CPS. Hence, we define service-based architectures of CPS. In defining the architecture, we consider the following observations and assumptions on CPS.

- Physical devices are connected over network to the control system which performs key computations.
- Software functionality is not tightly coupled to hardware elements.
- CPS requires real-time and on-demand processing.

1. Sensor Network Model

We consider a sensor network composed of a large number of small sensor nodes. We further assume that the sensor nodes are deployed in high density, so that a stimulus can be detected by multiple sensors. Network consists of number of sensors which sends data to center node and which after authentication send data to mobile node. This identifies that sensor node able to send data means travelling data through network.

2. Thread model

We assume that the attacker may know the basic approaches of the deployed security mechanisms, and may be able to either compromise a node through the radio communication channel, or even physically capture a node to obtain the security information installed in the node. However, we assume that attackers cannot subvert the data collection unit, i.e., the sink, because the protection at the sink is powerful enough to defeat such sub version efforts. Once compromised, a node can be used to inject false reports into the sensor network. Node and message authentication mechanisms prevent naive impersonation of a sensor node. However, they cannot block false injection of sensing reports by compromised nodes.

VI. DETECTION OR FILTERING SCHEMES FOR FALSE DATA INJECTION

In the past, a number of schemes have been designed to filter the false injected data in sensor networks .However, those schemes have their limitations and cannot be used to effectively deal with attacks related to CPNS. For example, SEF [10] and IHA.SEF aims at achieving the following goals [10]:

- Early detection of false data reports: by detecting false re-ports the user can avoid responding to fabricated events.
- Low computation and communication overhead: The rule out solutions based on computation-intensive asymmetric cryptography and only use efficient on way functions.

SEF have the T -threshold limitation, that is, if the attackers compromise T nodes from different groups, they could launch node impersonating attack on legitimate nodes. Thus, it lacks resilience to the increased number of compromised nodes.

LBRS, LEDS [9] and CCEF [4] improve the resilience to the number of compromised nodes by introducing static routes for data dissemination and node localization. The static routes are not only vulnerable to node failure and denial-of-service (DoS) attacks (causing the controller not to receive measurement on time and loss of control over the system), but also not suitable for monitoring mobile physical components or systems. DEFS [9] and GRSEF do not depend on static routes, but they achieve low resilience to the number of compromised nodes, and DEFS introduces lots of extra control messages, incurring energy consumption on nodes.

VII. CONCLUSION

In the paper, the overview of cyber physical system with security issues, different attacks and challenges were briefly discussed and different techniques to overcomes the problem which are already proposed in past papers were discussed.

ACKNOWLEDGMENT

We express our sincere thanks to all the authors, whose papers in the area of cyber physical system are published in various conferences proceedings and journals.

REFERENCES

[1] Eric Ke Wang,Yunming Ye, Xia of eiX u ,“Security Issues and Challenges for cyber Physical Sy stem”, *IEEE/ACM International Conference*on Cyber, Physical and Social Computing,2010.

[2] Xinyu Yang, Jie Lin, Paul Moulema,Wei Yu, Xinwen Fu and Wei Zhao Xian JiaotongCyber-Physical Networked Systems",*32nd IEEE International Conference on Dis-tributed Computing Systems*,2012.

[3] Yu-Shian Chen,Chin-Laung Lei,"Filtering False Message En-route in Wireless Multi-hop Networks",*IEEE Communication Society*,2010.

[4] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao, "On False DataAttacks against Power System State Estimation: Modeling and Counter-measures", *IEEE Transactions On Parallel And Distributed Systems,*2013.

[5] Thomas M. Chen, Senior Member,Juan Carlos Sanchez-Aarnoutse, and John Buford, "Petri Net Modeling of Cyber Physical Attacks on Smart Grid", *IEEE TransactionsOnSmart Grid,* Vol. 2, No. 4, December 2011.

[6] Hyun Jung La and Soo Dong Kim,“A Service-based Approach to Designing Cyber Physical Systems“,*9th IEEE/ACIS International Conference on Computer and Information Science*,2010.

[7] M. A. Massoumnia, G. C. Verghese, and A. S. Willsky, "Failure de- tection andidentification", *IEEE Transactions on Automatic Control*, vol. 34, no. 3, pp. 316321,1989.

[8] Jie Lin,Wei Yu,Xinyu Yang,Guobin Xu and Wei Zhao,"On False Data Injection At-tacks against Distributed Energy Routing in Smart Grid",*IEEE/ACM Third Inter-national Conference on Cyber-Physical Systems*,2010.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang,"Statistical en-route Filtering of injection false data in sensor networks",*In Proc. of the 23th IEEE INFOCOM*, 2004.

[10] http://www.cse.iitm.ac.in/

[11] http://www.cyphylab.ee.ucla.edu/