Chapter 6
Smart IDS and IPS for Cyber-Physical Systems

Sara A. Mahboub
Sudan University of Science and Technology, Sudan

Elmustafa Sayed Ali Ahmed
Red Sea University, Sudan

Rashid A. Saeed
https://orcid.org/0000-0002-9872-081X
Taif University, Saudi Arabia

ABSTRACT

One of the most important requirements is security and accessibility efforts which are represented as a critical issue that should be considered in many applications for the purpose of system confidentiality and safety. To ensure the security of current and emerging CPSs by taking into consideration the unique challenges present in this environment, development of current security mechanisms should be further studied and deployed in a manner that make it becomes more compatible with CPS environment, introduce a safer environment and maintain the quality of service at the same time. Systems known as intrusion detection systems (IDS) and intrusion prevention systems (IPS) are the most common security mechanisms used in networking and communication applications. These systems are based on artificial intelligence (AI) where computer-based algorithms are used to analyze, diagnose, and recognize that threats pattern according to an expected suspicious pattern.

INTRODUCTION

The extreme development and rapid spread of technology in numerous communication aspects led the requirement to focus efforts on security and privacy, especially when these technologies are deployed with industry and infrastructure applications. These applications have multiple control loops, strict timing requirements, predictable network traffic, legacy components, and possibly wireless network segments.

DOI: 10.4018/978-1-7998-5101-1.ch006

Such as in industry 4.0, which integrates the internet of things (IoT), and machine-to-machine technology (M2M) with Cyber-Physical Systems (CPS). The CPS intrusion detection is more important to addresses the attacks in the physical environment of CPS (Juan et al, 2018). The use of CPS IDS/IPS detection and prevention techniques will help to monitor the misbehavior of a physical component the IDS look for to detect intrusions. For unknown misbehavior threats that are not defined in the signatures database of the security systems, the use of conventional cybersecurity mechanisms, like intrusion detection and prevention systems (IDS/IPS), and access control have not the capability to detect, prevent and block this category of cyber-attacks (Juan et al,2017).

Artificial intelligence (AI), with CPS cybersecurity mechanisms, can protect the CPSs from such attacks. Machine learning can be used to manage a huge amount of heterogeneous data that come from different sources of information to generate automatically different attacks patents and hence predict accurately the future attackers' misbehavior. Due to the importance of security and privacy issues in the industry 4.0 application. The authors present this chapter to contribute and provide a concept about smart IDS and IPS for the cyber-physical system. The rest of the chapter is organized as follows: a background of the chapter is presented, followed by a detailed review of vulnerability analysis and threat modeling in CPS. The chapter reviews the description of CPS security and privacy in industrial control. Besides, it provides a brief concept about IDS and IPS system methodological and effective management. The chapter also reviews the concept of the IDS/IPS protection mechanism for the CPS system and provides a smart IDS and IPS security solutions based on AI. Moreover, the chapter discussed two types of IDS and IPS for CPS applications, gives a brief review of IDS and IPS deployment strategies in CPS with possible future research directions.

BACKGROUND

Cyber-physical system (CPS) enables control and monitoring of the physical systems in many smart communications and networking applications. These applications are requiring improvement in CPS because it exceeds the simple embedded systems in operation concerning capability, adaptability, scalability, and security issues. Information security is a critical mission in cyber systems; it includes the detection of different types of threats and attacks, also, to prevent them from infecting the system (Huang et al, 2009). IDS and IPS provides a secure means to the current and emerging CPSs. Smart intrusion detection and prevention systems involve developed AI and ML techniques to enhance detection techniques which depended on patterns comparison. AI-based security solutions introduce day zero attack detection, which made it more suitable for CPS applications in the industry 4.0 revolution. Vulnerability analysis provides a routine for penetration testing or examining the strength of the configured security procedures. The threat modeling helps for security experts to find system weakness that can introduce a threat and develop the opposite solution to prevent it (Nazarenko & Safdar, 2019). Both of these techniques as essential and basics of security procedures that are used in legacy and modern security solutions considered in CPSs in addition to other developed security mechanisms.

Security aspects for CPS addressed by the CyBOK project (Bristol, 2020) are divided into internal and external threats. Each of these threats has an associated menace. NIST standard sets procedures and methods to improve the security and privacy in such a cyber system and even for the industrial environment (Amin et al, 2019). Attacks and threats in cyber systems are categorized according to their relevant layer. For example, in basic CPS architecture, there are three layers; physical, network, and application