Chapter 71
Survey of Recent Cyber Security Attacks on Robotic Systems and Their Mitigation Approaches

Abdullahi Chowdhury
Federation University, Australia

Gour Karmakar
Federation University, Australia

Joarder Kamruzzaman
Federation University, Australia

ABSTRACT

With the rapid expansion of digital media and the advancement of the artificial intelligence, robotics has drawn the attention of cyber security research community. Robotics systems use many Internet of Things (IoT) devices, web interface, internal and external wireless sensor networks and cellular networks for better communication and smart services. Individuals, industries and governments organisations are facing financial loses, losing time and sensitive data due these cyber attacks. The use these different devices and networks in robotics systems are creating new vulnerabilities and potential risk for cyber attacks. This chapter discusses about the possible cyber attacks and economics losses due to these attacks in robotics systems. In this chapter, we analyse the increasing uses of public and private robots, which has created possibility of having more cyber-crimes. Finally, contemporary and important mitigation approaches for these cyber attacks in robotic systems have been discussed in this chapter.

1. INTRODUCTION

Dependency on computer and information technology is increasing day by day. Individual person, small and large businesses and government offices are using different online and offline technologies to store data. These stored data can be normal day-to-day personal or business data or can be highly secured private and confidential data. This data storage and exchange is attracting cyber criminals to make cyber

DOI: 10.4018/978-1-5225-8897-9.ch071

attacks to these services for financial gain, defamation or simple knowledge gathering. Different kinds of attacks like email bombing, information or the data theft, Denial of Service (DoS) attacks, Trojan attacks, and hacking the data or system can be defined as cyber attacks (Ben-Asher & Gonzalez, 2015). There are two types of attacks that can occur, one is physical attack and another one is cyber attack. While physical attack (e.g. Damage of Hard Disk Drive) normally cause by physical means and cyber attack occurs in online means. Use of automated and networked systems are increasing day by day. Artificially intelligent and networked devices are being used in industrial domain, smart transportation and smart cities. These services often heavily rely on computer networks. This is generating formidable cyber physical vulnerabilities.

At the early stage of Human-Robot Interaction (HRI), a robot was considered only tool which performs some simple physical tasks on command. Further research into HRI, robots are envisioned work in collaboration with human being in different field. Human and robots are working together in manufacturing industries, construction farms, home and hospitals. From the past few decades, HRI has focused on Human-Robot collaboration that involves a robot interacting with a human in real environment, requiring robustness and seamless interactions (Sandor, Cross, & Chang, 2015).

Robots or Intelligent systems will be very vital part of our life in the near future. Content-oriented traffic, billions of people with mobile devices, heterogeneous communications between hosts and smart objects with strict requirement of connecting people anywhere anytime will be the dominant objective of the Internet of Things (IoT), the Internet of the Future. One of the key component of IoT is Internet of Service (IoS), which will aim to make every possible service from managing the Smart home remotely to managing the whole industrial production process. To manage smart home, smart industries, smart health system, and smart power grid and so on, devices use Internet to connect to each other. These devices use wireless communication method and web based services to communicate with other devices which makes the system vulnerable to cyber or physical attacks or cyber-physical attacks. The security breaches in cyber space that affects the physical system as well is known as cyber physical attacks. The main focus of the cyber-physical security research is the industrial automation control system. Authors (Lyons, Arkin, Liu, Jiang, & Nirmal, 2013) argue that when robots works in uncertain environment, that makes them less predictable. Uncertain situation is referred to when robots are not fully automated but also requires human intervention. If any robot is controlled by remote command or web base software, that makes the robots vulnerable to cyber-physical attacks.

Cyber security is used to safeguard the information transmitted and used in cyber physical systems. Increasing use of web based applications that includes cloud computing, mobile commerce (m-Commerce), eHealth, robotics systems and smart transportation made cyber security is one of the most challenging and important issues for the researchers. Attackers are using different types of attacks in new and existing systems. To develop a proper security policy and reduce the risk of cyber attacks it is important to now the contemporary and existing cysber attacks(Seo, Kim, Park, & Eom, 2016). This chapter mainly focused on the recent cyber attacks on robotic system, impact of these cyber attacks and the mitigation process of these cyber attacks.

This chapter will be organised as following sections:

Section 1 Introduction, Section 2 Overview of Cyber attacks of Robotics Systems, Section 3 Risk assessment and impact of Cyber attacks, Section 4 Mitigation Strategies, Section 5 Conclusion