Chapter 11
Cyber Secure Man-in-the-Middle Attack Intrusion Detection Using Machine Learning Algorithms

Jayapandian Natarajan
https://orcid.org/0000-0002-7054-0163
Christ University, India

ABSTRACT

The main objective of this chapter is to enhance security system in network communication by using machine learning algorithm. Cyber security network attack issues and possible machine learning solutions are also elaborated. The basic network communication component and working principle are also addressed. Cyber security and data analytics are two major pillars in modern technology. Data attackers try to attack network data in the name of man-in-the-middle attack. Machine learning algorithm is providing numerous solutions for this cyber-attack. Application of machine learning algorithm is also discussed in this chapter. The proposed method is to solve man-in-the-middle attack problem by using reinforcement machine learning algorithm. The reinforcement learning is to create virtual agent that should predict cyber-attack based on previous history. This proposed solution is to avoid future cyber middle man attack in network transmission.

INTRODUCTION

Data security and data analytics are a two major pillars of the modern business world. Cyber security is not only the association of data security and privacy, it also consists of a multiple of other components. Cyber security is a process that comprises data, network, storage and computing. The market growth of cyber security reached around 135 billion US dollar in the year 2017. The expected market growth during the period 2018 to 2022 is projected to be 200 billion US dollars (Steve Morgan, 2018). Almost all the utilization services are migrating to the cloud platform. These utilization services are storage,

DOI: 10.4018/978-1-5225-9687-5.ch011

network and infrastructure. The reason for this migration is easy accessibility and lower cost. The other positive aspect of this migration is reducing establishment and computational costs. Third party service providers are also facing serious data security problems. This security problem is termed cybersecurity and addresses data and network security. Cyber security issues and crimes are officially published in many documents in more than fifty countries (Gercke, 2012). The nature and scope of the problem is network security. Cyber security is similar to the banyan tree, where the leaf of this tree is to maintain security and risk management. This cybersecurity is a part of information security to manage various security tools (Kaufman, 2009). The Figure 1. illustrates different elements of cyber security (Schatz, Bashroush & Wall, 2017). The role of the roots is to provide higher security data.

Cyber security is the attainment of data organization and device computation. This device computation relates to various computers and deals with many traditional and non-traditional data. The objective of information security is a circle of three elements that is termed availability, integrity and confidentiality (Jouini & Rabai, 2019). Data availability refers to accessing data from server machines. The second element is integrity which deals with data accuracy and quality (Luo, Hong & Fang, 2018). The most important element is confidentiality which concerns handling data security mechanisms. Both cybersecurity and information security are communication security protocols (Von Solms & Van Niekerk, 2013).

The Table 1 illustrates the fundamental differences between cyber and information security systems (Luiijf, Besseling, Spoelstra & De Graaf, 2011). The primary difference between these two securities mechanisms refers to dealing with physical and digital data. The second difference is dealing with its own organization and public data. Public data means handling internet digital information. Cybersecurity signifies operating at a level above boundary level, which means handling cyber and physical attacks. Physical attack implies the physically theft of information (Pasqualetti, Dörfler & Bullo, 2013). This physical data protection consists of handling the information security protocols. Recently, apart from this physical data, all data is managed in digital format with the help of the cloud computing platform which is a technology that provides different levels of servers. Customers who utilize this technology

Figure 1. Cyber Security Elements