Chapter 11
A Generic Self-Evolving Multi-Agent Defense Approach Against Cyber Attacks

Stephen Mugisha Akandwanaho
University of KwaZulu-Natal, South Africa

Irene Govender
University of KwaZulu-Natal, South Africa

ABSTRACT

A generic self-evolving multi-agent approach is proposed in this chapter. Most of the existing security approaches are custom designed for specific threats and attacks. However, the fusion of technologies and systems in the fourth industrial revolution and therefore the nature of its current cyber environment increasingly attracts multiple cyber threats in a single interface. In order to solve this problem, a generic self-evolving multi-agent approach is proposed. Multiple agents interact with each other in light of their reactions towards the environment and its inherent changes. Information from individual agents is collected and integrated to form the abstract compartment of the structure. The important aspects are analyzed including demonstrating how the abstract domain can be obtained from the custom interactions at the low-level domain of the proposed approach. The analysis explores the existing works in the area and how they have been advanced in the fourth industrial revolution.

INTRODUCTION

Cyber-security in the fourth industrial revolution has increasingly become a high-priority area of research due to its significant importance. Moreover, cyber-security is not only about the safety of cyberspace information (Igor, 2007), but encompasses networks and systems operating in the cyber world as well. It is also one of the three strands of the fourth industrial revolution aside from biological and physical realms that form the *industry 4.0* or what is commonly known as the *fourth industrial revolution*. In this revolution there is a massive convergence and confluence of technologies and systems which create a new digital world with immense benefits but also enormous challenges (Piggin, 2016; Prisecaru, 2016).

DOI: 10.4018/978-1-5225-8897-9.ch011

One of the intrinsic challenges of this revolution include cyber-attacks which are as complicated and evolving as these hyper-inter-connected systems. The magnitude of the risks posed by these attacks require intelligent and agile mechanisms that can adapt and evolve their capabilities to outmatch the strengths and complexities of today's cyber threats. The convergence of different technologies and networked systems create a new level of sophistication in cyber-attacks. This convergence should therefore be considered when developing cyber defense mechanisms. One of the reasons behind this sophistication is that more advanced tools and techniques are being used to breach into networks and systems. This is aggravated by not only the ubiquitous nature of the attacks but the ability of these attacks to circumvent detection and cause enormous harm to people and systems. Given the adoption of mobile devices and proliferation of various devices in the cyber space, new levels of threats have sprang up due to this unprecedented convergence of disparate technologies and systems (Grobler, vanVuuren, & Jannie, 2013). The reality of globalization has dramatically changed under the fourth industrial revolution due to the unmitigated dependence on cyber systems by people and organizations. Hence, the risks have grown in large proportions as the severity of attacks increases in today's hyper-globalization. Even though the advent of globalization brought about a host of benefits such as improved communication and a multitude of opportunities (Herzog, 2011), the ever increasing and evolving cyber security threats and vulnerabilities have increasingly detracted from the benefits and increased anxiety. The existing strategies are not keeping up with the rapidly evolving and complicated cyber threats of this time adequately. Towards this end, multi-layered intelligent techniques are needed to give robust protection to systems and information on many fronts within the same interface. The bespoke protection methods cause runaway attacks when the specific category of the attack is not covered by the protective approach employed since the protective approach can only protect a specific category of cyber-attacks.

In order to combat these threats a multifaceted approach that is reactive, proactive and self-evaluating is required. Firstly, the reactive aspect should encompass both static and dynamic protection controls in neutralizing and fending off attacks. The second aspect which is proactive should be a key component of any security measure in the fourth industrial revolution. The current cyber threats are difficult to track due to their dynamic and adaptive nature (Walters, 2017; Ganapathy, Yogesh, & Kannan, 2012). Hence the combative defense mechanisms should be prescient with the ability not only to detect but also counteract cyber-attacks in a rapidly changing cyber environment. The third component is self-evaluation of the intelligent defense mechanisms. This aspect involves evaluating the mechanism's capabilities against the threat being posed. The evaluation entails a self- evolving capacity to ensure that the optimality and applicability of the defense system in mitigating the risks are dynamically strong as the threats continue to evolve diversely in cyber space.

An effective cyber security defense mechanism should also be multi-layered so that protection is provided on multiple security fronts (Igor, 2005; Igor & Alexander, 2005). The threats in the fourth industrial revolution have increasingly become nested and evolving as systems converge into a single interface. The majority of traditional methods have always been based on niche designs where for example some of them focus on prevention, detection, intrusion detection, and others (Igor, 2010). The current attack patterns require integrated solution systems in cyber space that can collect data, analyze patterns, trace threats, avert attacks and other capabilities integrated into a single interface. The required mechanisms should demonstrate intelligent ability to interact and cooperate with systems so as to learn behaviors and provide robust protection on many fronts in the cyber realm.

One of the objectives of this chapter is to explore the current trends of cyber-attacks in the fourth industrial revolution. In particular a premium is placed on exploring the vulnerabilities brought about by