Chapter 30
Data Mining Techniques for Distributed Denial of Service Attacks Detection in the Internet of Things: A Research Survey

Pheeha Machaka
University of South Africa, South Africa

Fulufhelo Nelwamondo
Council for Scientific and Industrial Research, South Africa

ABSTRACT

This chapter reviews the evolution of the traditional internet into the Internet of Things (IoT). The characteristics and application of the IoT are also reviewed, together with its security concerns in terms of distributed denial of service attacks. The chapter further investigates the state-of-the-art in data mining techniques for Distributed Denial of Service (DDoS) attacks targeting the various infrastructures. The chapter explores the characteristics and pervasiveness of DDoS attacks. It also explores the motives, mechanisms and techniques used to execute a DDoS attack. The chapter further investigates the current data mining techniques that are used to combat and detect these attacks, their advantages and disadvantages are explored. Future direction of the research is also provided.

DOI: 10.4018/978-1-5225-9866-4.ch030

INTRODUCTION

We are living in a rapidly changing information age, were information is available at our fingertips. The use of Information Communications Technology (ICT) has made access to information-on-demand relatively easy and cheaper. Computing has now moved away from the era of the traditional desktop computer to the paradigm of the Internet of Things (IoT). In the IoT, many of the objects that surround us will be on the internet network in one form or another. The use of the technology in the IoT has resulted in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. However, having so many devices connected to the internet brings about interesting internet security challenges.

The proliferate use of internet and network technologies has led to significant dependence of society on ICT systems. Consequently, any malfunction and disruption to the services provided by these systems directly affects major aspects of society. This interruption may be sharply felt even if it is momentary. For example, an interruption in a business organisation or government's ICT infrastructure may have a substantial impact on their day-to-day activities. This may lead to significant financial losses (business and law suits) and increased operational costs from fraudulent activities.

The resulting disruptions may be due to a hacker's attempt to disrupt services using Denial of Service (DoS) attacks. A DoS attack is a malicious attempt by an attacker to disrupt the online services of a service provider to make it unavailable to its legitimate users. A large scale variant of DoS is the Distributed Denial of Service (DDoS). This kind of attack on an organisation may have catastrophic results. This may lead to disgruntled service consumers and major financial losses; it may also lead to losses in an organisation's intellectual property which in turn affects the long term competitiveness of businesses and governments in industrial and military espionage incidents (Choo, 2011). It is therefore important that organisations and governments deploy methods and techniques that will help them to accurately and reliably detect the onset and occurrence of the DDoS attacks.

This chapter studies the IoT phenomena. It provides a background overview and how the internet and evolved into the Internet of Things. The chapter also explores the characteristics of an IoT system. The current use of IoT applications in homes and business is also investigated.

The research further investigates the security concerns of the Internet of things, together with how the technology can be used as a platform to perpetrate and even inject threats and attacks. The research further investigates the landscape of distributed denial-of-service attacks by attempting to answer the following questions:

- What are DDoS attacks? How pervasive are these attacks?
- Why are DDoS attacks executed? How are DDoS executed?
- What is the attack targeting? Which DDoS attacks are common?
- What strategies and mechanisms are used for a successful DDoS attack? Which tools are used to conduct a DDoS attack?
- What defense mechanisms are currently used to combat DDoS attacks? What are their advantages and disadvantages?

The sections that follow will give a background of how the internet evolved into the IoT. It will explore the characteristics and current applications of the IoT paradigm. The security concerns that are present

Related Content