Chapter 21
Zero-Crossing Analysis of Lévy Walks and a DDoS Dataset for Real-Time Feature Extraction:
Composite and Applied Signal Analysis for Strengthening the Internet-of-Things Against DDoS Attacks

Jesus David Terrazas Gonzalez
Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, Canada

Witold Kinsner
Cognitive Systems Laboratory, Department of Electrical and Computer Engineering, University of Manitoba, Winnipeg, Canada & Telecommunications Research Laboratories (TRLabs), Winnipeg, Canada

ABSTRACT

A comparison between the probability similarities of a Distributed Denial-of-Service (DDoS) dataset and Lévy walks is presented. This effort validates Lévy walks as a model resembling DDoS probability features. In addition, a method, based on the Smirnov transform, for generating synthetic data with the statistical properties of Lévy-walks is demonstrated. The Smirnov transform is used to address a cyber-security problem associated with the Internet-of-things (IoT). The synthetic Lévy-walk is merged with sections of distinct signals (uniform noise, Gaussian noise, and an ordinary sinusoid). Zero-crossing rate (ZCR) within a varying-size window is utilized to analyze both the composite signal and the DDoS dataset. ZCR identifies all the distinct sections in the composite signal and successfully detects the occurrence of the cyberattack. The ZCR value increases as the signal under analysis becomes more complex and produces steadier values as the varying window size increases. The ZCR computation directly in the time-domain is its most notorious advantage for real-time implementations.

DOI: 10.4018/978-1-7998-5348-0.ch021

1. INTRODUCTION

The Internet has become an important part of our society in numerous ways, such as in economics, government, business, and daily personal life. An increasing amount of critical infrastructures (e.g., power grid and air traffic control) are managed and controlled via the Internet (Knowles, Prince, Hutchison, Disso, & Jones, 2015; Kriaa, Pietre-Cambacedes, Bouissou, & Halgand, 2015; Özçelik & Brooks, 2015), in addition to traditional infrastructure for communication. Today's cyberspace is full of attacks, such as Distributed Denial of Service (DDoS), information phishing, financial fraud, email spamming, and so on (Karim, Salleh, Shiraz, Shah, Awan, & Anuar, 2014; Yu, 2004).

Among various Internet based attacks, denial-of-service (DoS) attack is a critical and continuous threat in cybersecurity (Kinsner, 2012). DoS attacks are implemented by either forcing a victim computer to reset or consume its resources (e.g., access to application programming interfaces (APIs) (Balkanli, Alves, & Zincir-Heywood, 2014), CPU cycles, memory or network bandwidth (Beitollahi & Deconinck, 2014; Bhuyan, Kashyap, Bhattacharyya, & Kalita, 2014). Hence, the targeted computer no longer provides its intended services to legitimate users. When the DoS attacks are organized by multiple distributed computers, it is called distributed denial-of- service (DDoS) attack, which is a popular attack method in the cyberspace (Kaspersky Lab., 2014). Network security branches into three categories: confidentiality, availability and integrity. DDoS attacks belong to the availability category (Yu, 2004).

Despite all the efforts from industry participants and academia, DDoS attack is still an open problem. Some of the essential reasons for this passive situation are: (1) the no security design of the ARPANET network. The Internet came from this private network, ARPANET. As a private network, there were very limited security concerns in the original design (Peng, Leckie, & Ramamohanarao, 2007). This private network became a public network in the 1990s, and now many killer applications are running on the Internet, such as e-business. Security patches have been developed and installed to circumvent the inherent vulnerabilities, however, the effectiveness of these efforts are sometimes limited. For example, the Internet was designed stateless, therefore, a receiver has no information about which routers a received packet went through. Hence, it is easy to perform source IP spoofing; (2) Internet is the largest man-made system in human history. Cyberspace is huge and complex, and stays in an anarchy status; (3) Cyber attackers are enjoying one incredible advantage of the cyberspace: it is hard for defenders to technically identify attackers. Moreover, there lacks international laws or agreements among nations to bring cyber criminals to justice who commit crimes in one country but are living in other countries; (4) Hacking tools and software are easy to obtain. An attacker may not need profound knowledge of networking or operating systems to initiate a cyber attack (Yu, 2004). This paper proposes the study of Lévy walks and explores their connection to real DDoS datasets considering the similarities in their probability distribution functions (pdf).

Biologists have found that mobility patterns of foraging animals (e.g., spider monkey, albatrosses (seabirds), jackals, and marine predators) resemble what physicists have long called Lévy-walks (Atkinson, Rhodes, Macdonald, & Anderson, 2002; Ramos-Fernandez, Morales, Miramontes, Cocho, Larralde, & Ayala-Orozco, 2004; Viswanathan, Afanasyev, Buldyrev, Murphy, Prince, & Stanley, 1996). The term "Lévy-walk" was coined by (Shlesinger, Klafter, & Wong, 1982) to explain atypical particle diffusion not governed by Brownian motion (BM) (Rhee, Shin, Hong, Lee, Kim, & Chong, 2011; Rhee, Shin, Hong, Lee, & Chong, 2008).

Patterns of human mobility have features resembling Lévy walks (e.g., heavy-tail flight and pause-time distributions and the superdiffusive nature of mobility (Rhee et al., 2011)). Some deviations from