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, Department of Electrical and Computer Engineering, University of Manitoba, 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 cybersecurity 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.

KEYWORDS


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))
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 pure Lévy walks, in human mobility, occur due to various factors specific to humans (e.g., geographical constraints such as roads, buildings, obstacles and traffic) (Rhee et al., 2008). General examples of Lévy-processes are: Poisson processes, compound Poisson processes, BM, Gamma processes, inverse Gaussian processes, and those with stable distributions (Kyprianou, 2014).

Biological systems exhibiting Lévy-walks have been of inspiration for designing adaptive behaviour in robotic applications and artificial agents. The behaviour imitation of biological creatures has contributed to the advancement of adaptive searching (Nurzaman, Matsumoto, Nakamura, Koizumi, & Ishiguro, 2009). Motion of bacteria responding to the presence of chemical concentration gradients, aka bacterial chemotaxis, has been adopted and implemented to realize simple yet effective searching behaviour for gradient-inducing targets in robots or artificial agents (Rhee et al., 2011). Lévy-walks are also applied in complex mobile sensing scenarios related to the Internet-of-Things (IoT), where smartphones are taking a central role. Smartphones allow crowd-sourced sensing in the IoT because of their embedded different types of sensors (e.g., camera, microphone, GPS, thermometer, accelerometer, and communications like Wi-Fi, Bluetooth, and near field communications (NFC)) (Thejaswini, Rajalakshmi, & Desai, 2014). Due to the nature of human mobility, smartphones are immersed in scenarios subjected to Lévy-walks when monitoring environmental factors like temperature, humidity, urban noise pollution, carbon footprint, air pollution, and urban traffic (Thejaswini et al., 2014).
Potentials of Quadratic Neural Unit for Applications
Ricardo Rodriguez, Ivo Bukovsky and Noriyasu Homma (2013). Advances in Abstract Intelligence and Soft Computing (pp. 343-354).
www.igi-global.com/chapter/potentials-quadratic-neural-unit-applications/72791?camid=4v1a

Using Data Masking for Balancing Security and Performance in Data Warehousing
www.igi-global.com/chapter/using-data-masking-balancing-security/72501?camid=4v1a