# Detecting DDoS Attacks Using Polyscale Analysis and Deep Learning

Maryam Ghanbari, University of Manitoba, Winnipeg, Canada

Witold Kinsner, University of Manitoba, Winnipeg, Canada

## ABSTRACT

Distributed denial-of-service (DDoS) attacks are serious threats to the availability of a smart grid infrastructure services because they can cause massive blackouts. This study describes an anomaly detection method for improving the detection rate of a DDoS attack in a smart grid. This improvement was achieved by increasing the classification of the training and testing phases in a convolutional neural network (CNN). A full version of the variance fractal dimension trajectory (VFDTv2) was used to extract inherent features from the stochastic fractal input data. A discrete wavelet transform (DWT) was applied to the input data and the VFDTv2 to extract significant distinguishing features during data pre-processing. A support vector machine (SVM) was used for data post-processing. The implementation detected the DDoS attack with 87.35% accuracy.

## KEYWORDS

Anomaly Detection Method, Convolutional Neural Network, Cyber and Physical Network Security, Discrete Wavelet Transform, Distributed Denial of Service Attack, Variance Fractal Dimension

## INTRODUCTION

A smart grid is an innovative electricity delivery system that uses a bidirectional communication network to connect the power providers' control systems and the consumers' smart meters (Yan, Qian, Sharif, & Tipper, 2013), (Beigi Mohammadi, Mišić, Mišić, & Khazaei, 2014). The purposes of the smart grid are (i) to increase the availability and the reliability of electricity, (ii) to control the system in real-time, (iii) to deliver power to users in a safe and secure infrastructure, (iv) to save energy, and (v) to reduce costs. However, hackers can attack the smart grid's cyber layer, which consequently can affect its physical domain. These attacks can disrupt the smart grid's benefits. A *distributed denial of service* (DDoS) attack is a common type of cyber-attack, which delays or blocks the communication in the smart grid, thus causing power outages (Asri & Pranggono, 2015). Cyber space infections can have serious impacts on the real world. A smart grid infrastructure and the *supervisory control and data acquisition* (SCADA) systems, used in power generation, water management and oil pipelines are examples of physical systems that are disrupted by cyber space infections (Nazir, Patel & Patel, 2017), (Asri & Pranggono, 2015). When the operation of physical devices is altered by the attack, the standard cybersecurity problem becomes a cyber-physical security problem. Since the impact of the alteration may also affect the society in a city, or a region, or even a country, the problem escalates to a cyber-physical-social security. Such security systems should be treated using cognitive informatics and cognitive computing (Wang, 2002), (Kinsner, 2012).

Identifying normal burst-data behaviors of a network and the abnormal burst-data behaviors caused by DDoS attacks is very challenging. Both classes of network traffic have similar intrinsic characteristics. They are both stochastic time-series signals, non-periodic, broadband, self-affine, and multi-fractal. Therefore, to differentiate the two classes of traffic, distinguishing features must be extracted. Furthermore, the attack patterns are almost always changing and the new attack patterns

DOI: 10.4018/IJCINI.2020010102

and behaviors must be detected in the smart grid, which is also a frequently-changing environment. Therefore, a learning method that can detect new attack patterns and behaviors in frequently changing environments must be used (Beqiri, 2009). A deep learning algorithm is a good candidate to learn and classify normal behaviors from anomalous behaviors in such an environment (Goodfellow, Bengio & Courville, 2016).

This paper reports on the improvement of an anomaly detection method that was developed previously by Ghanbari, Kinsner, & Ferens (2017). The original detection method had two steps: (i) the pre-processing step that used a *discrete wavelet transform* (DWT) and (ii) the processing step that used a *convolutional neural network* (CNN). To improve the detection rate of the original method, in this study we added a full version of *the variance fractal dimension trajectory* (VFDTv2) to extract features from the non-pure fractal data that rely on long-range dependence as proposed originally by Kinsner (2007, 2012, 2015). The VFDTv2 was adjusted to consider all points including the boundary points of a dataset not just the marginal points. Moreover, the variance equation of the data series was adjusted to consider all points. In addition, the pre-processing step was used to extract more distinguishing features. Also, we added a support vector machine (SVM) as a post-processing step.

Some algorithms have been proposed to detect anomalous behavior in computer networks and smart grid infrastructures. Barford, Kline, Plonka, and Ron (2002) proposed an anomaly detection algorithm based on signal processing. The algorithm derived and summed high frequency, mid frequency and low frequency part of signals. DDoS attacks were detected based on 1.5 and 2 thresholds. However, the length of window and weighted sum for detection attack was static. Hu, Pota, and Guo (2014) offered an anomaly detection based on phase angle, current and voltage in a frame. The algorithm detected DDoS attacks based on unavailability or delaying phase angle. Due to their architecture, there might be instances where the attackers attack the root node, and take advantages of the bottleneck problem. Mohammadi et al. (2014) proposed a hierarchical IDS by considering several rules to detect known and unknown attacks. Khan, Ferens, and Kinsner (2015) offered an anomaly detection method to extract features of the Internet traffic time series by an autonomous sliding windowed the *variance fractal dimension trajectory* (VFDT) to extract the bursts of data sample, accurately. However, the current study applied the machine learning tools to distinguish DDoS attack from normal burst data behaviors with a higher detection rate. The paper that was developed previously reports on anomaly detection method (Ghanbari et al., 2017). The fundamental idea of this method was to enhance the sensitivity of detection by using distinguishing features by the DWT to increase the sensitivity of the CNN. However, the detection rate of 80.77% was not high enough in a smart-grid infrastructure.

The organization of this paper is as follows. Section 2 presents the dataset. Section 3 presents the proposed an anomaly detection method algorithm. Section 4 presents the simulation. Section 5 presents the results and discussion, and section 6 offers some concluding remarks.

## DATASET

The dataset that was used for training and testing in this research was downloaded from the *Center for Applied Internet Data Analysis* (CAIDA). CAIDA obtains different types of real time network traffic from around the world, and it has become one of the most reliable networks for downloading datasets. Commercial organizations, research sectors, and governments donate and collaborate with CAIDA while their privacy is protected (Center for Applied Internet Data Analysis, CAIDA, (2018). This center supports large-scale data collection for the scientific research community.

The dataset used in this research was chosen from CAIDA's 2007 DDoS-attack traffic, and it contained UDP Flood, TCP, ICMP (Ping) Flood, and SYN Flood packets. Each packet in the dataset contains a source IP address, a destination IP address, length of packet, protocol and packet-arrival time. The number of packets with 0.1ms duration within the stationary frame size is shown in Figure 1.