Chapter 23
The Improved LSTM and CNN Models for DDoS Attacks Prediction in Social Media

Rasim M. Alguliyev
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

Ramiz M. Aliguliyev
https://orcid.org/0000-0001-9795-1694
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

Fargana J Abdullayeva
https://orcid.org/0000-0003-2288-6255
Institute of Information Technology, Azerbaijan National Academy of Sciences, Baku, Azerbaijan

ABSTRACT

Automatic identification of conversations related to DDoS events in social networking logs helps the organizations act proactively through early detection of negative and positive sentiments in cyberspace. In this article, the authors describe the novel application of a deep learning method to the automatic identification of negative and positive sentiments in large volumes of social networking texts. The authors present classifiers based on Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) to address this problem domain. The improved CNN and LSTM architecture outperform the classification techniques that are common in this domain including classic CNN and classic LSTM in terms of classification performance, which is measured by recall, precision, f-measure, train loss, train accuracy, test loss, and test accuracy. In order to predict the occurrence probability of the DDoS events the next day, the negative and positive sentiments in social networking texts are used. To verify the efficacy of the proposed method experiments is conducted on Twitter data.

DOI: 10.4018/978-1-7998-5348-0.ch023

1. INTRODUCTION

Recently, cyber-attacks have become widespread, targeting giant corporations such as Sony, Verizon, Yahoo, Target, JP Morgan, Ashley Madison, and government agencies. Cyber-attacks are cause of leakage of sensitive information of users, loss of lives, the destruction of critical infrastructures.

The most common cyber-attacks are DDoS (Distributed Denial of Service) attacks (Kaur et al., 2017), uses multiple compressed systems to cut or stop the services of hosts connected to the Internet (Carl et al., 2006). Usually, web servers of the bank or credit card payment networks are the target of such attacks. Therefore, a single attack may cause considerable loss (Matthews, 2014). Detecting and predicting DDoS attacks is a challenging task (Bleakley & Vert, 2014; Imamverdiyev & Abdullayeva, 2018). The purpose of the traditional DDoS detection system is to distinguish malicious packet traffic from normal traffic (Mirkovic & Reiher, 2004). The malicious traffic in the network occurs after the DDoS attack takes place. In the detection of DDoS attacks prior to occurring the data of the social network have a great importance. On the basis of social media data, it is possible to track the traces of subjects targeted by the object.

Most information security experts believe that hacking attacks on businesses will be carried out through social media channels. Facebook, LinkedIn, Twitter are the most widely used networks. Social networks, besides allowing people to connect with each other, but also become a powerful political tool (Hua et al., 2013). Social media is regarded as the next big cybercrime vector (George, 2014).

At usual social media is considered as a sensor that collects information about various social events such as, disease epidemics, protests, elections and so on. The exponential growth of data containing the society opinion in the Web environment led researchers to focus on opinion mining and sentiment analysis of social media data (Ebrahimi et al., 2016). Among social media websites, the Twitter is a site that publishes more information on social issues, natural disasters, incidents and DDoS attacks planning. By analyzing Twitter, it is possible to identify the discussed events that will be occurred and analyze the trajectories (sources) of these events. Additionally, when analyzing the sentiments of the peoples related to the events which will be occurring, it is possible to get a lot of information about a certain event. Analysis of the sentimental traces allows to conduct the sentiment analysis by space and time, and predict the sentiments of the users in advance.

In (Liu & Zhang, 2012), the review of the various approaches related to opinion mining and sentiment analysis is provided. In (Jiang et al., 2011), the method for the providing classification of the sentiments in social media discussions into positive, negative, and neutral classes is proposed. This is a targeted sentiment analysis.

Another application area of the targeted sentiment analysis is to determine what do think people of one country about people of another country. In (Chambers et al., 2015), in order to model the relations between states, the "country-to-country sentiment data" are used. The data classification here is provided based on Bootstrapped classifiers.

The subject of the sentiment analysis is a text. There are two methods of sentiment analysis:

1. **Dictionary-based methods:** In (Taboada et al., 2011), sentiment analysis method, named as SO-CAL (Semantic Orientation CALculator) is proposed. Here in order to classify positive and negative sentiment, the dictionary is used. In this approach, each word is assigned a numerical value;
2. **Machine learning methods:** In the machine learning based sentiment analysis method, by using the statistical method called word embedding, each word is assigned values as a vector form and