Chapter 9
Detection of DDoS Attack Using Naive Bayes Classifier

Md Amir Khusru Akhtar
Usha Martin University, India

Mohit Kumar
Cambridge Institute of Technology, India

ABSTRACT

Naive Bayes classifiers are a set of categorization techniques based on Bayes' theorem. It is a collection of algorithms where all these algorithms share a common principle. This chapter presents the detection of DDos attack using scoreboard dataset. The dataset is separated into two parts, that is, feature vector and the reaction vector. Feature vector contains all the rows of dataset in which each vector consists of the value of dependent features such as IP address, port, counter, flag, syncnt, no. of packets, etc. The reaction vector contains the value of class variable (prediction or output) for each row. Result shows the effectiveness of the model in preventing DDoS attack by classifying request.

INTRODUCTION

A denial-of-service attack is an attempt that makes a computer resource unavailable to the intended users by flooding of Internet traffic. In DDoS attack, the incoming internet traffic flooding the sufferer originates from a lot ofdiverse sources. Thus it is impossible to stop because it originates from many different sources(Salim et al., 2019; Srivastava et al., 2011; *US20190182266A1—System and method for out of path ddos attack detection—Google Patents*, n.d.; Zargar et al., 2013).In literature

DOI: 10.4018/978-1-7998-2795-5.ch009

several defense mechanisms for denial-of-service attacks and mechanisms (Fenil & Kumar, 2019; Swami et al., 2019) have been proposed but these mechanisms are still in its natal stage.

This paper presents the detection of DDOS attack using Naive Bayes Classifier. Naive Bayes classifiers are a set of categorization algorithms and it uses Bayes' Theorem(Murphy, 2006). Naive Bayes classifiers are a set of probabilistic classifiers which uses Bayes' theorem and conditional probability model to classify instance of a problem. These methods are highly scalable and used for categorization in terms of features(Dinov, 2018). The proposed model uses a vector representing independent variables and assign probabilities to each instance of classes(*Pattern Recognition—An Algorithmic Approach | M.N. Murty | Springer*, n.d.). It uses Scoreboard Dataset(*DDoS attack scoreboard dataset*, 2019)and describes a number of parameters for the DDos Attack. Each record classifies the conditions as fit or unfit for detection and exclusion. The dataset is separated into two parts, that is, feature vector and the reaction vector. Feature vector contains all the rows of dataset in which each vector consists of the value of dependent features such as IP address, port, counter, flag, syncnt, no of packets etc. The Reaction vector contains the value of class variable (prediction or output) for each row. Result shows the effectiveness of the model in preventing DDoS attack by classifying request.

A lot of work have been proposed in the literature for the detection of DDos attack using Naive Bayes Classifier (Benferhat et al., 2008; Fouladi et al., 2016; Metsis et al., 2006; Mukherjee & Sharma, 2012).

Several digital watermarking techniques (Kumar, 2019; Kumar et al., 2014, 2016, 2017)along with cryptography have been proposed which uses digital content to protect the digital document from authorized and unauthorized users. These watermarking protocolsoffer secure and private transaction among the communicating parties.

In literature several defense mechanisms for denial-of-service attacks and mechanisms have been proposed. Finally, this gives an insight into future prospects in the research field for secured Internet services.

Hema and Shyni(Hema & Shyni, 2015)proposed a traffic classification method using naive bayes predictions for traffic flows. This classification scheme is based on posterior probability to identify attacks. The experimental outcome shows that the proposed system efficiently classifies packets.

Berguiget al. (Berguig et al., 2018) presented mobile agent-based techniques to resist Dos flooding attack. This work uses distributed Denial of service filter system that uses mobile agent and Naive Bayesian Filter. Experimental result shows the effectiveness and refuses Dos flooding attack.

A new Naive Bayes classification algorithm (Mehmood et al., 2018)has been proposed for intrusion detection systems (IDSs). It is defined to protect IoT