Chapter 2
One-Class ELM Ensemble-Based DDoS Attack Detection in Multimedia Cloud Computing

Gopal Singh Kushwah
National Institute of Technology, Kurukshetra, India

Surjit Singh
https://orcid.org/0000-0002-2386-7729
Thapar Institute of Engineering and Technology, India

Sumit Kumar Mahana
National Institute of Technology, Kurukshetra, India

ABSTRACT

Distributed denial of service (DDoS) attack affects the availability of multimedia cloud services to its users. In this attack, a huge traffic load is put on the victim server. Hence initially the server becomes slow to process legitimate requests and later becomes unavailable. Therefore implementing defensive solutions against these attacks is of utmost importance. In this work, the authors propose a bagging ensemble-based DDoS attack detection system for multimedia cloud computing. One class extreme learning machine (ELM) is used as a base classifier. An outlier detection based approach has been used to detect these attacks. Experiments have been performed using two benchmark datasets NSL-KDD and CICIDS2017 to evaluate the performance of the proposed system.

DOI: 10.4018/978-1-6684-6864-7.ch002

INTRODUCTION

In recent years, there is enormous growth in the number of multimedia devices due to the rapid development of the Internet and mobile networks. This increases the demand for multimedia applications and services such as online image editing, online gaming, video conferencing, storage, etc. Since these services require high storage and processing capabilities, the adoption of cloud infrastructure for this purpose has become popular which is known as multimedia cloud computing (Zhu et al., 2011). In this model, the service providers offer various types of multimedia services like storage and processing. Users with resource-constrained devices can use these services as utilities. Multimedia cloud computing must provide multimedia content according to the user's quality of service requirements in an efficient and timely manner. For the smooth functioning of this technology, its services must be available all the time. Attackers can use DDoS attacks (Lau et al., 2000) to hinder the availability of these services. In these types of attacks, the attacker uses many devices from the Internet to send huge traffic to the cloud server. It results in the exhaustion of bandwidth and other resources in the cloud and it becomes unavailable to its legitimate users. Therefore developing solutions against these attacks becomes important.

Machine learning has become popular in the area of intrusion detection. Several machine learning-based solutions for detecting DDoS attacks and other types of intrusions have been proposed in the literature. In (Bhushan & Gupta, 2019), a method to detect and mitigate fraudulent resource consumption (FRC) attacks is proposed. The attack detection approach is based on a hypothesis test. After detecting the attack, network flow analysis and Turing test are used to identify the bots. In (Garg et al., 2019), a deep learning-based anomaly detection system is proposed. An ensemble of restricted Boltzmann machine (RBM) and support vector machine is used as a classifier. RBM is modified to incorporate dropout functionality, and SVM is modified by encapsulating mixed kernel function and gradient descent. A hybrid intrusion detection system is proposed in (Venkatraman & Surendiran, 2020). The first module is signature-based and uses rules from Snort and IoT networks. Signature updation is performed by using crowd sourced framework. The second module is based on timed automata that works as anomaly based IDS. In (Sathya et al., 2021), a detection technique based on dual weight updation-based optimal deep belief network is proposed. It uses median absolute deviation around the median-based Kolmogorov-Smirnov test for feature extraction and robust confidence interval-based chimp optimization technique for feature selection.

The authors in (Gopi et al., 2021) proposed an ANN-based method for DDoS attack detection. They used Levenberg – Marquardt (LM) method to train the ANN. The principal component analysis is used for feature reduction. In (Hsu et al., 2021),