An Empirical Evaluation of Cognitive DDoS Detection Methods and Influential Factors

Xiaoyu Liang  
University of Pittsburgh,  
Computer Science Department  
xi160@pitt.edu

Taieb Znati  
University of Pittsburgh,  
Computer Science Department  
znati@pitt.edu

Introduction

Distributed Denial of Service (DDoS) Attacks attempt to prevent legitimate users from accessing information or services by overwhelming the server and saturating the network connections through multiple compromised systems. DDoS attacks have been growing dramatically in frequency, sophistication and impact, making it one of the most challenging threats in the Internet.

Several surveys provide an extensive classifications of both DDoS attacks and defense mechanisms, from different perspectives [1,2]. However, there is little effort dedicated to evaluating empirically the proposed solutions to DDoS attacks. This is due, not to intentional neglect, but rather to the limited number of publicly available benchmarks and the complexity to carry out empirical evaluation of DDoS defense methods, in a realistic environment. In this paper, an attempt is made to address the shortcoming. It is worth noting that an accurate and robust detection strategy plays an indispensable role in any successful defense systems. Thus, in this paper, we carry out an empirical evaluation of a representative class of DDoS detection techniques.

Datasets

We combine the advantages of CAIDA 2007[3] and DARPA 1999 datasets[4]. CAIDA benchmark is useful in modelling DDoS attacks, as it exclusively recorded DDoS attack traffic. DARPA benchmark is useful in modelling legitimate traffic, as it ensures the similarity with real world network traffic. To generate a dataset that is as closely representative of an "ideal" dataset as possible, we carefully select data from DARPA and CAIDA benchmarks and mix them to build our evaluation benchmark.

Experiments

• Comparative Analysis: is there a specific method that outperforms others in all test cases?
• Sensitivity Analysis: analyzing the influence of four impact factors:
  o Proportion of observed traffic
  o DDoS attacking phases
  o Different types of flows (elephant vs. mice)
  o Different attacking intensity

There is no method that outperforms all others in all traffic sets (Fig 3). Statistical methods are very sensitive to the observed proportion of traffic (Fig 4).

Results

While machine learning based methods are relatively resistant to this factor. Different DDoS attacking phases clearly impact the detection accuracy for all assessed methods. Traffic flow types and attack intensity did not play a significant role for statistical methods. However, they influenced the performance of machine learning based methods. Training with higher percentage of elephant flows lead to a lower accuracy performance and higher standard deviations (Table 1).

Table 1: Average accuracy of ANN, naive with different attack intensities and different percentage of elephant flows.

References