An Empirical Evaluation of Cognitive DDoS Detection Methods and Influential Factors

Xiaoyu Liang
University of Pittsburgh,
Computer Science Department
xil160@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

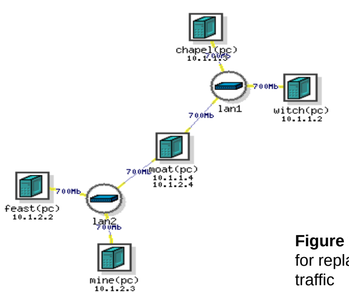

Figure 1. Environment setup for replaying captured network traffic

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.

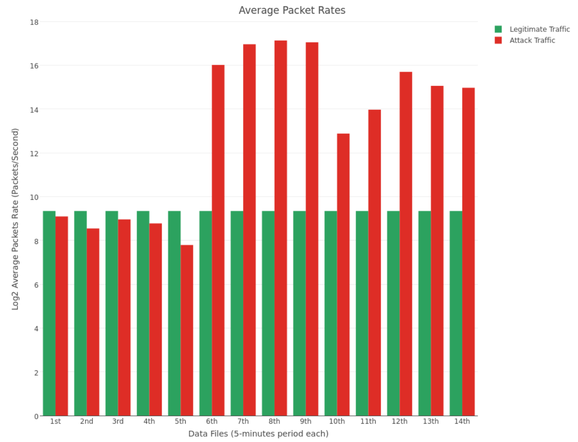

Figure 2. Packet rate of legitimate and attack traffic

Experiments

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

Results

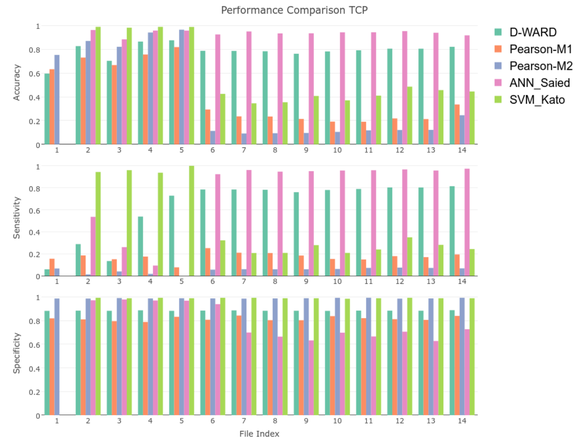

Figure 3 Comparative analysis results -- TCP

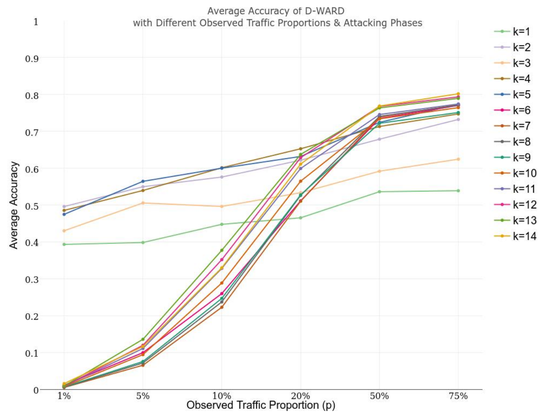

Figure 4 Average accuracy of D-WARD with different proportions of observed traffic

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). 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).

Percentage of Elephant Flows in Training	Attack Traffic Intensities (p_a)	Average Accuracy	Standard Deviation
1%	10%	0.9485	0.0960
	20%	0.9582	0.0997
	30%	0.9605	0.0845
	40%	0.9637	0.0650
	50%	0.9591	0.0694
	60%	0.9444	0.1077
	70%	0.9342	0.1402
5%	10%	0.9664	0.0318
	20%	0.975	0.0265
	30%	0.9715	0.0332
	40%	0.9693	0.0381
	50%	0.9684	0.0421
	60%	0.96	0.0544
	70%	0.9562	0.0608
10%	10%	0.7194	0.3558
	20%	0.7157	0.3795
	30%	0.7098	0.3858
	40%	0.7105	0.3849
	50%	0.7129	0.3822
	60%	0.7119	0.3758
	70%	0.7119	0.3690
25%	10%	0.7464	0.3417
	20%	0.7451	0.3633
	30%	0.7381	0.3734
	40%	0.7368	0.3776
	50%	0.7377	0.3789
	60%	0.7343	0.3816
	70%	0.7334	0.3830

Table 1. Average accuracy of ANN_saied with different attack intensities and different percentage of elephant flows.

References

[1] J.Mirkovic and P.Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms”, *SIGCOMM Compt. Commun. Rev.,* vol. 34, no.2, pp. 39-53, 2004.

[2] M.H.Bhuyan, H.J.Kashyap, D.K.Bhattacharyya and J.K.Kalita, “Detecting distributed denial of service attacks: Methods, tools and future directions”. Computer Journal, vol. 57, pp.537-556, 2014.

[3] “The CAIDA ‘DDoS attack 2007’ Dataset”, https://www.caida.org/data/passive/ddos-20070804_dataset.xml. Accessed: March 2018.

[4] “1999 DARPA Intrusion Detection Evaluation Data Set”, https://www.ll.mit.edu/ideval/1999data.html. Accessed: March 2018.