Chapter 1
Dual-Level Attack Detection, Characterization, and Response for Networks under DDoS Attacks

Anjali Sardana
Indian Institute of Technology Roorkee, India

Ramesh C. Joshi
Indian Institute of Technology Roorkee, India

ABSTRACT

DDoS attacks aim to deny legitimate users of the services. In this paper, the authors introduce dual-level attack detection (D-LAD) scheme for defending against the DDoS attacks. At higher and coarse level, the macroscopic level detectors (MaLAD) attempt to detect congestion inducing attacks which cause apparent slowdown in network functionality. At lower and fine level, the microscopic level detectors (MiLAD) detect sophisticated attacks that cause network performance to degrade gracefully and stealth attacks that remain undetected in transit domain and do not impact the victim. The response mechanism then redirects the suspicious traffic of anomalous flows to honeypot trap for further evaluation. It selectively drops the attack packets and minimizes collateral damage in addressing the DDoS problem. Results demonstrate that this scheme is very effective and provides the quite demanded solution to the DDoS problem.

INTRODUCTION

Attack detection is the first necessary element of a complete DDoS defense system. The DDoS attack detection problem consists of designating those points in time at which network is experiencing an attack. Only by timely detection of DDoS attacks, system can make proper response to escape big loss.

Many techniques have been suggested so far for DDoS attack detection (Bencsath & Vajda, 2004; Blazek, Kim, Rozovskii, & Tartakovsky,
2001; Carl, Kesidis, Brooks, & Rai, 2005; Gil & Poletto, 2001; Ioannidis & Bellovin, 2002; Lakhina, Crovella, & Diot, 2005; Mahajan, Floyd, & Wetherall, 2001). Detecting a DDoS attack is relatively easy at the victim network (Bencsath & Vajda, 2004; Blazek et al., 2001; Gil & Poletto, 2001) because it can observe all the attack packets. However, attack packets clog a large part of the network before they are detected at the victim. Early attack detection schemes (Carl et al., 2005; Ioannidis & Bellovin, 2002; Mahajan et al., 2001) unfortunately, have to wait for the flooding to become widespread. Consequently, they are ineffective to fence off the DDoS timely. Moreover, early packet drops can cause collateral damage, as legitimate packets are also dropped with aggregate of attack flows. Many of the present DDoS attack detection techniques are complex, difficult to deploy or lead to computational and memory overheads (Bencsath & Vajda, 2004; Blazek et al., 2001; Carl et al., 2005; Gil & Poletto, 2001; Ioannidis & Bellovin, 2002; Lakhina et al., 2005; Mahajan et al., 2001).

Unlike earlier proposals for attack detection (Bencsath & Vajda, 2004; Blazek et al., 2001; Carl et al., 2005; Gil & Poletto, 2001; Ioannidis & Bellovin, 2002; Lakhina et al., 2005; Mahajan et al., 2001) that are either based on unreliable assumptions or too complicated to implement, our dual-level based scheme is simple to understand and implement. It is capable of handling infiltrating, sophisticated as well as highly distributed attacks and provides a basis for characterization. It adapts to varying network conditions with minimum false alarms.

The rest of the paper is organized as follows. The traffic feature selection is described, followed by an overview of dual-level attack detection (D-LAD) scheme. Design of macroscopic level attack detector is explained next whereas design of microscopic level attack detector is given after that. Then, the overall response technique is discussed and the performance of our proposed scheme is evaluated. Finally, the paper is concluded.

TRAFFIC FEATURE SELECTION

DDoS attacks are launched from distributed sources. Hence the attack traffic is spread across multiple links. As the distance from the victim increases, attack traffic is more diffused and harder to detect because the volume of attack flows are indistinguishable from legitimate flows. Current schemes for early attack detection are based on detecting aggregates causing sustained congestion on communication links (Ioannidis & Bellovin, 2002; Mahajan et al., 2001), imbalance between incoming or outgoing traffic volume on routers (Carl et al., 2005) and probabilistic packet marking techniques. These early detection methods, unfortunately, have to wait for the flooding to become widespread, consequently, they are ineffective to fence off the DDoS timely.

Lakhina et al. (2005) observed that most of traffic anomalies despite their diversity share a common characteristic: they induce a change in distributional aspects of packet header fields (i.e., source address, source port, destination address, and destination port etc called traffic features).

Let an information source have n independent symbols each with probability of choice $p_i$. Then the entropy H is defined as:

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{1}$$

Entropy can be computed on a sample of consecutive packets. The entropy detection method is used to calculate the distribution of randomness of some attributes which are fields in the network packets’ headers. These attributes can be values like source IP address, TTL etc. that indicate the packet’s properties. Entropy captures in a single value the distributional changes in traffic features, and observing the time series of entropy on the features exposes unusual traffic behavior.

Source IP based entropy algorithms are efficient in case of highly distributed DDoS attacks.
Related Content

Imagine Mobile Learning in your Pocket
www.igi-global.com/chapter/imagine-mobile-learning-your-pocket/46566?camid=4v1a

Adoption of Mobile Reading Devices in the Book Industry
www.igi-global.com/chapter/adoption-mobile-reading-devices-book/68083?camid=4v1a

Reconstructing Handwriting Character Font Models with Incorrect Stroke Order
Hirotsugu Matsukida, Yuta Mieno and Hiroyuki Fujioka (2014). International Journal of Mobile Computing and Multimedia Communications (pp. 1-12).
www.igi-global.com/article/reconstructing-handwriting-character-font-models-with-incorrect-stroke-order/128996?camid=4v1a

The Robustness of RM-DSR Multipath Routing Protocol with Different Network Size in MANET
www.igi-global.com/article/robustness-dsr-multipath-routing-protocol/78385?camid=4v1a