Detecting DDoS Attacks Based on Multi-stream Fused HMM in Source-End Network

Jian Kang, Yuan Zhang, and Jiu-bin Ju

Department of Computer Science & Technology, Jilin University,
Changchun, 130012, China
kj885788@gmail.com

Abstract. DDoS (Distributed Denial-of-Service) attacks detection system deployed in source-end network is superior in detection and prevention than that in victim network, because it can perceive and throttle attacks before data flow to Internet. However, the current existed works in source-end network lead to a high false-positive rate and false-negative rate for the reason that they are based on single-feature, and they couldn't synthesize multi-features simultaneously. This paper proposes a novel approach using Multi-stream Fused Hidden Markov Model (MF-HMM) on source-end DDoS detection for integrating multi-features simultaneously. The multi-features include the S-D-P feature, TCP header Flags, and IP header ID field. Through experiments, we compared our original approach based on multiple detection feature with other main algorithms (such as CUSUM and HMM) based on single-feature. The results present that our approach effectively reduces false-positive rate and false-negative rate, and improve the precision of detection.

1 Introduction

Comparing with DDoS detection system in victim network, source-end DDoS detection not only can perceive and prevent from attacks early, but also enhance security and QoS of the whole network. However, the attack flow in source-end network is so dispersive that the traditional detecting algorithm troubled in distinguishing attack flows and normal flows, and led to high false-positive rate and false-negative rate. Thus, the key problem is how to raise precision and sensitivity of source-end DDoS detection.

The existed detection sysytems are based on single-feature extracted from source-end network, so they could not synthesize multiple factors. Although the single-feature detection algorithm has been improved, it limited in precision rising—it cannot describe complex diversification in source-end network.

Therefore, this paper proposes a novel approach using Multi-stream Fused Hidden Markov Model (MF-HMM) on source-end DDoS detecting for integrating multi-features simultaneously. The multiple factors include the S-D-P feature, the Flags and the ID field contained in TCP/IP header. Experiments can help us compare MF-HMM with other models like CUSUM algorithm and HMM based on single observing feature. The results present that MF-HMM

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 342–353, 2006.

effectively reduce the false-positive rate and false-negative rate. The MF-HMM proposed in this paper can adapt to diversified network and raise the precision of detection.

2 Related Work

Mirkovic et al. proposed D-WARD as a representative source-end DDoS detection system in [1]. In a normal TCP session, the flow from source to destination (which is defined as TCP_sent_to) is controlled by the reverse acknowledge flow (TCP_received_from). Under DDoS attacking, TCP_sent_to is far greater than TCP_received_from. D-WARD defines max_tcprto as the max possible rate for TCP_sent_to/TCP_received_from under normal network environments. If the observed rate is higher than max_tcprto in real time, it is determined as an attack. However, the false-positive rate and false-negative rate in D-WARD is high.

Paper [2] extracted the same ratio with that in D-WORD as observing feature. But because of introducing a nonparametric change point detection method in statistics and improving D-WARD by nonparametric recursive CUSUM algorithm, the improved system is more advanced in detecting precision than D-WARD.

Peng et al. in [3] considered the number of new source IP addresses appeared in data flow in unit time as observing feature. The abnormal increase of this number determines if attacks appeared. They used CUSUM algorithm to detect source-end DDoS attacks. However, high false-positive rate is led because they took only one feature into account.

Zhou et al. in [4] used HMM to detect DDoS attacks. They use TCP Header Flags to describe TCP package as observing feature. They constructed the observing sequence with the weight sum of each bit of TCP Header Flags, and trained HMM by data packages under normal network. The trained HMM can be seen as criterion to judge if there are attacks.

Therefore, existing researches on source-end DDoS detecting system are based on single-feature. Although there are improvements to the algorithms themselves, the insufficient detection information contained in single-feature constrains the enhancement of the detecting precision.

3 Multi-features Extraction

Moore et al. in [5] presented a famous result: most DDoS attacks use TCP package (over 94%), then UDP package (2%) and ICMP package (2%). From the result, we can see the importance of detecting TCP packages in DDoS attacks. Thus, in this paper, extracting and detecting multi-features of TCP Flooding attacks are to be discussed. Analyzed characteristics and mechanisms of representative DDoS attacks, we defined the conception of S-D-P feature. Preparing for MF-HMM represented in Sect.4, we constructed multi-features including S-D-P feature, TCP Header Flags and ID field in IP Header.