International Journal of Innovative Computing, Information and Control
Volume **4**, Number **3**, March **2008**

 ISSN 1349-4198
pp. 749–759

OBSERVATION-BASED DETECTIVE METHOD FOR SYN FLOODING ATTACKS

Takuo Nakashima[1,2], Shunsuke Oshima[3] and Toshinori Sueyoshi[2]

[1]Department of Information Science
Kyushu Tokai University
9-1-1 Toroku, Kumamoto 862-8652, Japan
taku@ktmail.ktokai-u.ac.jp

[2]Graduate School of Science and Technology
Kumamoto University
2-39-1 Kurokami, Kumamoto, Japan
sueyoshi@cs.kumamoto-u.ac.jp

[3]Information and Electronic Engineering
Yatsushiro National College of Technology
2627, Hirayama-Shinmachi, Yatsushiro, Kumamoto, Japan
oshima@as.yatsushiro-nct.ac.jp

Received February 2007; revised August 2007

Abstract. *The SYN flooding attack is a typical DoS (Denial of Service) method causing servers to retain the half-open state which results in the exhaustion of its memory resources. This attack is difficult to defend by routers in such a case that the source IP address is spoofed. In this paper, we present an observation-based detective method for SYN flooding attacks at an early stage. We implement an attacking program, and experiment to observe response packets and syncache area. Firstly, our method explores sensitive metrics based on the measured data to detect a condition caused by SYN flooding attacks. Secondly, the packet loss rate and syncache rate are adopted as a metric to identify whether the server is attacked or not, then the threshold values for each metric are determined. Finally, we detect the server performance if it exceeds the pre-determined threshold values, then the detective host sends RST packets to release the half-open state on TCP accordingly.*

Keywords : Observation-based method, SYN flooding attacks, Detective system, Denial of service

1. **Introduction.** DoS attacks easily happen taking advantage of the weakness of the network protocol and iterating requests of service for the application. Most organizations have opened their http and other ports on TCP to maintain their Web sites. DoS attacks aim directly at the application of Web server or TCP protocol to suspend their Internet services. In a DDoS (Distributed Denial of Service) attack, the assault is done together with many hijacked systems by a single attacker [1]. SYN flooding attacks [2, 3] disturb the establishment of the TCP connection. In this paper, "SYN" means that the SYN flag on TCP header is set and the Sequence number field on TCP header is valid synchronizing sequential numbers of data segment during the connection. "SYN+ACK" also means that the SYN and ACK flags on TCP header are set and the Sequence number and Acknowledgement number fields on TCP header are valid. An attacker does not respond to the SYN+ACK response from the server to which a huge amount of SYN requests is sent from the attacker with spoofed source IP addresses. As a result, TCP on the server should keep the huge number of the half-open state for each connection leading to the