International Journal of Innovative Computing, Information and Control
Volume **6**, Number **8**, August **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 3725–3735

EXTRACTION OF ANOMALY ACCESSED IP PACKETS FEATURES USING STATISTICAL METHOD

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

[1]Kumamoto National College of Technology
2627, Hirayama-Shinmachi, Yatsushiro, Kumamoto, Japan
oshima@kumamoto-nct.ac.jp

[2]School of Industrial Engineering
Tokai University
9-1-1 Toroku, Kumamoto, Japan
taku@ktmail.tokai-u.jp

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

Received April 2009; revised October 2009

Abstract. *To defend DoS (Denial of Service) attacks, an access filtering mechanism is adopted in the firewall or the IDS (Intrusion Detection System). The difficulty to define the filtering rules lies where normal and anomaly packets have to be distinguished in incoming packets. The purpose of our research is to explore the early detective method for anomaly accesses based on statistic analysis. In this paper, we defined the entropy and the chi-square method, and then analyzed the all amount of incoming packets to our College focusing on the source IP address. As the results, we extracted the following features. Firstly, the number of packets was the more suitable scale of the window in the chi-square method than the time scale. Secondly, the setting of the window size with 500 packets and 2 bins made the detection of the DoS attacks within 10 minutes for DNS packets possible. Finally, we verified that the DoS attacks from the same source IP address were detected using the chi-square method.*

Keywords: Entropy, Chi-square method, Statistical method, Detective system, Denial of service

1. **Introduction.** The rapid development of science and technology provides the diverse communication over the real and virtual world. The increase of private and P2P communication requires the secure communication. Chen et al. [1] showed the experimental study of secure communication of different scroll chaotic systems with identical structure, and concluded that two systems of generating different scrolls under different conditions can achieve the synchronization communication by a proper synchronizing method. To develop the secure communication systems, the quality of software systems is maintained for different users. Mu et al. [2] proposed the new flexibility theory and key technology for the software development of information system. The security software system also requires not the flexibility but the mechanism for the new detection and controlling technology for the attackers.

Weaknesses of the Internet protocol and the security hole of server software have caused indiscriminate DoS/DDoS (Distributed DoS) attacks. The damages of these attacks are not limited to the crash of servers, spreading to leak the confidential information to the public. Attacking packets concentrate on the well-known ports such as HTTP, DNS