International Journal of Innovative Computing, Information and Control
Volume **7**, Number **8**, August **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **4779–4788**

EFFICIENT CONTEXT-FREE GRAMMAR INTRUSION DETECTION SYSTEM

G. Gowrison[1], K. Ramar[2], K. Muneeswaran[3] and T. Revathi[4]

[1]Department of ECE
Institute of Road and Transport Technology
Post Box No. 2, Sri Vasavi College Post Erode, Tamilnadu 638316, India
gowrison@rediffmail.com

[2]Department of CSE
National Engineering College
K. R. Nagar, Kovilpatti, Thoothukudi District, Tamil Nadu 628503, India
kramar_nec@rediffmail.com

[3]Department of CSE
[4]Department of IT
Mepco Schlenk Engineering College
Sivakasi 626005, India
{ kmuni; trevathi }@mepcoeng.ac.in

Received February 2010; revised June 2010

Abstract. *Intrusion detection systems are becoming ubiquitous defenses in current networks and no complete and systematic methodologies available to test the effectiveness of these systems. Though there are various approaches, they are relatively ineffective in the classification and alarm rate dimensions. This paper proposes an intrusion detection system defined by a set of rules based on simple context-free grammar for normal and attacks. The packet data are passed through a Multi Stage Filter with focused capabilities. The proposed method promises good classification rate with low alarm rates tested with the one of the popular benchmark databases, KDD cup99 dataset.*
Keywords: Network security, Intrusion detection system, Grammar rule

1. **Introduction.** An intrusion is a malicious harm on information resources in which the troublemaker attempts to gain doorway into a system or disturb the normal operations. Incident response is the recognition of, classification of, response to, and revival from an incident called Intrusion Detection System (IDS). IDS is broadly classified into anomaly detection system and misuse detection model. An anomaly detection system uses normal user profile and identifies intrusions by detecting some discrepancy from the normal behavior. Furthermore, anomaly detection has the disadvantages: 1) it requires a large number of data to be observed to produce user behavior profiles and 2) causes rather high false alarm rates because any new user behavior which is not included in the user behavior profile is considered an intrusion. In misuse detection model, the IDS collects the non normal operating characteristics, and builds related database features. Also, misuse detection concentrates an intrusion by comparing the security activities with predefined security attack patterns, which are stored in attack database. These two classes of procedures applied in any embedded IDS methods to recognize attacks with very high certainty. Unfortunately, misuse detection is not able to identify novel or new intrusions because their pattern is not already defined and stored in a database. Hence, the disadvantage of misuse detection is the complexity of updating the database and the software system whenever new types of security attacks are discovered periodically. There are lots of works