The Parallelized Header Matching Algorithm for Intrusion Detection Systems

[1]Mohammad A. Alia, [1]Adnan A. Hnaif

[1] Faculty of Science and Information Technology – Al Zaytoonah University of Jordan,
P.O.Box: 130 Amman (11733) Jordan
dr.m.alia, dr.adnan_hnaif@zuj.edu.jo

Abstract

With the rapid evolution of the Internet and its applications, the current used network intrusion detection systems (NIDS) are becoming inefficient because of the amount of the traffic that needs to be processed daily. Moreover, current used NIDS implementations are inadequate to process all the traffic in real time. Therefore, the main objective of this paper is to enhance the speed of engine detection in real time for packet header in NIDS. We proposed a new parallelized matching algorithm for intrusion detection system called distributed packet header matching algorithm (DPHM). This algorithm can be run on a single processor or multiple-cores platform.

Keywords: Intrusion Detection System (IDS), Network Intrusion Detection System (NIDS), Packet Detection, Packet Header Matching (PHM) and Distributed Packet Header Matching (DPHM)