Multiprocessing Scalable String Matching Algorithm for Network Intrusion Detection System.

By

Duaa Hani Nazzal

Supervisor
Prof. Ali Al-Dahoud

Co-Supervisor
Dr. Adnan Ahmad Hnaif

Abstract

With high increasing speed of today's computer networks, which directly affects the performance of security issues in terms of detection speed, the traditional security tools such as firewall is insufficient to provide integrated, reliable and secure networks.

Intrusion Detection Systems (IDS) are one of the most reliable tools that can be used to monitor all the incoming and outgoing network traffic to identify unauthorized usage and mishandling of computer system networks.

Due to the fact, software which is used in Network Intrusion Detection System (NIDS) are still unable to detect all the growing threats in high-speed link. The main function of these kinds of attacks is to generate a large amount of traffic in high speed link which leads to slow down the performance of the detection engine in NIDS.

In this study, we have proposed a NIDS based on a scalable string matching algorithm to enhance the speed of NIDS detection engine, which called Multiprocessing Scalable String Matching Algorithm for Network Intrusion Detection System

(MSNIDS). The MSNIDS implemented by using enhanced weighted exact matching algorithm (EWEMA) in both sequential and parallel processing scenarios.

It is found that, the speed of detection engine can be improved in both sequential and in parallel processing via enhanced WEMA algorithm called (EWEMA). The sequential processing enhancements of EWEMA reduced the number of comparisons needs to match all the incoming packet payload with rule sets. In addition, the parallel processing which used the hybrid multiprocessors with multicores technique is also increased the speed of detection engine to make NIDS detection engine works with high speed link efficiently.

It is concluded that, the MSNIDS based on EWEMA enhanced the speed of detection engine in sequential processing more than 89% compared with WEMA algorithm. Furthermore, the MSNIDS enhanced the speed of detection engine in parallel processing more than 86% over sequential processing time.