Development of an Improved Intrusion Detection based Secured Robust Header Compression Technique

Abstract

This research presents the development of an Improved Intrusion Detection Secured RObstust Header Compression (IDSROHC) technique for handling brute force attack. The Secured RObstust Header Compression (Secured ROHC) was developed to secure internet protocol version six (IPv6) packets against false initial refresh attack by encrypting the cyclic redundancy check field. However, the CRC is only 3-8 bits long, which implies that a malicious node could still attempt a brute force approach, where it sends fake packets with all possible CRC combinations. An IDSROHC was developed using a modified selective watchdog intrusion detection algorithm. A MATLAB graphical user interface was design to aid presentation. IDSROHC was validated with Secured ROHC using throughput and packet delivery success. The results of this work show that IDSROHC produced 4.97% improvement in throughput and 29% improvement in packet delivery success over Secured ROHC.

References


Index Terms

Computer Science Information Sciences

Keywords

IDSROHC, Secured ROH, Brute force-Attack, Throughput, Packet delivery Success