DETECTING AND ELIMINATING ACTIVE TRAFFIC ATTACKS BY MONITORING NETWORK FLOW PATTERNS

SIVASUBRAMANIAM SIVARAJ

Postgraduate Institute of Science
P.O. Box 25, Peradeniya 20400
Sri Lanka

Pattern matching and traffic analysis are used in network instruction systems, which is formed from a detailed analysis of pattern matching statistics of the network traffic. In this work, we develop a monitoring system that can monitor online data traffic and identify patterns of suspicious data traffic which may be form malicious attacks. We design our system to generate synthetic traffic consisting of network systems targeting four different protocol data packets including ICMP, IGMP, TCP and UDP simultaneously, and then apply different pattern matching algorithms to detect differing patterns of traffic. Our initial investigation results are promising and our Enhanced experimental study with snort capturing software performance of our work show approximately similar behavior.