Adaptive Network Intrusion Detection Systems in Hardware

Farnaz Gharibian, Junaid A. Khan, and Ali Ghorbani
(W99bg, junaidk, ghorbani@unb.ca)

With increased growth in malicious network activity, Network Intrusion Detection Systems (NIDS) are exploited to protect distributed computer installations from attacks. NIDS, normally, performs complete payload inspection for each packet in order to detect an attack. Traditional software-based NIDS architectures fail to keep up their throughput on high speed networks because of complete payload inspection of packets. In recent years, hardware based computational intensive components, especially pattern matching, of the NIDS have been much favored. Current approaches in hardware implementation of NIDS components are based on Ternary Content-Addressable Memory (TCAM), Static Random Access Memory (SRAM), Network Processor, Reconfigurable Discrete Logic (RDL) and Application-Specific Integrated Circuit (ASIC) with each approach having its own pros and cons. However, there is a lack of complete and efficient hardware-based NIDS architectures, not just pattern matching. Furthermore, it is hard to keep high throughput in the architectures which does not need hardware changes to update NIDS rules. Reconfiguring hardware is not always a feasible option, especially if the NIDS rules are adaptive and may need updating frequently. Based on these shortcomings in current solutions, we aim to introduce an optimized entirely hardware-based NIDS that supports adaptive rule update, while keeping the high throughput to match multi Gigabit rates in high speed networks. Currently, we are in the starting phase of this research and have completed initial but ongoing literature review on hardware based NIDS.