SC26 Network Research Exhibition: Demonstration Publishable Abstract

Demonstrating FPGA-Accelerated Packet Processing for Network Anomaly Detection and Pre-Trade Risk Management

Yu-Kuen Lai, Chung Yuan Christian University, ylai@cnsrl.cycu.edu.tw
Jim Hao Chen, iCAIR, Northwestern University, jim-chen@northwestern.edu

Abstract

This demonstration presents two high-speed packet processing applications leveraging FPGA-based hardware acceleration for network anomaly detection and financial trading risk management. It builds on our SC25 Network Research Exhibition demonstration, which showcased a hybrid FPGA-P4 architecture for 400G line-rate packet processing. A Tofino2 P4 switch extracts the 5-tuple (source and destination Internet Protocol (IP) address, source and destination port, and protocol) from each incoming packet and buffers it in on-chip registers. After every four packets, the switch packs all four 5-tuples into a single Ethernet frame and forwards it to the FPGA. We extend the same packet-header processing pipeline to two latency-critical applications.

In anomaly detection, the flow-size distribution (FSD) describes how many traffic flows carry a given number of packets and captures the fine-grained structure of network traffic. Small flows, commonly called "mice flows," account for up to 99% of the FSD. Reconnaissance attacks often consist of such low-packet-count flows aimed at many hosts or ports, so a change in the mice-flow distribution can signal an emerging attack or anomaly. We propose MiceRadar, a compact fingerprint-counter data structure that accurately estimates the flow-size distribution by targeting the mice-flow region. To detect attacks, the system compares the FSD of the current interval with that of the previous interval using the Jensen–Shannon divergence (JSD), a measure of the difference between two distributions; a large JSD indicates a sudden change in traffic. An exponentially weighted moving average (EWMA) keeps a running mean and variance of the JSD, and an anomaly is flagged when the current JSD exceeds the resulting threshold. The threshold adapts to normal traffic changes that reduces false alarms while detecting both high-volume and low-rate attacks.

In financial trading, an order cannot be withdrawn once it reaches the exchange. There's a need for pre-trade risk checks before orders leave the broker. In collaboration with KGI Securities, we implement pre-trading risk checks on the FPGA. Implemented in the order path between the broker's trading system and the exchange. The system takes four inputs: Financial Information eXchange (FIX) orders, orders in the Taiwan Futures Exchange (TAIFEX) TMP format, execution reports, and market data. Its five-stage pipeline (1) parses network headers (layers 2 to 4) together with FIX, TMP and market-data messages; (2) reorders out-of-order and retransmitted Transmission Control Protocol (TCP) segments to reconstruct a continuous byte stream; (3) rebuilds FIX messages by identifying message boundaries while keeping parsing state across segments; (4) enforces limits on order amount and quantity, per-instrument positions, order rates, consecutive cancellations and whitelist membership; and (5) maintains a client-level order book in on-chip memory, calculates margins according to product-specific rules, and tracks execution reports and the trade book. A host computer sets the rule parameters and monitors system status. This work is covered by three patents (TW I769534B, TW I820977B and US 11979479B1).

Goals

1. Demonstrate anomaly detection using JSD and adaptive EWMA threshold detecting both volumetric and low-rate DDoS attacks.
2. Demonstrate FPGA pre-trade risk checks on FIX order traffic at 10 Gbps line rate with 1.3 to 2.3 microseconds of end-to-end latency.
3. Demonstrate the complete anomaly detection pipeline in FPGA hardware on live 400 Gbps traffic validating the current software-based evaluation.

Impacts

Network operators need monitoring that keeps pace with 400 Gbps links. In anomaly detection, focusing on the mice-flow region of the flow-size distribution gives an additional practical early-warning signal, as recent reconnaissance and low-rate attacks hide in the traffic volume. In finance technology, moving pre-trade risk checks from software-based into an FPGA-based cuts the processing latency to the microsecond level while keeping every order under risk control, and validation on mirrored live traffic in a broker's data center shows the approach is practical outside the laboratory. The collaboration of Chung Yuan Christian University, KGI Securities, and the

International Center for Advanced Internet Research (iCAIR) at Northwestern University links academic research, industry practice, and international research networking. The next steps are implementing the complete MiceRadar detection pipeline in FPGA hardware at 400 Gbps and demonstrating the risk-management system.

Resources

The demonstration uses the iCAIR P4/FPGA programmable real-time packet header processing testbed. It includes a Tofino2 P4 programmable switch; two traffic generators, the Monsterbox (two 200 Gbps MT28908 NICs) and AMD5DTN1 (one 400 Gbps MT2910 NIC); an AMD Xilinx Alveo U200 FPGA running the NetFPGA-PLUS framework and a host computer for configuration and monitoring. The anomaly detection demonstration replays MAWI backbone traffic mixed with CAIDA DDoS 2007 and CICDDoS2019 attack traces. The risk-management demonstration uses an FPGA with 10 Gbps Ethernet interfaces carrying FIX orders, TAIFEX TMP orders, execution reports, and market data.

Involved Parties

- Drixter V. Hernandez, Chung Yuan Christian University
- Sheena Chang, Chung Yuan Christian University
- Rui-Jie Chang, Chung Yuan Christian University
- He-Ping Li, Chung Yuan Christian University
- Cheng-Han Chuang, Chung Yuan Christian University
- Cheng-Sheng Chang, Chung Yuan Christian University
- Kai-Po Chang, Chung Yuan Christian University
- Chao-Lin Wang, KGI Securities Co., Ltd.
- Fei Yeh, iCAIR, Northwestern University
- Joe Mambretti, iCAIR, Northwestern University