Accelerate Pattern Recognition for Cyber Security Analysis

Mohammad Tahghighi, Wei Zhang

Electrical and Computer Engineering Dept., Hong Kong University of Science & Technology
Introduction and Motivation

- **Goal:**
  - Capture interesting network pattern (Security application)

- **Input:**
  - Netflow record (generated by routers)
  - Has several fields like src/dest IP address

- **Challenge:**
  - Rate: several kilo netflow/sec
  - Processing is complex and time consuming
  - Difficult to parallelize

- **Solution**
  - hardware/software co-designed system

- **Example of a pattern:**
  - IP a accesses IP b
  - Then IP a accesses IP c
  - The above sequence repeated many times
Overall System Architecture

- **Software**
  - Log parser: parse raw input and import into DB
  - Processing layer
    1. Prewritten SQL query
    2. Data processing methods

- **Hardware:**
  - Performs pattern capture
  - ADM-PCIE-7V3 board
  - Communicates with host through PCIe bus

- **GUI**
  - Interface with user
  - Visualize analysis reports as charts.
Hardware details

- Chain of PEs
- Ping pong buffers
  - Overlap processing with data transfers
- PE processes tokens
- Token is a 65-bits wide multifield record
- Context Token
  - initializing PE
- Record Tokens
  - data to be processed
Experiments and Results

- Database: PostgreSQL
- Software library in C
- GUI in QT
- Hardware logic Verilog and HLS
- Host memory and device data exchange: SDAccel and Opencl

<table>
<thead>
<tr>
<th>No.</th>
<th># of Records</th>
<th>Rule Type</th>
<th>Sw-only exec. time</th>
<th>HW/Sw co-des. exec. time</th>
<th>Speedup</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1 \times 10^6$</td>
<td>1</td>
<td>363</td>
<td>24</td>
<td>91X</td>
</tr>
<tr>
<td>2</td>
<td>$3 \times 10^6$</td>
<td>2</td>
<td>1320</td>
<td>46</td>
<td>28X</td>
</tr>
<tr>
<td>3</td>
<td>$10 \times 10^6$</td>
<td>3</td>
<td>5832</td>
<td>61</td>
<td>95X</td>
</tr>
</tbody>
</table>