Accelerate Pattern Recognition for Cyber Security Analysis

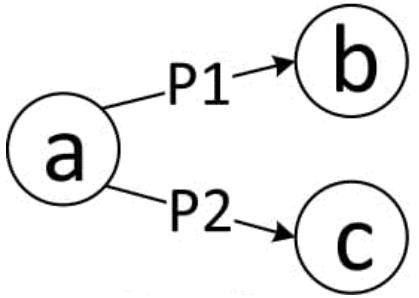
Mohammad Tahghighi, Wei Zhang

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

Introduction and Motivation

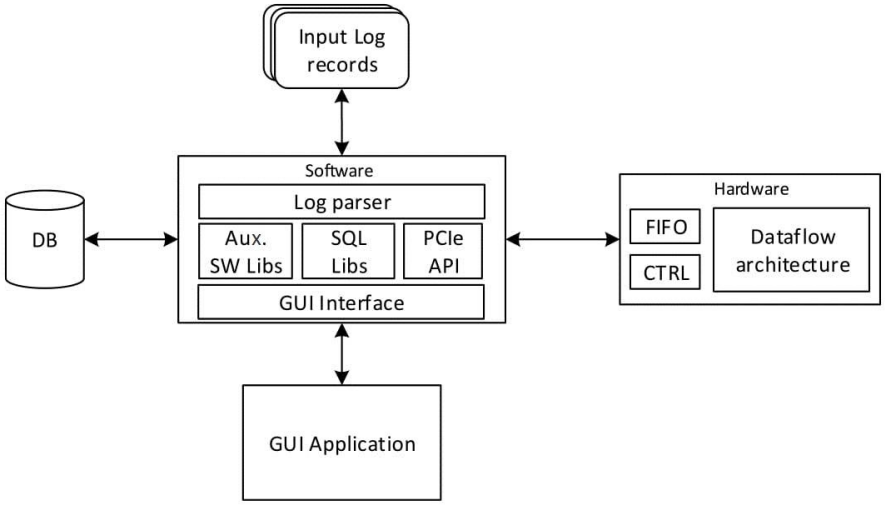
- Goal:
  - Capture interesting network pattern (Security application)
- Input:
  - Netflow record (generated by routers)
  - Has several fields like src/dest IP address
- Challenge:
  - Rate: several kilo netflow/sec
  - Processing is complex and time consuming
  - Difficult to parallelize
- Solution
  - 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

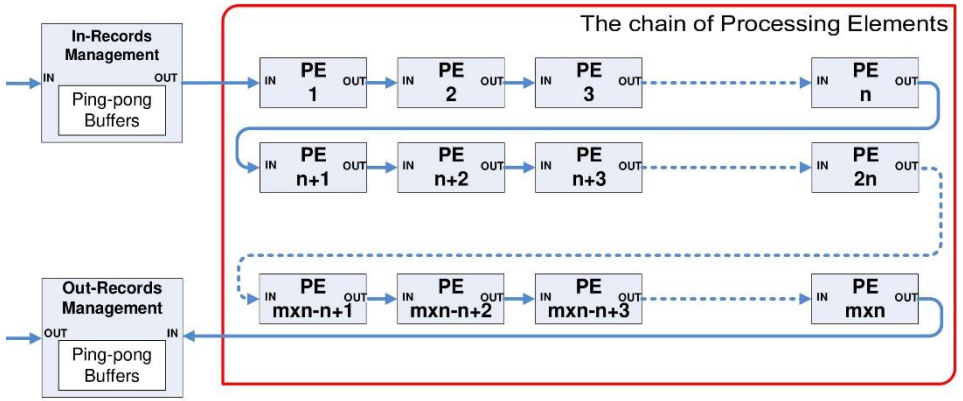
- Software
  - log parser: parse raw input and import into DB
  - Processing layer
    1- Prewritten SQL query
    2- Data processing methods
- Hardware:
  - Performs pattern capture
  - ADM-PCIE-7V3 board
  - Communicates with host through PCIe bus



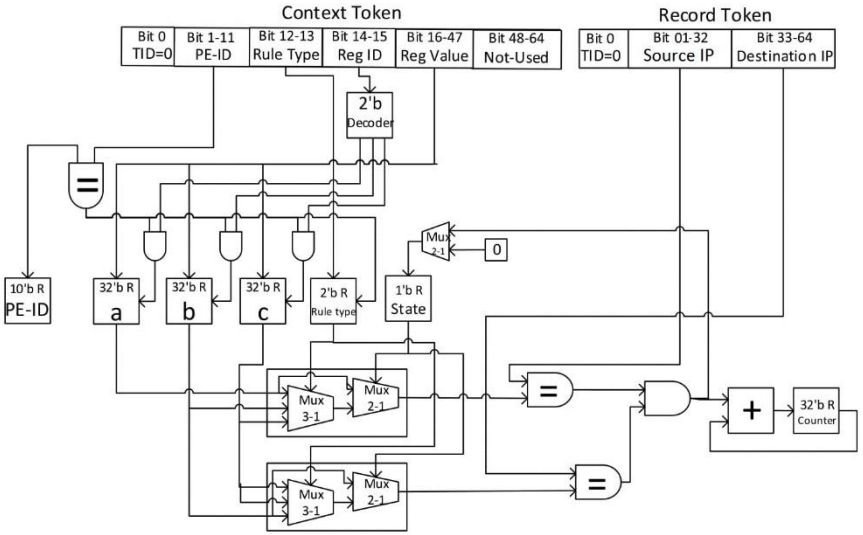
- GUI
  - Interface with user
  - Visualize analysis reports as charts.

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 I
PATTERN RECOGNITION EXECUTION TIME (SECONDS) COMPARISION

No.	# of Records	Rule Type	Sw-only exec. time	HW/Sw co-des. exec. time	Speedup
1	$1 * 10^6$	1	363	24	91X
2	$3 * 10^6$	2	1320	46	28X
3	$10 * 10^6$	3	5832	61	95X