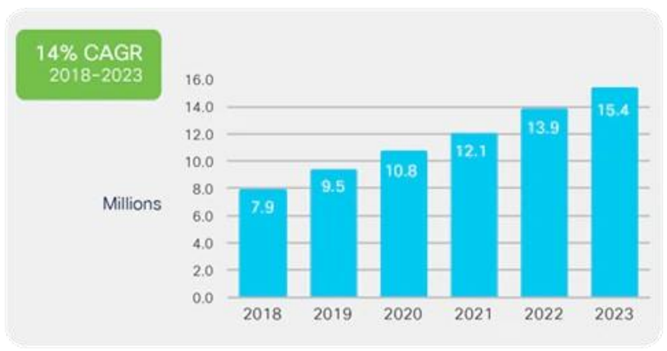
Hybrid Hardware/Software Datapath for Near Real-Time Reconfigurable High-Speed Packet Filtering

Student: Denis Salopek, denis.salopek@fer.hr
Advisor: Miljenko Mikuc
University of Zagreb, Faculty of Electrical Engineering and Computing, Croatia

UNIVERSITY OF ZAGREB
Faculty of Electrical Engineering and Computing

Introduction

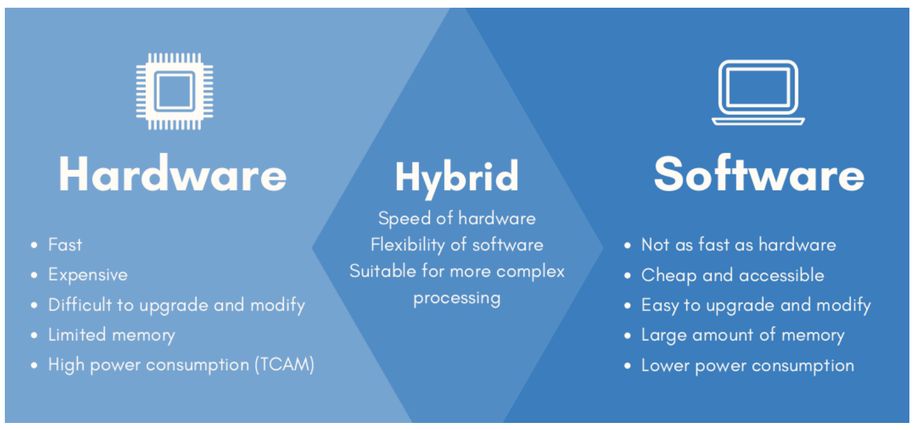
- Growth of high-throughput networks
- The need for high-performance network equipment – routers, firewalls, load-balancers…
- Undesirable effects because of slower equipment
  - Packet loss, device failure, denying service
- High number of Distributed Denial of Service (DDoS) attacks
- How to protect against DDoS attacks?



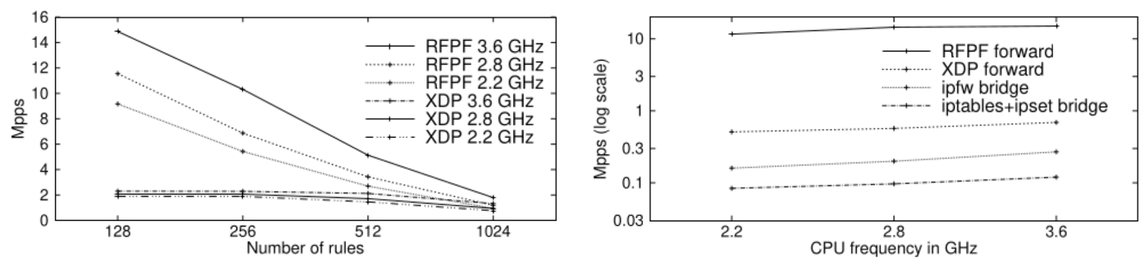
Predicted DDoS attack trends [1]

Methodology

- Hybrid hardware/software solutions
  - Alternative to both hardware and software solutions
  - FPGA [2], GPU [3], smart NICs [4]

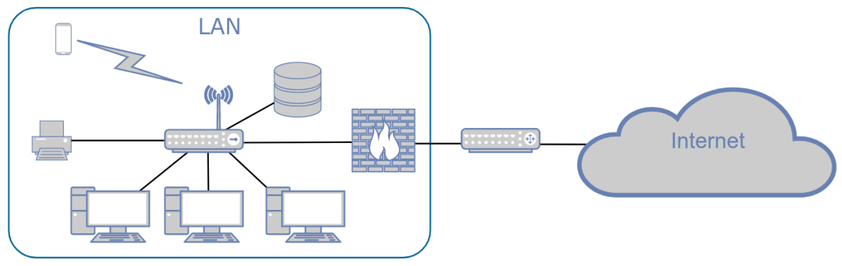


- Hardware – NetFPGA [5] – parallelism
  - Enables near real-time reconfiguration
- Software
  - Replaces rule-by-rule filtering with blocklists and safelists – longest prefix matching (LPM) suitable
- Distributor
  - Maximizes hardware offload to speed up software as much as possible: whole rules, parts of rules, additional functionalities, or part(s) of LPM algorithm
  - Finds the best possible workload distribution



Rule-by-rule and LPM classification performances

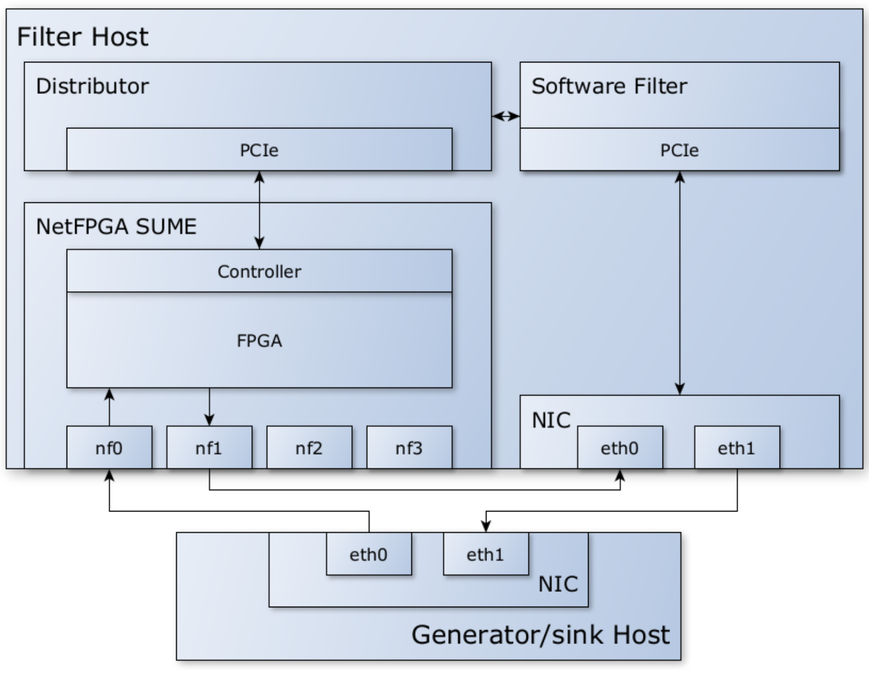
- We see throughput deterioration due to increase of rules number
- On the other hand, performance gap between standard firewalls and LPM classification



- Filter is placed between the insecure network and LAN
  - Alternative to third party scrubbing services – latency and privacy concerns

Implementation

- Multiple individual components
  - Hardware pre-filter, software filter, workload distributor



Hybrid packet classification model and testbed setup

Conclusion

- LPM is suitable against large scale DDoS attacks
- Initial results are promising – increased throughput for synthetic traffic (in comparison with software firewalls)
- Even more performance gain by using a hybrid model and a separate component for distributing workload between hardware and software
  - Improving LPM by offloading parts of it to hardware

References

[1] Cisco Annual Internet Report, 2018–2023
[2] Fiessler, et al. “Hypafilter+: enhanced hybrid packet filtering using hardware assisted classification and header space analysis” IEEE/ACM Transactions on Networking, 2017
[3] Go et al. “Apunet: Revitalizing GPU as packet processing accelerator”, NSDI 2017
[4] Miano, et al. “High-performance server-based DDoS mitigation through programmable data planes”, CREATE-NET, 2019
[5] Zilberman, et al. “Netfpga SUME: Toward research commodity 100gb/s”, 2014

16th International Conference on Telecommunications – PhD forum
July 2nd, 2021
Zagreb, Croatia