



Brzo i energetske uinkovito filtriranje paketa

IoT4us

Denis Salopek (denis.salopek@fer.hr)

Sveučilište u Zagrebu

Fakultet elektrotehnike i računarstva

Zavod za telekomunikacije

Travanj 2022.



Pregled

- Uvod
 - Raspodijeljeni napadi uskraćivanjem resursa (DDoS)
- Zaštita od DDoS napada
 - sklopovsko i programsko filtriranje paketa
- Hibridna obrada paketa
 - IoT uređaji
- Rezultati
- Zaključak

Uvod

- Širenje Interneta
 - rast brzine mreža
 - 10G je već "sporo"
 - rast broja uređaja - IoT

- Raspodijeljeni napadi uskraćivanjem resursa (DDoS)
 - povećana učestalost, snaga
 - dostupnost
 - zaštita (od) IoT uređaja

Zaštita od DDoS napada

- Filtriranje sklopovljem

- uglavnom nefleksibilno i složeno (ASIC, FPGA)
- teško za modificirati i nadograđivati
- energetska neučinkovito (TCAM)
- skupo
- velike brzine obrade

- Filtriranje programskom podrškom

- fleksibilno, relativno jednostavno za modificirati i nadograđivati
- jeftino - "off-the-shelf" uređaji
- povećani zahtjevi za postizanje velikih brzina

Programska zaštita od DDoS-a

- Najmanji ethernet okvir: 84 okteta

- 10 Gbps:

$$\frac{10 \cdot 10^9 \text{ bit/s}}{84 \text{ okteta} \cdot 8 \text{ bita}} = 14.880.952 \text{ pkt/s} = 14.88 \text{ Mpkt/s}$$

- 100 Gbps: 148.81 Mpps

- vrijeme dostupno za obradu svakog paketa:

$$\frac{1 \text{ pkt}}{148.809.520 \text{ pkt/s}} = 6,7 \text{ ns}$$

- CPU od 3 GHz:

$$\frac{3 \cdot 10^9 \text{ c/s}}{148.809.520 \text{ pkt/s}} = 21 \text{ c/pkt}$$

- „cache-misses”: **32 ns**; vrijeme pristupa L2: **4,3 ns**; vrijeme pristupa L3: **7,9 ns**; sistemski poziv na Linuxu: minimalno **41,85 ns**

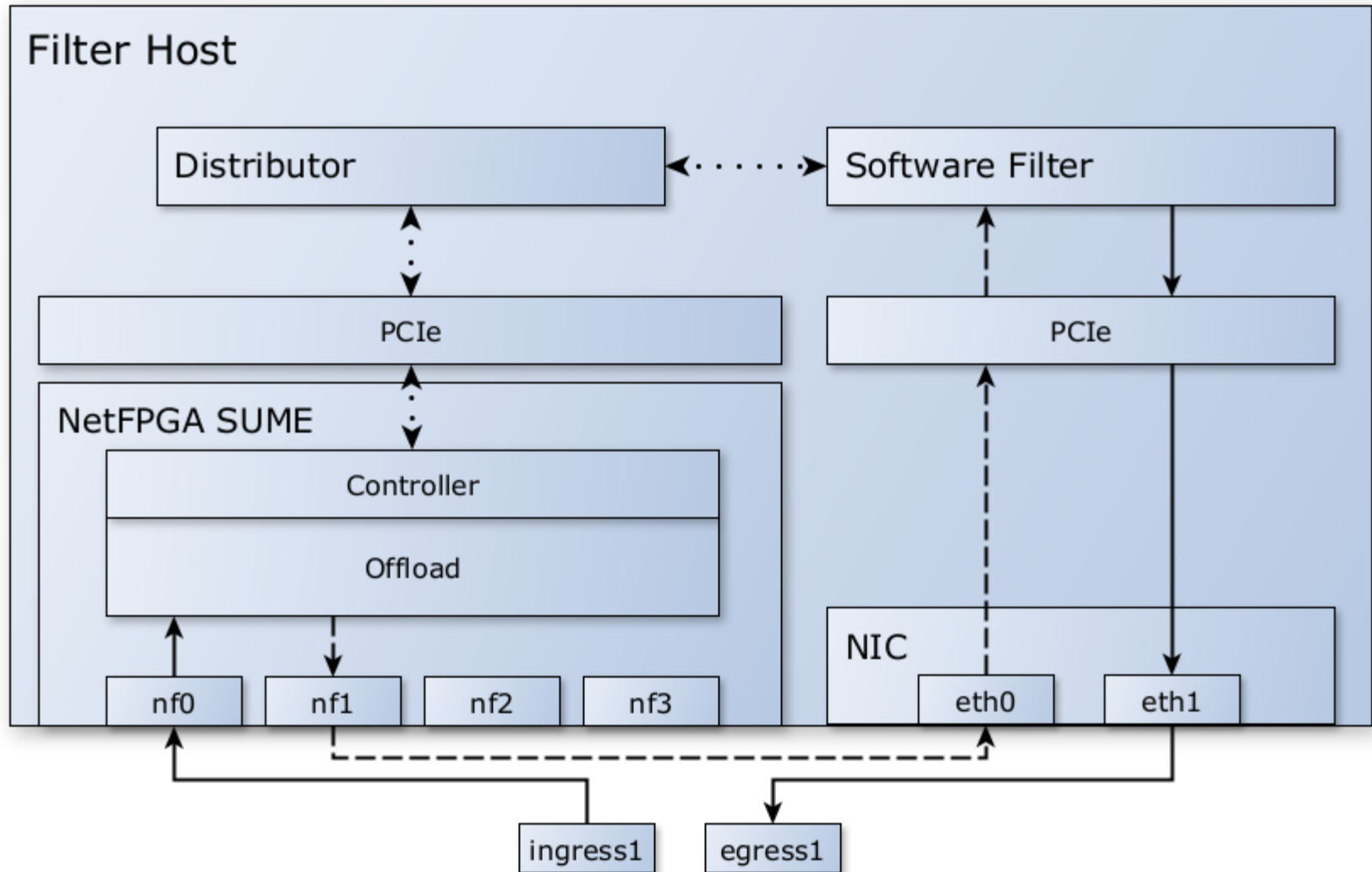
Hibridna obrada paketa

- Hibrid sklopovskog i programskog filtriranja
 - najbolje od obje strane
 - pred-procesiranje na sklopovlju + proslijeđivanje programskoj podršci
- SmartNIC
 - specijalizirani uređaji
 - NetFPGA SUME - prototip
 - off-the-shelf računala i programska podrška



Slika: Xilinx - NetFPGA-SUME Virtex-7 FPGA Development Board
<https://www.xilinx.com/products/boards-and-kits/1-6ogkf5.html>

Hibridna obrada paketa

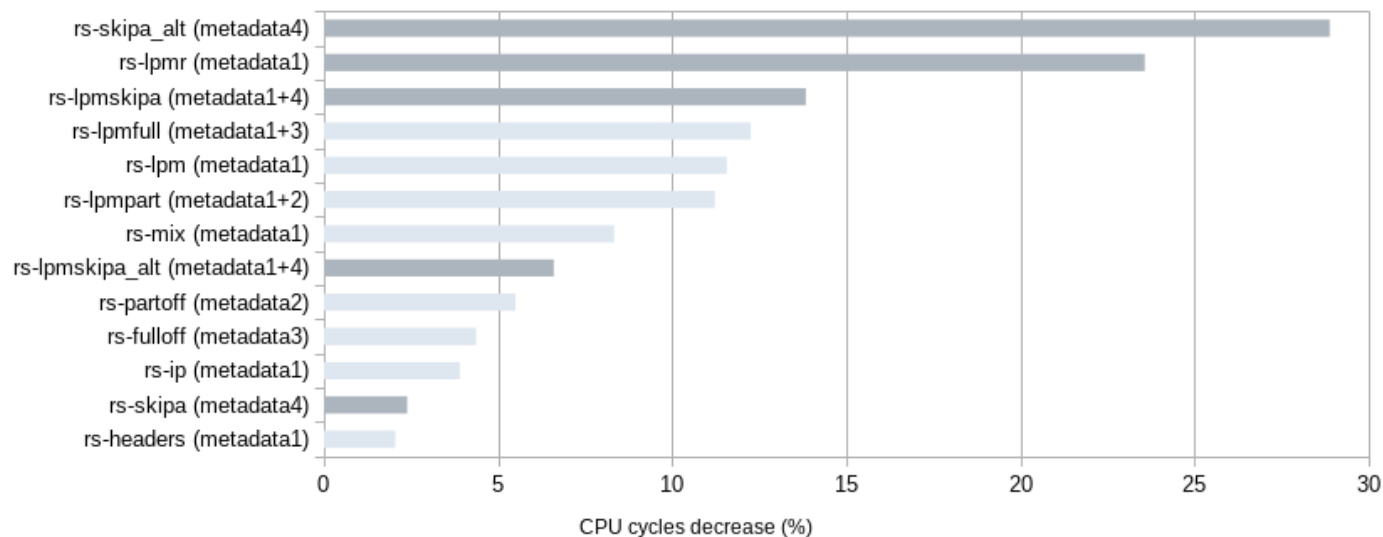
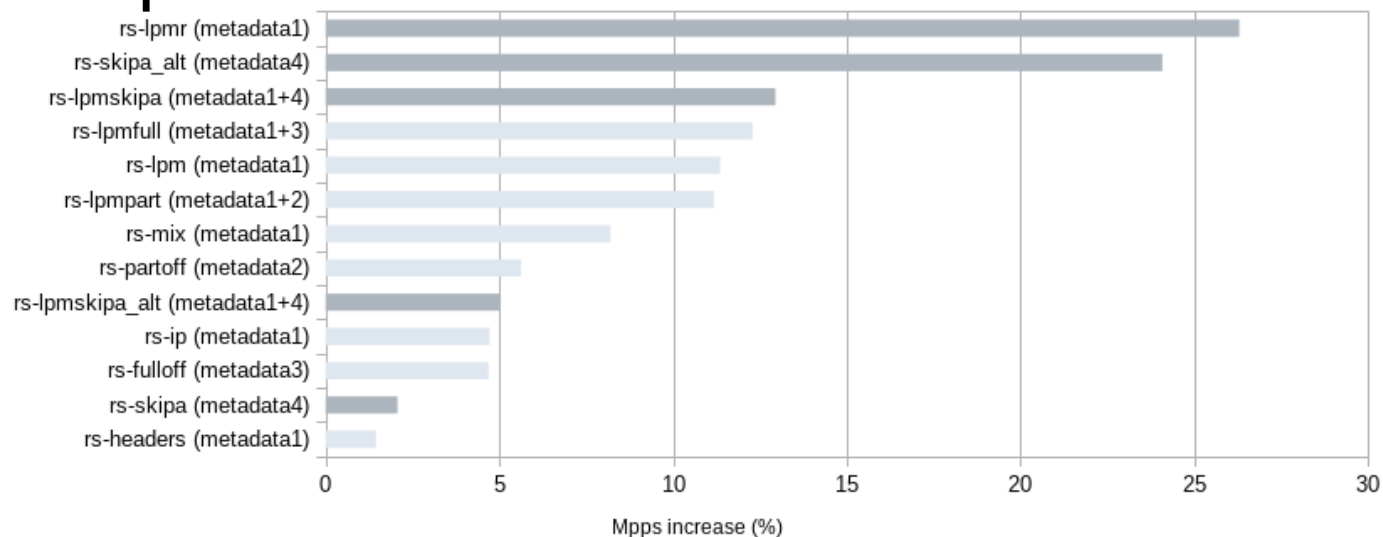


IoT uređaji

- Na uređajima
 - štednja energija
 - mala količina prometa
 - dodatno (FPGA) sklopovlje za “offload”
 - efikasnost?
- Gateway - obrada u oba smjera
 - akumulator prometa
 - dodatna obrada na hibridni način
 - obrada i analiza mrežnog prometa
 - moje istraživanje: filtriranje

Rezultati istraživanja

- DDoS napad



Zaključak

- DDoS
 - česti napadi
 - potrebna zaštita (od) IoT uređaja
- Hibridni pristup obradi paketa
 - sklopovlje + programski dio
 - SmartNIC
 - IoT - neprikladno?
- Gateway
 - jeftino i energetske učinkovito
 - hibridna zaštita (ili druga obrada)
- Rezulati
 - do 30% poboljšanja kod filtriranja
 - štednja energije u programskom dijelu

Hvala na pažnji!