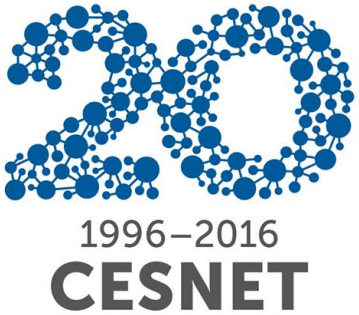


Tomáš Čejka
cejkat@cesnet.cz

Monitorování sítě se strojem času

Internet a Technologie 31. 05. 2016

Úvod & Motivace

Monitorování založené na síťových tocích

- Nutné zejména na vysokorychlostních sítích (objem dat)
- Bezpečnostní analýza, provozní měření, účtování, . . .

Nedostatky

- Agregované záznamy o tocích nedostačují pro:
  - forenzní analýzu
  - hledání vzorů škodlivého provozu pro vylepšení detekce
  - ověření správnosti detekce
  - důkazní materiál

Naše cíle

- Automatický záchyt provozu (na základě zpětné vazby)
- Krátkodobý záchyt paketů
- Dohromady: „stroj času“
  kombinace paketového a tokového monitorování

Záznamy o tocích (Flow Records)

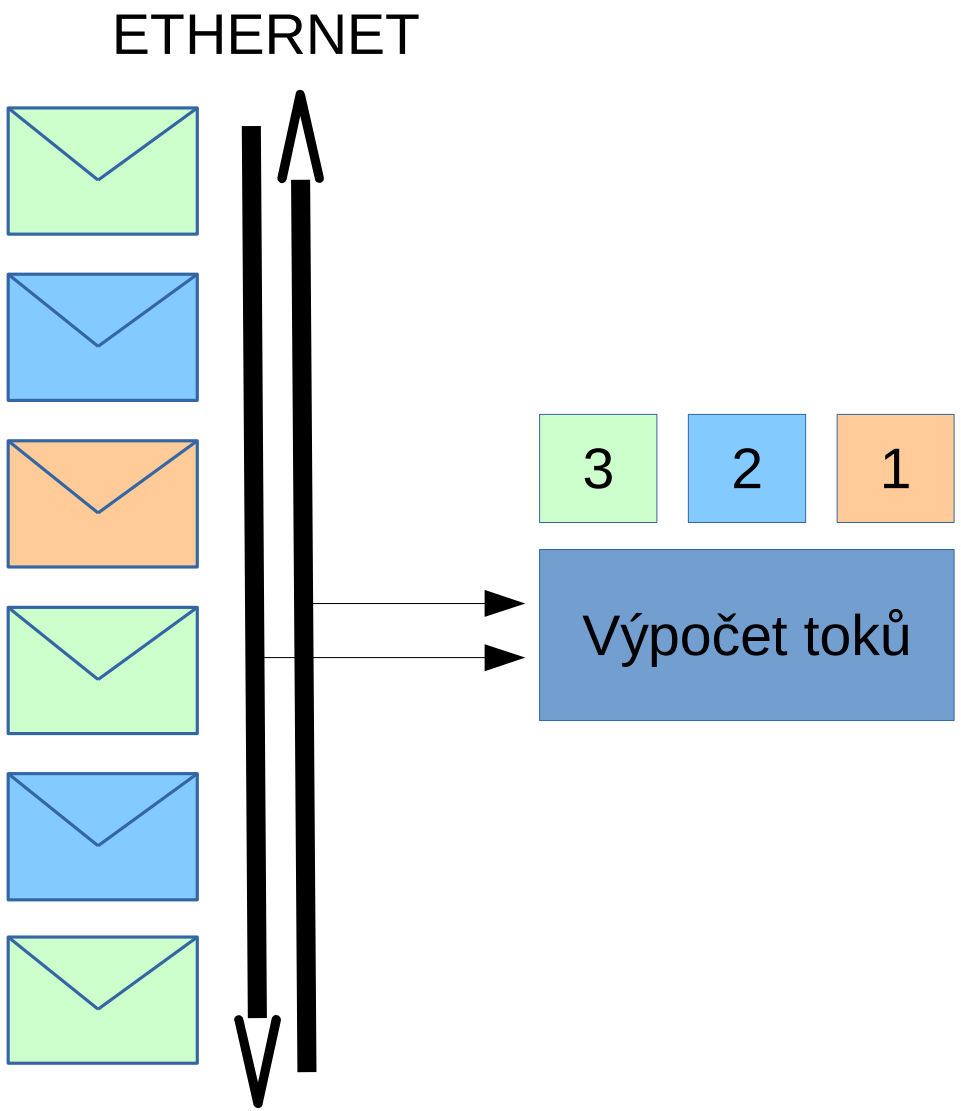
Vysvětlení

- Tok je identifikován zdrojovými a cílovými adresami a porty, protokolem, časem.
- Tok obsahuje informace o objemu dat: # bajtů, # paketů.
- Podle potřeby je možné přidat i další informace.

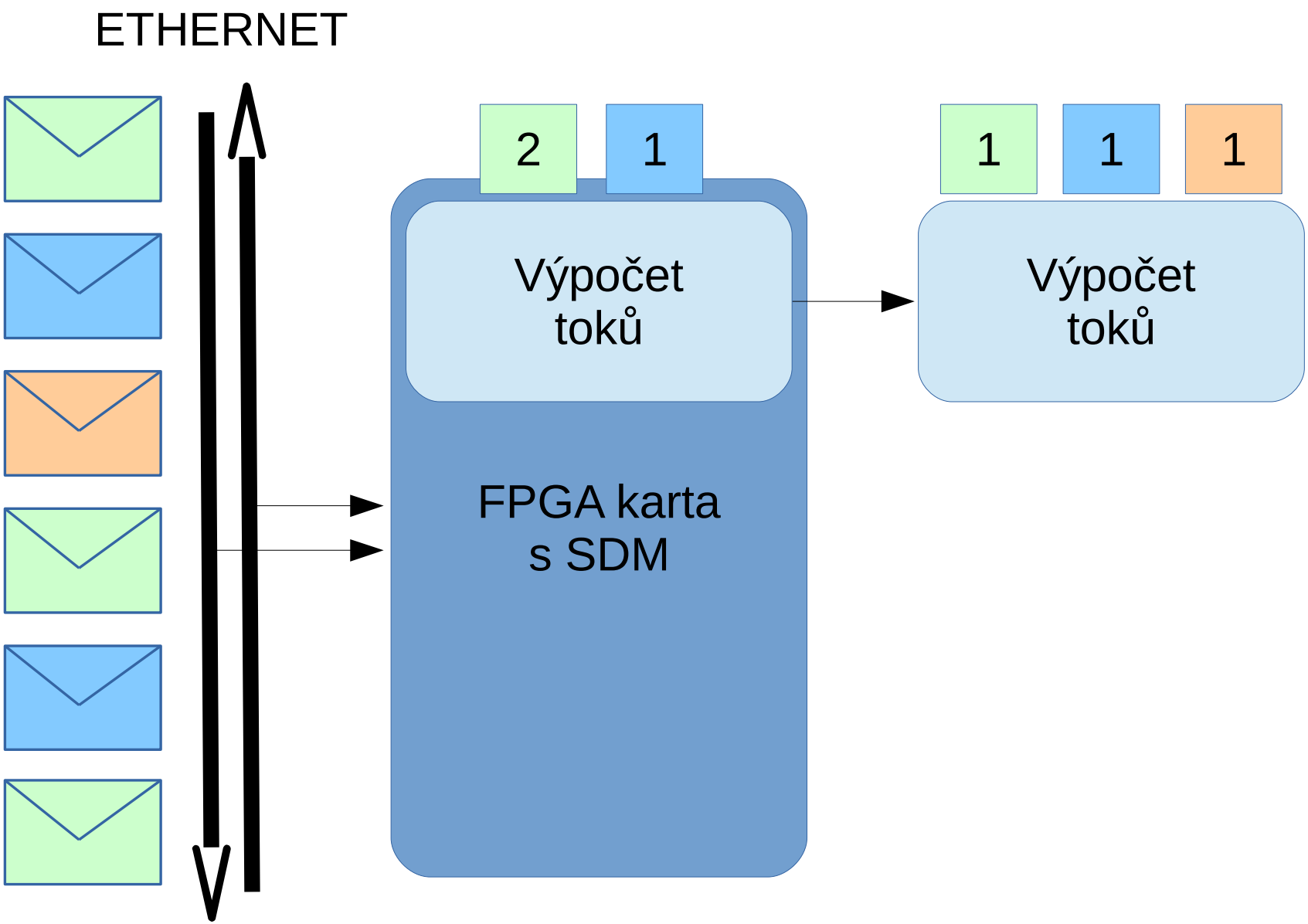
Reprezentace záznamů o tocích

- NetFlow (existuje několik verzí)
- IPFIX

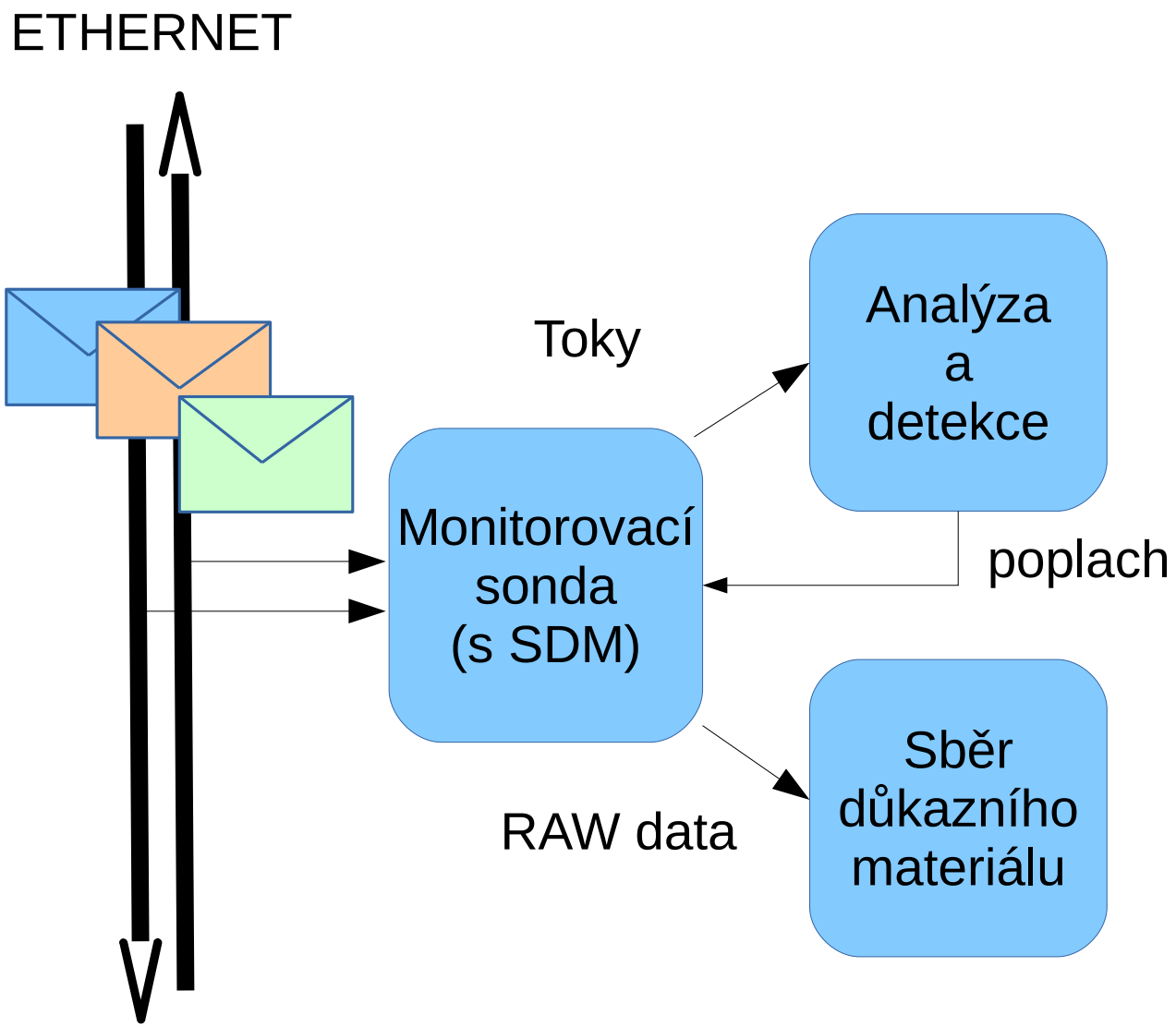
Běžná monitorovací sonda



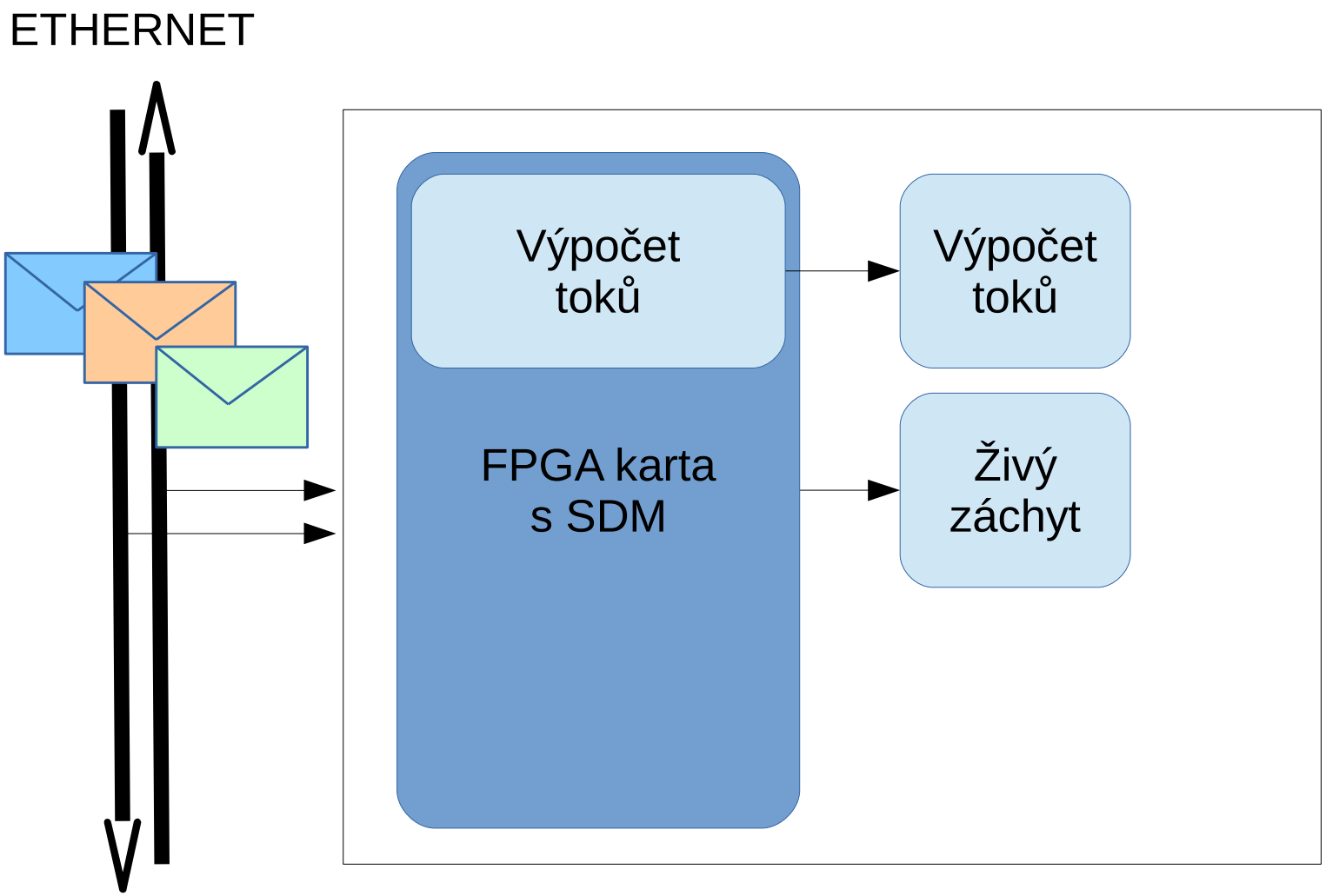
Software Defined Monitoring (SDM)



Využití detekce: Infrastruktura SDM zpětné vazby



Živý záchyt po detekci



Jak se podívat na pakety z minulosti? Když je detekce rychlá, stačí spustit záchyt. . . ?

Time Machine od Kornexl & Paxson

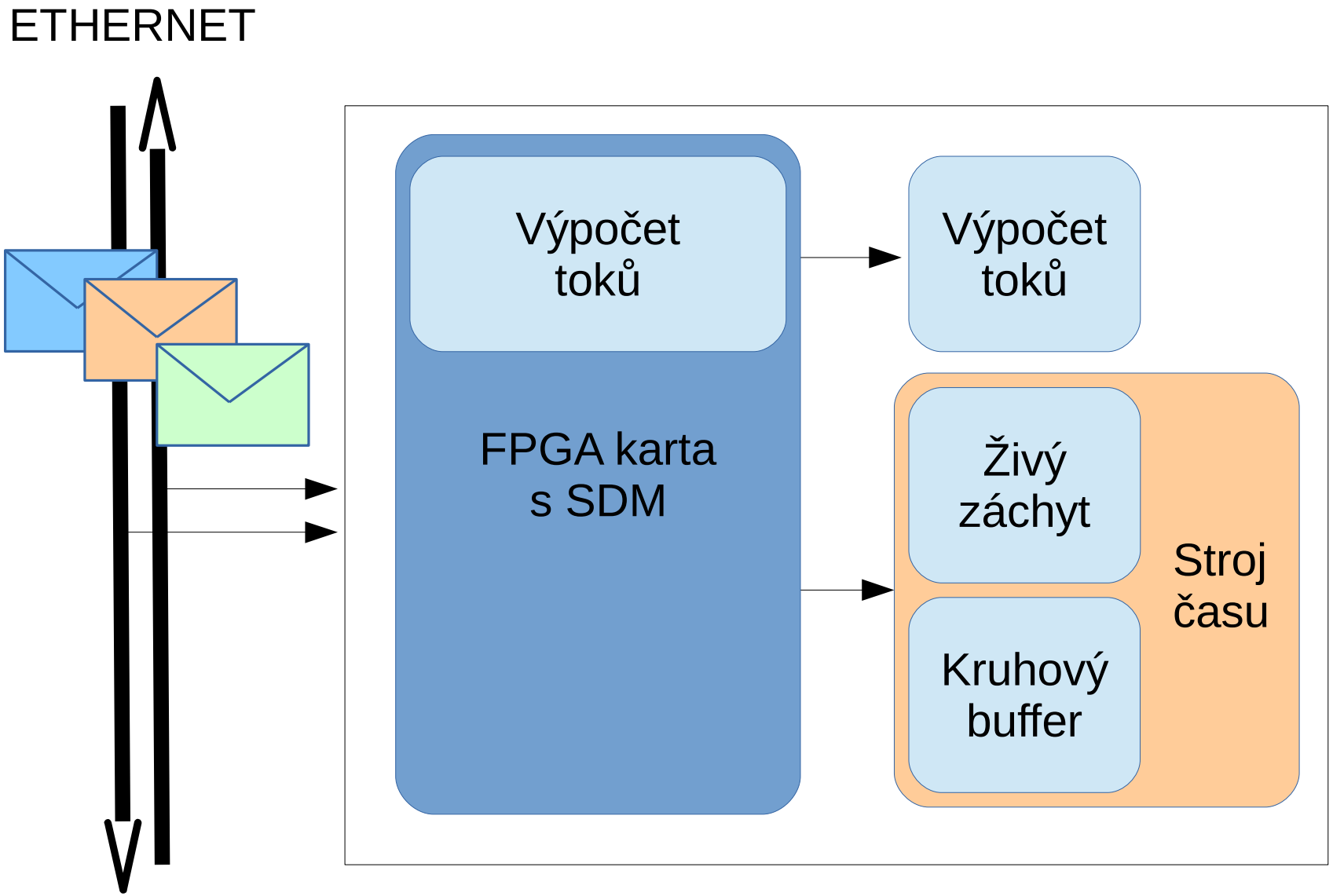
- „Clever Caveman Approach“
- Publikováno v:
  Kornexl, Stefan, et al. "Building a **time machine** for efficient recording and retrieval of high-volume network traffic."Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. USENIX Association, 2005.
- Ukládání paketů na **pevné disky**
- **Dlouhodobé** ukládání
- „Clever“ = jen některé pakety, **začátky toků** (které obsahují hlavičky)

Náš „stroj času“ v SDM

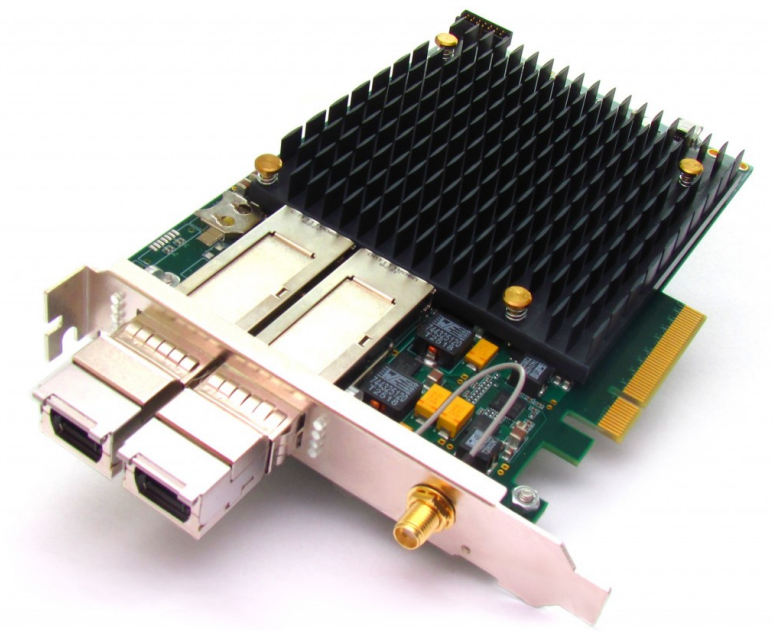
Princip našeho řešení (pro 80–100 Gb/s)

- Ukládání paketů v **operační paměti** (kvůli rychlosti)
- Naimplementovaný softwarový **kruhový buffer**
- Ukládá se **prvních *n* paketů** každého toku
  na co nejdelší dobu (stará data se přepisují)
- Po detekci se začne **zachytávat provoz** podezřelé IP
  navíc máme historická data z kruhového bufferu
  = můžeme se podívat do minulosti!

Náš stroj času v SDM



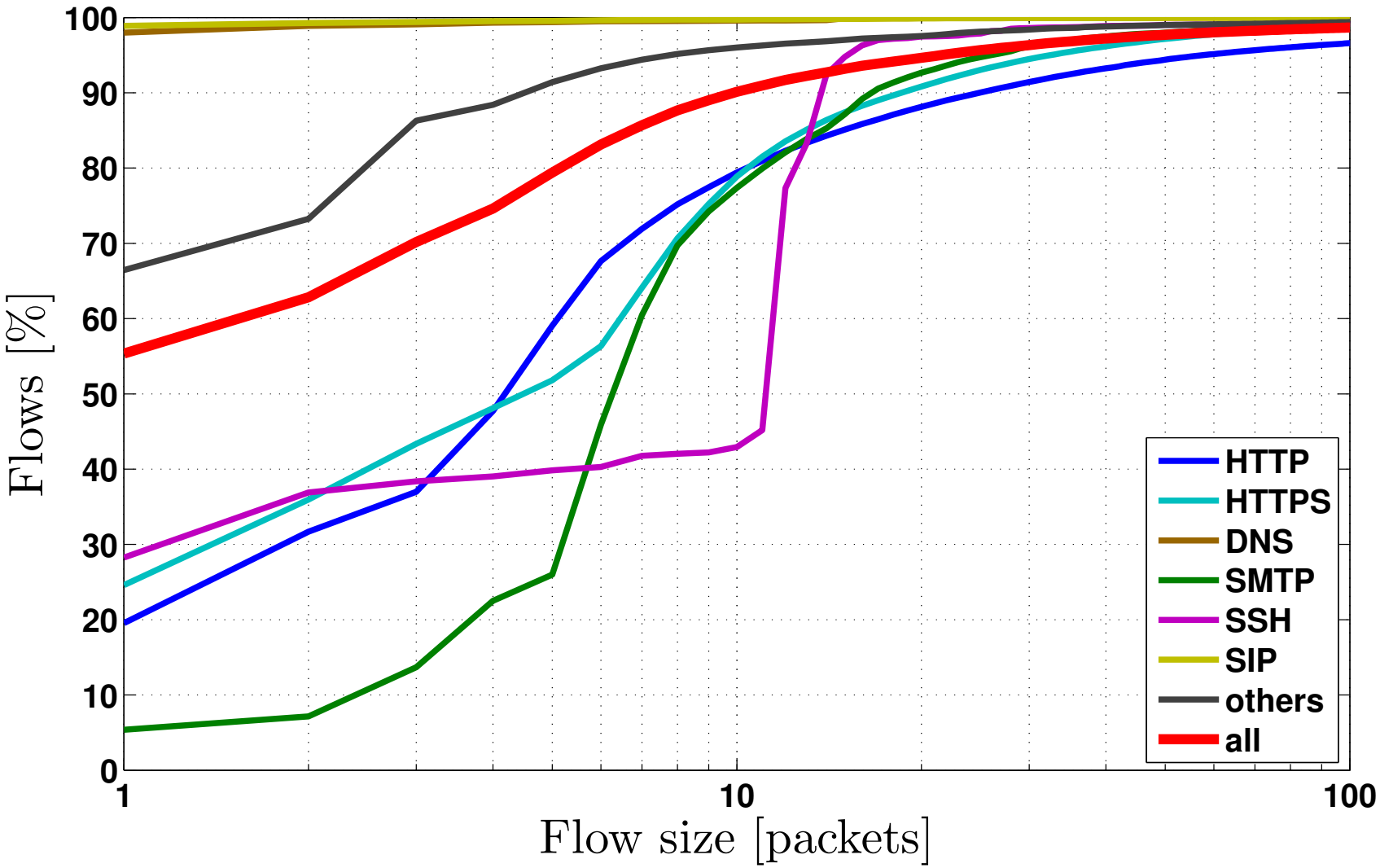
Co už jsme testovali



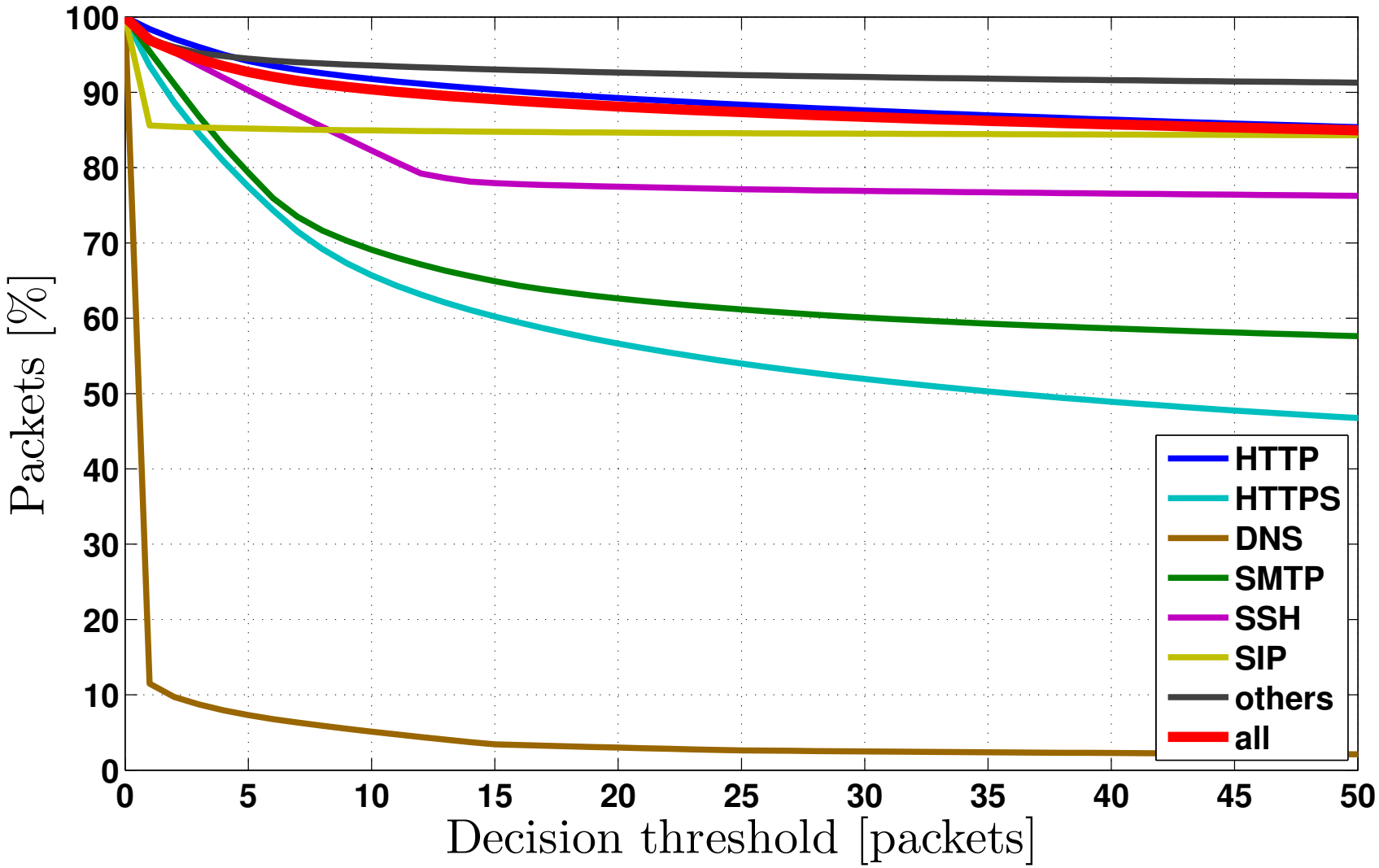
- Detekce síťových skenů
- Komunikační tunely přes DNS
- Hádání vytáčecího schématu SIP

Pomocí SDM se strojem času můžeme získat důkazní materiál pro bezpečnostní týmy a ověřit detekované události.

Velikost toku – je *n* paketů dost?



Uložené/přeskočené pakety

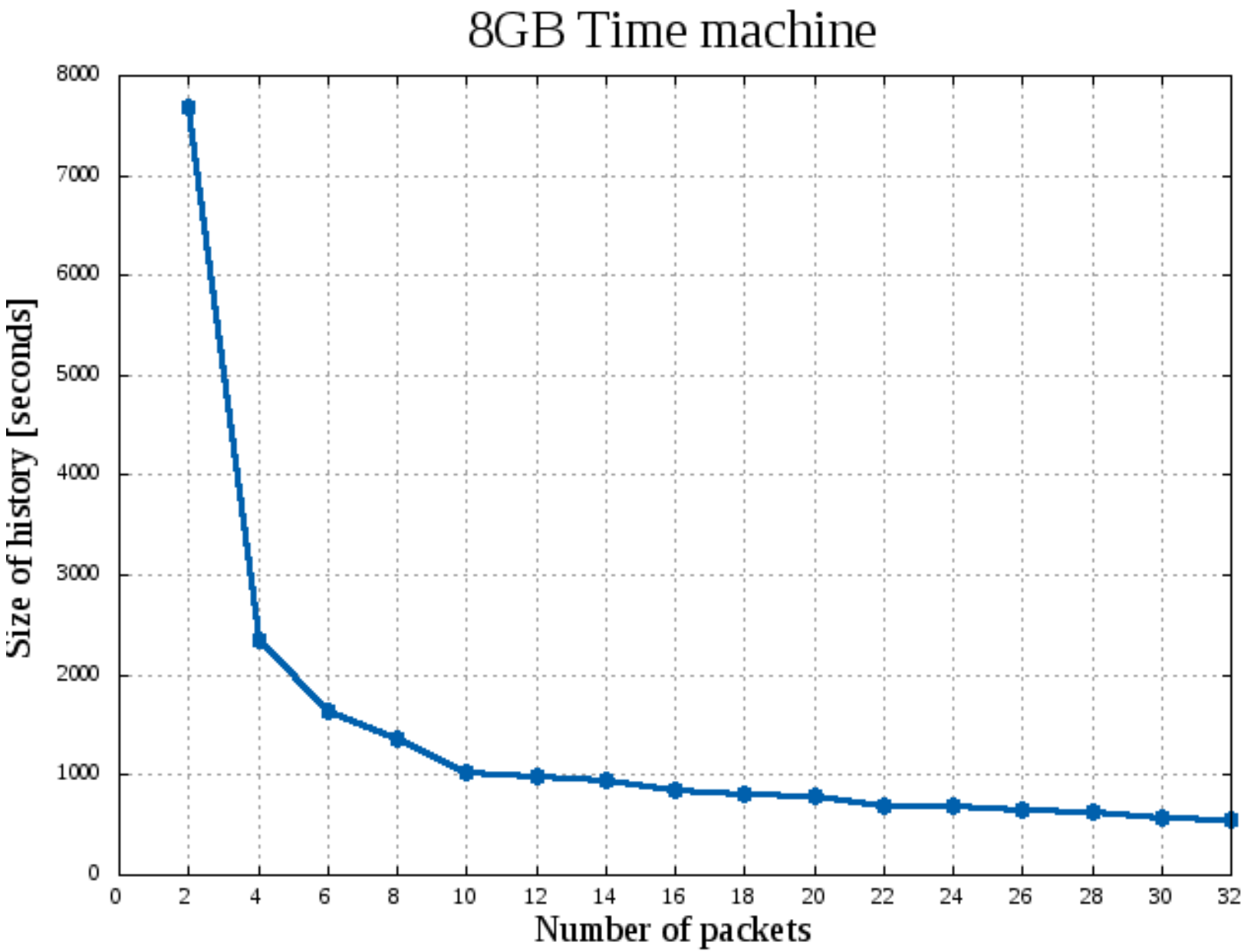


Statistiky

- 24 CPU jader
- 64 GB RAM
- 80 Gb/s COMBO karta (podporující SDM)

- Použijeme-li 8 GB paměti,
  na 80 Gb/s lince,
  a budeme-li ukládat prvních 20 paketů každého toku,
  můžeme uložit kolem 15 min provozu
- Pozn.: délka historie závisí na objemu a rozložení provozu

Délka historie



Závěr

- Umíme monitorovat 100 Gb/s, stroj času byl testován na 80 Gb/s.
- Detekce používá (rozšířené) záznamy o tocích
- Prezentovaný systém poskytuje:
  - záznamy o tocích
  - zachycený plný provoz detekované IP (živý záchyt)
  - historii před detekcí: začátky toků detekované IP

Děkuji za pozornost

Pozvánka na Demo