

Klasifikace šifrovaného provozu v počítačových sítích s využitím technologie FPGA

Motivace

Šifrování síťového provozu komplikuje blokování škodlivých služeb, prioritizaci aplikací i další správu sítě. Neuronové sítě přitom dokáží toky rozlišit i bez dešifrování, pouze podle délek paketů a intervalů mezi nimi (například při odeslání e-mailu mají pakety jiné velikosti a časování než při streamování videa). Nasazení těchto sítí pro analýzu vysokorychlostních linek v reálném čase (řádově 100 Gb/s a více) vyžaduje jejich integraci přímo do síťové karty.

Cíle práce:



Navržení neuronové sítě (modelu) pro klasifikaci šifrovaných síťových toků



Implementace modelu v síťové kartě s FPGA



Výsledky

Spojením GRU, 4bitové kvantizace a specializovaného FPGA akcelérátoru práce překonává dosavadní online klasifikátory šifrovaného provozu (N3IC, Kaleidoscope, FENIX).

Na datové sadě ISCX-VPN2016 dosahuje řešení v porovnání s existujícím systémem FENIX:

- o 4,2 % vyšší F1 skóre (93,4 %)
- latence 83 ns (oproti 3000 ns)
- 9× méně LUT (zdrojů FPGA)
- 3,8× menší stavové informace

Navržená metoda

Navržený model. Modelem je rekurentní síť GRU, jejíž vstupní příznaky (velikosti a časové rozestupy paketů) jsou předzpracovány učitelnými embedding tabulkami.

Kvantizace modelu. Váhy i aktivace modelu jsou kvantizovány do 4 bitů a díky quantization-aware training (QAT) je i po kvantizaci zachována vysoká přesnost klasifikace. Celý model lze vyhodnotit pouze pomocí celočíselné aritmetiky.

Mapování do FPGA. Model je kompletně rozbalen a namapován na výpočetní jednotky v FPGA. Díky plnému rozbalení a plné paralelizaci modelu provádí každá jednotka jen jeden fixní výpočet a lze ji proto specializovat. Tím se sníží spotřeba FPGA zdrojů i latence.

