HEADER FIELD EXTRACTION USING FPGA

Libor Polčák
Master Degree Programme (2), FIT BUT
E-mail: xpolca03@stud.fit.vutbr.cz

Supervised by: Jan Kořenek
E-mail: korenek@fit.vutbr.cz

ABSTRAKT

Lately, data processing inside high-speed networks has become a very important task. Packet header field analysis and extraction is a common task performed in most of the network systems. This paper contains problem definition and description of a higly configurable unit implemtented using Virtex 5 FPGA. The unit is able to process all packets on 10 Gbps network.

1 ÚVOD

Jednou ze základních funkcí, které je potřeba vykonávat ve většině síťových zařízení je analýza obsahu hlaviček paketů a extrakce položek specifických pro dané zařízení. Jedná se o směrovací prvky, monitorovací prvky, bezpečnostní sondy atd. Vzhledem k neustálému zvyšování přenosové kapacity je potřeba se vypořádat s rostoucími nároky na výkonnost těchto zařízení.

Specializované síťové procesory [3] jsou schopné zvládat analýzu hlaviček obsažených v paketech a provádět extrakci dat i v sítích s rychlostí 10–100 Gb/s. Tyto procesory však nejsou vhodné pro návazné úkoly [1, 2, 4]. Proto bývají síťové procesory v cílovém zařízení často doplněny dalšími obvody ASIC, nebo FPGA. Pokud by se podařilo přesunout činnosti prováděné síťovým procesorem do těchto přídavných obvodů, značně by to snížilo cenu kompletního zařízení.

V tomto článku se budeme zabývat akcelerací analýzy protokolů a extrakcí specifikovaných položek v hlavičkách paketů v sítích s přenosovou kapacitou 10 Gb/s a vyšší pomocí technologie FPGA. V sekci 2 je úloha formálně definována. Sekce 3 obsahuje informace o architektuře hardwarové jednotky řešící tuto úlohu. Dosažené výsledky jsou prezentovány v sekci 4.

2 DEFINICE ÚLOHY

Analýzou paketů budeme v tomto textu z formálního pohledu rozumět zobrazení, které binárně zakódovaný obsah paketu zobrazí do n-tice. Prvky této n-tice jsou dvojice reprezentující každou položku, která se vyskytuje v rámci hlaviček zpracovávaných protokolů obsažených ve zkoumaném paketu. První prvek každé dvojice jednoznačně identifikuje jednu konkrétního síťového protokolu a druhý prvek obsahuje hodnotu této položky. Nalezené položky se ve výsledné n-tici vyskytují ve stejném pořadí, jako se vyskytovaly ve zkoumaném paketu.

Nechť I je konečná množina všech položek zkoumaných protokolů a $C \subset \{0,1\}^+$ je konečná množina všech možných obsahů paketů. Pak analýzou paketů označíme každé zobrazení $\alpha: C \rightarrow (d_1, d_2, \ldots d_m)$, kde $\forall j \in \langle 1; m \rangle : d_j \in I \times \{0,1\}^+$.

Extrakcí dat z paketů budeme označovat takové zobrazení $\sigma: C \rightarrow \{0,1\}^l$, které každému síťovému paketu na vstupu, obecně různé délky, přiřadí výstupní řetězec pevné délky l.

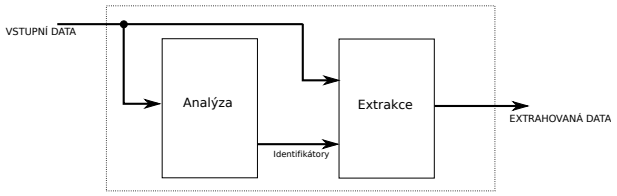
Pro naše účely se budeme zabývat takovými σ, které mají tu vlastnost, že pro nějakou konkrétní podmnožinu položek z hlaviček zpracovávaných protokolů $I_u \subseteq I$ a analýzu paketů α zachovávají ve výstupním řetězci obsah těchto položek ze vstupního řetězce a obsah konkrétní položky extrahují vždy na předem definovanou pozici.

$\forall i \in I_u \exists p_i \in \langle 1;l \rangle \forall c \in C: (\alpha(c) = ((i_1,v_1),(i_2,v_2),\ldots(i_m,v_m))) \Rightarrow (\forall j \in \langle 1;m \rangle : i_j = i \Rightarrow p_i \in \mathrm{strpos}(\sigma(c),v_j))$

V předchozím zápise označuje $\mathrm{strpos}(s,s')$ množinu, která obsahuje všechny pozice výskytů podřetězce s' v řetězci s.

3 HARDWAROVÁ ARCHITEKTURA

Zkoumaný problém je možné, jak vyplývá i z formální definice, rozdělit na dva menší problémy. Prvním z nich je detekce obsažených protokolů a analýza obsahu hlaviček. Druhým je extrakce specifikovaných položek a jejich umístění do výstupního unifikovaného formátu. Toto rozdělení dodržuje i popisovaná jednotka (viz obrázek 1).



Obrázek 1: Architektura jednotky

Část provádějící analýzu přijímaného paketu je implementována jako stavový automat, který vstupní slova transformuje na identifikátory určující položky vyskytující se ve zkoumaném slově a jejich pořadí. Stavem tohoto automatu je informace o aktuálně zpracovávaném protokolu, o tom, které položky již byly analyzovány, a případně další sémantické informace specifické pro analyzovaný protokol.

Identifikátory obsahu vstupního slova jsou v extrakční části využity jako adresa do vestavěné paměti dostupné na čipu. Obsah této paměti určuje, které položky se extrahují. Jednou z nejdůležitějších podčástí extrakčního modulu je křížový přepínač, který umožňuje libovolné umístění extrahované položky ve výstupním rámci pevné velikosti. Součástí výstupních dat může být i informace o platnosti extrahovaných položek.

Činnost jednotky je možné konfigurovat. Struktura zpracovávaných protokolů je popsána ve formátu XML, takže pro přidání dalšího protokolu není nutná znalost popisu hardware. Z popisu síťových protokolů je vytvořena jejich vnitřní grafová reprezentace, která je dále transformována tak, aby umožňovala v hardwarové reprezentaci zpracovávat pevný počet bitů v každém hodinovém cyklu. V případě krátkých hlaviček některých protokolů je dokonce zpracováno několik protokolů v jednom hodinovém cyklu. S touto reprezentaci jsou dále prováděny optimalizace, které ovlivňují nejvyšší hodinovou frekvenci, se kterou je možné bezchybně provozovat cílovou hardwarovou reprezentaci. Nakonec je vygenerován popis stavového automatu ve VHDL.

Extrakční část je možné konfigurovat za běhu změnou obsahu vestavěné paměti, čehož se dá například využít v monitorovacím systému, který je tak schopen reagovat na aktuální situaci na síti a měnit sadu zkoumaných položek.

4 VÝSLEDKY

Tabulka 1 obsahuje množství zdrojů, které zabírají jednotky o různých datových šířkách na FPGA Virtex 5 dodávaných firmou Xilinx. Ve všech případech je dosaženo propustnosti 10 Gb/s, ve dvou z nich jsou však použity jednotky o nižší datové šířce než je potřeba na zpracování celého toku. Požadované propustnosti je dosaženo zapojením více jednotek paralelně. Obsazené zdroje zahrnují pomocné jednotky pro distribuci, transformaci šířky toku a opětovné spojení.

Datová šířka [b]	Paralelních větví	LUT – Flip Flop párů	Blokových pamětí
32	3	10773	11
64	2	12857	13
128	1	15906	10

Tabulka 1: Potřebné zdroje na čipu Virtex 5

Z tabulky 1 je patrné, že i když je jediná jednotka schopna při datové šířce 128 b zpracovat celý datový tok, je výhodnější použít více jednotek o nižší datové šířce. Důvodem je charakter síťových protokolů, především jejich obvyklá délka. Dalším důležitým faktorem je velikost křížového přepínače, který má na obsazené zdroje podstatný vliv a roste kvadraticky v závislosti na šířce datového vstupu jednotky. Na druhou stranu řešení za použití jednotky schopné zpracovávat 128 b v každém hodinovém cyklu potřebuje o něco méně blokových pamětí, které jsou využívané pro distribuci jediného datového toků do více a zpátky do jednoho.

5 ZÁVĚR

Na základě specifikace analýzy hlaviček paketu a extrakce specifikovaných položek byla vytvořena jednotka schopna zpracovávat datový tok o propustnosti 10 Gb/s. Nicméně se ukazuje, že z pohledu počtu zdrojů zabraných na čipu je výhodnější použít více paralelně zapojených jednotek o nižší propustnosti.

REFERENCE

[1] Baker, Z. K.; Prasanna, V. K.: Automatic Synthesis of Efficient Intrusion Detection Systems on FPGAs. In *Proceedings of the 14th Annual International Conference on Field-Programmable Logic and Applications (FPL '04)*, 2004.

[2] Clark, C. R.; Schimmel, D. E.: Scalable Pattern Matching for High-Speed Networks. In *IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM)*, 2004.

[3] Crowley, P.; Franklin, M. A.; Hadimioglu, H.; aj.: *Network Processor Design: Issues and Practices, Volume 1*. Morgan Kaufmann, San Francisco, CA, 2003.

[4] Song, H.; Lockwood, J. W.: Efficient packet classification for network intrusion detection using FPGA. In *FPGA '05: Proceedings of the 2005 ACM/SIGDA 13th international symposium on FPGA*, 2005.