FAST PATTERN MATCHING USING FPGA AND TCAM

Jiří TOBOLA, Bachelor Degree Programme (3)
Dept. of Computer Systems, FIT, BUT
E-mail: tobola@liberouter.org

Supervised by: Ing. Jan Kořenek

ABSTRACT

This paper deals with fast pattern matching in packets payloads with utilization of FPGA and ternary content addressable memory (TCAM). Software solution of pattern matching is limited by slow system bus (about hundreds Mbps). Hardware solution based on a PCI board (with Virtex II FPGA and 2Mb TCAM) provides throughput 3.2 Gbps and it's possible to search up to 512 patterns. This component is called Payload checker (PCK) and it's part of 10 Gbps network monitoring adapter.

1 ÚVOD

Rozvoj počítačových sítí a zvláště Internetu přináší stále rychlejší technologie pro přenos dat. Zároveň s rychlostmi se zvyšují i nároky na bezpečnost sítí, možnost jejich efektivního sledování a monitorování dat, která jimi procházejí. Právě vysoké rychlosti dat (v současné době tok až 10 Gbps) ale neumožňují zpracování kompletního datového toku na klasickém PC, které je limitováno relativně pomalou systémovou sběrnicí, přes kterou není možné všechny data do softwaru přenést. Řešením je vyhledávat vzorky ve specializovaném hardwaru, který je předřazen toku dat do softwaru.

Velmi flexibilním řešením tohoto problému je využití technologie programovatelného hardware (FPGA). Tato technologie spolu s dalšími zdroji na PCI kartě COMBO6 (obsahuje výkonné FPGA Virtex II, asociativní a statistické paměti a s doplňující kartou se síťovým rozhraním i další zdroje) se stala základem projektu SCAMPI. Cílem tohoto projektu je vytvořit monitorovací síťový adaptér pracující na 10 Gbps, který umožní vstupní datový tok filtrovat podle IP pravidel (IPv4 i IPv6), vzorkovat pakety (deterministicky i nedeterministicky), vyhledávat vzory v datech paketu a vytvářet statistiky nad vstupním tokem. Pouze pakety, které vyhoví filtrovacím a vzorkovacím pravidlům, případně pakety, v nichž jsou nalezeny požadované vzory, jsou odeslány přes PCI sběrnici ke zpracování programovému vybavení počítače. Filtrovací a vzorkovací pravidla spolu s vyhledáváním

vzorů je možné libovolně kombinovat, a tak sledovat pouze požadované pakety, přičemž datový tok do softwaru je těmito pravidly dostatečně redukován.

Jednou ze základních komponent SCAMPI adaptéru je Payload checker, který umožňuje rychlé vyhledávání vzorů. Komponenta porovnává data ze vstupu s obsahem asociativní paměti a na základě výsledku vyhledání buď data paketu označí jako podezřelá (paket obsahuje vzor uložený v paměti) a paket je předán programovému vybavení počítače, nebo jsou data označena jako pro software nezajímavá a dále se nezpracovávají.

Prvkem umožňujícím rychlé vyhledání vzorů je asociativní paměť. Karta COMBO6 obsahuje tuto paměť s velikostí dva megabity, kterou lze pro daný úkol nejlépe využít v konfiguraci šířky slova 272 bitů a počtu řádků 8192. Co možná nejefektivnější využití této paměti je klíčem k dosažení velkých rychlostí vyhledání. Řízení této paměti, zabezpečení vstupního a výstupního protokolu a dočasné uložení dat k vyhledání je realizováno v FPGA Virtex II.

2 ANALÝZA

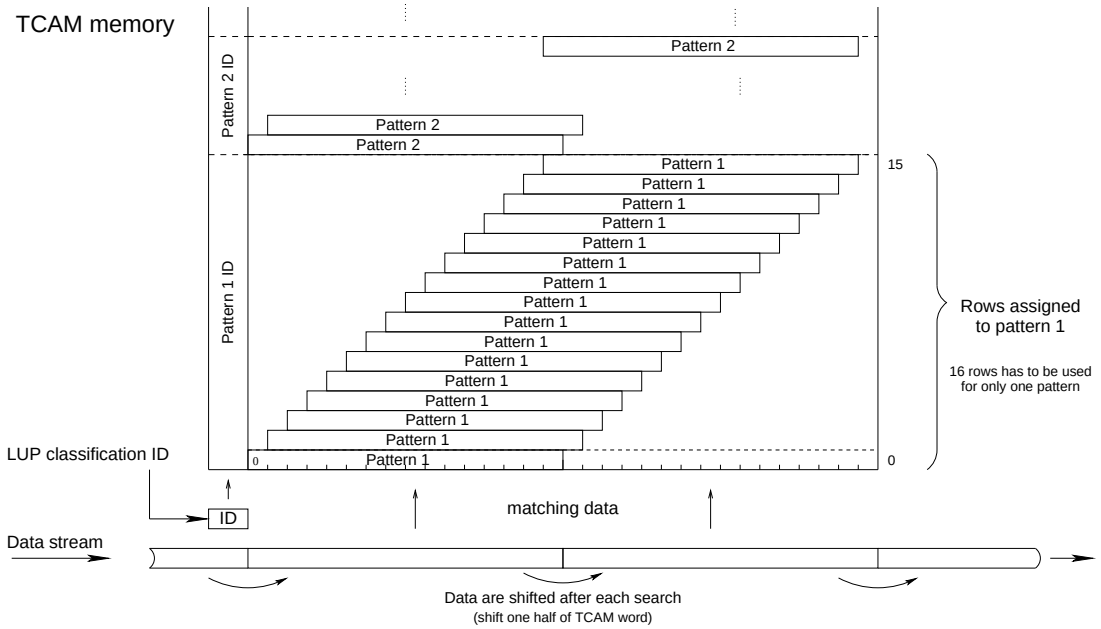
Pro dosažení maximální propustnosti je nutné najít takové využití asociativní paměti, které umožní zpracovávat objemný tok dat ze vstupu. Není například možné uložit na každý řádek paměti jeden vzor, protože by bylo nutné vstupní data posouvat po každém vyhledání o jeden bajt, což by znamenalo zpracování pouze 8 bitů při jednom vyhledání (mimo prvního). Proto je asociativní paměť využita jak je naznačeno na obrázku 1. Každý vzor je uložen v paměti na 16 řádcích, vždy posunut o jeden byte oproti předchozímu řádku (délka vzoru je 16B, zbývajících 16B na řádku je pomocí masky nastaveno tak, že se podle nich nevyhledává). To umožňuje posouvat vstupní data vždy o polovinu šířky slova asociativní paměti a při jednom vyhledání tak zpracovat 128 bitů vstupních dat.

Šířka slova asociativní paměti je 272 bitů, avšak pro vyhledávání dat se využívá pouze 256 bitů. Zbývajících 16 bitů je využito pro rozdělení vzorů do 16 skupin. Vyhledání je pak možné omezit na jednu, popř. libovolnou kombinaci těchto skupin. Toto se děje na základě výsledku vyhledávacího procesoru (Look-up processor, LUP), jenž zajišťuje klasifikaci příchozích paketů.

3 ARCHITEKTURA

Architektura komponenty pro vyhledávání vzorů byla rozvržena do pěti částí: řadič asociativní paměti, řídicí jednotka, datový buffer, výstupní jednotka a adresový dekodér. Řadič umožňuje operace čtení, zápisu a vyhledání v asociativní paměti. Řídicí jednotka zabezpečuje vstupní protokol, ukládání dat do datového bufferu a zahajuje operace vyhledání. Výstupní jednotka zpracovává výsledky vyhledání a řídí výstupní protokol. Adresový dekodér pak zpřístupňuje softwaru přes lokální sběrnici řídicí a stavové registry a umožňuje nahrávat a číst obsah CAM paměti.

Implementace byla provedena v jazyce VHDL pro cílovou technologii FPGA, konkrétně Virtex II od firmy Xilinx. Frekvence designu je dána frekvencí všech komponent SCAMPI adaptéru, což je 100 MHz. Při této frekvenci je propustnost vyhledávací komponenty 3,2 Gbps.



Obrázek 1: Datový tok

4 ZÁVĚR

S využitím asociativní paměti a technologie FPGA byla navržena a implementována komponenta pro rychlé vyhledávání vzorů v datech paketů při rychlosti 3,2 Gbps. To přináší významné urychlení proti klasickým SW řešením, jejichž propustnost se pohybuje v řádech 100 Mbps a je závislá na počtu hledaných vzorů. Výhodou návrhu je i možnost rychlé přidávání a změny hledaných vzorů, což je nezbytné pro detekci rychle se šířících virů a jiných nebezpečných útoků. Maximální propustnost komponenty je dána vlastnostmi asociativní paměti. Při použití výkonější a větší TCAM paměti, by navržená architektura byla schopna dosáhnou i vyšších propustností v řádu 10 Gbps.

PODĚKOVÁNÍ

Tento příspěvek vznikl v rámci Evropského projektu SCAMPI (IST-2001-32404) a výzkumné aktivity *Programovatelný hardware* sdružení CESNET z.s.p.o.

REFERENCE

[1] Martínek, T., Kořenek, J., Novotný, J.: Passive network monitoring adapter intended for 10Gbps technology, Sborník příspěvků z XXV. konference EurOpen, Plzeň, CZ, 2004, s. 55-63, ISBN 80-86583-07-4

[2] Novotný, J., Fučík, O., Kokotek, R.: Schematics and PCB of COMBO6, CESNET, URL http://www.liberouter.org/documents/combo6.pdf (březen 2005)

[3] WWW stránka projektu Liberouter, CESNET, http://www.liberouter.org