TCP STATE PROCESSING FOR FPGA TECHNOLOGY

Martin Košek
Bachelor Degree Programme (3), FIT BUT
E-mail: xkosek00@stud.fit.vutbr.cz

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

ABSTRACT

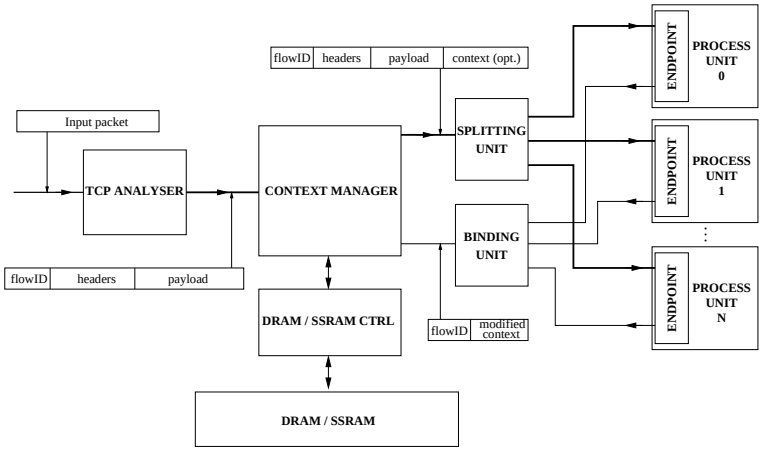
TCP State Processing becomes more and more valuated in a today's world of network technologies. It allows us to analyse and process incoming network traffic with flow-based approach rather than packet-based one. Flow-based approach is essential for Intrusion Detection Systems, Flow and Protocol Analysis and other network security systems. This paper introduces an architecture of TCP State Processing System, targeted at multigigabit networks (1 Gbps and 10 Gbps). Designed architecture will be implemented in VHDL and tested on FPGA in a Combo6X card [2].

1 ÚVOD

V poslední době jsme svědky výrazného rozvoje Internetu. Počet uživatelů a poskytovaných služeb rychle roste a s ním i potřeba analyzovat a zpracovávat informace, které jsou vyměňovány mezi uživateli. Mnoho síťových zařízení, provádějících podobné analýzy, je schopno pracovat pouze nad jednotlivými pakety, ne nad celými datovými toky. Tento přístup je však v mnoha případech nevyhovující. Tak je tomu například u aplikací typu vyhledávání řetězců v paketech, systémů pro analýzu protokolů a dalších bezpečnostních systémů. Zde je potřeba pracovat se stavovou informací k danému datovému toku. Tento problém může být demonstrován na systému vyhledávání řetězců v datovém toku, který bez možnosti ukládát aktuální stav vyhledávání není schopen nalézt řetězce rozdělěné mezi pakety. Této slabiny může využít potenciální útočník a oklamat tak detekční systém.
Cílem tohoto článku je prezentace návrhu architektury systému pro stavové zpracování TCP/IP toků pro multigigabitové sítě. Vzhledem k cílovým rychlostem zpracovávané sítě (1 až 10 Gb/s) není možné použít klasické zpracování založené na obecném procesoru a odpovídajícím software, ale je nutné pracovat na nižší vrstvě - hardware. Ta poskytne potřebný paralelismus a dostatečný výpočetní výkon.
Jako cílová technologie pro implementaci tohoto systému byla zvolena programovatelná hradlová pole (FPGA) poskytující flexibilitu při rekonfiguraci a dostatečný výkon pro zpracování síťového provozu. Systém bude implementován v jazyce VHDL a otestován na kartě Combo6X [2].

2 ARCHITEKTURA

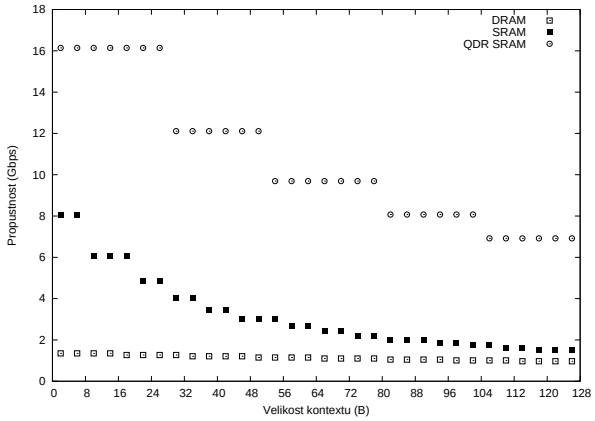
Architektura systému je založena na principu prezentovaném pány Schuehlerem a Lockwoodem [1]. Jejich koncept byl však upraven, aby vyhovoval požadavkům na vyvíjený systém. Byla přidána podpora pro zpětný zápis upravených stavových informací (kontextů) a možnost použít obecný počet procesních jednotek. Blokové schéma navržené architektury je prezentováno na obrázku 1. Skládá se ze tří klíčových jednotek. První je TCP Analyser, který provádí analýzu vstupních paketů a výpočet identifikátoru datového toku, ke kterému paket patří. Tento identifikátor je vypočítán jako hash libovolných hlaviček paketu; nejčastěji to bude zdrojová a cílová IP adresa a port. Druhá a nejdůležitější jednotka je Context Manager, která spravuje vyčítání a zpětné ukládání aktualizované stavové informace k datovému toku. Musí být použit vždy aktuální kontext, jehož konzistenci zajistí právě tato jednotka. To obnáší kontrolu, zda je upravená stavová informace k datovému toku již uložena v externí paměti, nebo je stále v systému. Podle výsledku se rozhodne o vyčtení kontextu z paměti, nebo o použití již vyčteného v systému. Jednotka musí také podporovat efektivní vyčítání a ukládání kontextů tak, aby byla co nejvíce potlačena latence externí paměti s uloženými kontexty. Vlastní uživatelské aplikace jsou umístěné v procesních jednotkách. Ty komunikují se zbytkem systému pomocí Endpoint komponenty, která umožňuje vyčítání hlaviček, payloadu a kontextu k paketu a zpětné odeslání aktualizovaného kontextu do Context Manageru.
Celá tato architektura je navržena tak, aby byla flexibilní jak k počtu uživatelských procesních jednotek (pro zajištění dostatečného výkonu), tak pro použitou externí paměť. Předpokládá se využití dynamické nebo statické paměti umístěné přímo na kartě Combo6X. Také je podporována obecná velikost poskytovaného kontextu. Tento obecný přístup je nutný, aby byl systém použitelný pro co nejširší spektrum aplikací.



Obrázek 1: Navrhovaná architektura

3 ANALÝZA SYSTÉMU

Vyvíjený systém byl analyzován v souvislosti s minimální propustností, která je závislá na použité paměti. Ta je uzkým hrdlem celého systému. Zvažuje se použití 3 druhů pamětí: dynamické paměti (latence 17 taktů, propustnost 16B/takt), statické paměti (lat. 2 takty, prop. 9B/takt) a rychlé dvouportové statické paměti (lat. 2 takty, prop. 26B/takt). Propustnost je uvedená pro nejhorší možný případ - tok malých paketů (délka 65B). Výsledný graf je na obrázku 2.



Obrázek 2: Minimální propustnost pro vybrané paměti

Z grafu je patrné, že dynamická paměť je dobře využitelná pouze pro 1 Gbps sítě. Naopak QDR SRAM paměť má rychlost dostatečnou i pro 10 Gbps sítě, ale nevyhovuje dostupnou kapacitou (8 MB). Vystává zde problém, zda použít pomalejší paměť s velkou kapacitou (DRAM), nebo rychlou paměť s menší kapacitou (QDR SRAM) a s tím souvisejícím mnohem menším počtem dostupných kontextů. Řešení bude záviset na uživateli systému, který musí zvážit, jaký charakter má jeho aplikace. Nabízí se využití rychlé paměti jako cache dynamické paměti, ale vzhledem k lokalitě datových toků na síti by tento přístup nemusel být dostatečně efektivní.

4 ZÁVĚR

Byla navržena architektura pro stavové zpracování TCP/IP toků na multigigabitových rychlostech. Systém poskytuje obecné rozhraní pro různé druhy pamětí pro uložení kontextů, genericku velikost kontextu a volitelný počet procesních jednotek. Tím je umožněno použití v širokém okruhu aplikací. Pro systém byl vytvořen abstraktní popis a následně implementován simulační model s využitím knihovny SIMLIB/C++ [3]. Analýzou simulací lze ověřit funkci celého systému, určit ideální počet procesních jednotek pro vybranou aplikaci, velikost kritických front nebo průměrnou dobu strávenou pakety v systému.

PODĚKOVÁNÍ

Tento příspěvek vznikl za podpory výzkumného záměru MSM6383917201 v rámci výzkumné aktivity *Programovatelný hardware* sdružení CESNET z.s.p.o.

REFERENCE

[1] Schuehler, David V., Lockwood, John W.: A Modular System for FPGA-Based TCP Flow Processing in High-Speed Networks. In: *FPL*, 2004, pp. 301-310

[2] WWW stránka projektu Liberouter. http://www.liberouter.org (únor 2007)

[3] WWW stránka projektu SIMLIB/C++. http://www.fit.vutbr.cz/~peringer/SIMLIB/ (únor 2007)