Oponentský posudek disertační práce

Název disertační práce: *Software-Controlled Network Traffic Monitoring*
Autor: Ing. Lukáš Kekely

Paketové sítě využívající protokoly TCP/IP jsou založeny, alespoň ve své čisté podobě, na jádru složeném ze směrovačů (routerů), jejichž primárním úkolem je co nejrychleji předávat pakety z jednoho síťového rozhraní na jiné na základě cílové adresy obsažené v hlavičce každého paketu. Relativní jednoduchost této úlohy umožnila dosáhnout, také za pomoci hardwarové akcelerace, fenomenálních přenosových rychlostí. Stejný princip ale na druhé straně paradoxně velmi znesnadňuje monitorování takových sítí, má-li se provádět na některém z velmi zatížených směrovačů anebo na vysokorychlostní lince. Pro operátory velkých sítí má ale takový monitoring zásadní důležitost, ať už z důvodů bezpečnostních anebo jako prostředek včasné detekce poruch.

Posuzovaná disertační práce popisuje v kapitole 2 dosud používané metody měření a analýzy provozu takových sítí. Ty jsou založeny buď na selektivním ředění, kdy je možné vybraný malý objem síťových toků detailně analyzovat, anebo na agregaci, při níž se část informací ztrácí, tyicky vše nad úrovní transportní vrstvy. Každá z těchto alternativ je přitom použitelná pro určité typy analýz, ale nevhodná pro jiné.

Hlavním výsledkem disertační práce je prototyp vysokorychlostního monitorovacího zařízení, které umožňuje aplikovat selekci anebo agregaci podle zadaných klasifikačních pravidel na zvolené podmnožiny síťových toků, a dokonce pravidla za běhu měnit podle aktuálního síťového provozu. To je velmi užitečná vlastnost umožňující například pružně reagovat na různé síťové útoky, které vyžadují specifické monitorovací postupy. Autor tuto flexibilitu demonstruje na pěti případových studiích – základní měření NetFlow, detekce skenování portů, detekce útoku Heartbleed, analýza HTTP hlaviček a kombinace měření NetFlow s analýzou HTTP hlaviček.

Velmi vítám formu disertační práce, jejíž podstatnou část tvoří šest článků publikovaných (až na jeden) na prestižních mezinárodních konferencích a v časopisu *IEEE Transactions on Computers*. To je také nejlepší zárukou kvality disertační práce. Ing. Kekely je také ve všech mezinárodních publikacích uveden jako první autor, což svědčí o jeho významném osobním přínosu. Na druhé straně bych ale uvítal, kdyby zbytek disertační práce doplnil některé technické detaily, které z pochopitelných důvodů nemohou být do mezinárodních publikací zařazeny. Konkrétně mi jde zejména o podrobnější popis

- klasifikačních pravidel, která se konfigurují ve firmwaru,
- pravidel softwarového SDM kontroléru.

Chci také výrazně vyzdvihnout, že posuzovaná disertační práce je součástí výzkumných a vývojových aktivit, které se pod hlavičkou projektu *Liberouter* rozvíjejí už prakticky 15 let ve spoluprácí vysokých škol, operátora národní akademické sítě (CESNET, z. s. p. o.) i technologických firem.

Moje jediná výhrada se netýká věcné podstaty konceptu síťového monitorování popsaného v disertační práci, ale jména zvoleného pro tento koncept – Software Defined Monitoring. Tento termín není v disertační práci ani v přiložených článcích definován a používá se spíš neformálně. Evidentně se odkazuje na technologii SDN (Software Defined Networking), která je ale podle mého názoru založena na jiném principu: centralizovaný kontrolér implementuje řídící logiku (control plane) a komunikuje s jednoduchými síťovými prvky, které implementují data plane. Monitorovací zařízení popsané v disertační práci naproti tomu zřejmě předpokládá firmwarovou i softwarovou část uvnitř jednoho zařízení – komunikují spolu přes PCI sběrnici.

Kromě toho monitoring není v softwaru nijak definován, spíše firmware a software řeší ve vzájemné interakci různé části dané úlohy. Tento princip ale není nijak nový a dlouho se pro něj používá termín *hardware-software codesign*. Chápu, že název SDM byl zvolen spíše z marketingových důvodů, domnívám se však, že technická podstata tohoto monitorovacího zařízení je natolik kvalitní a inovativní, že by se prosadila i se sušším a přesnějším označením.

Po formální stránce je disertační práce napsána pečlivě a přehledně. Publikované články byly zřejmě podrobeny i jazykové korektuře (což je další výhoda), ale i ostatní text je vesměs napsán dobrou angličtinou. Autor se v ale v některých případech pouští do zbytečně složitých jazykových konstrukcí, které jsou na úkor srozumitelnosti. Například věta na str. 21 by rozhodně zasloužila přeformulovat: „Granular (per flow) utilization management of the described forms of hardware preprocessing enables for an interestingness based division of network traffic processing.“ Častou chybou, která se vyskytuje i ve výše uvedené větě, jsou chybějící spojovníky ve víceslovných spojeních v pozici shodného přívlastku (např. místo „flow based monitoring“ má být „flow-based monitoring“).

Závěry

1. Téma disertační práce odpovídá zvolenému oboru studia a je aktuální z hlediska současného stavu vědy a technologií.
2. Původní přínos autora spatřuji především ve
   — vytvoření návrhu a fungujícího prototypu zařízení pro monitorování vysokorychlostních sítí založeného na hardware-software codesignu;
   — verifikaci funkce tohoto zařízení ve vysokorychlostní síti CESNET2;
   — návrhu a implementaci paketového parseru pro FPGA.
3. Všechny původní přínosy autora byly publikovány formou prestižních mezinárodních publikací, které jsou k práci přiloženy.
4. Disertační práce dostatečně dokládá vědeckou erudici Ing. Lukáše Kekelyho a **odpovídá obecně uznávaným požadavkům pro udělení akademického titulu PhD**.

V Litvínovicích, 13. srpna 2017 Ing. Ladislav Lhotka, CSc.