Hardwarově akcelerovaná sonda pro legální odposlechy

FIT VUT Technický report

Lukáš Kekely, Martin Žádník

Technický report č. FIT-TR-2012-005
Fakulta informačních technologií, Vysoké učení technické v Brně

Poslední změna: 11. prosince 2012

Hardwarově akcelerovaná sonda pro legální odposlechy

Lukáš Kekely, Martin Žádník

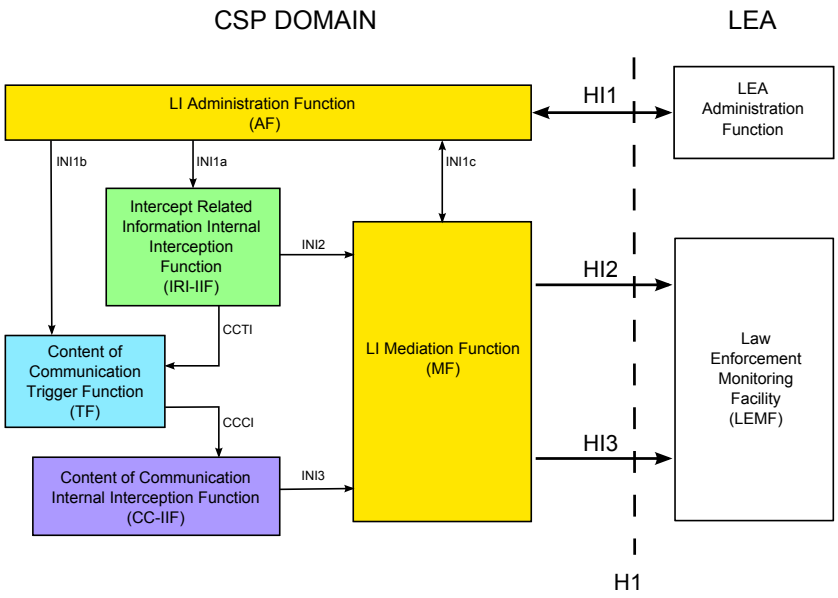
Fakulta informačních technologií
Vysoké učení technické v Brně
Božetěchova 1/2, 612 66 Brno
{xkekel00, izadnik}@fit.vutbr.cz

Abstrakt Technický report se zabývá vysokorychlostní sondou, která je určena pro zachycení a export síťového provozu pro účely zákonných odposlechů. Specifická oblast zákonných odposlechů vyžaduje zajištění bezeztrátového zachycení zájmového provozu. Z tohoto důvodu je sonda postavena na platformě využívající programovatelnou síťovou kartu a hostitelského počítače. Hardwarová akcelerace na kartě je realizována pomocí programovatelného hradlového pole FPGA. Výsledky experimentů ukazují, že funkcionalita a parametry takového řešení jsou odpovídající pro nasazení v oblasti legálních odposlechů.

1 Úvod

Legální odposlechy slouží pro pořizování důkazního materiálu při podezření na páchání trestné činnosti. Vzhledem k tomu, že velká část komunikace uživatelů je realizována po Internetu, je nutné i v této oblasti zajistit možnost odposlechů. Na tuto možnost pamatuje i norma definující strukturu systému zákonných odposlechů (LI, Lawful Interception) vydaná ETSI [2]. Tato norma definuje systém odposlechů jako několik vzájemně propojených funkcí, které mohou být realizovány pomocí samostatných zařízení. Případně může být více funkcí sloučeno do jednoho zařízení. Sběr dat ze sítě zajišťuje CC (CC, Content of Comunication) funkce, která bývá nejčastěji realizována prostřednictvím specializovaných hardwarových sond. Konfigurace těchto sond probíhá pomocí CCCI (CC Configuration Interface) rozhraní a INI3 odposlouchávaný provoz do mediační funkce (MF, Mediation Function), která získaná data transformuje do HI3 rozhraní a přenáší do bezpečnostní agentury (LEA, Law Enforcement Agency). Současně mediační funkce posílá do agentury ve formě HI2 rozhraní informace z IRI (IRI, Intercept Related Information) funkce, která poskytuje doplňující informace k jednotlivým odposlechům. Například informace o přihlášení nebo odhlášení odposlouchávaného uživatele nebo informace o změně přidělené IP adresy. Celé řízení systému pro zákonné odposlechy pak zajišťuje administrační funkce (AF, Administration Funtion), se kterou komunikuje LEA prostřednictvím HI1 rozhraní.

V prostředí velkých poskytovatelů dochází k agregaci provozu mnoha uživatelů. Výsledkem jsou vysoké nároky na výkonnost sondy realizující odposlech



Obrázek 1. Architektura systému pro zákonné odposlechy podle norem ETSI.

tak, aby nedocházelo ke ztrátám paketů. Z tohoto důvodu je sonda implementována jako speciální hardwarové zařízení. Toto zařízení se sestává z programovatelné síťové karty a hostitelského počítače. Programovatelná síťová karta obsahuje programovatelné hradlové pole (FPGA), ve kterém jsou umístěny jednotky realizující primární zachycení a filtraci provozu. V hostitelském počítači je realizována komunikace s MF za účelem konfigurace a odesílání odposlechnutého provozu.

Pro monitorování sítě a sběr dat je nutné využít sondy, které jsou schopny zajistit odposlech požadovaného provozu. Aby mohly sondy využít orgány činné v trestním řízení, je nutné zajistit zaznamenání veškeré komunikace beze ztráty paketu. V opačném případě by mohly být získané informace zpochybněny a nebyly by použity při vyšetřování. Proto je nutné realizovat sondy jako speciální hardwarová zařízení, která pracují na rychlosti vstupních linek beze ztráty jediného paketu.

Tato technická zpráva je zaměřena na popis realizace a výsledky testování vysokorychlostní sondy, která je vyvíjena v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*. Dokument je členěn následovně. Na úvod navazuje kapitola popisující vývojovou platformu. Architektura vysokorychlostní sondy a funkcionalita jednotlivých částí je popsána v další kapitole. Následuje kapitola z testování. Závěrečná kapitola shrnuje podstatné informace a nastiňuje práci v dalším období realizace projektu.

2 Architektura

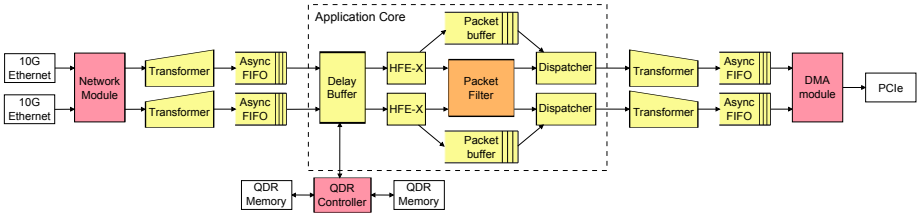
Vysokorychlostní sonda je určena pro nasazení k velkým ISP a na páteřní linky, jejichž přenosová rychlost je velmi vysoká. Sledování a filtrování komunikace na takovéto rychlosti je výpočetně velmi náročná úloha. Dnešní počítače v kombinaci s dostupnými síťovými kartami neumožňují konstrukci sond, které by zajistily filtraci zájmového provozu beze ztráty jediného paketu pro zatížené 10 Gb/s linky. Problémem je nejen nízká přenosová rychlost síťových karet, ale i práce z pamětí a výkonem procesoru. Vysokorychlostní sonda je proto postavena tak, aby většina síťové komunikace byla odfiltrována na kartě a pouze zájmový provoz byl dále zpracováván.

3 Přehled architektury

Úloha LI sondy je rozdělena na akcelerační jádro a řídicí ale i datový software. Akcelerační jádro je umístěno do FPGA a implementuje časově kritické části úlohy odposlechu provozu. Řídicí software zajišťuje zejména správu, řízení a komunikaci akceleračního jádra s dalšími prvky ve struktuře LI přes rozhraní CCCI. Datový software umožňuje export zachycené zájmové komunikace na mediační zařízení pomocí INI3 rozhraní.

Hardwarová architektura vysokorychlostní sondy vychází z vlastností akceleračních karet COMBO a platformy NetCOPE. Na kartě v FPGA je realizováno zachycení provozu s přesnou časovou značkou, uložení do mezipaměti, zpracování paketu a filtrace síťového provozu. Software zajišťuje management filtru a komunikaci s mediační a administrační funkcí LI systému. Díky vysokým přenosovým rychlostem mezi akcelerační kartou a hostitelským počítačem je navíc u navrženého rozdělení úlohy mezi hardware a software možné vybírat ze sítě i relativně velký objem zájmového provozu.

Aby filtrace provozu byla prováděna na rychlosti linky i pro multi-gigabitové propustnosti a nedocházelo k nekontrolované ztrátě paketů, je nutné věnovat zvláštní pozornost návrhu hardwarové architektury firmware akcelerační karty. Na základě analýzy problematiky zákonných odposlechů byla proto navržena architektura znázorněna na obrázku 2.

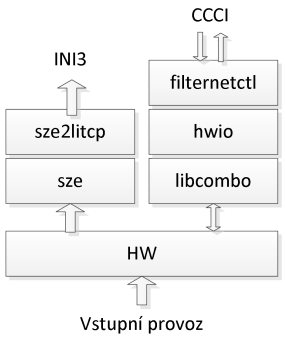


Obrázek 2. Navržená architektura firmware vysokorychlostní sondy.

Architektura firmware je založena na zřetězené lince procesních jednotek. Pro každý vstupní port je přijetí paketu zabezpečeno platformou NetCOPE. Platforma NetCOPE poskytuje rozhraní pro aplikační jádro, tzv. Application CORE. NetCOPE a aplikační jádro jsou od sebe asynchroně odděleny, aby bylo možné obě části provozovat na odlišných frekvencích.

První jednotkou aplikačního jádra je zpožďovacího buffer (DB, Delay Buffer). DB realizuje definované zpoždění síťového provozu. Z jednotky DB pokračují pakety do jednotky HFE-X (HFE-X, Header Field Extraction XML), kde jsou z hlaviček paketu získány položky potřebné k provedení filtrace. Jednotka HFE-X současně rozděluje paketový tok na datovou a řídicí cestu. Extrahované položky jsou posílány řídicí cestou do filtrační jednotky, zatímco pakety pokračují po datové cestě do FIFO paměti, která slouží pouze k překrytí latence výpočtu ve filtrační jednotce. Filtrační jednotka na základě položek z hlaviček paketů rozhodne, jestli se má paket zahodit nebo propustit. Výsledek filtrace je odeslán do jednotky Disp (Disp, Dispatcher), která zajišťuje fyzické zahazování nepotřebných paketů tak, aby bylo možné propagovat dále pouze zájmový provoz. V jednotce Disp se tak opět spojuje datová a řídicí cesta. Nepotřebné pakety jsou zahozený a zájmový provoz je propagován do přijímací FIFO paměti, odkud je DMA přenosy platformy NetCOPE přenášen do paměti hostitelského počítače.

Architektura software běžícího na hostitelském počítači se skládá z knihoven pro práci s kartou a pro práci s jednotkami aplikačního jádra. Architektura software je uvedena na obrázku 3.



Obrázek 3. Navržená architektura software vysokorychlostní sondy.

Na nejnižší vrstvě se nachází knihovny implementující základní operace s kartou jako jsou nahrání firmware na kartu nebo zápis či čtení do/z paměťového místa na kartě. Tyto funkce se nacházejí v modulu libcombo. Za účelem odstínění specifik dané karty je nad libcombo implementována knihovna hwio. Pro přenos objemných dat přes DMA kanály je využito SZE rozhraní umožňující předávat pakety bez kopírování paměti. Na vyšší úrovni jsou implementovány dva uživatelské moduly implementující aplikaci funkcionalitu potřebnou pro komunikaci

s dalšími LI prvky. První modul filternetctl přijímá příkazy přes CCCI rozhraní a převádí je na příkazy pro filtr modul v kartě. Tyto příkazy jsou orientovány na přidání či odebrání pravidla na odposlech. Druhý modul sze2litcp přijímá zachycený provoz a odesílá ho přes INI3 rozhraní na mediační zařízení.

3.1 Akcelerační karta a platforma NetCOPE

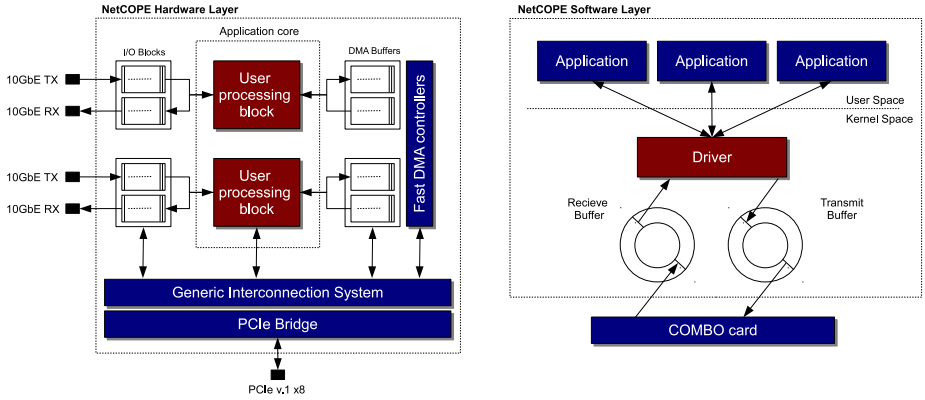
Pro realizaci vysokorychlostní sondy byly zvoleny akcelerační karty COMBO [3], které byly vyvinuty v rámci spolupráce FIT VUT se sdružením CESNET [1]. COMBO karta je zachycena na obrázku 4. Je osazena výkonným FPGA Virtex-5, rychlou pamětí QDR SRAM, slotem pro DRAM s kapacitou až 2 GB, dvěma 10 Gb/s síťovými porty a rychlým PCI express rozhraním (PCIe v.1 x8). Díky výkonnému FPGA je možné kartu využít pro hardwarovou akceleraci časově kritických úloh. Umožňuje tak konstrukci zařízení pro vysokorychlostní sítě, které i pro propustnosti v řádech 10 Gb/s umožní zpracovat veškerý síťový provoz bez ztráty paketu. Pro vývoj sondy byly zakoupeny celkem 3 karty včetně vývojových serverů a platformy NetCOPE [5,4], která umožňuje rychlý vývoj hardwarově akcelerovaných síťových aplikací.

Obrázek 4. Karta COMBO se dvěma 10 Gb/s porty.

Prostředí NetCOPE dovoluje rychle vyvinout aplikace využívající FPGA ve spolupráci s procesorem v hostitelském počítači. Především přesně definuje vzájemná rozhraní mez hardware a software a poskytuje jejich realizaci. Architektura platformy je zachycena na obrázku 5. Kromě aplikačního jádra se skládá z I/O bloků, propojovacího systému a rychlých DMA řadičů, a dalších předpřipravených modulů.

– **I/O blok** implementuje příjem a vysílání paketů na plné rychlosti linky podle standardu IEEE 802.3.

– **Propojovací systém (Generic Interconnection System)** umožňuje rychlou komunikaci mezi komponenty v FPGA a systémovou sběrnicí. Podporuje režimy bus master a slave. V režimu slave zpracovává transakce systémové sběrnice a posílá je jednotlivým komponentám v FPGA. V režimu bus master umožňuje komponentám iniciovat na systémové sběrnici čtecí a zápisové transakce a přistupovat tak zcela autonomně do paměti hostitelského počítače.
– **Rychlé DMA řadiče** zajišťují rychlé přenosy mezi akceleračním jádrem a pamětí hostitelského počítače.



Obrázek 5. Architektura platformy NetCOPE.

Díky rychlým DMA přenosům poskytuje platforma NetCOPE možnost efektivně rozdělit činnost zařízení mezi hardwarové a softwarové prostředky. Je tak možné akcelerovat pouze časově kritické části aplikace a šetřit plochu na čipu. DMA přenosy jsou realizovány prostřednictvím datových přenosů mezi dvojicí kruhových bufferů. Jeden kruhový buffer je umístěn v paměti hostitelského počítače a poskytuje data softwarové aplikace nebo vláknům. Druhý buffer je implementovaný v FPGA na akcelerační kartě, kde poskytuje data akceleračnímu jádru. Buffer v paměti je fyzicky rozdělen do stránek o velikosti 4 kB, které jsou souvisle mapovány do adresového prostoru aplikace pomocí systémového volání `nmap()`. Součásti platformy NetCOPE jsou ovladače a knihovny, které umožňují aplikaci jednoduše přistupovat k datům přenášených do nebo z akcelerační karty. Kruhové buffery jsou v návaznosti na aplikaci a akcelerační kartu zachyceny na obrázku 5.

3.2 Moduly aplikačního jádra

V architektuře systému jsou klíčovými jednotkami zejména zpožďovací buffer (DB), jednotka pro extrakci položek z hlaviček paketů (HFE-X) a jednotka pro

filtraci paketů (Filtr). Detailní popis těchto jednotek je uveden v této sekci. Je proto vhodné uvést charakteristiku uvedených komponent.

Jednotka pro zpoždění vstupního provozu - (DB) vytváří zpoždění vstupního provozu o přesně definovaný čas t_d, přičemž samotnou dobu zpoždění je možné nastavovat za běhu pomocí konfiguračního nástroje delayctl. V DB dochází k uložení příchozích paketů do externí paměti, která tak tvoří de facto frontu paketů. V současné době jsou využívány dva moduly SRAM o celkové kapacitě 16MB. Jejich kapacita je sdílena mezi oba vstupní porty. Plná kapacita tak může být využita i případech, kdy je aktivní pouze jeden port. Uložené pakety jsou z paměti vyčteny po uplynutí t_d nebo pokud je paměť plná a je nutné uvolnit místo pro nově příchozí pakety. Aby bylo možné určit dobu, po kterou je paket v paměti uložen je nutné část paketu s časovou z fronty vyčíst. Pakety se v paměti oddělují pomocí paratních bitů, do kterých je zakódován začátek a konec paketu. Pro různé hodnoty vytížení linky dostáváme maximální možnou dobu, po kterou je možné provoz zpozdit. Údaje pro vytížení jsou uvedeny v experimentech na obrázku 6.

Jednotka pro analýzu a extrakci položek z hlaviček paketů - (HFE-X) slouží k analýze a extrakci položek z hlaviček paketů. Jedná se o automat, který je sestaven na základě definice protokolů. Definice protokolů je uvedena v XML formátu. Automat parsuje příchozí paket dle definice a označuje jednotlivé pole. Následuje extraktor, který dle další definice vybere pouze zájmová pole. V případě zákonných odposlechů je zájmová množina sestavena následovně:

0	1	2	3
	src IP address 3		
	src IP address 2		
	src IP address 1		
	src IP address 0		
	dst IP address 3		
	dst IP address 2		
	dst IP address 1		
	dst IP address 0		
src Port		dst Port	
Protocol			

Pokud se jedná o IPv6 adresu, jsou využity všechny položky 0-3, pokud se jedná o IPv4 je využita pouze položka 0.

Filtrační jednotka - klasifikuje extrahovaná pole ze záhlaví paketu podle různých typů pravidel.

Cílem je rozlišit zájmový provoz od zbylého provozu, předat dále informaci, které pakety se mají v jednotce Disp zahodit, a které propustit. Aby bylo možné identifikovat zájmový provoz musí filtrační jednotka provádět klasifikaci paketů na základě tří typů pravidel:

- Typ A – zdrojové nebo cílové IP adresy,
- Typ B – TCP/UDP spojení (síťových toků) a
- Typ C – TCP/UDP portů, které určují důležité služby (SIP, IMAP a další) na dané IP adrese.

Pro každý typ je vytvořen samostatný filtr. Za zájmový provoz je pak považován každý paket, který je označen alespoň jedním z těchto tří filtrů. Fitlry jsou implementovány pomocí kukaččí hash tabulky. Logika algoritmu kukaččcí hash je plně implementována v FPGA. Jako paměť tabulky slouží interní BlockRAM v FPGA. Počet pravidel je proto omezen pro jednotlivé typy na následující hodnoty:

- Typ A – max. 1537 rules.
- Typ B – max. 1537 rules.
- Typ C – max. 513 rules.

Kukaččí hash dokáže plně zaplnit všechna místa v tabulce pouze v ideálním případě. Ve skutečnosti bude kapacita každého filtru o něco nižší v závislosti na zvolených pravidlech. Dosažené výsledky zaplnění jsou rozebrány v kapitole 4.1.

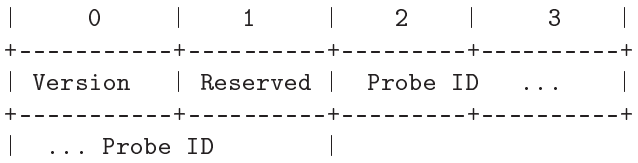
Architektura jednotky je navržena tak, aby umožňovala zpracovávat na rychlosti linky provoz až ze dvou 10 Gb/s rozhraní.

3.3 Aplikační software

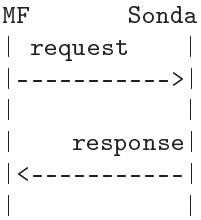
Z pohledu napojení na systém zákonných odposlechů jsou nejdůležitější software moduly fitlernetctl a sze2litcp.

Ovládání filtru – filternetctl – přijímá příkazy přes síťové rozhraní a převádí je na příkazy pro filtrační komponentu v FPGA, čímž implementuje CCCI rozhraní. Po spuštění se filternetctl připojí přes TCP soket na mediační funkci. Mediační funkce využívá toto spojení pro zasílání příkazů na přidání či odebrání pravidla na odposlech. Filternetctl přetváří tato pravidla na příkazy zápisu pravidla do komponenty Filtr. Každé pravidlo odposlechu má přiděleno na mediační funkci jednoznačný identifikátor dlouhý 32 bitů. Vzhledem k úspoře místa potřebného pro každé pravidlo je identifikátor pravidla přečíslován na 16 bitů při převodu pravidla pro Filtr. Toto 16 bitové číslo je rovněž předáno do MF. MF provede příslušný převod pravidla Protokol pro předávání příkazů mezi sondou a mediační funkcí pracuje následovně.

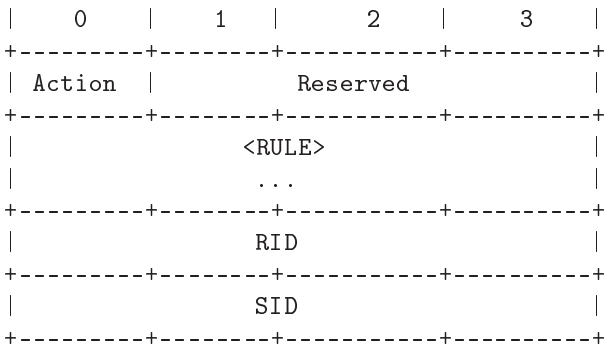
Nejprve dojde k výměně informace o používané verzi CCCI protokolu a identifikátoru sondy. Po připojení sondy na MF zašle MF sondě následující záhlaví CCCI protokolu:



Sonda po obdržení záhlaví od MF odpoví ve stejné struktuře. Položka Version značí verzi CCCI protokolu. Jednotlivé verze se mohou lišit ve svém formátu. Položka ProbeID jedinečně označuje sondu v rámci LI systému. Následují příkazy typu požadavek-potvrzení.

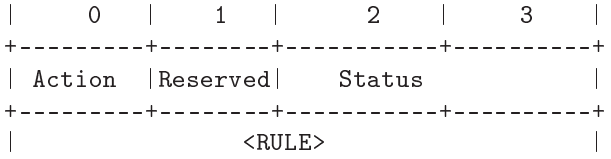


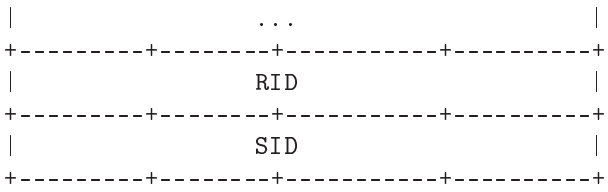
Zpráva typu request má následující strukturu:



Položka Action udává, zda se jedná o přidání (hodnta 0), nebo odebrání pravidla (hodnota 1). Struktura <RULE> obsahuje pravidlo a je rozebrána níže. Položka RID (Rule ID) obsahuje číslo pravidla přiřazeného sondou ke zaslanému požadavku/pravidlu, je povinností sondy zajistit, aby dané RID bylo unikátní v rámci pravidel nakonfigurovaných v daný okamžik a v průběhu odposlechu se nezměnilo. SID (Session ID) obsahuje číslo pravidla přiřazeného MF danému požadavku/pravidlu

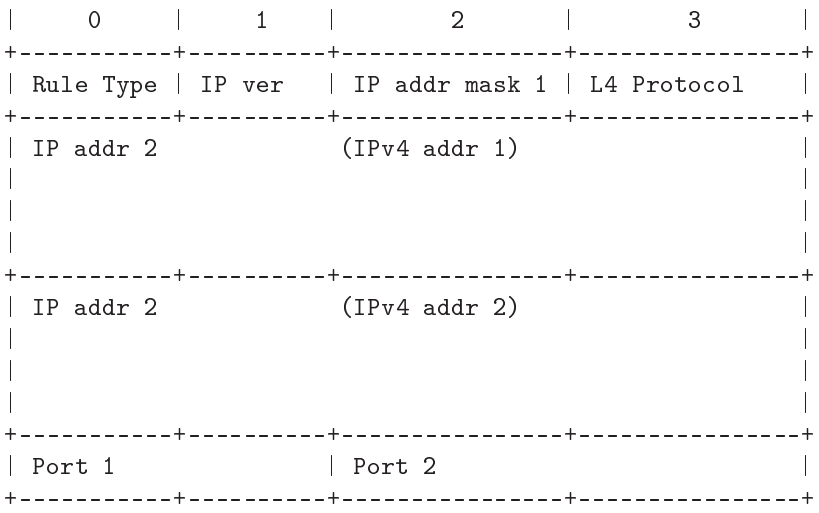
Zpráva typu response obsahuje oproti request navíc položku Status.





Položka Status udává návratový kód provedené operace, záporná hodnota a nula značí neúspěch.

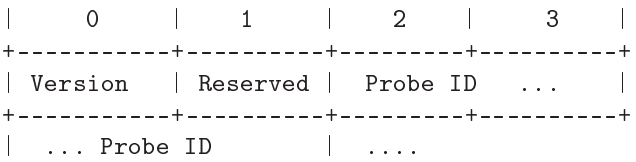
Samotné pravidlo <RULE> má následující strukturu.



Položka Rule Type udává typ pravidla, kde 0 nula odpovídá pravidlu typu A, 1 odpovídá typu B a 3 odpovídá typu C. Položka IP ver určuje verze IP protokolu (položka je platná pro pravidla typu 0, 1, 3) a nabývá hodnot 4 - IPv4 protokol či 6 - IPv6 protokol. Položka IP addr mask 1 udává masku položky IP adr 1 v rozsahu 0 - 128. Položka je platná pro pravidla typu 0. Pro pravidla typu 1 a 3 musí být nastavená na 32 pro IPv4 a 128 pro IPv6. Položka IP addr 1 obsahuje IPv4 nebo IPv6 adresu dle IP ver. Tato položka je platná pro pravidla typu A, B, C. IP addr 2 obsahuje IPv4 nebo IPv6 adresu dle IP ver. Tato položka je platná pro pravidla typu B. Položka Proto značí číslo transportního protokolu a je platná pro pravidla B a C. Položka Port 1 obsahuje číslo trasportního protokolu a je platná pro pravidla typu B a C. Položka Port 2 obsahuje číslo trasportního protokolu a je platná pro pravidla typu B. Při filtrování se uvažuje vždy obousměrná komunikace. Tzn. buď nastane situace, kdy se IP addr 1, IP addr 2, Port 1, Port 2 porovnává se zdrojovu, cílovou IP adresou, zdrojovým a cílovým portem, nebo se IP addr 1, IP addr 2, Port 1, Port 2 porovnává s cílovou, zdrojovou IP adresou a cílovým a zdrojovým portem.

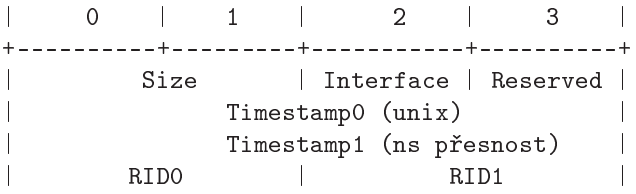
Export data – sze2litcp - přijímá zachycené pakety a odesílá je přes síťové rozhraní na mediační funkci, implementuje tak INI3 rozhraní. Sze2litcp se přes

TCP soket připojí k mediační funkci. Jakmile obdrží sze2lictp zachycený paket ze SZE rozhraní, pak tento paket upraví do formátu INI3 a pošle přes TCP do MF. Protokol INI3 je pro sondu definovaný následovně. Nejprve se pošle právě jednou záhlaví protokolu INI3 před exportem dat ze sondy na MF. Struktura INI3 záhlaví je obdobná jako CCCI.



Položka Version definuje formát INI3 prototokolu Položka Probe ID, která jedinečně označuje sondu v rámci LI systému a musí být shodná na CCCI i INI3 rozhraní.

Následně se zasílají zachycené pakety, ke kterým se předřazuje dodatečná informace (tyto položky jsou zakódovány jako little endian). Struktura přidávané informace je definována jako:



Položka Size určuje délku následného zachycených data v bajtech. Položka Interface určuje rozhraní, na které byla zachycená data odposlechnuta. Položka Timestamp obsahuje časovou značku příchodu paketu ze sítě na rozhraní a je rozdělena do dvou 4-bajtových částí. Timestamp0 obsahuje počet sekund od začátku Unixové éry a Timestamp1 obsahuje počet nanosekund od začátku aktuální sekundy. Položky RID jsou získány k danému paketu z filtru a značí číslo pravidla, které se shodovalo s daným paketem. RID0 obsahuje číslo pravidla, které se shoduje se zdrojovými položkami paketu a RID1 obsahuje číslo pravidla, které se shoduje s cílovými položkami. Pokud je RID0 anebo RID1 neplatný (vždy je platný alespoň jeden, jinak je rámec v FPGA zahozen), pak nastavíme RID0 rovno RID1 nebo obrácené podle toho, které RID je platné. Typicky bude odposloucháván pouze zdroj, nebo cíl komunikace, ale ve výjimečných případech může být požadován odposlech obou stran.

Další software - se sestáva ze skriptů pro nahrávání a inicializaci firmware do FPGA a dalších ovládacích nástrojů. Mezi nejvýznamnější patří:

- tsuctl – spouští a řídí modul v FPGA, který vyplňuje časovou značku paketu na síťovém rozhraní
- delayctl – konfiguruje modul Delay Buffer, který zpožďuje příchozí pakety
- hfexctl – konfiguruje a spouští modul HFE-X

4 Testy

Poté, co byl sestaven firmware, byly provedeny různé testy, které mají za úkol dokumentovat některé vlasnosti vyvíjeného řešení.

4.1 Počet pravidel

Každý typ filtrovacího pravidla má vyhrazenu tabulku. Zaplněnost této tabulky (tedy množství pravidel), které je možné využít závisí na obsahu pravidel. Pokud dodje k namapování více pravidel do stejných polí, pak již není možné vložit další pravidlo do filtrovací tabulky. Tabulka 1 udává průměrně dosažené zaplnění filtrovací tabulky při pokusech o dosáhnutí jejího maximálního zaplnění. Každá průměrná hodnota byla vypočítána ze 100 experimentů. Jednotlivé sloupce značí typ filtrovacího pravidla a kapacitu příslušné filtrovací tabulky. Dle řádků můžeme zjistit způsob generování pravidel.

Prvním ze způsobů označným v tabulce písmenem N je náhodné generování pravidla, kdy obsah pravidla je vygenerován pseudonáhodným generátorem čísel. Druhým způsobem je generování pravidla inkrementálně, značené písmenem I. Počáteční offset a inkrement jsou zvoleny náhodně, ale po dobu generování pravidel do zaplnění tabulky zůstávají neměnné. Třetím způsobem je generování po sobě jdoucích pravidel lišících se pouze v jednom bitu, značeno písmemem B. První pravidlo je zvoleno náhodně, následující pravidla jsou vždy od předcházejícího vzdálena o Hammingovu vzdálenost 1.

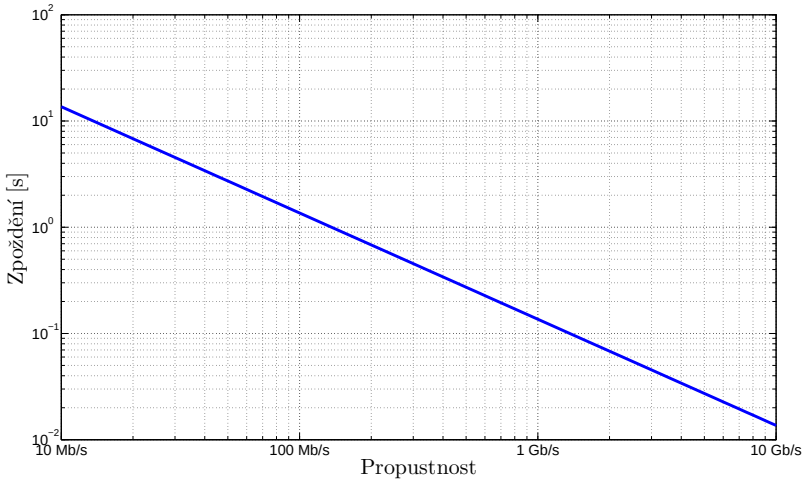
Tabulka 1. Průměrně zaplnitelná kapacita filtrovacích tabulek pouze IPv4 pravidly, pouze IPv6 pravidly nebo jejich kombinací v poměru 1:1

	Pouze IPv4				Pouze IPv6				IPv4 i IPv6			
	Typ A	Typ B	Typ C		Typ A	Typ B	Typ C		Typ A	Typ B	Typ C	
N	91,6%	54,0%	91,6%	N	91,7%	54,7%	91,6%	N	91,8%	53,9%	91,9%	
I	78,1%	61,1%	81,5%	I	87,8%	70,7%	79,7%	I	91,6%	51,2%	88,6%	
B	82,7%	62,9%	82,2%	B	83,8%	67,2%	85,6%	B	88,5%	50,1%	90,5%	

Z tabulky je možné pozorovat, že průměrně se daří tabulky pro pravidla typu A a C zaplnit přibližně na 80%. Tyto tabulky mají k dispozici každá 1537 řádků. Z toho vyplývá, že je průměrně možné obsadit přibližně 1100 řádků i při nepříznivém složení generované sady. Typ B dosahuje přibližně 50% úspěšnosit zaplnění z důvodu využití méně paměťových modulů v FPGA. Z tohoto důvodu musí být použito méně hash funkcí pro implementaci kukaččí hash tabulky. Průměrné zaplnění tabulky klesá, neboť je méně možností, kam přemístit kolizní pravidla. Celkově je pro tabulku pro pravidla typu B alokováno 1025 řádků, průměrně se daří obsadit pouze 512.

4.2 Zpoždění

Jednotka vstupního zpoždění DB dokáže dočasně pozdržet provoz. Doba, po kterou je provoz možné v DB uchovat je závislá na intenzitě provozu linky. Obrázek 6 vykresluje závislost zpoždění na intenzitě provozu linky.



Obrázek 6. Závislost délky zpoždění na intenzitě provozu.

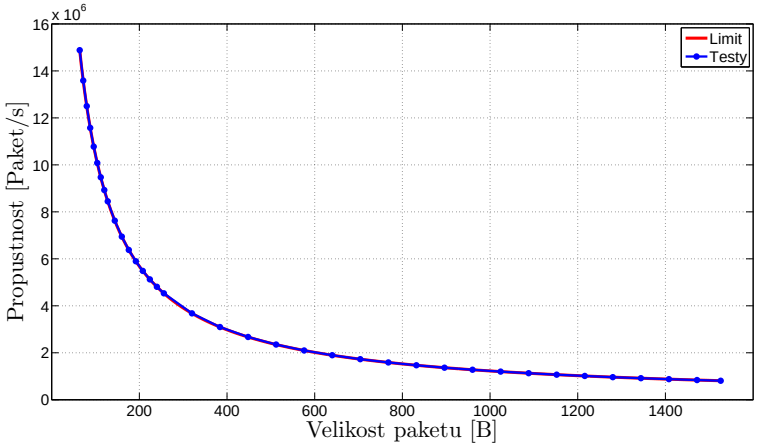
Z obrázku je možné pozorovat, že pro vysoké rychlosti je zpoždění poměrně malé v řádu jednotek milisekund. Toto zpoždění je potřebné pro překlenutí doby mezi začátkem komunikace IP adresy v síti a dobou než je registrována IRI-IIF. Otázkou zůstává, zda je nutné vůbec síťový provoz zpožďovat, tedy zda dochází ke zpoždění zaregistrování IP adresy v IRI-IIF oproti jejímu začátku komunikace.

4.3 Propustnost

Vzhledem k nasazení sond na linkách s vysokým zatížením jsme testovali propustnost sondy. Propustnost jsme rozdělili na propustnost procesní linky v FPGA a na propustnost software části sondy. Testování probíhalo pomocí generátoru paketů Spirent.

Test procesní linky v FPGA proběhnul tak, že filtr byl nastaven na zahazování veškerého provozu a pakety tak nebyly vůbec přeposílány do SW. V takovém případě stačí sledovat čítače paketů jednotlivých komponent, na základě kterých je možné dovodit počet zahozených paketů/bytů. Grafy v obrázcích 7, 7 zachycují dosaženou propustnost procesní linky v paketech či bytech za sekundu při zatížení jednoho portu. Grafy v obrázcích 9, 10 zachycují dosaženou propustnost

procesní linky v paketech či bytech za sekundu při zatížení obou portu zároveň. Spirent vždy generoval provoz na maximální propustnosti. Měření bylo prováděno postupně pro různé délky paketů. Pro každou délku proběhlo deset testů v délce trvání jednu minutu a nejnižší z naměřených hodnot je uvedena v grafu.



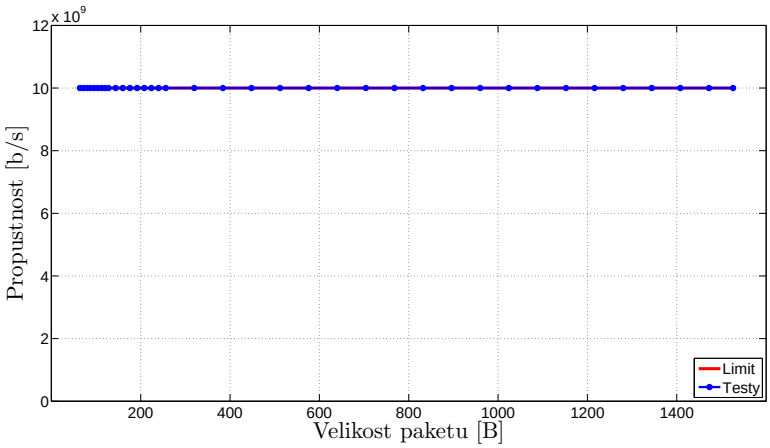
Obrázek 7. Propustnost procesní linky při zpracování jednoho maximálně vytíženého portu (měřeno v milionech paketů za sekundu).

Z grafů 7, 8 je patrné, že procesní linka zvládá zpracovat veškerý provoz na jedné lince bez jediné ztráty paketu bez ohledu na délku paketů. Grafy 9, 10 naopak ukazují, že pokud jsou oba porty zatíženy na maxímální propustnost pak dochází k zahazování paketů. Toto zahazování je způsobeno modulem DB, který má omezenou propustnost pamětí. Řešením je tento DB alokovat pouze pro jeden ze vstupních portů a druhý port zapojit napřímo do procesní linky. V takovém případě je procesní linka schopna zpracovat oba vstupní porty na maximálním zatížení bez ztráty paketu.

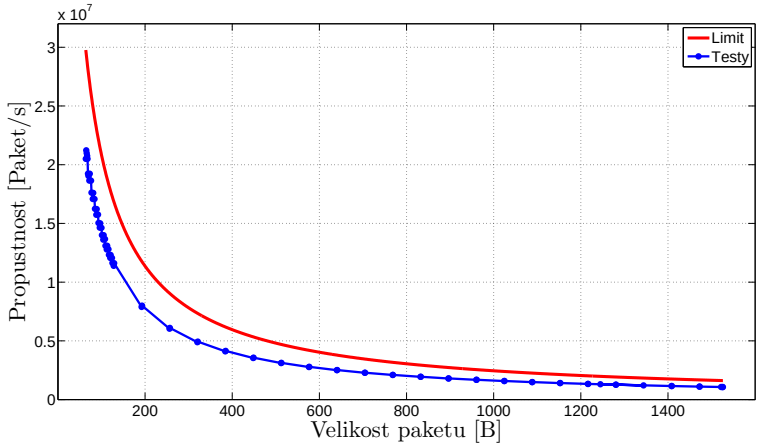
Měření propustnosti software části sondy probíhalo tak, že veškerý provoz generovaný prostředkem Spirent byl filtrem přeposlán do SW. V SW byl měřen počet přijatých paketů či bytů. Nejnižší změřená hodnota byla 6,5 Gb/s. To je více než dostatečné pro odposlech vybraných uživatelů. Lze předpokládat, že množství odposlouchávaných dat bude násobně nižší než propustnost linky.

5 Závěr

Tato technická zpráva popisuje stav vývoje vysokorychlostní sondy pro zákonné odposlechy. V rámci roku 2012 se podařilo vyrobit první verzi firmware a tu dále rozvíjet a rozšiřovat o novou funkcionalitu. Dále byl implementován software pro



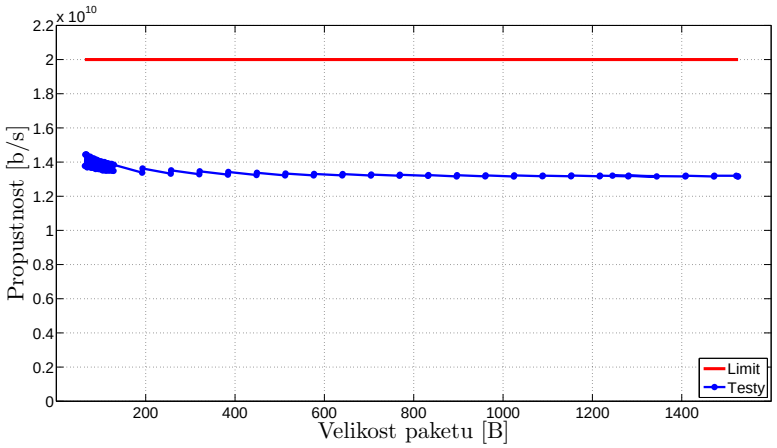
Obrázek 8. Propustnost procesní linky při zpracování jednoho maximálně vytíženého portu (měřeno v miliardách bitů za sekundu).



Obrázek 9. Propustnost procesní linky při zpracování dvou maximálně vytížených portů (měřeno v milionech paketů za sekundu).

konfiguraci a ovládání sondy, stejně tak pro odesílání dat ze sondy na mediační funkci. Tento software byl úspěšně odzkoušen proti generátoru Spirent. Dále byl úspěšně otestován ve spolupráci s mediačním zařízením vyvíjeném v rámci projektu Sec6net.

Do budoucna bude výzkum a vývoj dále směřovat ke zlepšování vlastností filtru. Primárním cílem je zvýšit množství pravidel, které je možné do filtru zapsat.



Obrázek 10. Propustnost procesní linky při zpracování dvou maximálně vytížených portů (měřeno v miliardách bitů za sekundu).

Tento cíl bude zkoumán v několika směrech. Jedním je využití paměti, která není využita v případech, kdy se IPv4 adresa zapíše na místo IPv6 adresy. Druhým směrem bude zvyšování efektivity zaplnění množství řádků použitím dalších technik. Dále se budeme zabývat novým konceptem sledování provozu tzv. Software Definded Monitoring a jeho využitím pro zákonné odposlechy.

Reference

1. CESNET; z.s.p.o.: Projekt Liberouter. 2011.
   URL `http://www.liberouter.org`
2. European Telecommunications Standards Institute: *ETSI TR 102 528: Lawful Interception (LI); Interception domain Architecture for IP networks.* 10 2006, version 1.1.1.
3. Invea-tech; a.s.: COMBO LXT a COMBO 10G2. 2011.
   URL `http://www.invea.cz/fpga-reseni/fpga-karty`
4. Martínek, T.; Košek, M.: NetCOPE: Platform for Rapid Development of Network Applications. In *Proceedings of 2008 IEEE Design and Diagnostics of Electronic Circuits and Systems Workshop*, IEEE CS, 2008, s. 219 – 224.
5. Málek, T.; Martínek, T.; Kořenek, J.: GICS: Generic Interconnection System. In *Proceedings of 2008 International Conference on Field Programmable Logic and Applications*, IEEE CS, 2008, s. 263 – 268.