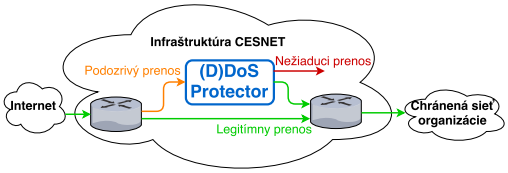
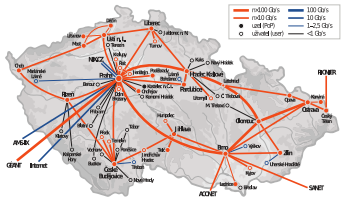
BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2017
http://excel.fit.vutbr.cz

Hardvérovo akcelerované zariadenie pre ochranu pred (D)DoS útokmi

Mário Kuka*





Abstrakt

Táto práca sa zaoberá vývojom firmvéru hardvérovej akcelerácie pre zariadenie na ochranu pred amplifikačnými (D)DoS útokmi. V dnešnej dobe sú útoky typu (D)DoS veľmi rozšírené a zapríčiňujú nemalé finančné škody. Cieľom je preto vytvoriť cenovo dostupné a ľahko nasaditeľné centralizované zariadenie na riešenie daného problému. K dosiahnutiu tohto cieľu využíva zariadenie hardvérový akcelerátor umožňujúci spracovávať vysoké dátové prenosy prostredníctvom jedného, bežne dostupného, serveru. Návrh a implementácia firmvéru je uskutočnená s ohľadom na použitie zariadenia v sieťach s rýchlosťami 100 Gbps. Celý systém prešiel funkčnou verifikáciou a v rámci laboratórneho testovania bola overená jeho reálna priepustnosť. Vytvorené zariadenie je aktuálne nasadené v sieťovej infraštruktúre CESNET a testované sieťovými administrátormi. Na základe spätnej väzby bude na vytvorenom zariadený pokračovať ďalší vývoj zameraný na rozširovanie detekcie o ďalšie typy útokov. O zariadenie aktuálne prejavili záujem aj niektorí z českých komerčných poskytovateľov sieťových služieb.

Kľúčové slová: DCPro, (D)DoS Protector, COMBO, CESNET, hardvérová akcelerácia, FPGA, vysokorýchlostné siete, 100 Gbps

Priložené materiály: *N/A*

*xkukam00@stud.fit.vutbr.cz, *Faculty of Information Technology, Brno University of Technology*

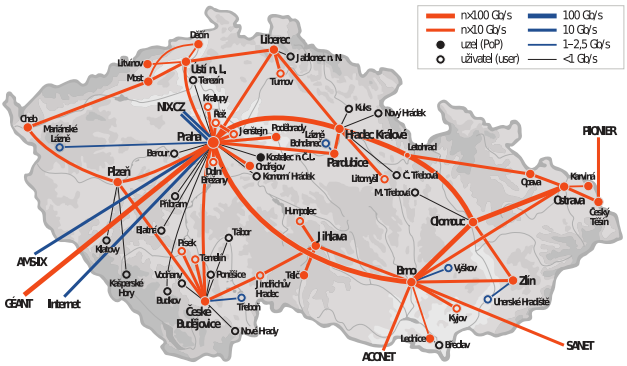
1. Úvod

Útoky typu odoprenie služby (D)DoS pracujú na princípe zahltenia určitého zdroja tak veľkým množstvom dát že nezostane žiadny čas na obsluhu legitímnych užívateľov. Tím sa zdroj z pohľadu užívateľa javí ako nedostupný a dochádza k priamym finančným škodám, prípadne poškodeniu dobrého mena prevádzkovateľa služby. Cieľom amplifikačných, reflektovaných útokov typu (D)DoS býva samotná sieťová infraštruktúra (počítačová sieť organizácie) a nie iba jedno koncové zariadenie.

Ukazovateľom takýchto útokov sú typicky obrovský počet paketov nezvyčajne veľkej dĺžky, na zraniteľných verejných službách ako je DNS alebo NTP [1, 2, 3]. Pred týmto útokom nie je možné sa brániť na koncových sieťach, pretože linky a vyhradené prenosové pásmo prostredníctvom ktorého sú koncové siete pripojené sú zahltené. Preto je potrebné tento problém riešiť už na úrovni počítačovej siete nadradenej organizácie.

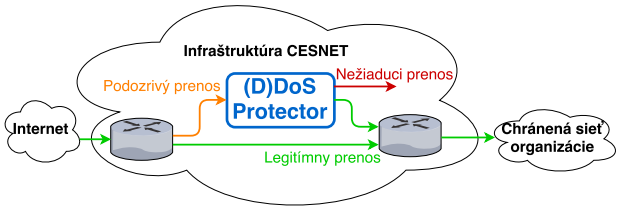
Takýmto príkladom je akademická sieť CESNET (obrázok 1), kde hlavná infraštruktúra pracuje na rýchlosti 100 Gbps a prenesie tak aj rozsiahle útoky. K tejto sieti sú pripojené organizácie, univerzity, s linkami nižších kapacít, ktoré môžu byť práve cieľom útoku. Preto je v spolupráci so združením CESNET

navrhované zariadenie, ktoré bude pripojené v hlavnej infraštruktúre, ale bude chrániť jednotlivé organizácie.



Obrázok 1. Topológia infraštruktúry CESNET [4]

Cieľom je tak vytvoriť centralizované zariadenie na ochranu pred amplifikačnými útokmi typu (D)DoS. Príklad zapojenia zariadenia je znázornený na obrázku 2. V danej infraštruktúre bude existovať iba jedno takéto zariadenie. Následne bude na toto zariadenie presmerovaná sieťová prevádzka, prostredníctvom smerovačov danej infraštruktúry, ktorú zariadenie očistí od nežiaducich dát (útoku). Takto vyčistená sieťová prevádzka bude preposlaná naspäť do sieťovej infraštruktúry a následne do chránenej siete, organizácie.



Obrázok 2. Zapojenie zariadenia

Výhodou takéhoto riešenia (z jedným zariadením, serverom) je predovšetkým jednoduchý spôsob nasadenia, administrácia a cenová dostupnosť. Vzhľadom na spôsob zapojenia zariadenia v sieťových infraštruktúrach ako je akademická sieť CESNET a taktiež s ohladom na mohutné mnostvo prenášaných dát pri amplifikačných útokoch typu (D)DoS, je nevyhnutné, aby zariadenie bolo schopné spracovávať a preposielať všetky prímané dáta (pakety) pri prenosovej rýchlosti 100 Gbps.

Cieľom tejto práce je navrhnúť a implementovať firmvér hardvérovej akcelerácie a príslušné komunikačné a riadiace rozhranie pre navrhované zariadenie.

2. Zariadenie

Pre zariadenie je použitá hardvérová akceleračná karta COMBO-100G1 [5] využívajúca technológiu FPGA, ktorá umožňuje spracovávanie sieťových prenosov na vysokorýchlostných sieťach s priepustnosťou až 100 Gbps. Akceleračná karta COMBO-100G1 (obrázok 3) bol vyvinutý v rámci spolupráce združenia CESNET a firmy Netcope Technologies.

Obrázok 3. Akcelerátor COMBO-100G1 [6]

2.1 Spôsob detekcie

Aby bolo možné vykonávať úspešnú detekciu a blokovanie nežiaduceho prenosu (útoku), je potrebné aby administrátori mohli zariadenie vhodne nakonfigurovať a presne vedeli ako sa bude zariadenie v danej situácii chovať.

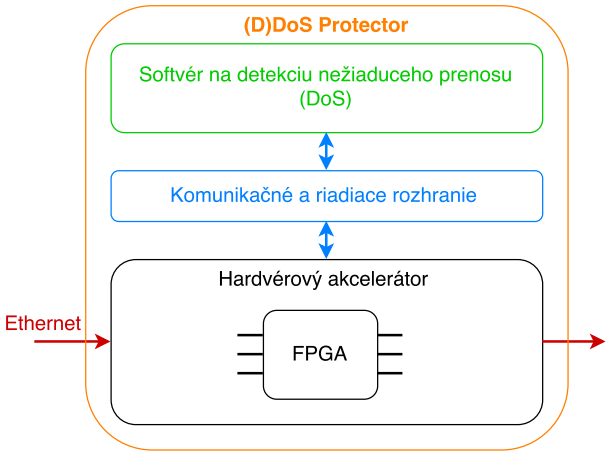
K tomuto účelu slúži možnosť špecifikácie užívateľských pravidiel. Týmito pravidlami si budú môcť administrátori chránených sietí definovať limity pre špecifikované sieťové prenosy a tým si určiť kedy bude takýto prenos (pre danú sieť) považovaný za útok. Napríklad v podobe: *UDP prenos na porte 53 s paketmi o veľkosti 1000–1200B smerované do chránenej siete s cieľovým prefixom 147.229.0.0/16 nesmie prekročiť limit 14500 pps* (pre jednoduchosť nie je uvedená presná syntax pre zápis týchto pravidiel). Po detekcií takéhoto prenosu, pre jednotlivé chránené siete, bude vykonaný patričný zásah takým spôsobom, aby sa zabránilo zahlteniu chránenej siete a legitímni prenos mohol naďalej pokračovať.

Okrem cieľového prefixu, ktorý definuje chránenú sieť, sú pravidlá tvorené ďalšími informáciami, ktoré bližšie špecifikujú daný sieťový prenos – jedná sa o rozsah portov, transportný protokol, fragmentáciu paketov, veľkosť paketov a príznaky protokolu TCP. Pravidlá ďalej obsahujú informácie o limitoch, ktoré špecifikujú maximálne povolené množstvo prenesených dát sieťového prenosu, ktoré môže byť prepustené a nebude tak vyhodnotené ako nežiaduci sieťový prenos (útok). Limity sú udávane v počte paketov a bajtov za jednotku času.

Po nakonfigurovaní týchto pravidiel prebieha kontrola a vyhodnocovanie sieťového prenosu. Pri zistený prekročenia limitu maximálneho povoleného sieťového prenosu pre niektoré zo špecifikovaných pravidiel, sú na základe zdrojovej adresy IP vybraný najväčší prispievatelia do tohto sieťového prenosu, tak aby po ich zablokovaní už nebol prekročený maximálni povolený limit pre dané pravidlo popisujúce sieťový prenos. Po výbere zdrojových IP adries, s príslušným popisom konkrétneho sieťového prenosu, sú vygenerované pravidlá pre blokovanie tohoto prenosu. Tieto pravidlá sú tvorené jednotlivými vybratými zdrojovými adresami IP a príslušným popisom (porty, protokol, príznaky TCP, fragmentácia, veľkosť) na základe ktorých budú sieťové dáta blokované.

2.2 Konceptuálny návrh zariadenia

Zariadenie je tvorené troma časťami (obrázok 4), a to softvérom na detekciu útokov a nežiaduceho prenosu (zelená časť obrázku), hardvérovým akcelerátorom COMBO-100G1, obsahujúcim vytvorený firmvér pre čip FPGA na spracovanie sieťového prenosu (čierna časť) a komunikačným (riadiacim) rozhraním určeného pre konfiguráciu hardvérového akcelerátoru a vzájomnú výmenu dát medzi softvérovou a hardvérovou častou zariadenia (modrá časť).



Obrázok 4. Zariadenie na ochranu pred (D)DoS

Hardvér poskytuje softvérovej časti zariadenia informácie o aktuálnom sieťovom prenose vo forme hlavičiek UH. Tieto hlavičky obsahujú už spracované (požadované) informácie o jednotlivých paketoch ako sú IP adresy, porty, protokol, fragmentácia, časová značka a veľkosť. Softvér sa už tak nemusí zaoberať filtrovaním a získavaním informácii z paketov sieťového prenosu.

Pravidlá pre blokovanie sieťového prenosu, špecifikované v predošlej časti, sú nahrávané do blokovacieho filtru v hardvéri, ktorý uskutočňuje samotné blokovanie sieťového prenosu. Hardvér si k týmto pravidlám ďalej uchováva štatistiky o počte zablokovaných bajtov a paketov. Softvér následne tieto štatistiky v periodických intervaloch vyčíta a kontroluje či ešte stále dochádza pri blokovaných sieťových prenosoch k prekračovaniu nastavených limitov v pravidlách (či ešte útok prebieha). V prípade zistenia že už nedochádza k tomuto prekračovaniu limitu, je pravidlo na blokovanie daného sieťového prenosu odstránené z filtru v hardvéri.

3. Hardvérová akcelerácia

Práca sa ďalej venuje návrhu a implementácii firmvéru pre akceleračnú kartu COMBO-100G1, realizujúcu potrebnú činnosť pre navrhované zariadenie. Súčasťou práce je taktiež návrh a implementácia softvérového komunikačného a riadiaceho rozhrania pre jednotlivé moduly vytvoreného firmvéru.

3.1 Požiadavky

Na základe miesta a spôsobu zapojenia zariadenia v sieťovej infraštruktúre vyplývajú na firmvér tri zásadné požiadavky.

Vysoká dátová priepustnosť. Firmvér musí byť schopný pracovať na vysokých prenosových rýchlostiach 100 Gbps. Sieťové dáta sú interne v rámci akcelerátoru prenášané po 512 bitovej zbernici. Aby bola zaručená sieťová priepustnosť 100 Gbps, aj pre najmenšie paketové veľkosti, musí implementácia firmvéru dosahovať minimálnu pracovnú frekvenciu 200 MHz.

Blokovanie nežiaduceho prenosu (útoku). Amplifikačné útoky typu (D)DoS sú charakteristické sieťovými prenosmi z veľkého počtu zdrojových adries IP. V prípade týchto (D)DoS útokov je potrebné, aby bol hardvérový filter schopný pracovať až s desaťtisícimi zdrojovými IP adresami. Súčasne je potrebné aby pridávanie a odoberanie týchto pravidiel mohlo byť realizovateľné dynamicky za chodu, bez zastavenia spracovávania sieťového prenosu.

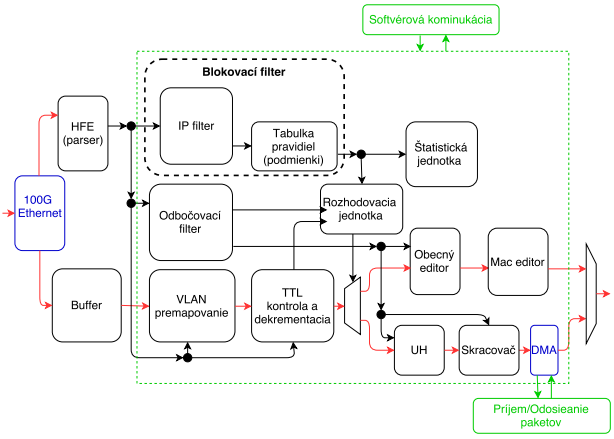
Modifikácia sieťového prenosu. Požadovaná modifikácia sieťového prenosu zahrnuje zásah do údajov slúžiacich pre samotné smerovanie vyčisteného sieťového prenosu naspäť do chránenej siete. Zariadenie preto musí poskytovať možnosť modifikácie položiek sieťových paketov ako je VLAN (Local Area Network), adresy sieťových rozhraní MAC (Media Access Control) a kontrolu (modifikáciu) položky reprezentujúcej dobu platnosti dát paketu TTL (Time To

Live). Bez týchto možností by bolo nutné pri zapojovaní zariadenia využívať výrazne náročnejšiu techniku smerovania (napríklad Policy based routing) namiesto jednoduchších prostriedkov ako je technológia VRF, prostredníctvom ktorej je možne realizovať smerovanie paketov na základe hodnôt VLAN.

3.2 Architektúra firmvéru

Za účelom dosiahnutia požadovanej dátovej priepustnosti je použitý princíp hlboko zreťazeného spracovania. Pre príjem dát zo sieťového rozhrania a preposielanie dát na sieťové rozhranie alebo do softvéru pracujúceho na zariadení, sú využívané prostriedky poskytované platformou NetCOPE [7]. NetCOPE je modulárne vývojové prostredie ktoré poskytuje infraštruktúru, sadu komponent a softvérových nástrojov, pre podporu rýchleho vývoja sieťových aplikácii na hardvérových akcelerátoroch rodiny COMBO.

Architektúra firmvéru je znázornená na obrázku 5. Firmvér je rozdelený na jednotlivé samostatné bloky (moduly) ktoré vykonávajú jednotlivé operácie. Moduly znázornené modrou farbou reprezentujú komponenty poskytované platformou NetCOPE. Moduly znázornené čiernou farbou reprezentujú navrhovanú firmvérovú časť zariadenia, realizujúcu požadovanú hardvérovú akceleráciu. Štruktúra firmvéru je rozdelená do troch hlavných častí (ciest) a to na dátovú cestu (znázornená červenou farbou), riadiacu cestu (znázornená čiernou farbou) a cestu určenú na konfiguráciu firmvéru a prenos dát prostredníctvom softvérového rozhrania (znázornená zelenou farbou).



Obrázok 5. Architektúra firmvéru

3.3 Činnosť firmvéru

Vyhodnocovanie sieťových dát začína v module HFE. Cielom je získať potrebné informácie o rámcoch z jednotlivých záhlaví protokolov, v ktorých sú zapuzdrené prenášané sieťové dáta. Informácie z HFE sú následne poskytované odbočovaciemu filtru, ktorý na základe týchto informácii a nakonfigurovaných filtračných pravidlách určí akcie. Tieto akcie budú následne vykonané nad prijatými sieťovými dátami (paketmi). Podľa vybratej akcie sa rozhoduje o tom, kam budú dáta preposlané. Pakety môžu byť preposlané na výstupné sieťové rozhranie alebo do radiču DMA, ktorý uskutoční prenos do softvérovej časti zariadenia, prípadne môžu byť pakety preposlané na oba tieto smery.

Súčasne pri vyhodnocovaní v obecnom filtri prebieha vyhodnocovanie v druhom, blokovacom filtri. Blokovací filter obsahuje blokovacie pravidlá nakonfigurované zo softvéru. Činnosť blokovacieho filtru je realizovaná dvomi samostatnými modulmi – IP filter a tabuľka špecifických podmienok.

IP filter je realizovaný (cuckoo) hash tabuľkou s podporou dynamického pridávania a odoberania pravidiel. Úlohou IP filtru je označiť primané pakety iba na základe zhody so zdrojovou IP adresou. Následne prebieha vyhodnocovanie modulom obsahujúci tabuľku so špecifickejšími podmienkami popisujúce konkrétne hľadané sieťové dáta (porty, protokol, veľkosť). Konkrétna podmienka, ktorá bude použitá na vyhodnotenie, je vybraná na základe výsledku označenia daného paketu IP filtrom. Na základe zhody alebo nezhody s vybratou podmienkou sa rozhoduje o zahodení alebo prepustený paketu k ďalšiemu spracovaniu. V prípade rozhodnutia o zahodení paketu v blokovacom filtri, sa už do úvahy neberie výsledná akcia odbočovacieho filtru a paket už neje prepustený k ďalšiemu spracovávaniu. Informácie o zahodených paketoch sa tak už neposielajú do softvérovej časti zariadenia a taktiež sa neposielajú na výstupné sieťové rozhranie.

Pakety, ktoré budú zahodené, sú následne započítvané v štatistickej jednotke, ktorá zaznamená požadované údaje v niektorom so štatistických čítačov. Vybrané akcie, na základne vyhodnotenia odbočovacieho filtru a blokovacieho filtru, sú ďalej poslané rozhodovaciemu modulu, ktorý na základe daných priorít určí výslednú akciu a vygeneruje príkazy pre jednotlivé moduly realizujúce tieto úkony.

Samotné sieťové dáta sú po dobu počas ktorej bude vyhodnotené ich spracovanie uložené vo vyrovnávacej pamäti typu FIFO (Buffer). Z tejto pamäte sa dáta dostavajú do jednotky ktorá slúži na výmenu položiek VLAN podľa zvolenej konfigurácie. Následne sú dáta preposlané na spracovanie do modulu pre kontrolu TTL. V tejto jednotke dochádza ku samotnej kontrole položky TTL a prípadnému prepočtu novej hodnoty. Pri nesplnení požadovanej podmienky pre hodnotu TTL, je vygenerovaná akcia požadujúca zahodenie daného paketu, ktorá je ďalej spracovaná v rozhodova-

com module.

Dáta pokračujú na spracovanie do preposielacieho modulu, ktorý na základe určených príkazov z rozhodovacieho modulu, vykoná zahodenie alebo preposlanie dát na výstupné sieťové rozhranie alebo do operačnej pamäte pomocou DMA. Pri preposlaní na sieťové rozhranie dáta prechádzajú ďalším spracovaním v obecnom editore. Obecný editor na základe svojej konfigurácie vykoná vloženie alebo modifikáciu štvôr bajtového bloku na požadovanom mieste v pakete. Následne sú dáta ďalej spracovávané v editore MAC adries. Tu dochádza k nahradeniu zdrojovej a cieľovej MAC adresy alebo ich vzájomnej výmene. Následne sú pakety predané výstupnému sieťovému rozhraniu platformy NetCOPE a poslané na príslušné sieťové rozhranie.

Pri preposlaní dát do operačnej pamäte sú následne dáta spracovávané v generátore hlavičiek UH. Na základe zvolenej konfigurácie sú ďalej posielané buďto samotné sieťové dáta (pakety) alebo vygenerované hlavičky UH, ktoré obsahujú spracované požadované informácie. Nasleduje spracovanie v skracovacom module, ktorý v prípade preposielania celých paketov do operačnej pamäte, vykoná skrátenie paketu na požadovanú maximálnu veľkosť. Pakety alebo hlavičky UH sú ďalej poslané na rozhranie radiču DMA, ktorý vykoná vlastný prenos dát do operačnej pamäte.

4. Dosiahnuté výsledky

Jednotlivé moduly firmvéru som implementoval podľa návrhu s dôrazom na definované požiadavky. Následne som uskutočnil integráciu firmvéru so softvérovou časťou zariadenia.

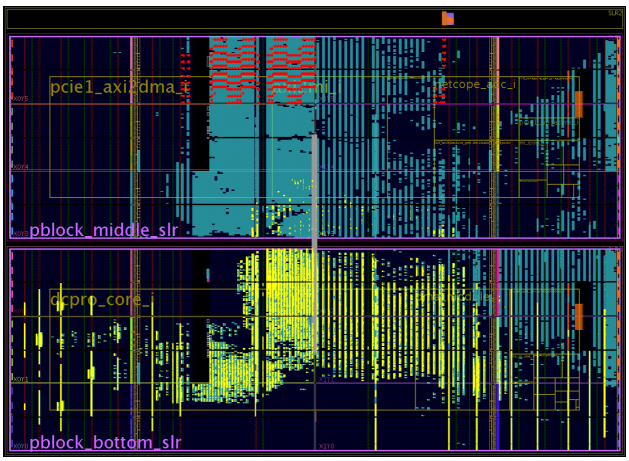
Pri implementácii firmvéru sú využívané základné generické komponenty poskytované platformou NetCOPE ako sú pamäte FIFO, multiplexory a aritmetické jednotky ALU. Platforma zároveň rieši spracovanie dát (paketov) na úrovni vrstiev PCS/PMA. Platforma taktiež zaisťuje prenos sieťových dát do operačnej pamäte prostredníctvom prenosov DMA.

Vzhľadom na použité nízkoúrovňové programovanie (jazyk VHDL) jednotlivých modulov, tvoriace celý firmvér, som vytvoril aj jednotlivé verifikačné prostredia (prostredníctvom SystemVerilog) pre komplexné overenie funkcionality modulov. K príslušným modulom som dalej vytvoril softvérové rozhranie (v jazyku C) umožňujúce komunikáciu a riadenie daného modulu. Po vytvorený celého firmvérového jadra, pomocou vytvorených modulov, bola následne realizovaná finálna verifikácia funkcionality a komunikácie medzi jednotlivými modulmi v celom firmvéri.

K dosiahnutiu čo najmenšieho množstva spotrebovaných zdrojov čipu FPGA, za účelom získať čo neväčšiu možnú pracovnú frekvenciu kvôli dátovej priepustnosti, som uskutočnil ručné optimalizácie zapojenia logických obvodov na úrovni primitív nachádzajúcich sa na čipe FPGA. Výsledok procesu syntézy je znázornený v tabuľke 1, kde je vidieť, že výsledná implementácia je veľmi efektívna a zaberá necelú polovicu čipu FPGA. Samotné jadro firmvéru pritom zaberá iba zlomok zdrojov. Výsledná implementácia na čipe FPGA je taktiež znázornená na obrázku 6, kde žltá časť reprezentuje vytvorené (naimplementované) jadro firmvéru a ostatné časti (modrá časť obrázku) reprezentujú použitú platformu NetCOPE.

Tabuľka 1. Využité zdroje čipu FPGA

Zdroje	Celkovo	Jadro firmvéru
LUT	107 168 (29%)	22 798 (6%)
LUTRAM	17 060 (12%)	11 680 (8%)
REG FF	106 840 (14%)	39 089 (5%)
BRAM	415 (44%)	289 (30%)
DSP	121 (8%)	36 (2%)



Obrázok 6. Zaplnenie čipu FPGA

Pri implementácii firmvéru pre FPGA sa podarilo za pomoci vykonaných optimalizácií dosiahnuť vysokej taktovacej frekvencie cez 200 MHz, čo umožňuje bezproblémové spracovávanie sieťových dát pri rýchlostiach 100 Gbps aj pre najmenšie paketové veľkosti.

Celé zariadenie prebehlo rozsiahlym laboratórnym testovaním čím bola overená funkcionalita a dosiahnutá reálna datová priepustnosť 100 Gbps. V súčasnej dobe je zariadenie nasadené v testovacej prevádzke v akademickej sieti CESNET. Cez nasadené zariadenie je aktuálne presmerovaná živá sieťová prevádzka libereckej univerzity prostredníctvom ktorej sieťový administrátori CESNET, v rámci testovania na reálnej sieti, realizujú vlastné testovanie detekcie nežiaducich sieťových prenosov ((D)DoS útokov)

a overujú činnosť samotného zariadenia. Na základe spätnej väzby bude na vytvorenom zariadený pokračovať ďalší vývoj zameraný na rozširovanie detekcie o ďalšie typy útokov s cieľom dosiahnuť čo najideálnejšie chovanie a vlastnosti zariadenia pre plné nasadenie.

5. Záver

Cieľom práce bolo realizovať hardvérovú akceleráciu na spracovanie sieťových dát pre zariadenie určeného na ochranu pred (D)DoS útokmi. Realizácia spočívala v návrhu a implementácii firmvéru na FPGA pre hardvérovú akceleračnú kartu COMBO-100G1, v integrácií firmvéru so softvérom uskutočňujúci detekciu nežiaduceho prenosu ((D)DoS) a otestovaní celého zariadenia v laboratórnych podmienkach.

Výsledkom práce je funkčné zariadenie s možnosťou centralizovaného nasadenia, umožňujúce vykonávať detekciu podľa nastavenej konfigurácie pri prenosových rýchlostiach 100 Gbps. Zariadenie je aktuálne nasadené na hlavnej linke akademickej siete CESNET a testované sieťovými administrátormi.

O zariadenie prejavili záujem aj niektoré z komerčných českých firiem zaoberajúce sa poskytovaním sieťových a internetových služieb, s korými aktuálne združenie CESNET diskutuje a jedná o spôsobe testovacieho a následné plného nasadenia zariadenia do ich sieťových infraštruktúr.

Ďalší vývoj hardvéru a celého zariadenia bude pokračovať vylepšovaním a rozširovaním funkcionality na základe spätnej odozvy z testovacieho nasadenia v reálnych podmienkach.

6. Poďakovanie

Táto práca vznikla v spolupráci so združením CESNET v rámci riešenia projektu Technológie pre ochranu vysokorýchlostných sietí (DCPro) pod označením TH01010229 podporeného Technologickou agenturou Českej republiky [8].

Literatúra

[1] Jelena Mirkovic. *Internet denial of service : attack and defense mechanisms*. Prentice Hall Professional Technical Reference, Upper Saddle River, N.J, 2005. ISBN: 01-3147-573-8.

[2] Stuart McClure. *Hacking bez tajemství. 3. aktualiz. vyd*. Computer Press, 2003. ISBN: 80-7226-948-8.

[3] Matthew Prince. Deep inside a DNS amplification DDoS attack. CloudfFlare – The web performance & security company. https://blog.cloudflare.com/.

[4] Jan Kolouch. Kibernetycké útoky. CESNET, zájmové sdružení právnických osob. https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf.

[5] CESNET / Designing a Card for 100 Gbps Network Monitoring. https://www.cesnet.cz/wp-content/uploads/2014/02/card.pdf.

[6] Liberouter / CESNET TMC group. https://www.liberouter.org/.

[7] M. Kosek T. Martinek. *NetCOPE: Platform for Rapid Development of Network Applications. Proceedings of the 11th IEEE Workshop on Design and Diagnostics of Electronic Circuits and Systems*. DDECS 2008. Bratislava, SK, 2008. ISBN: 978-1-4244-2277-7.

[8] Technologická agentura České republiky. https://vavai.tacr.cz/.