Optimalizace řízení a bezpečnosti síťových toků pomocí softwarově definovaných sítí

Technická zpráva FIT VUT v Brně

Barbora Franková, Martin Holkovič, Libor Polčák

Technická zpráva č. FIT-TR-2015-02
Fakulta informačních technologií, Vysoké učení technické v Brně

Last modified: 15. září 2015

Optimalizace řízení a bezpečnosti síťových toků pomocí softwarově definovaných sítí

Barbora Franková, Martin Holkovič, Libor Polčák

Vysoké učení technické v Brně, email:
{ifrankova,iholkovic,ipolcak}@fit.vutbr.cz

Abstrakt Cílem této souhrnné technické zprávy je představení využití možností spojených s detekcí identity v softwarově definovaných sítích (SDN). Zpráva se zaměřuje na zákonné odposlechy v SDN a na řízení toků podle identity uživatelů, nasaditelné například ve firemních sítích. V práci je popsána činnost softwarových nástrojů vytvořených pro SDN, včetně jejich testování.

1 Úvod

Počítačové sítě propojují koncové stanice pomocí prostředníků, tedy prvků, které jsou určeny pro zpracování a přenos síťových dat od zdroje dat k jejich cíli. Mezi tyto prostředníky řadíme především přepínače (určené pro předávání dat v lokální síti) a směrovače (umožňující propojení několika různých síťových domén včetně propojení sítí založených na různých technologiích). Postupem času však v sítích narostl význam i dalších prostředníků jako jsou firewally (prvky nasazované většinou na hranicích sítě, které omezují provoz a odfiltrovávají nechtěné pokusy o přenos dat, např. útoky), systémy IDS/IPS (zkoumající přenášená data a hledající vzory odpovídající možným útokům), antivirové a antispamové vyhledávače a další. V neposlední řadě jsou do sítí nasazovány i systémy pro monitorování provozu v síti, pro získávání dat potřebných pro uchování, předávání a likvidaci provozních a lokalizačních údajů (v ČR podle vyhlášky 357/2012 Sb.) a pro systémy pro zákonné odposlechy (v ČR podle Zákona o elektronických komunikacích 127/2005 Sb. ve znění pozdějších předpisů).

V poslední době narůstá počet aplikací, které koncový uživatelé sítí využívají a potřebují pro práci, či zábavu. Požadavky těchto aplikací se však různí. Přenos objemných souborů a obrázků vyžaduje velkou šířku pásma, ale zpoždění v řádech zlomků sekundy a někdy i více nejsou podstatná. Telefonní hovory skrze počítačovou síť vyžadují nízkou a stabilní odezvu, i když nároky na přenosovou rychlost nejsou příliš vysoké. V některých situacích může být žádoucí zvyšovat prioritu určitým aplikacím [4], či konkrétním uživatelům [29]. Tyto požadavky přinášejí nové výzvy pro architekturu a principy počítačových sítí.

Přepínače, směrovače a další prostředníci byly historicky svázané s konkrétními firmware a dalším softwarem dodávaným konkrétním výrobcem zařízení. Inovace a přidávání dalších vlastností byla závislá [22] na nových verzích softwaru

poskytovaného výrobcem a uzpůsobení činnosti zařízení potřebám konkrétních sítí bylo složité.

Softwarově řízené sítě (Software Defined Networks – SDN) je nové paradigma [22] zvyšující možnost inovace [19] v počítačových sítích. Sítě SDN jsou postaveny na oddělení řídící a datové vrstvy na jednotlivých síťových prvcích. Zatímco datová vrstva zajišťující zpracování a předávání dat musí fungovat rychle a být proto přítomna na konkrétním síťovém prvku, řízení daného prvku může být přesunuto, či centralizováno do speciálních zařízení (často označovaných jako kontrolery) programovatelných správcem sítě. SDN dává správci sítě možnost definovat pravidla pomocí vlastních aplikací ovlivňujících chování sítě a zpracování jednotlivých datových toků.

Tato technická zpráva se zabývá sítěmi SDN se zaměřením na řízení toků pro optimalizaci jejich zpracování a pro zajištění bezpečnosti sítě. Myšlenky prezentované v této technické zprávě vycházejí z diplomových prací *Zákonné odposlechy v SDN* [14] a *SDN řízené pomocí identity uživatelů* [17]. Technická zpráva ukazuje jak je možné zajistit přeposílání určitých toků skrze konkrétní monitorovací stanoviště, např. pro účely monitorování, IDS/IPS a zákonných odposlechů. Druhá část zprávy se věnuje optimalizaci řízení sítě podle konkrétních uživatelů se zaměřením na bezpečnost.

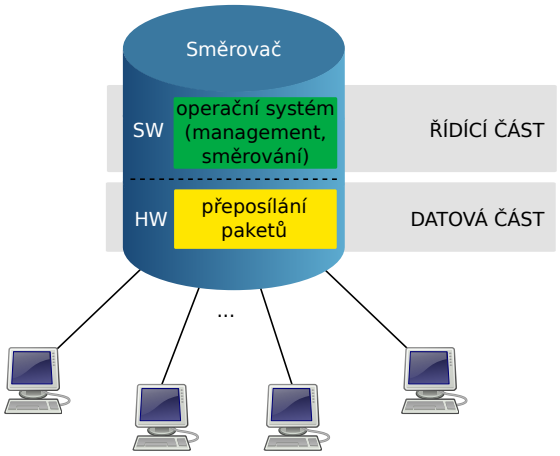
Sekce 2 se zabývá detailnějších představením SDN a uvedením základních pojmů. Sekce 3 se zabývá identitou uživatelů a představuje softwarové nástroje již dříve vytvořené v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*. Výhody řízení sítě na základě znalosti identit uživatelů jsou představeny v sekci 4. Sekce 5 se zabývá zákonnými odposlechy v prostředí sítí SDN. Sekce 6 se zabývá rozšířením SDN zaměřeným na řízení provozu podle znalosti identity uživatele. Sekce 7 uzavírá tuto technickou zprávu.

2 Softwarově definované sítě

Cílem této sekce je vysvětlit pojem softwarově definované sítě. V podsekci 2.1 je popsána obecná architektura síťových zařízení. Sekce 2.2 vysvětluje princip softwarově definovaných sítí (SDN), sekce 2.3 je věnována protokolu OpenFlow a sekce 2.4 představuje použité OpenFlow kontrolery.

2.1 Architektura síťových zařízení

Klasické síťové zařízení, jak je znázorněno na obrázku 1, obsahuje vlastní hardware pro přeposílání paketů (*datová část, data plane*) a operační systém v software pro management a logiku (*řídící část, control plane*). Součástí operačního systému mohou být moduly, u managmentu jde například o podporu protokolu SNMP nebo konfigurace pomocí příkazové řádky, logika ze strany uživatele je dána moduly podporujícími směrovací protokoly, přepínání nebo QoS. Všechna tato zařízení ale mají pevně danou funkcionalitu od výrobce, složitý operační systém a jsou uzavřená k inovacím.



Obrázek 1: Architektura klasického síťového zařízení.

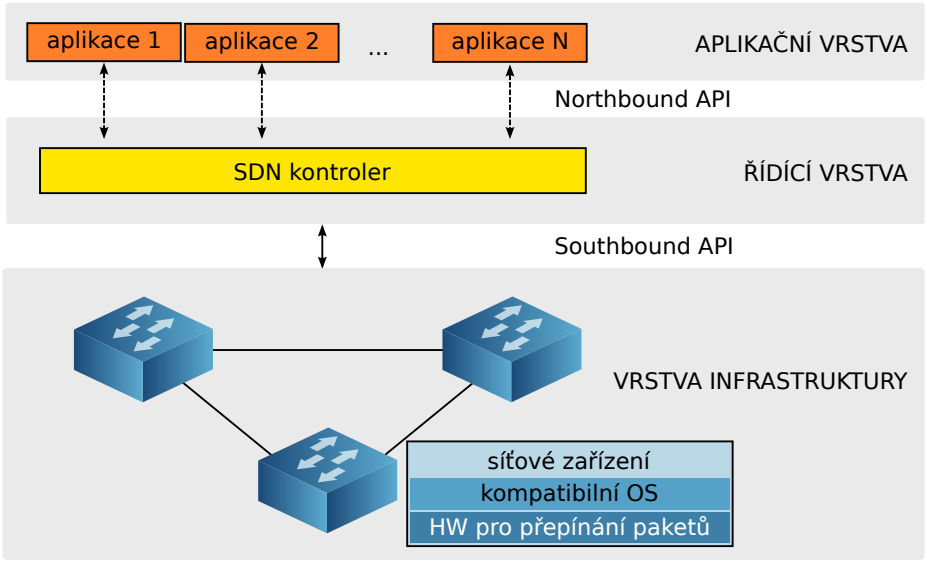
Řídící část (Control Plane) Funkce řídící části zahrnují konfiguraci systému, vysokoúrovňový management a statistiky. Ve směrovačích slouží ke správě směrovací tabulky (Routing Information Base – RIB) a přepínací tabulky (Forwarding Information Base – FIB). Informace ve směrovací tabulce se aktualizují pomocí směrovacích protokolů, jako je např. RIP, OSPF nebo BGP [32]. Vzhledem k tomu, že funkce v řídící části se typicky neprovádí nad každým paketem, nejsou obvykle limitovány časem a proto mohou být implementovány v software [3].

Datová část (Data Plane) Funkce datové části provádí menší množství operací a týkají se především přijímání, zpracování a přepínaní paketů. Ve chvíli, kdy je paket přijat na vstupním rozhraní se sníží time-to-live (TTL) a vyhledá se cílová adresa na základě informací ze směrovací tabulky. Na základě zdrojové a cílové IP adresy, čísla portu transportní vrstvy a typu protokolu se paket klasifikuje a zahodí (např. firewall) nebo odešle na výstupní rozhraní. Před odesláním paketu se přepočítá se kontrolní součet hlavičky [32]. Funkce datové části se provádí nad každým paketem, což vyžaduje vysokou výkonnost v reálném čase a implementaci v hardware [3].

2.2 Princip softwarově definovaných sítí

Softwarově definované sítě (Software Defined Networking – SDN) oddělují rozhodovací logiku a rychlé přepínání paketů v hardware. Zatímco vrstva infrastruktury zůstává na síťovém zařízení, řídící vrstva a vyšší logika se přesouvá do tzv. kontroleru. Kontroler je oddělené zařízení, které má přehled o topologii celé sítě a o prostředcích k přepínání paketů, které fyzicky umožňují jednotlivá síťová zařízení. S využitím těchto informací je kontroler schopný určit cesty pro toky v síti a podle toho posílat pokyny jednotlivým síťovým zařízením.

Architektura softwarově definovaných sítí se tedy skládá z vrstvy infrastruktury, což je datová část původní architektury a řídící vrstvy, ve které je oddělená kontrolní část ve formě kontroleru. Nad řídící vrstvou lze vytvářet různé aplikace, které tvoří aplikační vrstvu. Jednotlivé vrstvy jsou propojeny programovacím rozhraním, tzv. *northbound* a *southbound* API. Architektura SDN je znázorněna na obrázku 2.



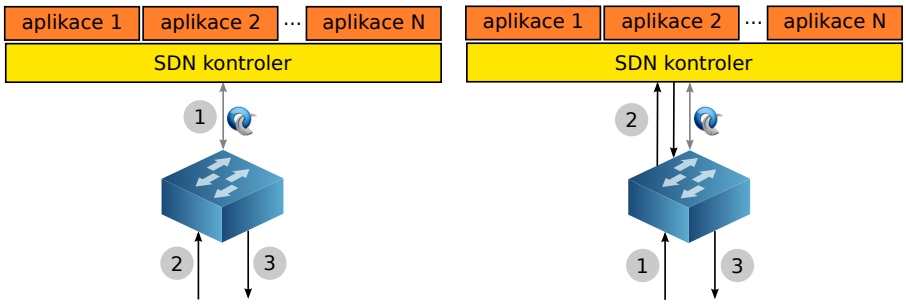
Obrázek 2: Architektura softwarově definovaných sítí.

Síťové zařízení V SDN je síťové zařízení abstrahováno od specifické činnosti jako je přepínání, směrování, filtrování nebo vyvažování zátěže. SDN přepínač obsahuje rychlý hardware pro přeposílání paketů a velmi jednoduchý operační systém, který sám o sobě musí umět pouze komunikovat s kontrolerem a rychle konfigurovat přeposílaní paketů mezi porty na základě na základě pokynů od kontroleru [21]. Je možné nastavit zařízení tak, aby samostatně odpovídalo na některé události, např. výpadky sítě nebo podpůrné funkce poskytované LLDP, STP nebo ICMP [2]. Funkcionalita samotného přepínače je tedy omezena pouze na datovou část, která přeposílá pakety na základě příkazů kontroleru [24].

Konfigurace síťového zařízení se dělí na proaktivní a reaktivní podle způsobu nahrávání pravidel. Rozdíl v těchto přístupech je znázorněn na obrázku 3. Proaktivní přístup je založen na předvyplnění tabulky před samotným přijmem paketů. Výhodou je nulové zpoždění pro nové toky, protože pravidlo je v přepínači už definováno. Zároveň přerušení spojení s kontrolerem neovlivní samotný proces přeposílání paketů. Nevýhodou pak může být nutnost přesně

definovat všechna pravidla, což vyžaduje například agregaci (wildcard) tak, aby byly pokryty všechny cesty [15].

U reaktivního přístupu je paket, který nemá záznam v tabulce toků, odeslán kontroleru. Kontroler na základě informací z paketu vytvoří nové pravidlo pro OpenFlow přepínače v síti. Tento přístup má výhodu v lepším řízením, ale pro každý nový tok znamená určité počáteční zpoždění. V případě, že dojde k přerušení spojení kontroleru a přepínače, pakety neznámých toků budou zahozeny.



Obrázek 3: Znázornění pořadí kroků u (a) proaktivního a (b) reaktivního vkládání pravidel do tabulky toků. U proaktivního přístupu je nejdříve vyplněna tabulka toků (1). Každý přijatý paket (2) se pak zahodí nebo přepošle (3) podle pravidel v tabulce. Reaktivní přístup musí nejdříve přijmout paket (1), který odešle kontroleru (2). Kontroler na základě tohoto paketu vytvoří záznam v tabulce toků, podle které se paket a všechny následující ve stejném toku zahodí nebo odešlou (3).

SDN kontroler SDN kontroler je software, který provádí kontrolu nad množinou zdrojů jednotlivých datových částí síťových zařízení. V síti může být nasazeno větší počet kontrolerů na několika fyzických zařízeních. Všechny části si udržují synchronizovaný a konzistentní pohled na topologii a stav sítě. Funkcionalita kontroleru obsahuje [26]:

- správu stavu sítě (informace o síťových uzlech a koncových zařízeních, konfigurace, statistiky apod.) a jeho případnou distribuci ostatním kontrolerům;
- vysokoúrovňový model pro zachycení vztahů mezi spravovanými zdroji, pravidly a dalšími poskytovanými službami;
- programové rozhraní, které umožní rozšířit funkcionalitu kontroleru z externí aplikace;
- správu toků;
- zjišťování topologie, směrování (algoritmy pro výpočet cesty).

Komunikační kanál Komunikační kanál je rozhraní, které propojuje síťové zařízení s kontrolerem. Přes komunikační kanál kontroler konfiguruje síťová za-

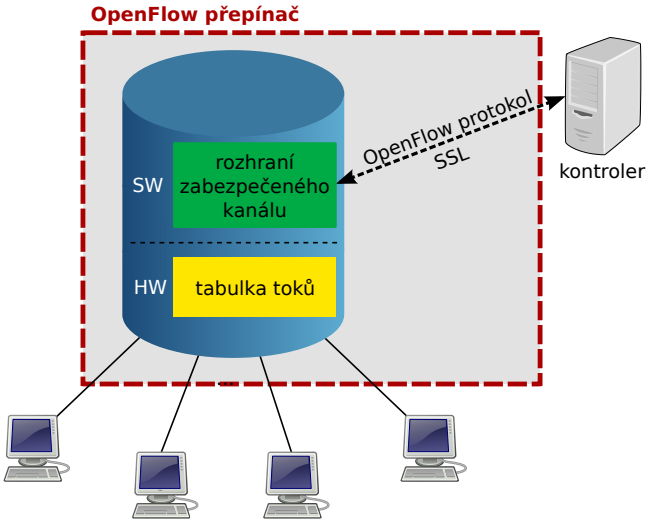
řízení, zjišťuje stav zařízení a statistiky z tabulka toků a přijímá nebo zasílá pakety.

Programové rozhraní V rámci SDN se využívají Southbound a Northbound API. Southbound API je nízkoúrovňové programovací rozhraní, které obvykle obsahuje nezbytnou funkcionalitu na programování parametrů poskytovaných operačním systémem síťových zařízení. Typickým příkladem je OpenFlow, I2RS, NETCONF nebo OnePK.

Northbound API je programovací rozhraní mezi aplikacemi a kontrolerem, které zapouzdřuje nízkou úroveň instrukcí southbound API a zjednodušuje programování složitějších síťových funkcí. S využitím Northbound API je možné implemetovat funkce jako výpočet cesty, STP, směrování, hloubková inspekce paketů a další [26]. V současné chvíli toto rozhraní není standardizováno [16].

2.3 OpenFlow

OpenFlow je první standard pro komunikační rozhraní mezi řídící vrstvou a síťovými zařízeními. Nejedná se o produkt nebo určitou vlastnost, ale o množinu protokolů, programové rozhraní a jeden z možných modelů softwarově definovaných sítí. Architektura OpenFlow je znáznorněna na obrázku 4. Skládá se z OpenFlow kontroleru (controller), OpenFlow přepínače (switch) a OpenFlow protokolu [22,27].



Obrázek 4: Architektura OpenFlow.

OpenFlow přepínač využívá koncept datových toků k identifikaci síťového provozu na základě pravidel, která jsou staticky nebo dynamicky naprogramo-

vána z centrálního kontroleru [27]. OpenFlow přepínač se skládá minimálně z následujících položek:

- Rozhraní zabezpečeného kanálu, které propojuje přepínač s kontrolerem, umožňuje posílání příkazů i paketů a obecně odpovídá definici southbound rozhraní.
- Tabulka toků, která obsahuje množinu záznamů o datových tocích. Každý záznam se skládá z priority, pole hlaviček, počítadla a množiny pravidel.
  - *Pole hlaviček (Header Fields)* se využívá k porovnání příchozích paketů a existujících záznamů v tabulce toků. V OpenFlow v1.0 je tok specifikován jako 12-tice, která se skládá ze vstupního portu, VLAN ID, VLAN priority, zdrojové a cílové MAC adresy, typu ethernetového rámce, zdrojové a cílové IP adresy, protokolu IP, IP ToS a zdrojového a cílového TCP/UDP portu. Každá z těchto položek může být nahrazena zástupným znakem (wildcard), což umožňuje agregaci toků.
  - *Počítadla (Counters)* aktualizují se s každým přijatým paketem, pro který byl nalezen záznam v tabulce toků a počítají se pro danou tabulku toků, tok, port a frontu.
  - *Množina instrukcí (Instructions)* určuje, jak bude přepínač zacházet s pakety, pro které byl nalezen záznam v tabulce toků. V OpenFlow protokolu verze 1.0 jsou definovány povinné akce (přeposlat a zahodit paket) a nepovinné akce (upravit paket). Při přeposlání paketu je nutné specifikovat fyzický, virtuální nebo některý z rezervovaných portů.
    OpenFlow v1.3 umožňuje využití více tabulek toků a rozšiřuje množinu instrukcí o položku skoč do tabulky X (*go-to table X*). Tabulky se prochází sekvenčně až do chvíle, kdy v seznamu instrukcí není další příkaz skoč do tabulky. Při průchodu tabulkami je možné paket modifikovat. Změnit lze jakoukoliv položku v paketu, která se dá porovnávat v rámci pravidel. Je také možné zvýšit nebo snížit TTL, případně vložit nebo odstranit tag (VLAN, MPLS, PBB).
    V každé tabulce se mohou zadané akce provést okamžitě, pokud se vloží do množiny akcí *apply-actions*. V případě, že se vloží do množiny *write-actions*, provedou se až po průchodu paketu poslední tabulkou.
- OpenFlow protokol, který je naimplementován na straně kontroleru i přepínače a používá se pro komunikaci přes zabezpečený kanál [22].

Všechny přijaté pakety se v přepínači porovnají s tabulkou toků. Pravidla se prochádzí sekvenčne podle priority. Pokud je v tabulce nalezen záznam, přepínač provede všechny akce, které jsou pro daný tok specifikovány.Pokud pro paket nebyla nalezena shoda, je přeposlán přes zabezpečený kanál do kontroleru. Kontroler pak pomocí přidávání, upravování a odstraňování záznamů v tabulce toků rozhoduje, jak se budou takové pakety zpracovávat [22].

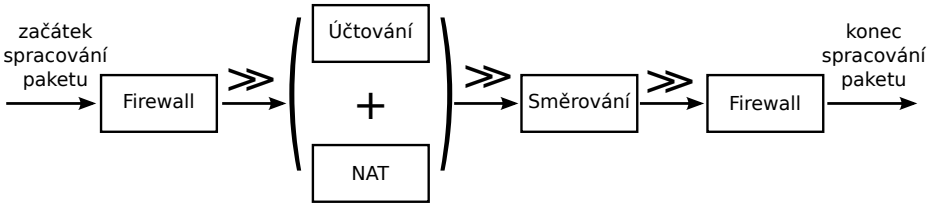
2.4 Použité kontrolery

V rámci výzkumu byly použity kontrolery OpenDaylight [23] a Pyretic [25]. OpenDaylight je open source projekt vyvíjený organizací Linux Foundation,

který má podporu i v komerční sféře (Big Switch Networks, Cisco, HP a další). Modulární struktura kontroleru umožňuje naprogramování libovolného modulu a jeho následné zapojení. Kontroler pracuje s protokolem OpenFlow v1.0 až v1.3 [23] a aplikacím poskytuje Northbound rozhraní pro Java a REST API. Z hlediska této práce je kontroler OpenDaylight významný tím, že umožnuje pracovat s více tabulkami toků.

Druhým použitým kontrolerem je Pyretic, který je rozšířením kontroleru POX [20]. Hlavním cílem tohoto kontroleru je zjednodušení vytváření komplexních aplikací pro řízení sítě pomocí tzv. síťových politik. Síťová politika je výstupem každé aplikace, která je prostřednictvím proprietárního Northbound rozhraní přenesena do kontroleru a na základě definovaných operátorů zkombinována s ostatními politikami. Tento princip umožňuje velmi jednoduchou tvorbu rozsáhlých síťových aplikací pomocí spojování univerzálních malých modulů.

Obrázek 5 znázorňuje příklad vytvoření komplexní aplikace pomocí politik Pyreticu. Výsledná aplikace je přeložena do OpenFlow pravidel a následně Southbound rozhraní nahrána na síťová zařízení. Každý obdélník na obrázku znázorňuje jednu politiku, která je výstupem z aplikace napsané bez ohledu na aktuální síťovou topologii a bez ohledu na jiné použité aplikace. Všechny aplikace je tak možné vzít a použít v libovolné síti a v libovolném kontexu, což výrazně zvyšuje znovupoužitelnost vytvořených aplikací.



Obrázek 5: Příklad skládání síťových politik kontrolerem Pyretic.

Síťové politiky jsou kombinovány pomocí paralerního a sekvenčního operátoru. Sekveční operátor (») vezme dvě libovolné politiky a zkombinuje je tak, že vytvoří jednou velkou politiku. Aplikováním vytvořené politiky se vytvoří dojem, že byly vykonány dvě původní politiky sekvenčně. Uvažujme například politiku *NAT*, překládající všechny pakety s cílovou IP adresou *147.229.176.19* na IP adresu *192.168.1.1*, a politiku *Směrování*, která všechny pakety pro IP adresu *192.168.1.1* odesílá na rozhraní *2*. Když obě politiky spojíme sekvenčním operátorem do podoby *NAT » Směrování*, vznikne nám politika, která všem paketům s cílovou adresou *147.229.176.19* přepíše cílovou adresu na *192.168.1.1* a odešle na rozhraní *2*.

Paralerní operátor (+) vytváří zkombinováním dvou politik dojem jejich současného vykonání. Příkladem je zkombinování politiky *Účtování* s politikou *NAT*. Politika *Účtování* slouží na měření odeslaných dat jednotlivými koncovými

stanicemi v síti. Politika *NAT* přepisuje všem paketům přijatých na rozhraní *1* zdrojovou IP adresu na adresu *147.229.176.14*. Zkombinováním politik paralelním operátorem (+) vznikne politika *NAT + Účtování*, která započte přenesená data podle zdrojové IP adresy a přepíše zdrojovou IP adresu na hodnotu *147.229.176.14*.

Jednotlivé síťové politiky jsou hierarchicky tvořeny pomocí jednodušších politik až po základní prvky. Základními prvky jsou *filtrovací pravidla* (match), *modifikační pravidla* (modify) a *pravidla pro zpracování paketu kontrolerem* (counts, packets). Filtrovací pravidlo je podmínka, kterou musí zpracovávaný paket splnit, aby byl zpracován modifikačním pravidlem nebo odeslán do kontroleru. Filtrovací i modifikační pravidla se skládají z pole hlaviček definovaných v protokolu OpenFlow, identifikátoru přepínače, vstupního port a výstupního port. Odeslání paketu se provede upravením výchozího portu. Speciálním případem odeslání paketu je zahození. Příkladem může být filtrovací pravidlo *match(přepínač: 1, cílová IP: 192.168.1.0/24)*, za kterým následuje modifikační pravidlo *modify(odeslat na port: 3)*.

V případě, že je na přijatý paket aplikováno pravidlo pro zpracování paketu kontrolerem, mohou nastat dvě možnosti:

- První možností je odeslání paketu do kontroleru, kde může proběhnout detailnější analýza paketu.
- Druhou možností zpracování paketu je pouze měření statistik kontrolerem. Pro statistiky jsou použita počítadla, která se nacházejí v každém OpenFlow pravidle. Zpracovávaný paket tak vůbec není odeslán do kontroleru a je přeposlán na některý fyzický port nebo zahozen. Kontroler sbírá statistiky pravidelným zjišťováním hodnot počítadel.

Poslední důležitou vlastností Pyreticu je možnost použití virtuálních hlaviček. Virtuální hlavičky mohou mít libovolný název a hodnotu. Názvy a hodnoty všech virtuálních hlaviček jsou zakódovány a uloženy do reálných hlaviček. Aktuální verze Pyreticu zakódovává virtuální hlavičky do hlaviček VLAN ID a VLAN priority. Příkladem využití virtuálních hlaviček je označování paketů podle přepínače, kterým byly do sítě přijaty. Paket přijatý na přepínači s ID *100* tak bude obsahovat virtuální hlavičku *Poloha* s hodnotou *100*. Všechny přepínače v síti tak budou bez nutnosti složité analýzy paketu vědet, na kterém přepínači byl paket přijat. Podle toho je možné vytvářet filtrovací a modifikační pravidla.

3 Identita uživatele

Detekce identity uživatele je založena na analýze identifikátorů, které jsou schopny identifikovat uživatele v rámci určitého kontextu. Analýzou jsou zjištěny správné hodnoty identifikátorů, začátek a konec doby, kdy jsou používany uživatelem nebo zařízením, a vztahy mezi nimi. V počítačových sítích jsou identifikátory využívány síťovými protokoly (např. IP adresa, MAC adresa) a aplikacemi (např. e-mailová adresa nebo SIP URI).

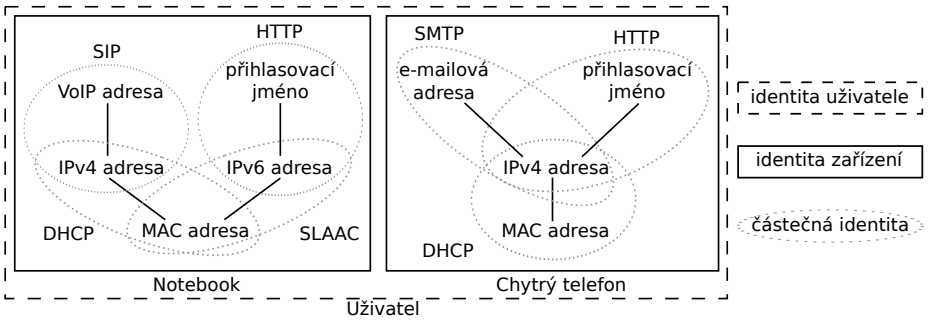
Obsahem této kapitoly je definice pojmů souvisejících s identitou uživatelů, popis detekce a spojování částečných identit, a představení nástroje Sec6Net Identity Management System ze systému Sec6Net Lawful Interception System.

3.1 Základní pojmy

Identita Podle terminologie o soukromí definované Pfitzmannem a Hansenem [28] je identita *množina hodnot atributů, které odlišují jeden subjekt od všech jiných subjektů.* Identita subjektu se skládá z mnoha částečných identit. Každá částečná identita je složena z množiny hodnot atributů a reprezentuje subjekt ve vymezeném kontextu nebo roli. Subjekt může být chápán jako lidská bytost, právnická osoba nebo zařízení. V rámci této technické zprávy se předpokládá, že v jednom čase je zařízení součástí identity pouze jedné osoby (osoba, která užívá dané zařízení, se nazývá uživatel).

Identita osoby může být vyjádřena pomocí identit zařízení, které osoba používá. Na každém zařízení, které uživatel používá, může být tento uživatel součástí několika rolí. Každá role je označovaná jako částečná identita zařízení a uživatele. Částečná identita může být přidělena zařízení a nebo jeho uživateli.

Obrázek 6 znázorňuje identitu osoby, která užívá dvě zařízení, notebook a chytrý telefon. Notebook má přiřazenou IP adresu prostřednictvím DHCP a SLAAC protokolu. IP adresy jsou používány protokolem SIP pro VoIP komunikaci a protokolem HTTP pro autentifikaci uživatele. Stejný uživatel zároveň využívá chytrý telefon s IP adresou přidělenou protokolem DHCP. Uživatel z chytrého telefonu odesílá e-mail protokolem SMTP a stejně jako v případě laptopu, je telefon autentizovaný protokolem HTTP. Identita uživatele se tedy skládá z identit zařízení, které se dále skladají z uvedených částečných identit.

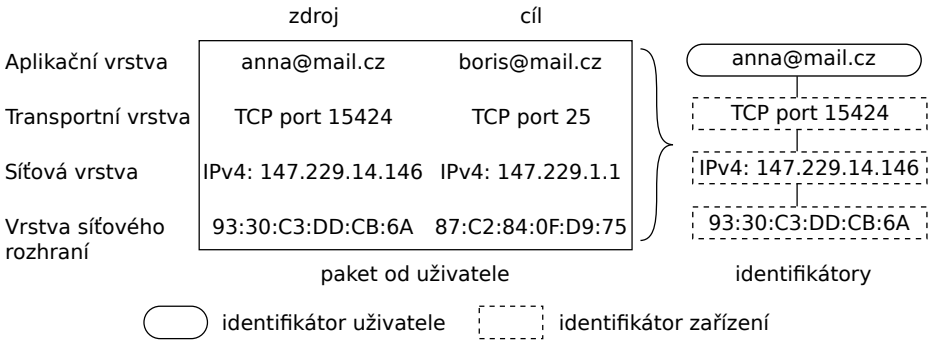


Obrázek 6: Příklad identity uživatele skládající se z identit zařízení notebook a chytrý telefon, která daný uživatel používá. Obě zařízení se účastní několika rolí. Každá role obsahuje jiné částečné identity s jinou množinou identifikátorů.

Identifikátory Identifikátor je atribut unikátní pro subjekt nebo skupinu subjektů a má obvykle formu čísla, jména nebo binárního řetězce [28]. V počíta-

čových sítích jsou identifikátory využívány síťovými službami pro identifikaci a rozlišení jejich účastníků. Identifikátory jsou rozděleny do dvou skupin (viz obrázek 7):

- *identifikátory uživatelů* - e-mailová adresa, PPP login, uživatelské jméno SIP, ICQ číslo a další,
- *identifikátory zařízení* - IP adresa, MAC adresa, DUID hodnota a další.



Obrázek 7: Paket odeslaný uživatelem obsahuje kromě identifikátorů zařízení i identifikátory uživatele. Propojením obou typů identifikátorů je možné získat údaje potřebné k pozdější detekci identity uživatele na základě identifikátorů zařízení.

Ačkoliv je správa počítačové sítě založena na základě identity uživatelů, znalost identifikátorů uživatelů není dostatečná. Většina paketů odeslaných do sítě neobsahuje identifikátory uživatelů, ale pouze identifikátory zařízení. Analýzou paketů jen pomocí identifikátorů zařízení není možné rozhodnout, které identitě uživatele patří, a proto je nutné znát propojení mezi identifikátory zařízení a identifikátory uživatelů. Na obrázku 7 je znázorněn paket, který je součástí e-mailové komunikace pro odeslání zprávy z adresy *anna@mail.cz* na adresu *boris@mail.cz*. Analýzou zobrazeného paketu je kromě e-mailové adresy *anna@mail.cz* možné detekovat i IP adresu tohoto uživatele. Další pakety, odeslané po vymezenou dobu z detekované zdrojové IP adresy, patří stejnému uživateli.

Přestože jsou identifikátory unikátní, nemusí mít pořád stejnou hodnotu. Některé aplikace a protokoly nepřiřazují identifikátory osobě nebo zařízení navždy, ale pouze dočasně. Dočasně přiřazené identifikátory se nazývají *dynamické identifikátory* a identity, které se skládají z dynamických identifikátorů, se nazývají *dynamické identity*. Pokud protokol nebo aplikace používá dynamické identifikátory, nelze nikdy předpokládat, že osoba, která používala v minulosti daný identifikátor, používá ten stejný i později.

Detekce identity uživatelů V současné době neexistuje univerzální způsob získávání znalosti o identitách uživatelů. Aplikace samotné znají pouze částečné identity svých uživatelů. Pro získaní znalosti identity uživatelů je potřeba shromáždit všechny částečné identity od aplikací a následně je spojit. Většina aplikací obvykle neobsahuje rozhraní, které by umožňovalo sloučení částečných identit, proto je nutné částečné identity získat detekcí identifikátorů, ze kterých se identita skládá.

Existuje několik způsobů detekce identifikátorů, např. statická definice, analýza logovacích souborů nebo analýza síťového provozu. Kromě hodnot identifikátorů je detekce zaměřena na zjištění začátku a konce platnosti identifikátoru spolu s kontextem, ve kterém je identifikátor použit. Pomocí kontextu identifikátorů je možné zjistit, které identifikátory patří stejné částečné identitě.

Po detekci jsou identifikátory odeslány na centrální bod, kde jsou propojeny s identifikátory ze stejné částečné identity. Postupně, jak se detekované identifikátory propojují, vzniká komplexní pohled na stav síťě v které provádíme detekci identit. Z vytvořeného komplexního pohledu je možné vyjádřit částečné identity, identity uživatelů a identitu zařízení.

Identita uživatele nebo zařízení je vytvořena z částečných identit, které jsou propojeny pomocí společných identifikátorů. Vazba částečných identit umožňuje přiřadit komunikaci k některé částečné identitě pomocí identifikátoru z jiné částečné identity. Propojování identifikátorů musí splňovat určité požadavky [30], které jsou mimo rozsah této práce. Obrázek 8 zobrazuje kombinaci dvou částečných identit, které patří stejnému uživateli.

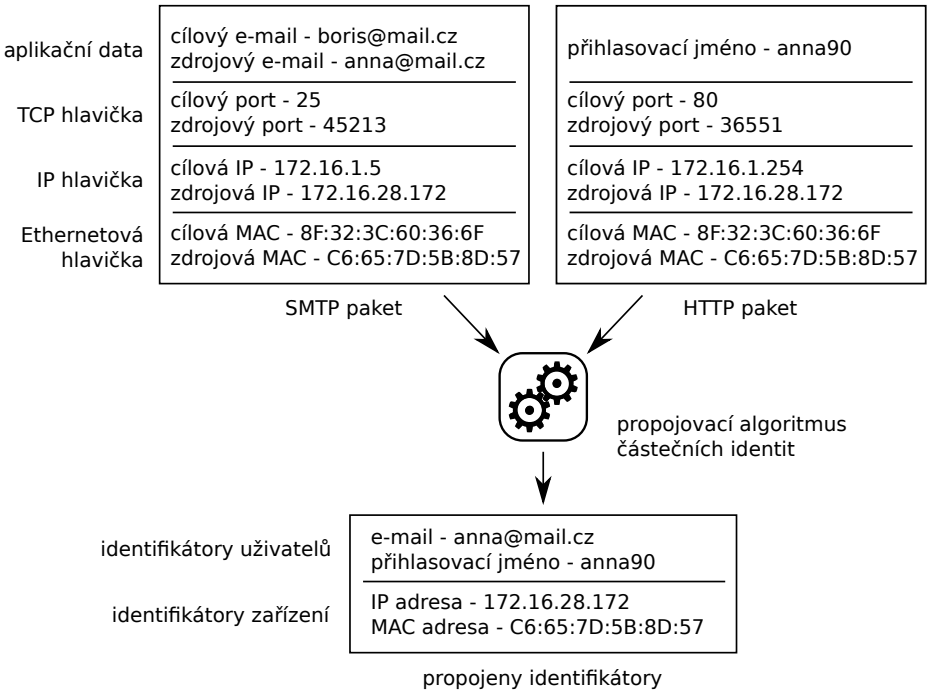
3.2 Sec6Net Lawful Interception System

Jedním z cílů projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace* bylo vytvořit systém pro zákonné odposlechy (Lawful Interception System – LIS) pojmenovaný Sec6Net Lawful Interception System (SLIS). Tento systém vychází z doporučení ETSI [5,6,8,10,7,11,9,12] a je také inspirován architekturou LIS firmy Cisco publikovanou v RFC 3924 [1]. Návrhu, architektuře a implementaci tohoto systému se věnuje samostatná technická zpráva [31].

Systém SLIS byl navržen s modulární architekturou. Dynamickou identitu uživatele je možné detekovat pomocí modulů specializovaných na konkrétní protokol, či metodu zjištění částečné identity. Informace o různých částečných identitách jediného uživatele jsou spojovány pomocí mechanismu založeném na grafové reprezentaci pomocí uzávěrových relací nad uzly grafu [30,31].

Součásti systému SLIS, které jsou důležité pro tuto práci, jsou následující:

- Funkce dynamické identity (IRI-IIF) – má za úkol dynamické zjišťování částečné identity sledováním probíhajících komunikací (relace, hovory, spojení apod.) a analýzou protokolů.
- Sondy pro odposlech (CC-IIF) – mají za úkol zachytávat obsah komunikace sledovaných uživatelů.



Obrázek 8: Počítač s MAC adresou C6:65:7D:5B:8D:57 a IPv4 adresou 147.229.8.53 je používán jedním uživatelem. Uživatel používá službu SMTP k odeslání emailu z adresy anna@mail.cz a službu HTTP k autentizaci na web serveru jako uživatel anna90. Každá služba reprezentuje jinou částečnou identitu, která obsahuje různé množiny identifikátorů. Identifikátory z obou služeb jsou spojeny do jedné množiny identifikátorů, která patří stejnému uživateli.

– Triggerovací funkce (CCTF) – konfiguruje jednotlivé sondy ve chvíli, kdy má být zahájen odposlech.

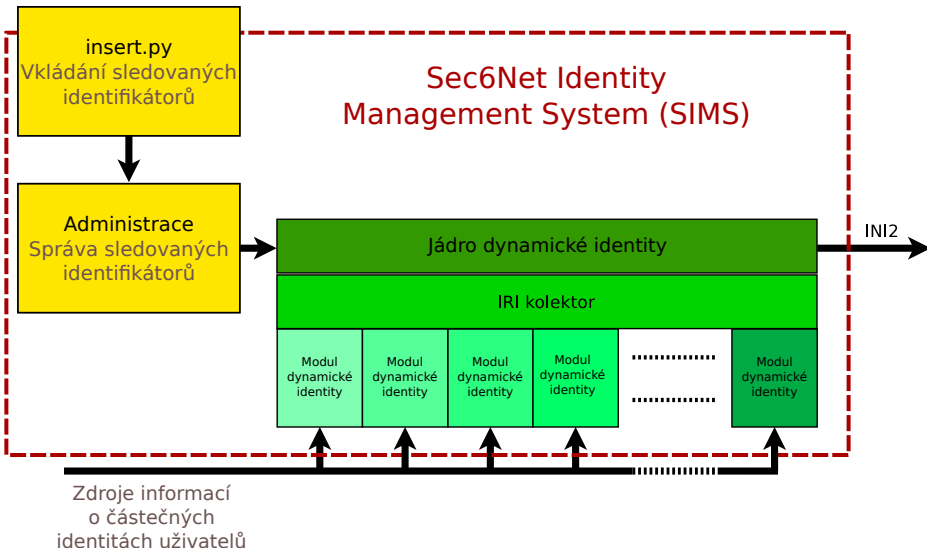
Jako příklad lze uvést požadavek na odposlech uživatele s určitou e-mailovou adresou. Pokud tento uživatel v průběhu odposlechu změní IP adresu svého zařízení nebo ke komunikaci použije jiné zařízení, IRI-IIF detekuje změnu a předá tuto informaci systému. CCTF pak může včas překonfigurovat připojené sondy CC-IIF a zachytit veškerý obsah komunikace.

3.3 Sec6Net Identity Management System

Pro demonstraci užitečnosti mechnismů implementovaných uvnitř systému SLIS vznikl nástroj Sec6Net Identity Management System (SIMS). Nástroj SIMS podporuje rozhraní [31] sytému SLIS pro moduly pro zjišťování dynamické identity a je tedy kompatibilní se všemi metodami dostupnými pro systém SLIS. Navíc systém SIMS přebírá mechanismus pro spojování částečných identit [30,31].

SIMS umožňuje sledování konkrétního síťového identifikátoru (Network Identifier – NID) [31] odpovídajícímu konkrétnímu uživateli, stroji, či skupině uživatelů nebo strojů.

Obrázek 9 zachycuje architekturu nástroje SIMS. Pomocí programu *insert.py* je možné sledovat nový NID. Jednotlivé moduly pro detekci identity uživatele zpracovávají síťový provoz, výstupní logy programů, či jiný vhodný zdroj dat a skrze IRI kolektor zasílají informace do jádra sledování dynamické identity uživatele, kde jsou informace o částečných identitách uživatele spojovány a případně signalizovány na výstup nástroje rozhraním INI2 [31].



Obrázek 9: Architektura nástroje SIMS.

Nástroj SIMS poslouchá na nastaveném portu a komunikuje s libovolnou aplikací, která implementuje dříve definované rozhraní INI2 [31]. SIMS tak dává ostatním aplikacím informace o rozpoznaných identitách uživatelů v síti. V této technické zprávě je ukázáno, jak je možné tyto informace využit při řízení sítě SDN. Sekce 6 popisuje konkrétní nástroje zaměřené na ovládání síťových toků na základě informací poskytovaných nástrojem SIMS.

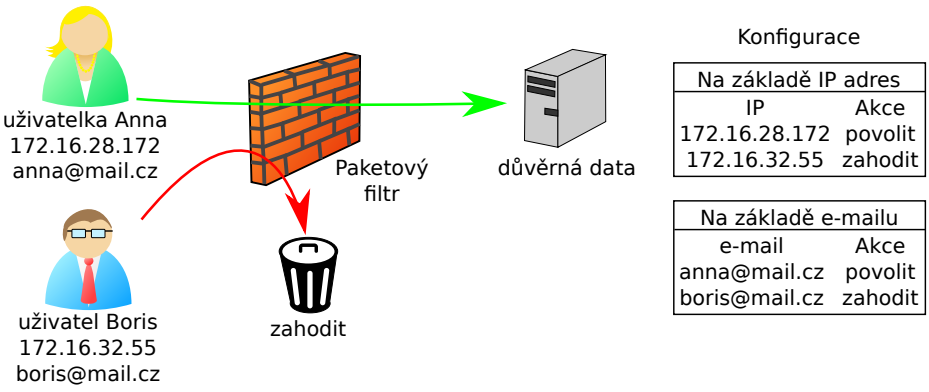
4 Využití znalosti identity uživatele v prostředí SDN

V dnešních počítačových sítích jsou síťové prvky (přepínače, směrovače a další) konfigurovány na základě zařízení, která jsou do sítě zapojena. Například paketový filtr je konfigurován seznamem pravidel, kde každé pravidlo obsahuje identifikátor zařízení – IP adresu, která může nebo nemůže projít filtrem. Nevýhodou

tohto přístupu je, že seznam pravidel je definovaný pro identifikátory koncových zařízení namísto pro identifikátory uživatelů sítě. Pro vytvoření konfigurace musí administrátor sítě vědet, kteří uživatelé toto zařízení používají a jaké IP adresy mají jednotlivá zařízení přiřazené. Kdyby se změnila zařízení, které uživatel používá, nebo by se změnily IP adresy přiřazené těmto zařízením, je nevyhnutné aktualizovat konfiguraci síťových prvků. Pro velmi dynamické sítě není manuální aktualizace síťových prvků efektivní (např. v sítích, kde si uživatelé mohou kdykoliv zapojit svá vlastní zařízení).

Pomocí znalosti identity uživatelů ze systému pro správu identit v řízení sítě SDN (kontroler) je možné rozšířit možnosti správy sítě. Jednou z možností rozšíření správy sítě je použití znalosti identit uživatelů při vytváření konfigurace síťových prvků. Místo konfigurace paketového filtru na základě IP adres je možné definovat pravidla filtru pomocí identity uživatelů (např. zablokovat přístup k určité službě vybranému uživateli bez ohledu na zařízení, které využívá).

Obrázek 10 zobrazuje rozdíl mezi konfigurací paketového filtru pomocí identifikátorů zařízení (IP adresa) a pomocí identifikátorů uživatelů (e-mail). Obě konfigurace povolují přístup k důvěrným datům pouze pro uživatelku se jménem *Anna*. Datový provoz uživatele *Boris* musí být paketovým filtrem zahozen. Při konfiguraci pomocí IP adres musí administrátor zajistit, aby uživatelé měli přiřazenu vždy stejnou IP adresu. V případě, že by si uživatel *Boris* nastavil staticky stejnou adresu jako uživatelka *Anna*, získal by přístup k důvěrným datům. Konfigurace na základě e-mailu pouze vyžaduje, aby řízení sítě vědelo e-mailové adresy uživatelů v síti. Tuto znalost poskytne kontroleru systém pro správu identit.



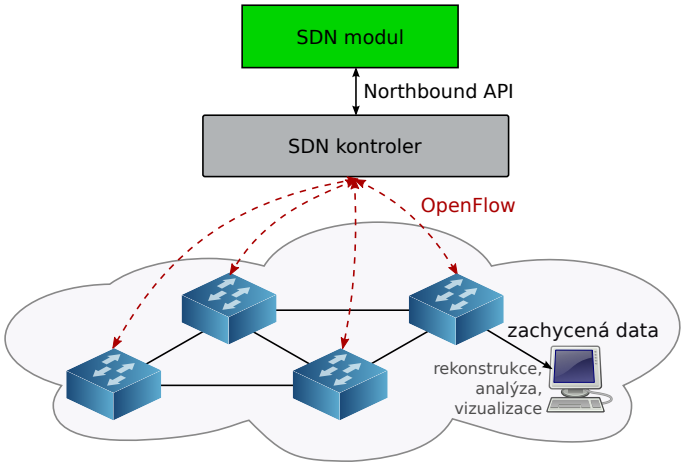
Obrázek 10: Firemní paketový filtr je použit pro zabezpečení přístupu k důvěrným datům. Pakety od uživatelů, kteří nemají povolen přístup k těmto datům, jsou zahozeny. Dvě možnosti kofigurace jsou znázorněny na pravé straně obrázku.

5 Případová studie: zákonné odposlechy

Softwarově definované sítě poskytují řadu nových přístupů a výhod, které lze použít například pro zjednodušení zachytávání dat. Jednou z možností jak aplikovat jednu z výhod, je využití znalosti topologie z kontroleru a vytvoření pravidel v tabulkách toků, na základě kterých je možné identifikovat provoz (například od určitých uživatelů nebo na základě IP adresy), zduplikovat a označit jednotlivé pakety. Označené pakety je pak možné přeposílat na předem určené zařízení, které může fungovat jako honeypot, IDS, spam filter, antivirová kontrola apod.

5.1 Princip řešení

K realizaci duplikace, označení a přeposílání zájmových paketů je nutné vytvoření nového modulu pro kontroler. Tento modul bude v pravidelných intervalech zjišťovat aktuální topologii a vkládat pravidla pro směrování kopií zájmových dat k zařízením, které pak data mohou sbírat a analyzovat. Schéma zapojení tohoto modulu a sběrného zařízení je znázorněna na obrázku 11.



Obrázek 11: Schéma zapojení modulu a zařízení pro zachytávání dat v SDN.

Pro modul je nezbytné znát kompletní topologii. Jedinou informaci, kterou není schopen získat dynamicky, je pozice zachytávacích zařízení v síti. Součástí modulu proto musí být konfigurační soubor, který specifikuje, na kterém rozhraní jsou připojeny. Modul by měl být navržen tak, aby v případě potřeby dokázal odesílat označené pakety na více zařízení, provádět jednoduché vyvažování zátěže a změnit cílové zařízení v případě změny topologie nebo výpadku linky.

Kombinací topologie získané z kontroleru a pozice sběrných zařízení z konfiguračního souboru modul vytvoří grafovou reprezentaci, kde vrcholy grafu jsou jednotlivá zařízení a hrany odpovádají linkám. Ve chvíli, kdy přijde požadavek

na zachytávání dat například s danou IP adresou, začíná modul s konfigurací síťových zařízení. Konfigurace spočívá ve využití tří tabulek toků. Do první tabulky modul ukládá pravidla, která porovnávají procházející hlavičky paketů s IP adresou, která má být zachytávána. Pokud zdrojová nebo cílová adresa paketu odpovídají, je paket označen VLAN tagem a odeslán na výstupní port směrem ke sběrnému zařízení. Následně je původní paket (bez VLAN tagu) předán třetí tabulce.

Druhá tabulka toků je na všech přepínačích stejná. Má za úkol porovnávat pakety s VLAN tagem a odesílat je směrem ke sběrnému zařízení. Pravidla se prochází postupně od nejvyšší priority, proto musí být v první tabulce pravidlo s vysokou prioritou, které bude také porovnávat VLAN tag. Pakety, které jsou takto označeny, pak nezpracovává a pouze je předá druhé tabulce.

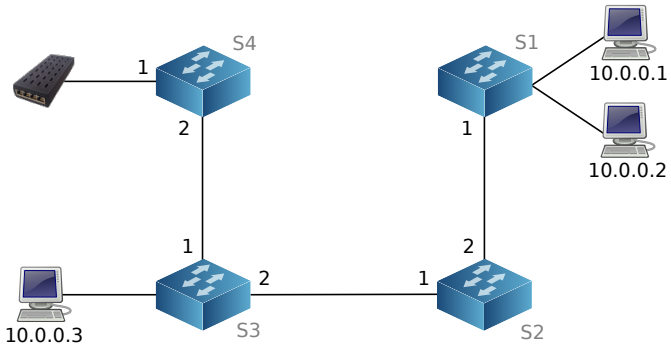
Třetí tabulka je plně pod správou kontroleru a přeposílá pakety k cílovým zařízením bez ohledu na pravidla v předchozích tabulkách. Tímto způsobem se tedy vytvoří duplikát paketu s VLAN tagem a původní nezměněný paket se přepošle podle pravidel z kontroleru.

5.2 Ukázka rekonfigurace zařízení

Uvažujme například topologii uvedenou na obrázku 12. Předpokládejme, že máme zájem zachytávat provoz se zdrojovou nebo cílovou IP adresou 10.0.0.1. Modul zná aktuální topologii sítě a tak může jednoduše zjistit, ke kterému přepínači je koncové zařízení s danou IP adresou přímo připojeno. V uvedeném případě je zařízení připojeno k přepínači S1. Na tento přepínač se vloží dvě pravidla s vysokou prioritou, která budou porovnávat danou zdrojovou a cílovou adresu v paketu. V případě, že jedna z těchto adres bude rovna 10.0.0.1, vloží se do paketu VLAN hlavička a odešle se na výstupní port 1. Ukázka pravidel je uvedena v tabulce 1 (porovnávání cílové IP adresy probíhá obdobně jako porovnávání zdrojové IP adresy). Na tomto i všech ostatních přepínačích se pak všechny pakety s VLAN hlavičkou budou přeposílat na rozhraní 1. Tato pravidla jsou uložena ve druhé tabulce a ukázka je uvedena v tabulce 2. Na přepínači S4 bude uloženo pravidlo, které ze všech paketů odesílaných na rozhraní 1 VLAN odstraní.

V případě, že je v topologii více zařízení, která mohou zachytávat duplikovaná data, lze jednoduchým způsobem nastavit bližší zařízení nebo rozdělovat zátěž. Každé takové zařízení bude mít vlastní VLAN tag. Při přidávání pravidla můžeme z grafu topologie zjistit, které sběrné zařízení je nejblíž koncovému zařízení s danou IP adresou, a při duplikování paketů vložit VLAN tag nejbližšího sběrného zařízení. V druhé tabulce toků na všech přepínačů pak budou pravidla, která pakety s VLAN hlavičkou odešlou směrem k tomuto zařízení.

V reálných OpenFlow přepínačích nemusí být k dispozici více tabulek toků. V takových případech je možné použít i alternativní přístupy. Jedním z nich je využití jednoho z fyzických portů přepínače, na který se bude duplikovat komunikace odposlouchávaného uživatele. Všechny pakety přijaté na tomto portu pak budou označeny a přeposlány směrem ke sběrnému zařízní. K implementaci



Obrázek 12: Ukázková topologie se zapojenou sondou pro zachytávání dat.

tohoto řešení stačí pouze jedna tabulka toků, ale nevýhodou je permanentní zablokování jednoho portu a nepřehlednost tabulky toků.

Prio	VLAN	IP zdroj	IP cíl	Ostatní	Akce
20	1	*	*	*	go-to tab 2
10	*	10.0.0.1	*	*	push VLAN outport 1 pop VLAN go-to tab 3
1	*	*	*	*	go-to tab 3

Tabulka 1: Ukázka pravidel pro odposlech v první tabulce toků. Porovnávání s hvězdičkou znamená, že na daném místě může být libovolná hodnota. *Push/pop VLAN* značí přidání/odstranění VLAN tagu, *go-to table* znamená skoč do tabulky a *outport* odeslání paketu na výstupní port.

Prio	VLAN	IP zdroj	IP cíl	Ostatní	Akce
10	1	*	*	*	outport 1

Tabulka 2: Ukázka pravidel v druhé tabulce toků.

5.3 Rozšíření systému pro zákonné odposlechy

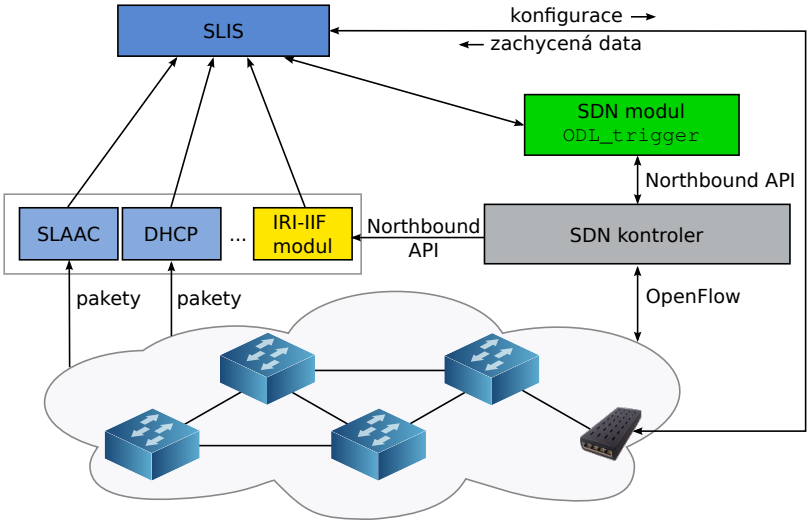
V rámci projektu vznikl samostatný software pro zachytávání dat – *SDN-tap* [13] a rozšíření systému pro zákonné odposlechy SLIS tak, aby bylo možné jej použít v prostředí SDN. Architektura systému pro zákonné odposlechy se znázorněnými nově vytvořenými moduly je uvedena na obrázku 13. Vytvořená rozšíření pro SLIS jsou následující:

- Moduly pro IRI-IIF, které jsou určeny k získávání částečné identity koncových zařízení a uživatelů. Modul pro OpenDaylight se periodicky dotazuje kontroleru na topologii sítě a informace o částečné identitě koncových zařízení zasílá IRI-IIF.
- Dynamická rekonfigurace CC-IIF sond a OpenFlow přepínačů. Jedná se především o implementaci CCTF, ze které bylo v rámci SLIS implementováno jen nutné minimum. CCTF nyní rozlišuje jednotlivé CC-IIF sondy podle jejich pozice v topologii. Na základě těchto informací systém vytvoří grafovou reprezentaci topologie a zvýší váhu hran, které používá OpenDaylight pro zasílání neodposlouchávaných paketů. Při vložení odposlechu se pak vybere vhodná sonda. Vybírá se především podle vzdálenosti a zároveň se provádí jednoduché vyvažování zátěže, aby se předešlo zahlcení jedné sondy. Administrátor může také nastavit cenu linek v konfiguračním souboru. Pokud zvolí cenu větší než 1000, přestane se provádět vyvažování zátěže a daná linka se bude využívat pouze jako záložní. V případě, že se ze systému odpojí sonda s aktivními odposlechy, rozdělí se tyto odposlechy mezi ostatní sondy.

Zjišťování identity koncových zařízení Z kontroleru je možné získat tři typy identifikátorů pro každé zařízení: IP adresu, MAC adresu a identifikátor přepínače, ke kterému je toto zařízení připojeno. Ve chvíli, kdy je detekován začátek spojení, je nutné odeslat funkci dynamické identity IRI zprávu. Součástí zprávy je uvedená trojice identifikátorů. IRI-IIF odpovídající identifikátory propojí a tím rozšíří zjištěnou identitu tohoto zařízení.

Vkládání odposlechů Pro vkládání a odstraňování pravidel pro označování zájmových paketů jsme vytvořili modul `ODL_trigger`, který je implementován v jazyce Python. Tento modul má za úkol poskytovat rozhraní mezi MF&CCTF a OpenDaylight. Ve chvíli, kdy do mediační funkce přijde z administrační funkce požadavek na zahájení odposlechu, zavolá CCTF funkci pro vložení odposlechu z modulu `ODL_trigger`. Tato funkce zjistí aktuální topologii, vytvoří odpovídající graf a zvýší hodnocení hran, které používá OpenDaylight.

Při výběru sondy, která bude zachytávat komunikaci daného zařízení, se provádí jednoduché vyvažování zátěže. Nejdříve se z kontroleru zjistí informace o topologii a pozice sond. Ve chvíli, kdy je vytvořen graf topologie, se najdou nejkratší cesty mezi zařízením, které chceme odposlouchávat, a všemi sondami. Pravidla pro odposlech se implicitně vkládají na sondu, která má nejnižší součet hodnocení hran na cestě k odposlouchávanému zařízení. Pokud je ale rozdíl



Obrázek 13: Schéma zapojení systému pro zákonné odposlechy, SDN kontroleru, modulu pro zjišťování dynamické identity – IRI-IIF modul, a modulu pro sledování topologie – SDN modul.

v počtu odposlechů některých sond více než trojnásobný, vybere se sonda s méně odposlechy nezávisle na pozici v topologii. Tím zajistíme, že se častěji využívají linky, které OpenDaylight nepoužívá pro provoz neodposlouchávaných paketů.

Pokud program zná nejvhodnější sondu a nejbližší přepínač, může nahrát pravidla pro odposlech, přičemž se budou označovat VLAN tagem nejvhodnější sondy. Triggerovací funkce na základě návratové hodnoty pak nastaví CC-IIF sondu.

Odstraňování odposlechů Odstranění odposlechu ze systému je jednodušší než vkládání. Ve chvíli, kde mediační funkci přijde požadavek na ukončení odposlechu, spustí se funkce z modulu `ODL_trigger` pro odstranění odposlechu. Tato funkce načte z kontroleru topologii sítě a zjistí pozici sond. Poté získá všechny aktuální pravidla v první tabulce.

V načtených pravidlech nalezne odpovídající dvě pravidla (v případě odstraňování pětice pouze jedno). Ze seznamu akcí v pravidle zjistí VLAN tag sondy, ke které byly zasílány označené pakety. Pak odstraní pravidla z přepínače a číslo sondy vrátí MF&CCTF. Triggerovací funkce na základě návratové hodnoty odstraní odposlech i z odpovídající CC-IIF sondy.

Dynamická rekonfigurace přepínačů a sond Zjišťování změn v topologii probíhá také v modulu pro MF&CCTF `ODL_trigger`. Modul v pravidelných intervalech zjišťovat topologii sítě a v případě změny rekonfigurovat přepínače a zajistit, aby triggerovací funkce překonfigurovala CC-IIF sondy.

`ODL_trigger` se spouští na samostatném vlákně v rámci MF&CCTF funkce. Periodicky zjišťuje aktuální topologii a pozici sond. Pokud nebyla nalezena žádná sonda, daný běh se ukončí. Pokud je nalezena alespoň jedna sonda, vytvoří se z topologie *networkx* graf. V prvním běhu program nahraje inicializační pravidla do první tabulky toků a pravidla pro přeposílání paketů označených VLAN tagem. Nakonec uloží graf topologie do souboru JSON.

Všechny další běhy pak porovnávají aktuální graf s tím, který byl při poslední změně uložen do JSON souboru. V případě, že došlo k jakékoliv změně topologie, démon postupně provede následující kroky:

1. Zjistí, zda jsou na všech přepínačích nahrána inicializační pravidla v první tabulce. V případě, že byl připojen nový přepínač a pravidla neobsahuje, nahrají se.
2. Aktualizuje pravidla v druhé tabulce toků. Pokud by byla připojena nová sonda, nahraje se nové pravidlo, které bude směrovat pakety označené VLAN tagem k této sondě. Pokud byla některá sonda odpojena, odstraní se pravidlo na přeposílání paketů.
3. Zkontroluje pravidla na označování paketů v první tabulce toků. Pro každé pravidlo pro odposlech je nutné zkontrolovat VLAN tag a výstupní rozhraní, na které se označené pakety odesílají. V případě, že se změní pouze rozhraní a VLAN tag zůstane stejný, upraví se pravidlo a sonda zůstane nastavená pořád stejně. Pokud se ale pakety mají začít zasílat na jinou sondu, musí se kromě úpravy pravidla také odstranit odposlech z původní sondy a vložit na novou sondu. `ODL_trigger` odešle triggerovací funkci zprávu, ze které sondy se má odposlech odstranit a na kterou se má nahrát. Triggerovací funkce na základě těchto informací odstraní odposlech z první sondy a vloží ho na druhou.

Pravidla v první i druhé tabulce toků ovlivňuje způsob změny topologie. Obecně může nastat jedna nebo více z následujících situací:

- přidání linky
  - Pravidla se nemění, ale při přidávání nového odposlechu se bude brát v úvahu i nová linka.
- výpadek linky
  - Zkontrolují se všechna aktuální pravidla, která odesílají paket na některé výstupní rozhraní a také cesty z jednotlivých přepínačů k sondám.
  - Výpadek linky, která jako jediná vede přímo k sondě, způsobí odstranění pravidel pro odposlech s VLAN tagem dané sondy. Všechna tato pravidla se aktualizují, změní VLAN tag a budou přeposílat pakety na rozhraní k některé jiné sondě.
  - Výpadek linky mezi přepínači ovlivní pouze pravidla, která jsou nahraná na těchto přepínačích. V případě, že se linka používala pro přeposílání označených paketů, musí se upravit všechna pravidla pro odposlech v první tabulce toků a pravidla pro přeposílání paketů s VLAN tagem ve druhé tabulce toků.
- přidání přepínače

    - Pokud přepínač ještě nebyl zapojen v topologii, nahrají se inicializační pravidla a pravidla pro přeposílání paketů s VLAN tagem.
    - Pokud přepínač byl zapojen v topologii a obsahuje nějaká pravidla na označování paketů, porovnají se se seznamem aktuálních odposlechů. Pokud byl odposlech mezitím zrušen, odstraní se i z přepínače. Pravidla pro přeposílání paketů s VLAN tagem se zkontrolují a případně aktualizují.
- odstranění přepínače
    - Podobně jako u výpadku linky se zkontrolují všechna pravidla a případně se aktualizují výstupní porty.
- přidání a odstranění koncového zařízení
    - Pravidla se nemění.
- přidání CC-IIF sondy
    - Do všech přepínačů se nahraje pravidlo pro přeposílání paketů s VLAN tagem nové sondy.
- odstranění CC-IIF sondy
    - Ze všech přepínačů se odstraní pravidlo pro přeposílání paketů s VLAN tagem dané sondy.
    - Pravidla pro odposlech, které označovaly pakety VLAN tagem této sondy, se aktualizují (změní se VLAN tag na tag jedné z dostupných CC-IIF sond a aktualizuje se výstupní rozhraní).

5.4 Experimenty

Dynamická rekonfigurace Experimenty v této sekci měly za cíl ověřit chování modulu `ODL_trigger` při vkládání, odstraňování nebo modifikaci odposlechu při změně topologie. Vytvořili jsme několik skriptů pro mininet[1] s různými topologiemi, které zjišťovaly následující chování systému:

- *Reakce systému na změnu topologie (výpadek linek)* – Cílem prvního experimentu bylo ověřit chování systému při výpadku linky, která se využívá pro přeposílání paketů označených VLAN tagem. Při vkládání odposlechů i při rekonfiguraci by systém měl brát ohled na využití linek. Pokud je to možné, systém použije k zachytávání dat sondu, ke které se označené pakety dostanou po linkách, které nejsou součástí kostry grafu.
- *Vyvažování zátěže mezi CC-IIF sondami* – Cílem tohoto experimentu je ověřit vyvažování zátěže mezi sondami. Vyvažování zátěže se řídí konstrou grafu, kterou OpenDaylight používá pro přeposílání paketů neodposlouchávané komunikace. Při vytváření grafové reprezentace topologie se váha hran kostry zvýší na 5, zatímco ostatní hrany mají hodnocení 1.
- *Kombinace vyvažování zátěže, kdy váhy některých hran jsou zadány administrátorem, a změny topologie* – Speciální případ, kdy hodnocení hran grafu je specifikováno administrátorem. Tato situace může nastat například ve chvíli, kdy se síť ISP nachází na dvou lokacích a je propojená jednou nebo více linkami. Pokud budou na obou místech zapojeny CC-IIF sondy, bude nejvýhodnější vložit odposlech na sondu, která se nachází v dané lokaci. Z tohoto

[1] http://mininet.org

důvodu je možné vložit do konfiguračního souboru řádky, na kterých administrátor uvede linku, které se ohodnocení týká, a její váhu. V případě, že je váha linky vyšší nebo rovna 1000, přestane se linka využívat pro vyvažování zátěže.

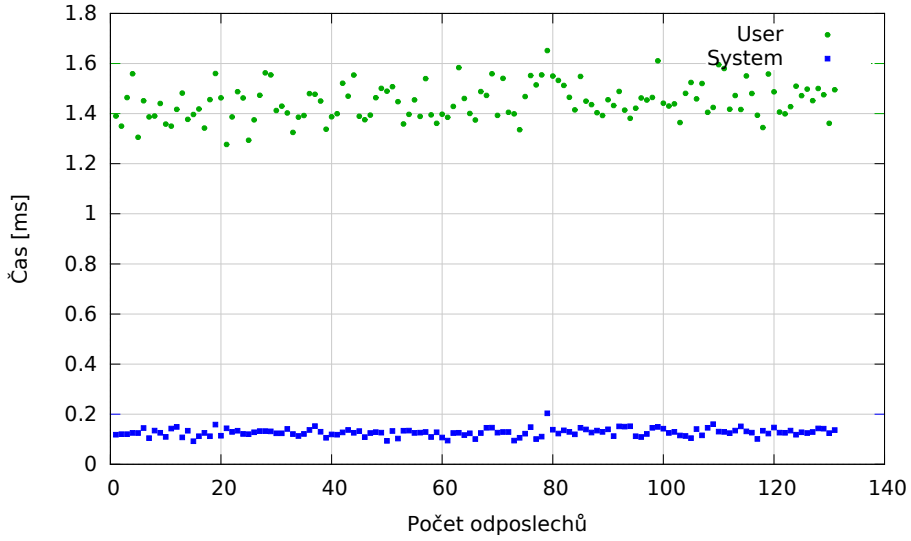
Výkonnost systému Experimenty v této sekci byly zaměřeny na zjištění rychlosti systému při manipulaci s toky. Topologie byla v obou případech stejná.

- *Zpoždění při vkládání odposlechu* – Cílem prvního experimentu bylo zjistit dobu, za kterou se nahraje nový odposlech do systému. Doba měření zahrnuje pouze činnosti, které provádí modul `ODL_trigger`. V průběhu experimentu se do systému postupně zadávaly požadavky na odposlech trojice: IP adresa `10.0.0.1` (vždy stejná), číslo portu (každým novým pravidlem se zvýšilo) a protokol TCP. V grafu 14 jsou znázorněny naměřené výsledky. Uživatelský čas značí dobu, kterou počítač strávil výpočtem a systémový čas potom dobu, kdy čekal v rámci procesu. Z grafu je zřejmé, že počet pravidel v přepínačích nemá vliv na dobu vkládání nového odposlechu. Průměrná doba vložení je přibližně 1,4 sekundy.
- *Zpoždění při změně topologie* – Cílem druhého experimentu je zjistit, jak dlouho trvá modulu `ODL_trigger` přesunout pravidla z jedné sondy na druhou v případě, že první sonda bude nedostupná. Doba měření zahrnuje jak zjišťování změn v topologii, tak následnou změnu pravidel na jednotlivých přepínačích. Při experimentu se do systému vkládal vždy určitý počet odposlechů, které se označovaly VLAN tagem sondy 1. Poté byla sonda 1 odstraněna z topologie. Reakcí systému bylo odstranění pravidla pro přeposílání paketů označených VLAN tagem 1 z tabulky 2 a úprava všech pravidel pro označování odposlouchávaných dat. V grafu 15 jsou znázorněny naměřené hodnoty.
  Zatímco v případě vkládání odposlechů nemá počet stávajích pravidel na přepínačích žádný vliv, u přesouvání toků je to logicky naopak. Čas roste lineárně s počtem odposlechů, přičemž u pětic je čas na úpravu jednoho odposlechu kratší, protože se upravuje pouze jedno pravidlo. Průměrný čas pro odstranění a vložení upraveného pravidla je přibližně 20 ms.

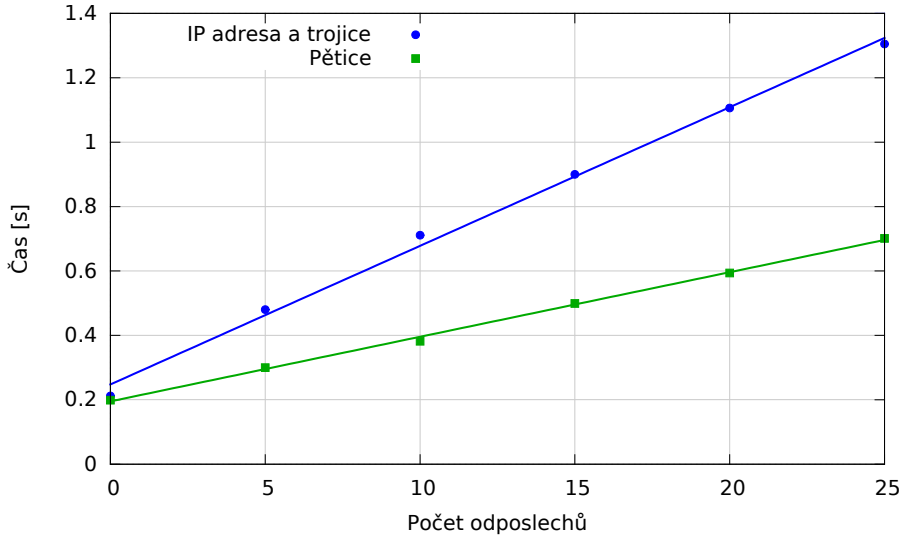
Shrnutí experimentů Součástí experimentů bylo také ověření funkčnosti nového modulu pro IRI-IIF. Ve všech uvedených případech se systém choval podle očekávání.

6 Případová studie: řízení toků podle identity uživatelů

Tato kapitola se zabývá rozšířením správy sítí pomocí znalosti identit jejich uživatelů. V rámci projektu vznikl software *Řízení SDN podle identit – SDNIM* [18]. Pro řízení byl použit kontroler Pyretic, který byl upraven pro možnost pracovat s identitami, a systém pro správu identit uživatelů SIMS, do kterého byla



Obrázek 14: Doba vložení jednoho odposlechu (dvojice pravidel) v závislosti na počtu pravidel v tabulce.



Obrázek 15: Doba upravení všech pravidel pro odposlech (odstranění pravidla, vypočítání nové cesty v grafu a nejvhodnější sondy, vložení pravidla) v závislosti na celkovém počtu pravidel.

přidána podpora nových identifikátorů (přihlasovací jméno a poloha uživatele). Uživatelé jsou součástí skupin, do kterých jsou přiřazeni na základě jejich přihlášení do webového informačního systému a podle kterých je aplikována síťová politika. Nad kontrolerem byla vytvořena aplikace zpřístupňující znalost identit libovolné další aplikaci nad stejným kontrolerem. Druhá část kapitoly popisuje tři případy užití, které jsou zaměřeny na zabezpečení sítě. Znalost identity uživatelů je však možné aplikovat na libovolnou oblast správy sítě (např. směrování).

Webová autentizace Pro jednoznačné určení identity uživatelů je použit identifikátor přihlašovací jméno do webového informačního systému. Pro tento účel byl vytvořen jednoduchý web, který po přihlášení nebo odhlášení každého uživatele odešle systému SIMS notifikaci. Součástí notifikace je typ události (přihlášení nebo odhlášení), přihlasovací jméno a IP adresa uživatele. V jednom okamžiku může být z jednoho počítače přihlášen maximálně jeden uživatel. Dříve než zařízení začne používat jiný uživatel, je nutné, aby byl předešlý uživatel odhlášen.

Systém SIMS Pro získávání znalostí o identitách je použit systém SIMS, který je nasazen do sítě. Množina podporovaných identifikátorů byla rozšířena o identifikátory přihlašovací jméno a poloha v síti. Přihlašovací jméno je získané po úspěšném přihlášení uživatele sítě do webového informačního systému. Poloha v síti vyjadřuje místo, kde je zapojena koncová stanice, a skládá se z ID přepínače a portu. Identifikátor poloha je získáván analýzou ARP paketů v kontroleru. Systém při každé změně množiny identifikátorů odešle její aktuální podobu kontroleru SDN.

Kontroler Pro případovou studii byl použit kontroler Pyretic, který byl rozšířen následujícími způsoby:

- Příjem a zpracování externích událostí - Konfigurace sítě je aktualizována pouze při přijetí paketu ze sítě nebo při změně síťové topologie. Pro možnost reagovat na změny v identitách uživatelů je nutné rozšířit možnosti aktualizace konfigurace sítě o externí události. Problém byl vyřešen vytvořením nového vlákna, které je schopno pomocí soketového rozhraní přijímat události a zároveň vyvolat aktualizaci konfigurace.
- Uložení poslední změny síťové topologie pro lepší reakci řídících aplikací na změny v síti - Reprezentace aktuální síťové topologie, byla rozšířena o seznam obsahující poslední změny v topologii. Každá změna v topologii je uložena do seznamu posledních změn a následně jsou zavolány Pyretic aplikace, které na základě aktuální topologie a seznamu posledních změn v topologii upraví chování sítě. Poté, co všechny aplikace aktualizují svoje výstupní politiky, je seznam posledních změn vymazán. V případě, že několik změn topologie nastane ve velmi krátky okamžik, bude se v seznamu nacházet větší množství změn.
- Uložení informací o koncových stanicích do globálně dostupného úložiště - Úložiště obsahuje informace o všech připojených zařízeních v rámci sítě. Pro

každé zařízení je uložena MAC adresa, IP adresa, poloha, přihlašovací jméno uživatele a název skupiny.
- Odstranění virtuálních hlaviček - Při použití virtuálních hlaviček kontroler přidává paketům VLAN tagy. Zpracování paketů s VLAN tagem koncovým zařízením není zaručeno, proto by se tagy měly používat pouze mezi přepínači a ne na linkách ke koncovým zařízením. Pyretic neodstraňuje VLAN tagy na linkách ke koncovým zařízením automaticky, proto byl hlavní kód Pyreticu je upraven tak, že není nutné přepisovat každou aplikaci, aby sama odstraňovala VLAN tagy. Poté co jsou politiky z aplikací spojeny a připraveny ke skompilování do pravidel OpenFlow, jsou všechna pravidla upravena tak, že z paketů odeslaných na linky s koncovým zařízením jsou odstraněny VLAN tagy.

Aplikace pro správu identit Nad kontrolerem Pyretic byla vytvořena aplikace *identityManagement*, která implementuje následující položky:

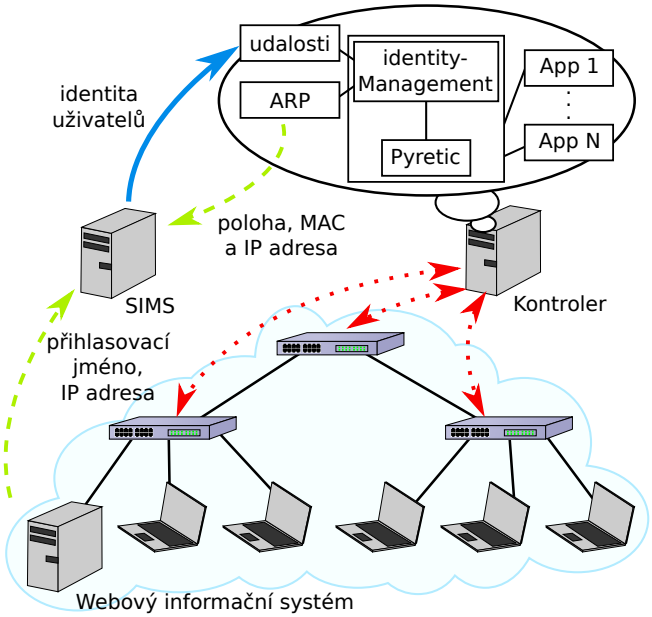
- virtuální hlavička *skupina* - Každý uživatel je součástí právě jedné skupiny uživatelů. Pomocí virtuální hlavičky obsahuje každý paket v síti informaci, do které skupiny patří odesílatel.
- monitorování zpráv ARP - Monitorování zpráv probíhá přeposíláním všech ARP paketů do kontroleru, kde se zjisťuje mapování mezi IP adresou, MAC adresou a polohou zařízení.
- propojení se systémem SIMS - Pomocí rozšíření kontroleru o možnost zpracování externích událostí bylo vytvořeno rozhraní mezi kontrolerem a systémem SIMS. Rozhraním se přenáší informace o identitách uživatelů.
- sdílení znalosti o identitách uživatelů - Aplikace *identityManagement* zpřístupňuje informace o uživatelích, které byly přijaty ze systému SIMS, pomocí úložiště dostupného pro všechny aplikace.

6.1 Schéma systému

Schéma výsledného systému je znázorněna na obrázku 16 a skladá se z:

- *Síťová topologie* - Počítačová síť obsahující síťové prvky a koncová zařízení. Všechen provoz ARP je ze sítě odeslán do kontroleru;
- *Kontroler* - Přijíma správy ARP ze sítě a podle aplikací konfiguruje síťové prvky. Kontroler se skladá z několika dílčích bloků:
  - *Pyretic* - Rozšířený kontroler Pyretic.
  - *identityManagement* - Aplikace běžící nad Nourhbound rozhraním kontroleru, která zajisťuje odeslání identifikátorů MAC adresa, IP adresa a poloha zařízení v síti do sytému SIMS od kterého zároveň přijímá informace o identitách uživatelů.
  - *Aplikace pro řízení sítě* - Vytvořené aplikace pro správu sítě, přičemž pomocí informací z aplikace *identityManagement* mohou k řízení využívat znalost uživatelských identit.

– *SIMS* - Přijímá částečné identity z kontroleru a informačního systému, které následně propojuje a odesílá do aplikace *identityManagement*;
– *Webový informační systém* - Server s webem na který se uživatelé autentifikují a následně po autentizaci jsou jejich přihlasovací jména společne s IP adresou odeslána systému SIMS.



Obrázek 16: Schéma propojení systému SIMS a kontroleru Pyretic pomocí aplikace identityManagement.

6.2 Případy použití

Zbytek této kapitoly popisuje tři případy užití, které mají za cíl ukázat výhody správy sítě s využitím znalosti uživatelských identit. Případy užití jsou zaměřeny na zabezpečení malé firmy. Každý z nich pracuje se skupinami uživatelů místo individuální práce s každým uživatelem zvlášť (místo konfigurace síťové politiky pro uživatelku *Anna*, budou aplikace vytvářet síťové politiky pro uživatele ze skupiny *Management*, do které uživatelka *Anna* patří). Předpokládá se, že více uživatelů uvnitř podnikové sítě sdílí stejnou síťovou politiku. Z hlediska optimalizace, je jednodušší a efektivnější pracovat s mnohem menším množstvím pravidel síťových politik. I když někteří uživatelé vyžadují zvláštní politiku jen pro sebe, je možné vytvořit skupinu obsahující pouze jednoho uživatele.

Tabulka 3 znázorňuje přiřazení zaměstnanců firmy do uživatelských skupin. Uživatelé jsou identifikováni na základě jejich přihlašovacích jmen do firemního informačního systému. V případě, že uživatel zatím není přihlášen, je považován za uživatele *default*, který patří do skupiny *default*.

Přihlasovací jméno	**Uživatelská skupina**
Anna	management
Boris	vývojáři
Cecília	vývojáři

Tabulka 3: Konfigurace přiřazení uživatelů do uživatelských skupin, které bude použito pro další případy užití v této kapitole.

6.3 Firewall chránící síťové služby

Firewall zdrojů filtruje pakety odeslané na předdefinovaný zdroj. Pojmem zdroj je myšleno síťová služba, která je definována IP adresou, typem protokolu a číslem protokolu. Firewall je konfigurován seznamem skupin uživatelů, které mohou přistupovat ke zdrojům. Funkčnost firewallu je rozprostřena mezi všechny síťové přepínače, které zajišťují zahazování paketů. Přepínače zajisťují aby pakety, které nejsou povoleny komunikovat se zdrojem byly zahozeny ještě předtím než k danému zdroji dorazí.

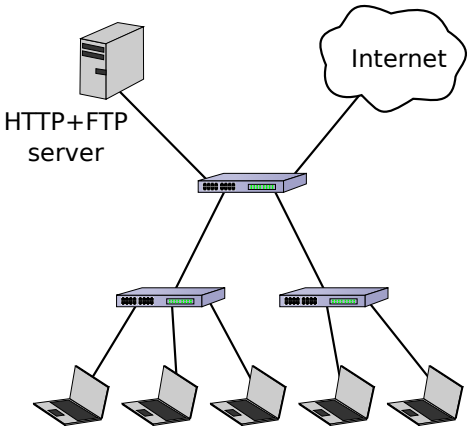
Příklad Společnost má jeden server, na kterém běží dvě služby:

- **HTTP** – port 80, web obsahující stránky wiki, každý uživatel sítě má právo přistupovat k této službě
- **FTP** – port 21, úložiště souborů obsahující osobní údaje o zaměstnancích, jenom zaměstnanci skupiny *management* mají přístup k této službě

Topologie sítě je znázorňena na obrázku 17.

Konfigurace firewallu podle kritérií zabezpečení služeb je znázorněna v tabulce 4. Skládá se z definice zdrojů a seznamu skupin uživatelů, kterým je povoleno přistupovat ke zdroji. Uživatelská skupina * reprezentuje libovolnou uživatelskou skupinu.

Popis řešení Každý zdroj má určený seznam skupin uživatelů, které by s ním měly být schopny komunikovat. Firewall sestavuje seznam uživatelů, kterým není povolen přístup k zdroji tak, že ze seznamu všech skupin odebere skupiny uživatelů, které mají povoleno komunikovat. Aplikace firewall poté zkontroluje všechny porty všech přepínačů v síti, zda v nich není zapojený uživatel patřící



Obrázek 17: Server s dvěmi službami nasazený ve firemní síti.

Zdroj	**Parametry**	**Skupiny**
HTTP	192.168.1.1:TCP:80	*
FTP	192.168.1.1:TCP:21	management

Tabulka 4: Konfigurace Firewallu z obrázku 17 na základě definovaných pravidel.

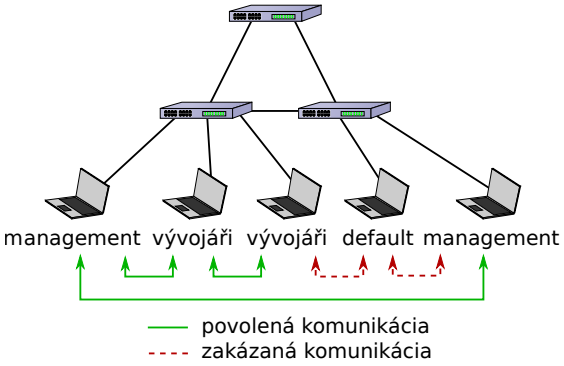
do skupiny, které není dovoleno komunikovat s některým ze zdrojů. Na každý takový přepínač je umístěno pravidlo, které blokuje provoz od uživatele ke zdroji. Provoz ve směru od zdroje k uživateli blokován není, jelikož odesílatelem daného provozu je síťová služba na kterou se daná omezení neaplikují.

6.4 Firewall uživatelů

Každá skupina uživatelů má různé omezení komunikace s jinými skupinami. Firewall uživatelů filtruje pakety odeslané mezi dvěma skupinami uživatelů, kterým není povoleno spolu komunikovat. Funkce firewallu je rozprostřena mezi všechny síťové přepínače v síti.

Příklad Bezpečnostní politika firmy je nastavena tak, že pouze autentifikovaní uživatelé počítačové sítě jsou schopni komunikovat s ostatními uživateli. Autentizovaným zaměstnancům skupin *Management* a *Vývojáři* je dovoleno navzájem libovolně komunikovat. Situace je znázorněna na obrázku 18, kde je zapojeno několik uživatelů.

Konfigurace politiky je znázorněna v tabulce 5. Každý řádek představuje jednu zdrojovou skupinu uživatelů a sloupce představují cílové skupiny. Písmeno x znamená, že uživatelům skupiny z daného řádku je povoleno komunikovat se skupinou z daného sloupce.



Obrázek 18: Firemní síť s uživateli, jejichž právo komunikovat s ostatními uživateli je definováno na základě jejich skupiny.

Data odeslané od	**management**	**vývojáři**	**default**
management	x	x	
vývojáři	x	x	
default			

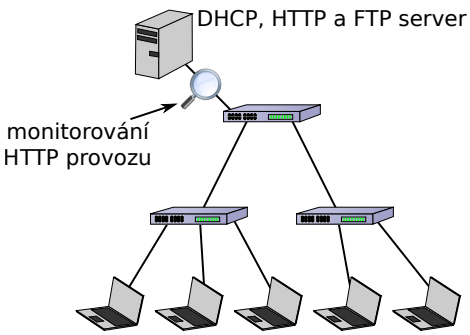
Tabulka 5: Příklad konfigurace bezpečnostní politiky z obrázku 18.

Popis řešení Každá skupina uživatelů má seznam skupin, kterým je schopna posílat pakety. Firewall projde všechny přepínače v síti a nalezne všechny porty, na kterých jsou zapojena koncová zařízení. K nalezeným portům vyhledá seznam skupin, které nejsou oprávněny posílat pakety na daný port. Pro každou skupinu, která nemá právo komunikovat s některým portem, je vytvořeno jedno pravidlo pro blokování všech paketů z dané skupiny na daný port.

6.5 Účtovnání

Pojem účtovámí v tomto případě znamená měření množství přenesených dat ke zdrojům. Bez znalosti uživatelských identit se množství dat počítá podle identifikátoru zařízení, typicky podle IP adresy. Cílem aplikace je výpočet množství přenesených dat pro každou skupinu uživatelů. Se znalostí identit uživatelů, je možné agregovat použití více zařízení v případě, že jeden uživatel používá více zařízení.

Příklad Společnost má zájem o monitorování využití serveru HTTP uživateli skupiny *vývojáři*. Na základě informací o přenesených datech chce management společnosti vyhodnocovat úroveň produktivity vývojářů. Příklad je zobrazen na obrázku 19.



Obrázek 19: Podniková síť s monitorovaným HTTP serverem.

Konfigurace se skládá z definování zdrojů, které je potřebné monitorovat, a seznamu skupin, pro které má být monitorování aplikováno. Definice zdrojů je stejná jako v případě užití Firewall zdrojů.

Zdroj	**Parametre**	**Skupiny uživatelů**
HTTP	192.168.1.1:TCP:80	vývojáři

Tabulka 6: Příklad konfigurace politiky účtování z obrázku 19.

Popis řešení Aplikace vyhledá port, na kterém je zapojený zdroj, a vytvoří dvě pravidla. Obě pravidla kromě toho, že složí na sběr statistik, přeposílají data na fyzický výstupní port. Jedno pravidlo je pro příchozí a druhé pro odchozí provoz ze zdroje. Kontroler jednou za 10 sekund shromáždí statistiky z vygenerovaných pravidel. Statistiky jsou ukládány do CSV souborů.

7 Závěr

Cílem této technické zprávy bylo zdokumentovat hlavní výsledek činnosti skupiny pro softwarově definované sítě působící v rámci projektu *Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace*. Softwarově definované sítě jsou nová architektura počítačových sítí, ve které je řídící část oddělena od datové části. Řídící části zařízení jsou centralizovány v kontroleru, který pomocí OpenFlow posílá pokyny jednotlivým síťovým zařízením (přepínačům). Nad kontrolerem je možné vytvářet další aplikace, které ovlivňují chování sítě. Koncept softwarově definovaných sítí je podrobně popsán v kapitole 2.

Kapitola 3 definuje pojmy identita, částečná identita, identifikátor a vztahy mezi nimi. Identifikátorem rozumíme například IP adresu, MAC adresu nebo

e-mailovou adresu. Spojením identifikátorů pak vzikají částečné identity, jejichž spojením získáme kompletní pohled na identity uživatelů a zařízení. Tato práce se zaměřuje především na identitu uživatele a její využití v řízení sítí. V rámci projektu Sec6Net byl již dříve vytvořen systém pro zákonné odposlechy SLIS, který obsahuje systém pro správu identit SIMS. Důležité části obou programů jsou v kapitole také uvedeny.

V rámci projektu byly vytvořeny dva prototypy, které demonstrují výhody propojení softwarově definovaných sítí se systémem pro správu identit:

- *Rozšíření systému pro zákonné odposlechy* tak, aby bylo možné duplikovat zájmové pakety a odesílat je na předem určené zařízení v síti. Na sběrném zařízení pak může probíhat analýza, rekonstrukce, vizualizace a další zpracování dat. Implementace využívá kontroler OpenDaylight, který má velké zastoupení v komerční sféře (je podporován firmami Cisco, Dell, HP a mnoha dalšími). Podrobnosti jsou uvedeny v kapitole 5. Pro systém SLIS byla navržena a implementována následující rozšíření:
  - Modul pro IRI-IIF, který je určen k získávání částečné identity koncových zařízení a uživatelů. Modul se periodicky dotazuje kontroleru OpenDaylight na topologii sítě a informace o částečné identitě koncových zařízení zasílá IRI-IIF.
  - Dynamická rekonfigurace CC-IIF sond a OpenFlow přepínačů. Jedná se především o vylepšení implementace CCTF, která nyní rozlišuje jednotlivé CC-IIF sondy podle jejich pozice v topologii. Na základě těchto informací systém vytvoří grafovou reprezentaci topologie a zvýší váhu hran, které používá OpenDaylight pro zasílání neodposlouchávaných paketů. Při vložení odposlechu se pak vybere vhodná sonda. Vybírá se především podle vzdálenosti a zároveň se provádí jednoduché vyvažování zátěže, aby se předešlo zahlcení jedné sondy. Váhy hran je možné specifikovat také manuálně v konfiguračním souboru. V případě, že váha hrany bude nastavena na hodnotu větší než 1000, použije se pouze v případě, že neexistuje jiná cesta k sondě.
  - *SDN-tap* [13] je samostatný program pro zachytávání dat, který lze spouštět bez systému pro zákonné odposlechy. Tento nástroj obsahuje kompletní funkcionalitu dynamické rekonfigurace OpenFlow přepínačů. Narozdíl od rozšíření systému pro zákonné odposlechy, kde se nachází správa identit, lze zájmové pakety zduplikovat, označit a přeposílat pouze na základě IP adresy, trojice nebo pětice.
- *Řízení SDN podle identit* [18] rozšiřuje možnosti řízení SDN sítí o znalost identit uživatelů. Takto rozšířené řízení umožňuje administrátorovi vykonávat správu sítě na základě identity uživatelů používajících připojené zařízení, což správu sítě zjednodušuje a zároveň snižuje riziko chybné konfigurace.
  Řešení spočívalo v úpravě kontroleru Pyretic, vytvoření rozhraní mezi systémem SIMS a kontrolerem Pyretic, a vytvoření rozšíření pro kontroler. Toto rozšíření spravuje identity získané ze systému SIMS a zjištěné informace poskytuje dalším aplikacím vytvořeným nad kontrolerem. Součástí programu jsou čtyři aplikace implementující čtyři různé případy užití týkající se filtrování, směrování a účtování. Kapitola 6 popisuje řešení pomocí propojení

SDN kontroleru se systémem pro správu uživatelských identit SIMS. V kapitole jsou podrobně popsány také uvedené příklady užití, které demonstrují funkčnost řešení.

Uvedené prototypy byly otestovány v laboratorním prostředí. Možným navazujícím výzkumem by mohlo být například vytvoření dalších případů užití (kvalita služeb, mobilita).

Reference

1. Baker, F.; Foster, B.; Sharp, C.: *Cisco Architecture for Lawful Intercept in IP Networks*. IETF, 2004, rFC 3924 (Informational).
2. Betts, M.; Davis, N.; Dolin, R.; aj.: SDN architecture. Technická zpráva, Open Networking Foundation, 2014, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf.
3. Chao, H. J.; Liu, B.: *High performance switches and routers*. John Wiley & Sons, 2013.
4. Cisco Systems: Cisco Medianet Architecture. 2014, http://www.cisco.com/web/solutions/trends/medianet.
5. ETSI: *ETSI TR 101 943: Telecommunications security; Lawful Interception (LI); Concepts of Interception in a generic Network Architecture*. European Telecommunications Standards Institute, 2001, version 1.1.1.
6. ETSI: *ETSI TR 101 944: Telecommunications security; Lawful Interception (LI); Issues on IP Interception*. European Telecommunications Standards Institute, 2001, version 1.1.2.
7. ETSI: *ETSI TR 102 528: Lawful Interception (LI); Interception domain Architecture for IP networks*. European Telecommunications Standards Institute, 2006, version 1.1.1.
8. ETSI: *ETSI TR 101 331: Lawful Interception (LI); Requirements of Law Enforcement Agencies*. European Telecommunications Standards Institute, 2009, version 1.3.1.
9. ETSI: *ETSI TR 102 232-3: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services*. European Telecommunications Standards Institute, 2009, version 2.2.1.
10. ETSI: *ETSI TR 101 671: Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic*. European Telecommunications Standards Institute, 2010, version 3.6.1.
11. ETSI: *ETSI TR 102 232-1: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery*. European Telecommunications Standards Institute, 2010, version 2.5.1.
12. ETSI: *ETSI TR 102 232-4: Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services*. European Telecommunications Standards Institute, 2010, version 2.3.1.

13. Franková, B.: SDN-tap. 2015, https://www.fit.vutbr.cz/$\sim$ifrankova/prods.php?id=437.
14. Franková, B.: Zákonné odposlechy v SDN. 2015, diplomová práce, Vysoké učení technické v Brně.
15. Frenandez, M. P.: Comparing OpenFlow Controller Paradigms Scalability: Reactive and Proactive. In *AINA '13 Proceedings of the 2013 IEEE 27th International Conference on Advanced Information Networking and Applications*, IEEE, 2013, s. 1009–1016.
16. Ganti, V.; Lubsey, V.; Shekhar, M.; aj.: Open Data Center Alliance: Software-Defined Networking Rev. 1.0. 2013.
17. Holkovič, M.: SDN Controlled According to User Identity. 2015, diplomová práce, Vysoké učení technické v Brně (psáno v anglickém jazyce).
18. Holkovič, M.: Řízení SDN podle identit – SDNIM. 2015, https://www.fit.vutbr.cz/$\sim$iholkovic/prods.php?id=436.
19. Jain, S.; Kumar, A.; Mandal, S.; aj.: B4: Experience with a Globally-deployed Software Defined Wan. *Computer Communication Review*, ročník 43, č. 4, 2013: s. 3–14, ISSN 0146-4833.
20. Kaur, S.; Singh, J.; Ghumman, N. S.: Network Programmability Using POX Controller.
21. Kaur, S.; Singh, J.; Ghumman, N. S.: Network Programmability Using POX Controller. In *ICCCS International Conference on Communication, Computing & Systems*, IEEE, 2014, s. 134–138.
22. McKeown, N.; Anderson, T.; Balakrishnan, H.; aj.: OpenFlow: enabling innovation in campus networks. *SIGCOMM Computer Communication Review*, ročník 38, č. 2, 2008: s. 69–74, ISSN 0146-4833.
23. Medved, J.; Varga, R.; Tkacik, A.; aj.: Opendaylight: Towards a model-driven sdn controller architecture. In *2014 IEEE 15th International Symposium on*, IEEE, 2014, s. 1–6.
24. Metzler, J.: What is SDN? And Why Should I Care? [online]. 2012, https://www.eiseverywhere.com/file_uploads/\458f97398bb66838e66ecb90c7a41eb7_Jim_Metzler.pdf.
25. Monsanto, C.; Reich, J.; Foster, N.; aj.: Composing Software Defined Networks. In *NSDI*, 2013, s. 1–13.
26. Nadeau, T.; Grey, K.: *SDN: Software Defined Networks*. O'Reilly Media, 2013.
27. Open Networking Foundation: Software-Defined Networking: The New Norm for Networks [online]. 2012, https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf.
28. Pfitzmann, A.; Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Technická zpráva, 2010, version 0.34, Available online at https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.
29. Polčák, L.: Challenges in Identification in Future Computer Networks. In *ICETE 2014 Doctoral Consortium*, SciTePress - Science and Technology Publications, 2014, s. 15–24.

30. Polčák, L.; Hranický, R.; Martínek, T.: On Identities in Modern Networks. *The Journal of Digital Forensics, Security and Law*, ročník 2014, č. 2, 2014: s. 9–22, ISSN 1558-7215.
31. Polčák, L.; Martínek, T.; Hranický, R.; aj.: Zákonné odposlechy v moderních sítích - Shrnutí výsledků skupiny pro zákonné odposlechy projektu Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace. Technická zpráva, 2014, faculty of Information Technology Brno University of Technology, FIT-TR-2014-07, Brno.
32. Rabaey, J. M.; Potkonjak, M.; Koushanfar, F.; aj.: Challenges and Opportunities in Broadband and Wireless Communication Designs. In *ICCAD-2000. IEEE/ACM International Conference on Computer Aided Design*, 2000, s. 76–82.