Acta Informatica Pragensia
2(1), 2013, 101–121, DOI: 10.18267/j.aip.17
Online: aip.vse.cz

Sekce / Section:
Recenzované stati / Peer-reviewed papers

Optimalizácia monitorovania sieťovej prevádzky

František Jakab[1], Adrián Pekár[1], Peter Feciľak[1], Miroslav Michalko[1]

[1] Katedra počítačov a informatiky, Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach, Letná 9, 04001 Košice, Slovenská republika

{frantisek.jakab, adrian.pekar, peter.fecilak, miroslav.michalko}@tuke.sk

Abstrakt: Tento príspevok sa zaoberá otvorenými problémami vyskytujúcimi sa pri pasívnom prístupe merania sieťových charakteristík. Opisuje najpoužívanejšie prístupy merania sieťových parametrov ako aj charakteristiky, ktoré sa pri monitorovaní najčastejšie sledujú. Hlavným cieľom tohto príspevku je predstavenie konceptuálneho návrhu riešenia opísaných problémov, ktorý by sa mal docieliť automatizovaným prispôsobením exportu záznamov o tokoch prevádzky k aktuálnemu stavu siete.

Klíčová slova: pasívne meranie, aktívne meranie, monitorovanie sieťovej prevádzky, tok, IPFIX

Title: Optimization of Network Traffic Monitoring

Abstract: This paper deals with problems which occur in passive measurement of network characteristics. It describes the most used approaches of measuring network parameters as well as those properties, which are most frequently monitored. The main aim of this paper is to introduce a conceptual design of a solution for the discussed problems, which should be achieved by automated adapting of flow records export of traffic to the actual state of the network.

Keywords: Passive measurement, active measurement, network traffic monitoring, flow, IPFIX

1 ÚVOD

Hlavným prostriedkom komunikačnej a informačnej infraštruktúry počas posledných rokov sa stal internet. Komunikačné siete boli pôvodne navrhnuté na nezávislé prenášanie rôznych typov údajov, t.j. rádio pre audio, televízor pre video a pod. Od jeho objavenia počet pripojených používateľov a počítačov výrazne rastie, čo vedie k neustálemu zvyšovaniu zložitosti a náročnosti sieťovej prevádzky. V dôsledku veľkého množstva používaných multimediálnych a distribuovaných aplikácií boli vyvinuté konvergované siete. Na rozdiel od klasických komunikačných sietí sú tie dnešné, konvergované, schopné súčasného prenášania údajov rôznych typov, akými sú video, hlas a dáta.

Jednou z najdôležitejších výziev konvergovaných sietí je zvýšená obťažnosť ich riadenia. Na zabezpečenie výkonnosti, bezpečnosti a spoľahlivosti týchto sietí sa využívajú rôzne merania a analýzy, ktoré sa kvôli nárastu požiadaviek sieťovo-orientovaných aplikácií používajú stále vo väčšej a väčšej miere. Napriek značnému úsiliu vedecko-výskumnej komunity, veľa problémov v oblasti monitorovania sieťových charakteristík zostáva otvorených.

V nasledujúcich kapitolách bude predstavená stručná motivácia pre monitorovanie sietí a ich vlastností. Následne budú opísané najdôležitejšie charakteristiky, ktorých meranie je z pohľadu monitorovania užitočné. Predmetom záujmu bude aj definícia a prehľad rôznych prístupov monitorovania a merania prevádzkových charakteristík. V pokračovaní sa predstavia otvorené problémy, ktoré sa pri monitorovaní prevádzkových charakteristík vyskytujú, ako aj výsledky experimentu vykonaného pre overenie prítomnosti vybraných problémov. Záverečná kapitola poskytuje konceptuálny návrh metódy pre vyriešenie opísaných problémov.

2 MOTIVÁCIA

Počítačové siete sa stali neoddeliteľnou súčasťou každodenného života. Využívajú sa pre osobnú komunikáciu, zdieľanie údajov, verejné šírenie správ, prenášanie privátnych údajov, kolaboráciu, telefonovanie, podnikanie, vzdelávanie, nakupovanie, zábavu, socializáciu, atď. Zdrojom týchto aktivít sú v drvivej väčšine používatelia a aplikácie, ktoré používajú. Výsledkom je obrovský objem údajov, ktoré tvoria prevádzku počítačových sietí. Pri prevádzke s takou širokou a rozmanitou charakteristikou, dôležitým aspektom počas návrhu, správy a optimalizácie dnešných komplexných a vysoko-rýchlostných počítačových sietí je meranie a monitorovanie ich rôznych vlastností. Meranie a monitorovanie sietí poskytuje významné informácie pre používateľov, poskytovateľov služieb (ISP), výskumníkov alebo iných členov verejnej a vedeckej komunity. Na základe týchto informácií je následne možné zabezpečiť kvalitu, výkonnosť a plnohodnotnú funkčnosť počítačových sietí, ich služieb a aplikácií.

Pre monitorovanie sieťovej prevádzky existuje aj veľa ďalších dôvodov. Charakteristiky vyťaženia siete výrazne ovplyvňujú sieťové komponenty a protokoly. Výkonnosť smerovačov napríklad podstatne závisí od štatistických vlastností prevádzky a rozdelení veľkosti paketu. Ďalej môže správna charakteristika topológie značne prispieť pri identifikácii miest potenciálneho výskytu výkonnostných problémov.

Meranie sieťových charakteristík je dôležité aj v prípade vedecko-výskumnej činnosti. Väčšina výskumov sa zameriava na získanie znalostí o dynamike sietí. Pochopenie dynamiky sieťovej prevádzky je nevyhnutné z pohľadu budovania rôznych sieťových modelov pre účely riešenia problémov týkajúcich sa vyhodnocovania, výkonnosti, zabezpečenia alebo optimalizácie sietí [6]. Avšak zhromažďovanie reprezentatívneho súboru nameraných dát nie je jednoduchý proces. S ohľadom na túto skutočnosť, autori v príspevku [5] poskytujú detailné vysvetlenie problémov týkajúcich sa simulácie internetu, z ktorých sa niektoré vyskytujú aj v prípade merania sieťovej prevádzky. Tieto problémy sú napríklad veľkosť a heterogénna povaha sieťovej prevádzky, neustále sa zvyšujúci počet sieťovo-orientovaných aplikácií, rýchly a nepredvídateľný spôsob zmien v sieťach, veľkosť a aktuálnosť zhromaždených vzorov alebo manipulácia s odľahlými hodnotami meracích procesov.

Aj keď počítačové siete patria medzi neustále sa vyvíjajúce oblasti informačných technológií, počet nových pripojení — či už v podobe zariadení alebo používateľov — a prudký nárast objemu, ako aj obsahu prevádzky robia ich monitorovanie čoraz zložitejším. Napriek tomu, že súčasné siete obsahujú množstvo sofistikovaných nástrojov pre detekciu a signalizáciu rôznych chýb a porúch, stále existuje skupina takých udalostí, ktoré väčšinou zostanú neodhalené [2]. Tieto udalosti sa nazývajú tiché poruchy (silent failures), medzi ktoré, okrem iných, patria najmä konfiguračné chyby (nesprávne nastavenia ACL), smerovacie anomálie (smerovacie slučky) alebo nečakané drobné závady v smerovačoch (neschopnosť smerovača detegovať svoju internú chybu). Všetky tieto udalosti môžu viesť k nepriaznivému ovplyvneniu výkonnosti počítačových sietí. Nedostatok schopnosti zachytávania týchto javov je evidentným dôkazom potreby vylepšovania monitorovacích a meracích mechanizmov.

3 MONITOROVANIE SIEŤOVEJ PREVÁDZKY

V terminológií počítačových sietí spolu s pojmom ‘monitorovanie’ často vystupuje aj ‘meranie’. V niektorých prípadoch sa o meraní dokonca hovorí, akoby bolo neoddeliteľnou súčasťou monitorovania [4]. Faktom je, že aj meranie, aj monitorovanie predstavuje rozsiahlu oblasť počítačových sietí, pričom spolu tvoria nenahraditeľný pilier mechanizmu, ktorý za dnešnými vysokorýchlostnými počítačovými sieťami stojí. Súvislosť medzi monitorovaním a meraním je veľmi jednoduchá. Bez merania charakteristík sieťovej prevádzky — a následného vyhodnotenia nameraných dát — by nebolo možné uskutočniť monitorovanie sietí. Bez monitorovania by následne nebolo možné vykonať úlohy akými sú kontrola, správa, zabezpečenie alebo optimalizácia počítačových sietí. Kým v prípade merania alebo monitorovania sietí sú najdôležitejšími entitami sledované prevádzkové charakteristiky, v prípade vyhodnocovania majú najvýznamnejšiu úlohu aparáty zvolené z oblasti matematických vied [4]. Preto pri monitorovaní a s ním súvisiacimi úkonmi je potrebné im venovať výnimočnú pozornosť.

Pojem monitorovanie siete slúži na opis činnosti takého systému, ktorý neprerušene sleduje celú sieť a jej prevádzku. Hlavnou charakteristikou takého systému je, že v prípade objavenia chýb, výpadkov alebo iných nezvyčajných javov okamžite upozorní (napr. prostredníctvom e-mailu) správcu siete. Okrem nepretržitého sledovania sa monitorovanie využíva aj v správe sieťovej prevádzky, rôznych prístupov, komponentov (uzlov) a pod. Tieto, už aj tak komplexné úkony, ďalej komplikuje

topologická (fyzické prepojenie všetkých komponentov) a výpočtová (smerovanie a riadiace úlohy sieťových komponentov) zložitosť dnešných konvergovaných sietí. Nasadenie monitorovania nie je obmedzené typom siete, t.j. prakticky sa môže sledovať ľubovoľná sieť, od lokálnych (LAN) alebo bezdrôtových, cez virtuálne privátne (VPN), až k metropolitným (MAN) alebo rozľahlým (WAN) sieťam. Monitorovanie sa neobmedzuje ani na jednotlivé sieťové komponenty (prepínače, smerovače, servery, IP telefóny, atď.). Monitorovanie siete sa vykonáva pomocou softvérových aplikácií a nástrojov. Pomocou týchto softvérov sa môžu jednoducho určiť metriky súvisiace s výkonom sietí, identifikovať jednotlivé aktivity a ich vplyv na softvérové a hardvérové prostriedky. Monitorovanie je nenahraditeľným nástrojom aj v detekcii a predchádzaní bezpečnostných hrozieb.

Ako bolo na začiatku spomenuté, monitorovanie počítačových sietí je podmienené zberom údajov. Táto činnosť sa označuje ako meranie charakteristík počítačových sietí a spolu s vyhodnocovaním nameraných hodnôt tvoria najdôležitejšie súčasti monitorovania.

4 MERANIE PREVÁDZKOVÝCH CHARAKTERISTÍK

Pri meraní prevádzkových parametrov sietí sa rozlišujú tri hlavné prístupy: aktívne, pasívne a kombinované. V súčasnosti sú najpoužívanejšie aktívne a pasívne prístupy merania. Obe poskytujú iné typy výsledkov, pričom aj aktívne, aj pasívne meranie sa zvyčajne používa v odlišných meracích zostavách a pre rôzne účely.

Okrem týchto prístupov, v poslednej dobe sa rozšírilo aj takzvané kombinované alebo semi-aktívne meranie, ktoré pri zisťovanie sieťových charakteristík zlučuje kladné vlastnosti aktívneho a pasívneho prístupu merania.

4.1 AKTÍVNE MERANIE

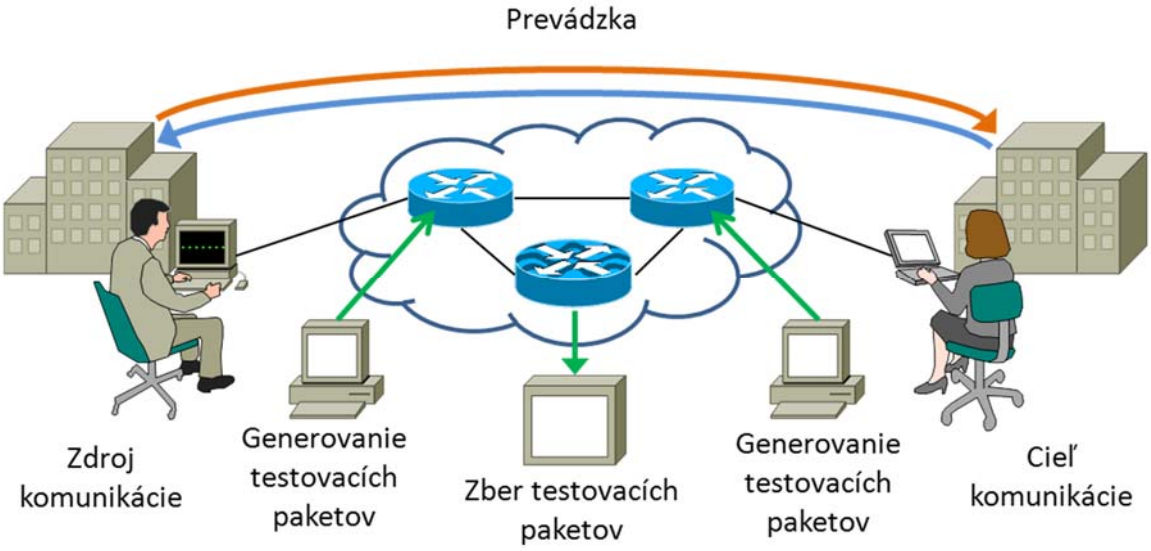
Aktívny prístup merania parametrov sietí je založený na schopnosti vložiť testovacie pakety (sondy) do monitorovanej siete. Sledovaním a následným meraním týchto paketov je možné dostať operatívnu viditeľnosť siete. Príklad aktívneho prístupu merania je uvedený na Obrázku 1. Obrázok opisuje situáciu, keď meranie charakteristík a ich export sa vykonáva z miesta, ktoré je odlišné od zhromaždovacieho bodu. Takáto situácia sa často vyskytuje v prípade merania charakteristík o IP tokoch sieťovej prevádzky s dvoma a viacerými meracími/exportovacími bodmi.

V niektorých prípadoch sa testovacie pakety posielajú priamo k serverom alebo aplikáciám. Takýmto spôsobom je možné dostať prehľad stavu služieb v sieti. Z toho je možné odvodiť nasledujúce dve vlastnosti:

- aktívne meranie si vyžaduje generovanie dodatočnej prevádzky,
- prevádzka a jej parametre sú umelé.

Objem a iné charakteristiky generovanej prevádzky sú ľubovoľne prispôsobiteľné, pričom pre získanie zmysluplných výsledkov stačí aj relatívne malý objem prevádzky. Aktívne meranie poskytuje explicitnú kontrolu generovania paketov pre rôzne meracie scenáre. Okrem iných zahŕňa kontrolu nad vlastnosťou generovania prevádzky, technikami vzorkovania, veľkosťou a typom paketov, trás,

funkcií, atď. Jedným nežiadaným vedľajším účinkom aktívnych meraní môže byť zvýšenie záťaže siete, ktoré môže viesť k ovplyvneniu alebo úplnému znehodnoteniu výsledkov meraní. Ďalšou nevýhodou aktívneho merania je, že poskytuje málo informácií o danom meracom bode. Namiesto toho ale poskytuje rôzne typy charakteristík o spojení medzi dvoma uzlami.



Obr. 1. Architektúra aktívneho prístupu merania.

Väčšinou sú to výkonnostné charakteristiky, ako napríklad:

- doba obehu paketu (RTT),
- priemerná stratovosť paketov,
- šírka pásma spojenia,
- priepustnosť paketov.

V niektorých prípadoch môžu aktívne merania poskytnúť informácie aj o časoch asymetrického oneskorenia alebo zmien v cestách smerovania medzi uzlami. Tieto charakteristiky si ale vyžadujú rozšírenie meracej zostavy o ďalšie podporné mechanizmy alebo dodatočnú kompenzáciu hodnôt.

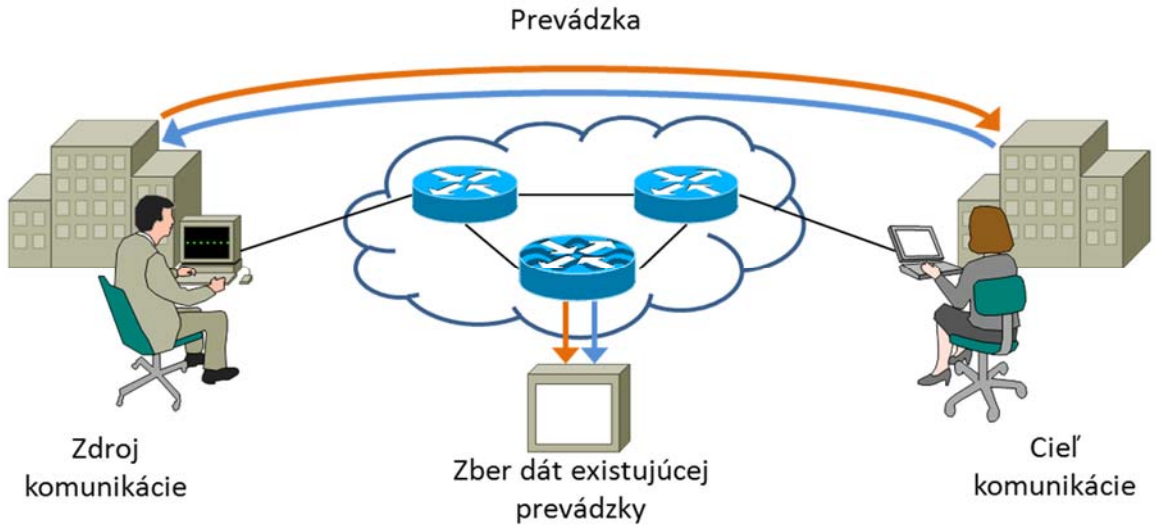
4.2 PASÍVNE MERANIE

Pasívny prístup merania predstavuje taký proces, ktorý si nevyžaduje generovanie dodatočnej alebo zmenu existujúcej prevádzky. Meraná prevádzka je teda generovaná len pripojenými používateľmi a aplikáciami siete. Príklad pasívneho prístupu merania je uvedený na Obrázku 2. Pasívne meranie sa spravidla vykonáva nasledujúcimi prostriedkami:

- Sieťové komponenty (smerovače, prepínače, koncové zariadenia) so zabudovaným mechanizmov zachytávania informácií o prevádzke. Takéto mechanizmy predstavujú napríklad protokoly NetFlow [3], SNMP [1] alebo RMON [21].
- Softvérové nástroje (BEEM [9], Wireshark [24], atď.) určené pre zber a spracovanie informácií o údajoch v sietí.

Zhromažďovanie nameraných údajov od týchto prostriedkov sa vykonáva periodicky. Na základe vyhodnotenia získaných informácií sa určujú charakteristiky siete (výkonnosť, stav a pod).

Výhodou pasívneho prístupu je meranie reálnej prevádzky. Ďalšou výhodou je, že na rozdiel od aktívneho merania, proces samotného pasívneho merania nezvyšuje zaťaženie prevádzky siete.



Obr. 2. Architektúra pasívneho prístupu merania.

Keďže spomenuté dotazovanie a zhromažďovanie nameraných údajov môže priniesť isté zvýšenie prevádzky (najmä v prípade zachytávania informácií o každom pakete), táto výhoda je len relatívna. Riešenie predstavuje vyhradenie osobitných liniek pre merané a namerané údaje. Takýmto spôsobom sa informácie súvisiace s pasívnym meraním nebudú miešať s reálnou prevádzkou, čo v konečnom dôsledku vedie k neovplyvneným výsledkom merania prevádzkových parametrov. Vzhľadom na to, že sa v niektorom prípade sleduje každý paket v sieti, pasívne meranie môže čeliť problémom týkajúcich sa súkromia alebo bezpečnosti informácií [18, 19].

Na rozdiel od aktívneho merania, pasívne meranie poskytuje detailný súbor informácií o meracom bode siete. Tieto informácie sú napríklad:

- z akých typov údajov, služieb alebo protokolov pozostáva prevádzka (traffic mix),
- intenzita paketov,
- časovanie paketov,
- oneskorenie paketov.

Okrem vlastností o reálnej prevádzke, pasívne meranie môže poskytnúť informácie aj o infraštruktúre siete. Takýto typ pasívneho merania pozostáva zo zachytávania a analýzy riadiacej roviny prevádzky, napríklad smerovača. Pasívne merania infraštruktúry umožňujú napríklad protokoly BGP [22] alebo OSPF [14].

4.3 KOMBINOVANÉ MERANIE

Meranie infraštruktúrnych alebo topologických charakteristík je často účinnejšie s kombináciou rôznych prístupov meraní. Napríklad nevýhodou aktívneho merania je veľký počet testovacích paketov pre zistenie už aj relatívne jednoduchých charakteristík (mapovanie jediného autonómneho systému). Množstvo testovacích paketov je možné redukovať, napríklad, pasívnym meraním. V tomto prípade, kombináciou aktívneho a pasívneho merania sa obmedzeniam aktívneho merania dá jednoducho vyhnúť. Použitím pohľadov protokolu BGP (BGP views) je možné napríklad identifikovať obmedzenú množinu adries, ktoré pravdepodobne patria do skúmaného autonómneho systému [16].

Medzi kombinované typy meraní patria aj semi-aktívne, ktoré pre zisťovanie sieťových charakteristík rozširuje existujúcu prevádzku o ďalšie informácie. Takýmito informáciami sú časová známka alebo jedinečný identifikátor paketu. Jednou z nevýhod semi-aktívnych meraní je modifikácia paketov, ktorá môže ovplyvniť výsledky meraní tým, že označené pakety môžu byť ďalej spracovávané. Semi-aktívne merania sú náročnejšie na výkon meracieho bodu.

Kombináciou rôznych druhov meraní je možné skvalitniť priebeh a presnosť ich výsledkov. Vo všeobecnosti pre zlúčené merania platí, že využívajú len pozitívne aspekty, ktoré v sebe zahŕňajú.

5 CHARAKTERISTIKY POČÍTAČOVÝCH SIETÍ

Počítačové siete charakterizuje veľa rôznych vlastností, ktoré je z pohľadu monitorovania sieťovej prevádzky dôležité merať. Niektoré z týchto vlastností sa týkajú fyzických komponentov, iné samotnej prevádzky počítačových sietí. Významnú skupinu predstavujú aj tie charakteristiky, ktoré vznikajú pri interakcii fyzických komponentov a prevádzky. Ďalšou dôležitou vlastnosťou počítačových sietí sú časové charakteristiky. Čas predstavuje jednu zo základných entít, ktorá má dôležitú úlohu v prípade takmer každého úkonu súvisiaceho s monitorovaním sietí.

5.1 VLASTNOSTI FYZICKÝCH KOMPONENTOV

Prvú skupinu vlastností infraštruktúry predstavujú charakteristiky fyzických komponentov. Fyzické komponenty tvoria základné prvky počítačových sietí, medzi ktoré okrem iných patria:

- **Linky** – V prípade liniek medzi zaujímavé parametre na meranie patria propagačné oneskorenie alebo kapacita liniek. Propagačné oneskorenie predstavuje potrebný čas signálu, aby prešiel cez linku. Kapacita linky predstavuje maximálne dosiahnutú intenzitu prenášania údajov.
- **Smerovače** – Smerovače charakterizuje tiež niekoľko vlastností. Zo statického hľadiska zaujímavými vlastnosťami smerovača sú IP adresy rozhraní, geologická poloha, typ smerovača, podporované protokoly. Z dynamického hľadiska je možné, napríklad merať čas potrebný na reakciu ICMP správy alebo čas potrebný na doručenie paketu.
- **Bezdrôtové zariadenia** – Meranie bezdrôtových komponentov sa väčšinou zameriava na silu signálu, intenzitu údajov, úroveň pokrytia, chybovosť alebo informácie týkajúce sa relácie (session). V prípade kombinácií bezdrôtových a bežných zariadení, zaujímavými vlastnosťami

na meranie predstavujú metriky, ako napríklad kapacita linky, dostupná šírka pásma, identifikácia úzkych profilov (bottleneck), atď.

5.2 PREVÁDZKOVÉ CHARAKTERISTIKY POČÍTAČOVÝCH SIETÍ

Dnešné počítačové siete sú schopné prenášať veľké množstvo údajov. Tieto údaje je možné považovať za určitú kolekciu paketov alebo zbierku bajtov, prostredníctvom ktorých sa definuje prevádzka počítačových sietí. Prevádzka sa zvyčajne vzťahuje na všetky druhy prenášaných údajov (video, hlas, dáta, riadiace správy, atď.) za daný časový okamih, avšak v niektorom prípade sa môže obmedziť len na určité prenosy, správy, záznamy alebo vybranú skupinu používateľov.

Častou požiadavkou pri monitorovaní sieťovej prevádzky je zachytávanie časových charakteristík. Presnosť nameraných vlastností, akými sú, napríklad, doba obehu (RTT), oneskorenie alebo výkonnosť sieťových zariadení značne závisia od meraní časových charakteristík. Kedže jednotlivé sieťové zariadenia sú od seba po sieti často rozptýlené do značnej vzdialenosti, získavanie presných informácií o čase môže byť náročnou úlohou. Najviac problémov sa týka presnosti hodín, na základe ktorých sa časové charakteristiky určujú [7]. Paradoxne, pripúšťajúc existenciu presných hodín, vzdialenosť medzi zariadeniami môže spôsobiť také komunikačné oneskorenie, ktoré môže mať negatívny vplyv na výsledky meraní časových charakteristík.

Nakoľko výsledky sledovaných charakteristík môžu mať presnosť z výrazne odlišných časových rozsahov, metódy merania a analýzy sa môžu značne líšiť. Napríklad pre výkonnostnú analýzu zvyčajná presnosť je od zopár mikrosekúnd do desiatok minút a pre sieťové inžinierstvo od niekoľko minút do niekoľko mesiacov. Za predpokladu, že každé meranie charakterizuje čas začatia a ukončenia, teda časový rozsah, všeobecne platí, že merania v malých časových rozsahoch, t.j. v nano-sekundových presnostiach sú oveľa náročnejšie ako merania vo väčších časových intervaloch, t.j. v sekundových alebo minútových presnostiach.

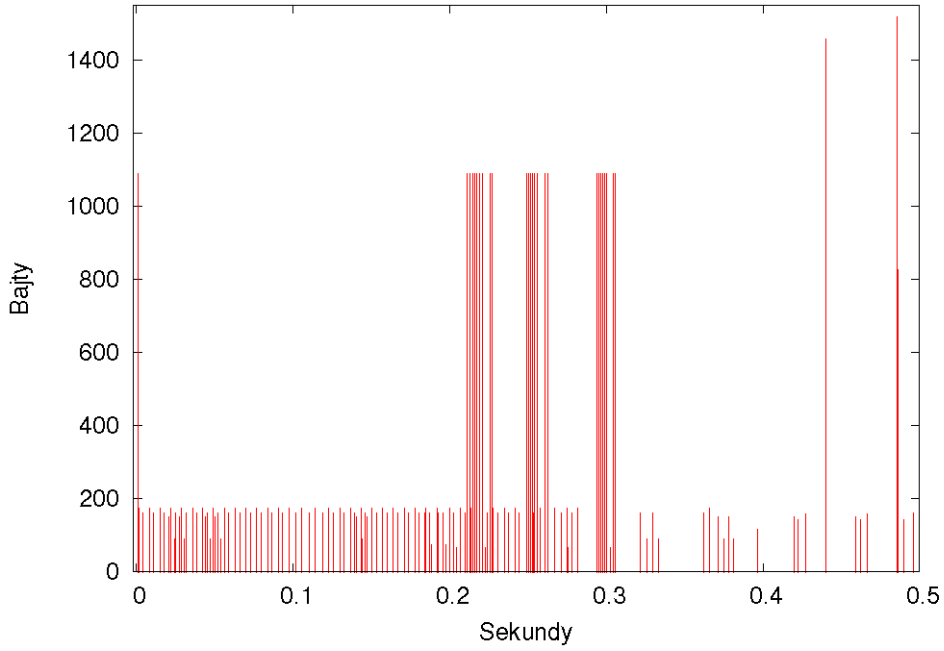
5.2.1 PAKETY

Ako bolo vyššie uvedené, prevádzka sa zvyčajne definuje (na úrovni protokolu IP) ako zbierka paketov za určitý časový okamih. Na spojeniach počítačových sietí nepodporujúcich pakety (napríklad tradičné dvojbodové (Point-to-Point) telekomunikačné linky) je možné prevádzku považovať za kolekciu bajtov, znakov alebo bitov. Z toho dôvodu sa pri reprezentácii sledovanej sieťovej prevádzky najčastejšie využívajú vlastnosti práve týchto dvoch základných prvkov.

Najjednoduchšia metóda reprezentácie nameranej prevádzky predstavuje jej sumarizáciu na základe nejakej vlastnosti alebo charakteristiky. Jeden spôsob sumarizácie obdržanej prevádzky predstavujú stochastické modely [4, 23]. Ak uvažujeme len tie časy, keď paket prišiel na pozorovací bod, t.j. $\{A_n, n = 0, 1, \dots\}$, potom výsledný súbor takýchto časov môže byť vyjadrený ako model príchodového procesu (arrival process). V takomto prípade sumarizácia príchodového procesu pozostáva z charakteristiky rozdelenia intervalov, t.j. distribučné vlastnosti súboru $\{I_n, n = 1, 2, \dots\}$, kde $I_n \equiv A_n - A_{n-1}$. Príklad takého modelu je uvedený na Obrázku 3, kde x-ová os predstavuje príchody jednotlivých paketov (A_n) a y-ová os reprezentuje veľkosť týchto paketov v čase ($size(t)$).

5.2.2 TOKY

Presná identifikácia dátových položiek aplikačnej vrstvy [17] je bez analýzy obsahu paketov často nemožná. Navyše, pre účtovanie, modelovanie alebo sumarizáciu je zhromaždenie každého paketu súvisiaceho s výmenou údajov medzi dvomi koncovými bodmi do jednej entity oveľa dôležitejšie ako identifikácia týchto dátových položiek. Pojem tok sa používa na vyjadrenie tejto podstaty. IP tok je podľa štandardu IPFIX [12, 26] definovaný ako množina IP paketov prechádzajúcich pozorovacím bodom v sieti počas určitého časového intervalu. Všetky pakety patriace do daného toku majú spoločné vlastnosti.



Obr. 3. Príchod paketov.

Každá vlastnosť je definovaná ako výsledok funkcie aplikovanej na niektorú z častí paketu. Takýmito časťami môžu byť:

- jedna alebo viac položiek hlavičky paketu (napríklad cieľová IP adresa), hlavičky transportného protokolu (napríklad cieľový port) alebo položky hlavičky aplikačného protokolu (napríklad položky hlavičky RTP).
- jedna alebo viac charakteristík samotného paketu (napríklad počet MPLS návestí).
- jedno alebo viac polí odvodených zo spracúvania paketu (IP adresa nasledujúceho smerovača, výstupné sieťové rozhranie).

Paket patrí do toku, ak spĺňa všetky podmienky definované vlastnosťami. IP toky je možné aj agregovať. Agregácia je možná na základe portu, protokolu, adresy, alebo ich kombinácie.

5.3 CHARAKTERISTIKY VYPLÝVAJÚCE Z INTERAKCIE INFRAŠTRUKTÚRY A PREVÁDZKY SIETE

Existuje veľa vlastností prevádzky, ktoré sú ovplyvnené stavom siete. Tieto vlastnosti môžu byť chápané ako výsledok interakcie medzi prevádzkou a infraštruktúrou siete. Charakteristiky vyplývajúce z tejto interakcie sa často označujú aj ako parametre súvisiace s kvalitou služieb (QoS) [10]. Najvýznamnejšie parametre kvality služieb sú opísané v Tabuľke 1.

Názov charakteristiky	**Opis**
Šírka pásma (bandwidth)	Používa sa pre vyjadrenie množstva údajov, ktoré môžu byť prenesené za jednotku času.
Stratovosť (packet loss)	Množstvo nedoručených alebo poškodených paketov.
Jednosmerné oneskorenie (one-way delay)	Absolútna hodnota rozdielu času odoslania paketu v jednom bode a času prijatia tohto paketu v inom bode.
Kolísanie oneskorenia (jitter)	Je miera plynulosti procesu príchodu paketu, ktorú je možné vyjadriť ako kolísavosť medzičasov príchodu paketu.
Spiatočné oneskorenie (round-trip time)	Čas potrebný na odoslanie paketu od zdroja k cieľu, jeho prijatie v cieli, okamžité spätné odoslanie paketu z cieľa a jeho prijatie naspäť v zdroji.
Priepustnosť (throughput)	Sa vzťahuje na mieru, ktorou je prevádzka schopná reálne ‘tiecť’ cez sieť. Hranica priepustnosti je všeobecne daná kombináciou kapacitných hraníc sieťových komponentov a nepriechodnosti zapríčineného prevádzkou.

Tab. 1. Najvýznamnejšie charakteristiky vyplývajúce z interakcie interakcie a prevádzky siete.

6 OTVORENÉ PROBLÉMY TÝKAJÚCE SA MONITOROVANIA SIEŤOVEJ PREVÁDZKY

Jednotlivé úkony súvisiace s monitorovaním a vyhodnocovaním nameraných hodnôt obklopuje veľa problémov. Niektoré sú z nich na logickej, iné na fyzickej alebo abstraktnej úrovni. Častým

problémom je napríklad určenie tých bodov siete, v ktorých môžu byť merania uskutočnené [4]. Ďalší problém predstavuje pojem času, ktorý má silný vplyv na presnosť výsledkov meraní [4, 25]. Primeraná časť týchto problémov bola za posledné desaťročie úspešne vyriešená. Vytvorili sa rôzne techniky, metódy a nástroje pre zachytávanie a vyhodnocovanie vlastností dnešných konvergovaných sietí. Niektoré problémy ale ostávajú naďalej otvorené.

6.1 PRISPÔSOBENIE INFRAŠTRUKTÚRY A ZARIADENÍ

Zhromažďovanie údajov na rôznych úrovniach si často vyžaduje zmeny v infraštruktúre. Je to kvôli tomu, že pri plánovaní nie sú zohľadnené spôsoby a možnosti vykonania meraní, ale sú len dodatočnou myšlienkou. Najväčší problém to spôsobuje v nižších úrovniach, kde je zvyčajne málo možností na vykonanie meraní.

Vyššie, na úrovni paketov, pre zvládnutie väčšieho objemu údajov je často potrebné rozšíriť siete o podporu špecifických zariadení. Zabezpečenie nezávislosti zhromažďovania paketov od základných funkcionalít smerovača si môže napríklad vyžadovať pridanie sieťových odbočovačov (taps) alebo rôznych zariadení pre pasívne monitorovanie a zrkadlenie paketov. Pre udržanie kroku s prudkým rastom rýchlosti prevádzky je potrebné aj výraznejšie prispôsobenie na úrovni hardvéru (napríklad pridanie rýchlejších sieťových kariet). Špeciálne karty sú ale často vyrábané len pre určitú generáciu alebo rodinu sieťových komponentov, čo niekedy môže značne obmedziť možnosti aktualizácie hardvérových prostriedkov a kapacít.

6.2 SYMBOLICKÝ CHARAKTER NAMERANÝCH DÁT

Medzi najdiskutovanejšie problémy pri monitorovaní v rozľahlých sieťach patrí zabezpečenie reprezentatívnosti (symbolického charakteru) nameraných entít. Možne riešenie predstavuje posielanie a následné sledovanie testovacích správ (sond) prostredníctvom rôznych ciest k veľkému počtu entít – teda aktívne meranie. Entity v takomto prípade môžu byť:

- zákazníci, od ktorých sú namerané údaje obdržané,
- trasy, cez ktoré sú údaje prenášané,
- webové stránky,
- alebo špecifický typ peer-to-peer zdroja pozostávajúceho z rôznych uzlov.

Ďalší problém, ktorý súvisí s reprezentatívnosťou údajov je, že merania v rozsiahlych sieťach nad veľkým počtom uzlov a webových stránok bez samotného prístupu k infraštruktúre je priam nemožné vykonať. Tieto ťažkosti niekedy prehlbuje aj častá neochota zo strany sieťových administrátorov, ktorí z bezpečnostných alebo konkurenčných dôvodov odmietajú prístup alebo monitorovanie údajov. Rastúci počet webových klientov, vrátane používaných prehliadačov a aplikácií, zvyšuje potrebu definovania symbolického charakteru kolekcie údajov.

6.3 OBJEM ÚDAJOV

Častým problémom pri zhromažďovaní údajov na smerovačoch alebo iných entitách infraštruktúry (napríklad linky) je určenie objemu sledovaných údajov. Hlavnou úlohou sieťových entít je

zabezpečenie plynulého a rýchleho prenosu dát. V prípade dnešných konvergovaných sietí to znamená obrovský objem údajov.

Nasadenie monitorovania prevádzky môže v niektorých prípadoch namiesto zvýšenia kvality alebo spravovateľnosti týchto sietí vyvolať opačný účinok, t.j. zaťaženie entít alebo prevádzky. Ak sú napríklad jednotlivé sieťové zariadenia ovplyvnené riadiacimi správami a nameranými dátami vymieňanými medzi monitorovacím systémom a meracími bodmi, môže ľahko dôjsť k zníženiu výkonnosti sieťových prenosov, oneskoreniu alebo dokonca aj k strate údajov. V závislosti od protokolu vyššej úrovne (TCP/UDP), strata údajov môže, ale nemusí byť ošetrená. V takomto prípade monitorovanie stratí na svojich výhodách a v istých prípadoch sa stáva 'nežiadúce'. Z dôvodu zvládnutia čoraz náročnejších požiadavok vysoko-rýchlostných liniek musia byť monitorovacie mechanizmy pravidelne optimalizované.

6.4 ASYMETRIA KAPACITY SYSTÉMOVÝCH PROSTRIEDKOV

Ďalší problém predstavuje asymetria kapacity systémových prostriedkov medzi meracím (monitorovacím) systémom a sieťou, ktorá sa meria (monitoruje) [11]. Aj keď sa meria len malá časť prevádzky, sieť stále obsahuje oveľa viac zariadení ako monitorovací systém. Výsledkom je neporovnateľný rozdiel medzi výpočtovými kapacitami. Navyše, zachytávanie a uloženie informácií o prevádzke pre neskoršiu analýzu ďalej obmedzujú parametre, akými sú šírka prenosu, rýchlosť a kapacita pamätí, diskových polí.

Keďže v niektorých prípadoch môžu vzniknúť aj neprerušované toky prevádzky, pre zabezpečenie bežných úloh, akými je určenie trás alebo filtrovanie, je ťažké odhadnúť nároky sieťových kariet smerovačov [4]. Ak smerovač musí vyčleniť pre merania nejakú pevnú čiastku použiteľných systémových prostriedkov, väčšinou to spraví na úkor iných funkcionalít (napríklad obmedzením schopnosti zvládnutia náhlych zmien v prevádzke). V prípade, ak aj existuje hardvér schopný sledovania primeraných častí tokov prevádzky, zhromažďovanie jednoduchších metrík ako počty (counts) môže spotrebovať výraznú časť dostupných systémových prostriedkov. Táto asymetria si vyžaduje budovanie efektívnych techník a prístupov monitorovania sieťovej prevádzky.

6.5 VYTVÁRANIE A EXPORT ZÁZNAMOV O TOKOCH PREVÁDZKY

Smerovače sa okrem zachytávania paketov často zúčastňujú aj vo vytváraní agregovaných informácií o tokoch prevádzky. Agregácia je zabezpečená vytvorením záznamov o tokoch, ktoré pozostávajú z informácií o kľúčových charakteristikách sieťovej prevádzky. Tieto záznamy sú pravidelne exportované pre rôzne účely, ako monitorovanie prevádzkových charakteristík, účtovanie alebo správa sietí [3, 25, 26]. Smerovače od spoločnosti Cisco sú schopné, prostredníctvom vlastného protokolu Netflow [3], vytvárania takýchto záznamov o tokoch, ktoré obsahujú dôležité štatistiky o prevádzke sietí. Najpoužívanejšími položkami týchto záznamov sú zdrojové a cieľové IP adresy/porty, protokol, čas začiatku a konca toku, typ služby (ToS) alebo autonómny systém (AS). Netflow záznam sa vytvára:

- po uplynutí ľubovoľne nastaviteľného času nečinnosti koncových bodov (passive timeout),
- ak jedna strana ukončí spojenie,

- po prekročení ľubovoľne nastaviteľného času, pričom koncové body sú ešte stále aktívne (active timeout),
- ak smerovač potrebuje vyprázdniť svoj zásobník.

Napriek tomu, že záznamy o tokoch predstavujú efektívnu formu agregovaných meta-informácií, jednoduché sledovanie veľkého počtu tokov a následné generovanie záznamov môžu značne zaťažiť smerovač [4]. Obmedzenia pamäte a výpočtových funkcionalít v kombinácii s hlavnou úlohou smerovača (smerovanie paketov) viedli k rôznym sofistikovaným metódam na redukciu množstva spracovaných dát, akým sú napríklad vzorkovanie alebo sumarizácia paketov.

Podobne ako smerovače, nástroje pre zhromažďovanie záznamov o tokoch (flow collector) — ktoré sú často nejakou externou softvérovou alebo hardvérovou súčiastkou merania — môžu mať svoju vlastnú šírku pásma, veľkosť pamäte alebo výpočtovú kapacitu. Z toho vyplýva, že bez ich optimalizácie môže dojsť k zahodeniu alebo strate dát [20].

6.6 MIERA CHYBOVOSTI MONITOROVACÍCH NÁSTROJOV

Väčšina súčasných monitorovacích mechanizmov pri analýze nameraných hodnôt zohľadňuje len jednu charakteristiku tokov prevádzky [15]. Ak vyhodnotená hodnota tejto charakteristiky sa kolíše okolo preddefinovanej hranice, z dôvodu potencionálnej hrozby môže dojsť k nesprávnym úsudkom monitorovacieho systému. Takýto prípad môže nastať, ak prípustná hodnota šírky pásma sa kolíše okolo štandardnej hodnoty, v dôsledku čoho monitorovací systém môže obmedziť isté funkcionality alebo hlásiť priveľa upozornení aj v prípade, ak sa v skutočnosti nejedná o žiadnu hrozbu alebo problém. V takomto prípade môže byť presnosť a kvalita monitorovacích mechanizmov spochybnená [15]. Výrazný vplyv na chybovosť merania má metodika vykonávania samotného merania, kde merací-exportovací proces nesmie ovplyvniť smerovacie procesy v danej topológii, čím by vnášal skreslenie do výsledného hodnotenia parametrov prevádzky. Množstvo monitorovacích systémov, ako je to aj v prípade projektu Basic Meter [9] pracuje so zrkadlenou prevádzkou z danej infraštruktúry, čo si vyžaduje prítomnosť prvkov siete umožňujúcich toto zrkadlenie.

6.7 VYHODNOCOVANIE ÚDAJOV V REÁLNOM ČASE

Schopnosť spracovania primeranej časti dát v reálnom čase predstavuje tiež zložitú úlohu [8]. Ukladanie údajov, napríklad v databáze, z pohľadu reálno-časového vyhodnocovania dát je absolútne vylúčené [20]. Pričasté posielanie záznamov o tokoch ale môže často spôsobiť zníženie výkonnosti sieťových prenosov, oneskorenie alebo dokonca aj stratu údajov. Z tohto dôvodu, výmena dát medzi monitorovacím systémom a meracím(mi) bodom(mi) sa bežne vykonáva po väčších časových úsekoch. Takýmto spôsobom je síce možné zredukovať nežiadané zaťažovanie sieťovej prevádzky, vyhodnocovanie údajov v reálnom čase sa ale stáva nemožnou. Z toho dôvodu je potrebné určiť správny pomer medzi intervalmi exportu záznamov o tokoch a efektívnym využitím dostupných prostriedkov. V prípade často sa meniacej charakteristiky dnešných sietí je to ale bez automatizovaných procesov priam nemožné.

7 OVERENIE IDENTIFIKOVANÝCH OTVORENÝCH PROBLÉMOV

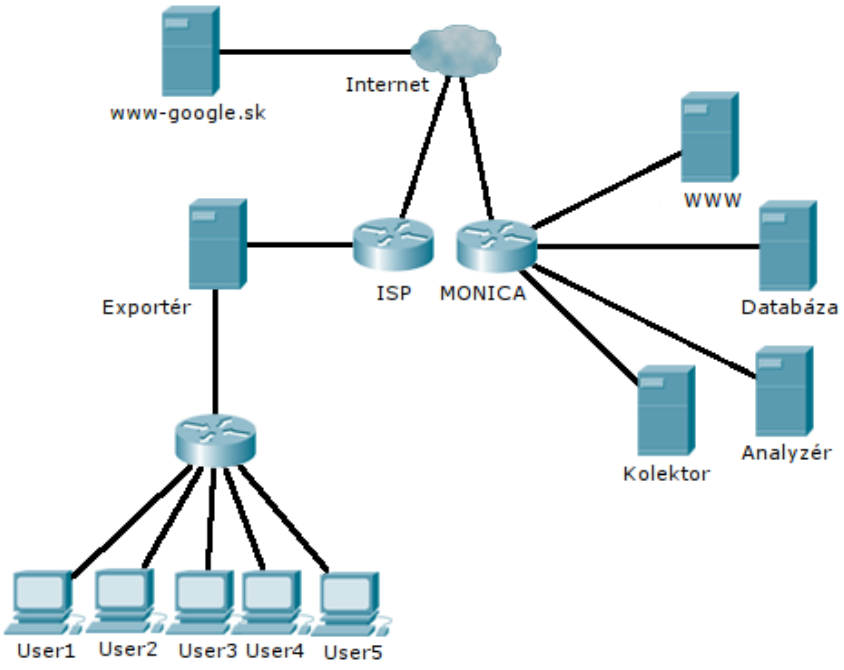
Na overenie vybraných problémov, vyskytujúcich sa pri monitorovaní sieťovej prevádzky, bola realizovaná skupina experimentov. Experimenty sa zameriavali:

- na odhad priemerného objemu dát, ktoré sa pri monitorovaní musia spracovať,
- určenie priemerného vyťaženia systémových prostriedkov, ktoré v sebe prináša monitorovanie.

Cieľom experimentov bolo potvrdenie domnienky, že s rastúcimi parametrami sieťovej infraštruktúry (čo sa týka priepustnosti a počtu klientov) narastú aj požiadavky kladené na monitorovaciu a vyhodnocovaciu platformu. Pri overení tejto domnienky bola využitá monitorovacia platforma BasicMeter (BM) [9], ktorá bola nasadená v prostredí podľa Obrázku 4. Export dátových tokov prebiehal na základe IPFIX protokolu prostredníctvom BM Exportéra, ktorý prijímal prevádzku generovanú v sieťovej topológii prostredníctvom zrkadleného portu v topológii.

Na zistenie priemerného objemu dát, ktorý je potrebné pri monitorovaní spracovať a približné vyťaženie systémových prostriedkov, boli realizované merania v dvoch existujúcich sieťach. Každá z nich mala rôzne množstvo pripojených koncových zariadení a rýchlosť liniek.

Experimenty boli realizované opakovane. Zo získaných výsledkov boli určené priemerné hodnoty objemu dát za 1 hodinu. Pri meraniach sa sledovalo aj priemerné vyťaženie smerovača (Cisco 2811, IOS 12.4T), ktorý sa okrem štandardných smerovacích úloh prostredníctvom protokolu Netflow [3] podieľal aj na vytváraní a exporte záznamov o tokoch prevádzky. Výsledky sú zhrnuté v Tabuľke 2.



Obr. 4. Meracia topológia.

	Sieť 1	**Sieť 2**
Počet koncových zariadení	11	442
Rýchlosť rozhrania linky	100 Mb/s	1 000 Mb/s
Objem prenesených údajov	210 MB	10 075 MB
Počet prenesených paketov	318 263	16 996 596
Priemerné využitie CPU s vypnutým Netflow	3%	31 %
Priemerné využitie CPU so zapnutým Netflow	6%	48 %

Tab. 2. Výsledky experimentov meraní.

Z výsledkov vyplýva, že síce ani jedno z monitorovaní sietí nevyťažovalo linku a systémové prostriedky na maximum ich výkonnosti, napriek tomu je možné konštatovať, že sieťou bolo prenesené relatívne veľké množstvo údajov. Navyše, so zvyšovaním rýchlosti liniek, by požiadavky na systémové prostriedky úmerne rástli. Napríklad pri monitorovaní prevádzky s rýchlosťou liniek 1 Gb/s by bolo potrebné počas jedného dňa spracovať a vyhodnotiť približne 112 TB údajov. V súčasnosti ale existujú aj oveľa rýchlejšie spôsoby prenosu dát [13].

Je možné teda konštatovať, že problémy týkajúce sa veľkého objemu dát, ktoré je potrebné počas monitorovania spracovať a z toho vyplývajúce vyťaženie systémových prostriedkov sú aktuálne.

8 ADAPTÍVNY EXPORT INFORMÁCIÍ O TOKOCH SIEŤOVEJ PREVÁDZKY

Pod pojmom optimalizácia monitorovania sieťovej prevádzky sa rozumie návrh a implementácia takých mechanizmov a metód, ktoré sú adresované na vyriešenie ich nedostatkov. Vzhľadom na otvorené problémy uvedené v predošlých kapitolách a výsledky experimentov sa má optimalizácia monitorovania sieťovej prevádzky hlavne zameriavať na:

- minimalizáciu celkového preťaženia siete spôsobeného ich monitorovaním,
- zvýšenie efektivity využívania a minimalizáciu zaťaženia systémových prostriedkov monitorovacími mechanizmami,
- zvýšenie presnosti vyhodnocovacích mechanizmov,
- a maximalizáciu schopnosti vyhodnocovania dát v reálnom čase.

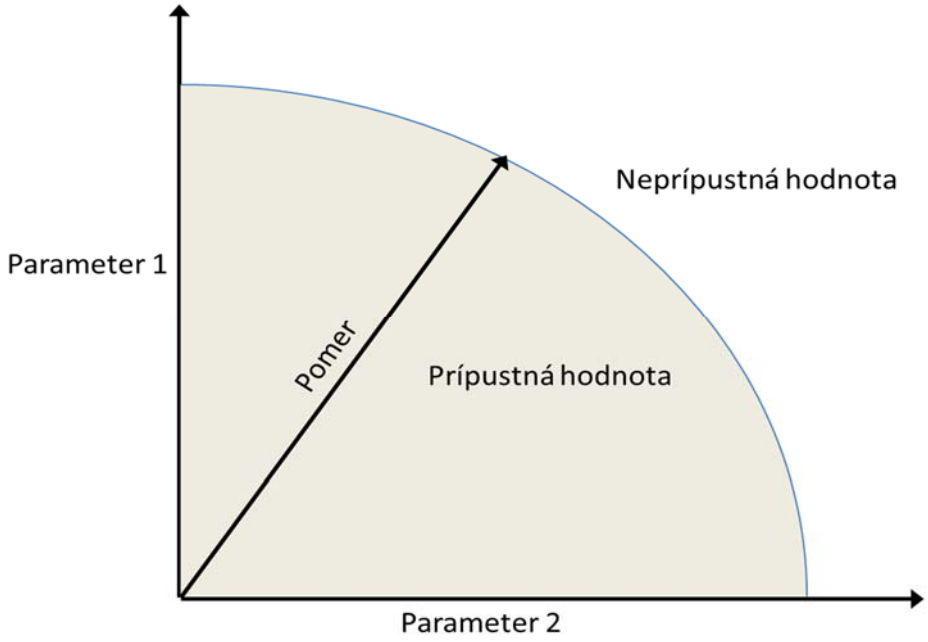
Dosiahnutie týchto cieľov je možné prostredníctvom adaptívneho exportu informácií o tokoch sieťovej prevádzky, na ktorý v súčasnosti neexistuje žiadna referencia v odbornej a ani vedecko-výskumnej sfére.

Využitie systémových prostriedkov monitorovacími mechanizmami je v dôsledku meniaceho sa charakteru sieťovej prevádzky často neefektívne. Výrazným nedostatkom existujúcich riešení je absencia adaptívnych exportovacích metód, ktoré by zohľadňovali stav a vlastnosti sieťovej prevádzky. Konceptuálny návrh adaptívneho exportu informácií o tokoch sieťovej prevádzky predstavuje:

- Prispôsobením určitých parameterov exportu informácií o tokoch k aktuálnemu stavu sieťovej prevádzky je možné značne prispieť k vyriešeniu vyššie uvedených cieľov optimalizácie. Takéto vlastnosti predstavujú napríklad objem dát, z ktorých sa vytvárajú záznamy o tokoch alebo ich čas exportu.
- Pri adaptívnom exporte je potrebné stanoviť aj správny pomer medzi intervalmi exportu a efektívnym využitím dostupných sieťových a systémových prostriedkov. Intervaly exportu sú dôležité z dôvodu monitorovania sieťovej prevádzky v reálnom čase, ktoré uprednostňujú čo najmenší časový úsek.
- Pre dosiahnutie efektívneho vyhodnotenia dát sa použije viacdimenzionálna analýza rôznych charakteristík sieťovej prevádzky. Pri takejto analýze, sa namiesto jedinej charakteristiky pri vyhodnotení aktuálneho stavu sieťovej prevádzky zohľadní viac parametrov. Prostredníctvom tejto metódy je možné výrazne zredukovať počet nesprávnych úsudkov monitorovacieho systému, akým je napríklad signalizácia chýb aj v prípade, keď sa v skutočnosti nejedná o žiadnu hrozbu alebo problém.

  V prípade dvoch parametrov, určenie správneho pomeru by mohol byť uskutočnený pomocou karteziánskej súradnicovej sústavy, kde x-ová os bude predstavovať maximálny objem prevádzky a y-ová os interval exportu záznamov o tokoch. Príklad takejto sústavy je uvedený na Obrázku 5.

  Každý analyzovaný parameter by bol priradený k jednej osi, nad ktorou by sa vykonávala zvolená matematicko-štatistická metóda (napríklad štatistické rozdelenie, vzdialenosť od preddefinovanej hodnoty alebo súboru hodnôt, atď.). Viacdimenzionálna analýza by sa dosiahla súčasným vykonaním analýz nad týmito parametrami.



Obr. 5. Určenie správneho pomeru parametrov adaptívneho exportu.

- Kľúčovým faktorom je teda definícia parametrov, ktoré budú jednou zo vstupných hodnôt metódy adaptívneho exportu. Táto úloha si vyžaduje realizáciu experimentov, ktoré by mali jednoznačne určiť charakteristiky prevádzky sietí, ktorých zmena výrazne ovplyvní výkonnosť siete a efektivitu využívania systémových prostriedkov monitorovacími systémami.
- Výsledkom má byť dosiahnutie vyššie uvedených cieľov optimalizácie.

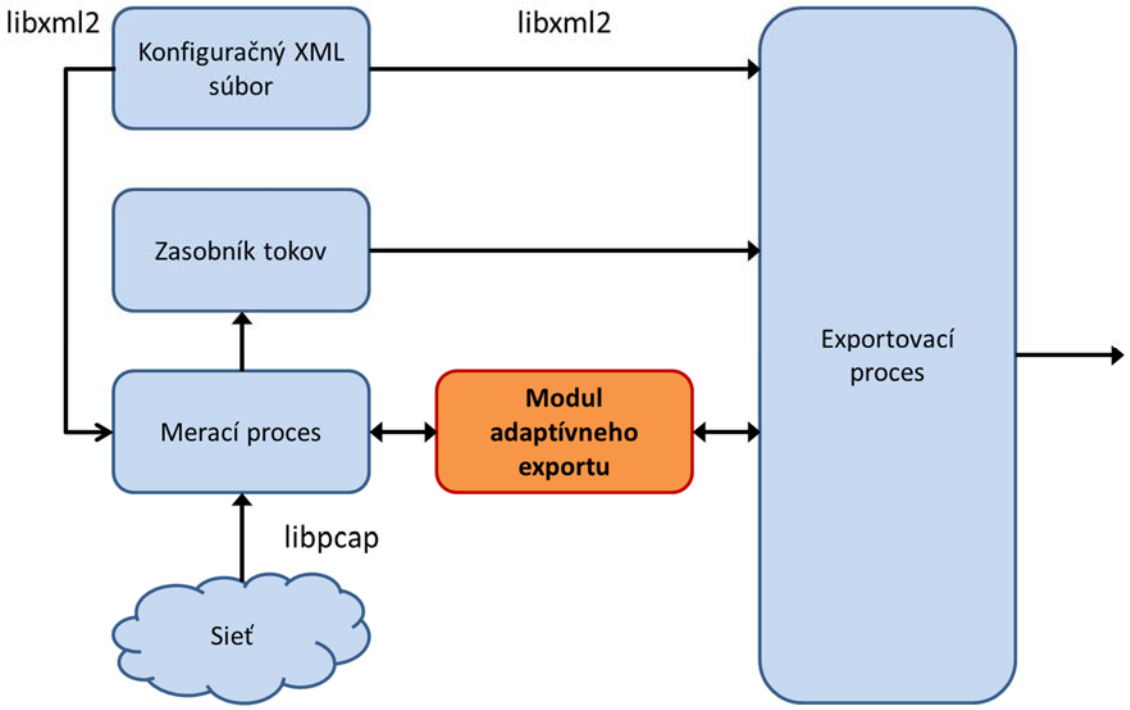
Umiestnenie modulu adaptívneho exportu sa navrhuje medzi meracím a exportovacím procesom (viď. Obrázok 6.) meracieho nástroja BasicMeter [9]. Takto sa dosiahne efektívne vyhodnotenie vyššie spomenutých vstupných parametrov, na základe ktorých bude export informácií o tokoch sieťovej prevádzky prispôsobený. Významnú úlohu okrem modulu pre adaptívny export informácií o tokoch prevádzky budú mať aj ďalšie dva procesy:

- *Merací proces* bude slúžiť na odchytávanie prevádzky a zaraďovanie jednotlivých paketov do tokov na základe prednastaveného kľúča toku. Tieto toky budú ukladané do zásobníka tokov. Pre odchytávanie paketov sa použije knižnica *libpcap*. Tento proces bude zároveň poskytovať informácie na základe ktorých sa určia vstupné parametre adaptívneho exportu.
- *Exportovací proces* na základe výstupov z modulu pre adaptívny export bude odosielať zhromažďovaciemu procesu informácie o tokoch s použitím protokolu IPFIX. Tieto údaje bude získavať zo zásobníka.

Pre dosiahnutie optimalizácie monitorovania sieťovej prevádzky sa v súčasnosti vyžadujú minimálne dva parametre:

1. Interval pre expiráciu záznamov o tokoch v závislosti od charakteru sieťovej prevádzky v prípade vyhodnotenia dát v reálnom čase.
2. Maximálny objem spracovanej prevádzky, ktorý neprináša žiadne alebo len akceptovateľné zaťaženie systémových a sieťových prostriedkov.

Rozšírenie týchto parametrov o ďalšie faktory sa v budúcnosti nevylučuje.



Obr. 6. Architektúra adaptívneho exportu.

9 ZÁVER

Dôležitým aspektom budovania, spravovania a optimalizácie rozsiahlych a komplexných počítačových sietí predstavuje meranie ich záťaže a správania sa. Nenahraditeľný prostriedok pre vykonanie tejto úlohy predstavuje monitorovanie sieťovej prevádzky. Pomocou monitorovania rôznych prevádzkových vlastností je možné zabezpečiť plynulú funkčnosť aplikácií, ako napríklad hlas cez internet (VoIP) alebo video na požiadanie (VoD). Okrem zabezpečenia funkčnosti multimediálnych aplikácií umožňuje aj odhalenie vnútorných a vonkajších útokov, dominantných zdrojov prevádzky alebo sledovanie, kto s kým komunikoval, ako dlho, pomocou ktorého protokolu. Taktiež umožňuje poskytovateľom internetových služieb (ISP) zabezpečiť splnenie podmienok uvedených v zmluve o dohodnutej úrovni poskytovania služby (SLA) a efektívnejšie plánovať budúci rozvoj siete.

Jednotlivé úkony súvisiace s monitorovaním a vyhodnocovaním nameraných hodnôt obklopuje veľa problémov. Primeraná časť týchto problémov bola za posledné desaťročie úspešne vyriešená. Vytvorili sa rôzne techniky, metódy a nástroje pre zachytávanie a vyhodnocovanie vlastností dnešných konvergovaných sietí. Niektoré problémy ale ostávajú naďalej otvorené.

Tento príspevok podáva stručný prehľad o problematike monitorovania sieťovej prevádzky. Uvádza vlastnosti sietí, ktoré sa pri ich monitorovaní a meraní najčastejšie sledujú, ako aj rôzne prístupy určovania charakteristík sieťovej prevádzky. Definuje otvorené problémy, ktoré sa pri monitorovaní vyskytujú, pričom jeho výstupom je konceptuálny návrh adaptívneho exportu informácií o tokoch, ktorá je adresovaná na optimalizáciu monitorovania sieťovej prevádzky.

POĎAKOVANIE

Tento príspevok vznikol vďaka podpore v rámci operačného programu Výskum a vývoj, pre projekt: Kompetenčné centrum znalostných technológií pre inovácie produkčných systémov v priemysle a službách, kód ITMS: 26220220155, spolufinancovaný zo zdrojov Európskeho fondu regionálneho rozvoja.

10 ZOZNAM POUŽITÝCH ZDROJOV

[1] CASE, J.D., M. FEDOR, M.L. SCHOFFSTALL a J. DAVIN. INTERNET ENGINEERING TASK FORCE (IETF). *Simple Network Management Protocol (SNMP): Request for Comments (RFC 1157)*. 1990. Dostupné z: http://www.ietf.org/rfc/rfc1157.txt

[2] CHOFFNES, D. R., F. E. BUSTAMANTE a Z. GE. Crowdsourcing service-level network event monitoring. *Proceedings of the ACM SIGCOMM 2010 conference on SIGCOMM - SIGCOMM '10*. New York, New York, USA: ACM Press, 2010, roč. 40, č. 4, s. 387-398. DOI: 10.1145/1851182.1851228.

[3] CLAISE, B. INTERNET ENGINEERING TASK FORCE (IETF). *Cisco Systems NetFlow Services Export Version 9: Request for Comments (RFC 3954)*. 2004. Dostupné z: http://www.ietf.org/rfc/rfc3954.txt

[4] CROVELLA, M. a B. KRISHNAMURTHY. *Internet measurement: infrastructure, traffic, and applications*. Hoboken, NJ: Wiley, 2006, xxii, 495 p. ISBN 978-047-0014-615.

[5] FLOYD, S. a V. PAXSON. Difficulties in simulating the Internet. *IEEE/ACM Transactions on Networking*. 2001, vol. 9, issue 4, s. 392-403. DOI: 10.1109/90.944338. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=944338

[6] GARCIA-DORADO, J., J. HERNANDEZ, J. ARACIL, J. LOPEZ DE VERGARA, F. MONSERRAT, E. ROBLES a T. DE MIGUEL. On the duration and spatial characteristics of internet traffic measurement experiments. *IEEE Communications Magazine*. 2008, vol. 46, issue 11, s. 148-155. DOI: 10.1109/MCOM.2008.4689258.

[7] GIERTL, J., Ľ. HUSIVARGA, M. RÉVÉS, A. PEKÁR a P. FECIĽAK. Measurement of Network Traffic Time Parameters. In: *Proceedings of the Eleventh International Conference on Informatics (INFORMATICS)*. Košice: TUKE, 2011, s. 33-37. ISBN 978-80-89284-94-8. DOI: 978-80-89284-94-8.

[8] JAKAB, F., R. JAKAB, Ľ. KOŠČO a J. GIERTL. Communication Protocol in Computer Network Performance Parameters Measurement. In: *4th International Information and Telecommunication Technologies Symposium (I2TS)*. Florianopolis, Santa Catarian Island, Brazil: Federal University of Santa Catarina, 2005, s. 161-162. ISBN 858926405X.

[9] JAKAB, F., Ľ. KOŠČO, M. POTOCKÝ a J. GIERTL. Contribution to QoS Parameters Measurement: The BasicMeter Project. In: *International Conference on Emerging eLearning Technologies and Applications (ICETA)*. Košice, Slovakia: elfa, s.r.o., 2005, s. 371-377. ISBN 8080860166.

[10] LEE, H.J., M.S. KIM, J.W. HONG a G.H. LEE. QoS Parameters to Network Performance Metrics Mapping for SLA Monitoring. In: *Proceedings of the Korean Network Operations and Management (KNOM)*. Korea: Korea University, 2002, s. 42-53.

[11] PANG, R. *Towards Understanding Application Semantics of Network Traffic*. Princetown, USA, 2008. Dizertačná práca. Princetown University.

[12] QUITTEK, J., T. ZSEBY, B. CLAISE a S. ZANDER. INTERNET ENGINEERING TASK FORCE (IETF). *Requirements for IP Flow Information Export (IPFIX): Request for Comments (RFC 3917)*. 2004. Dostupné z: http://www.ietf.org/rfc/rfc3917.txt

[13] SCHLEPPLE, N., M. NISHIGAKI, H. UEMURA, K. OBARA, H. FURUYAMA, Y. SUGIZAKI, H. SHIBATA a Y. KOIKE. 4x10 Gb/s High-Speed Link Over Thin GI 50/125 Plastic Optical Fibers and Compact Optical Sub-Assembly. *IEEE Photonics Technology Letters*. 2012, vol. 24, issue 19, s. 1670-1672. DOI: 10.1109/LPT.2012.2209636.

[14] SHAIKH, A., C. ISETT, A. GREENBERG, M. ROUGHAN a J. GOTTLIEB. A case study of OSPF behavior in a large enterprise network. In: *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment*. New York, NY, USA: ACM, 2002, s. 217-230. DOI: 10.1145/637201.637236.

[15] SHIMOKAWA, I. a T. TARUI. Network Monitoring Method Based on Self-learning and Multi-dimensional Analysis. In: *The Second International Conference on Advances in Information Mining and Management (IMMM)*. Venice, Italy: IARIA, 2012, s. 47-53. ISBN 978-1-61208-227-1. Dostupné z: http://www.thinkmind.org/download.php?articleid=immm_2012_3_10_20025

[16] SPRING, N., R. MAHAJAN, D. WETHERALL a T. ANDERSON. Measuring ISP Topologies With Rocketfuel. *IEEE/ACM Transactions on Networking*. 2004, vol. 12, issue 1, s. 2-16. DOI: 10.1109/TNET.2003.822655.

[17] TANENBAUM, A. S. a D. WETHERALL. *Computer networks*. 5th ed. Boston: Pearson, 2011, 951 s. International edition. ISBN 978-013-2553-179.

[18] VOKOROKOS, L., N. ÁDÁM a A. BALÁŽ. Application of intrusion detection systems in distributed computer systems and dynamic networks. In: *Computer Science and Technology Research Survey (CST)*. Košice, Slovakia: elfa, s.r.o., 2008, s. 19-24. ISBN 9788080861001.

[19] VOKOROKOS, L., A. KLEINOVÁ a O. LÁTKA. Network Security on the Intrusion Detection System Level. In: *Proceedings of the IEEE International Conference on Intelligent Engineering Systems (INES)*. Budapest, Hungary: Óbuda University, 2006, s. 270-275. DOI: 10.1109/INES.2006.1689382.

[20] VOKOROKOS, L., A. PEKÁR a N. ÁDÁM. Data preprocessing for efficient evaluation of network traffic parameters. In: *Proceedings of the IEEE 16th International Conference on Intelligent Engineering Systems (INES)*. Budapest, Hungary: Óbuda University, 2012, s. 363-367. DOI: 10.1109/INES.2012.6249860.

[21] WALDBUSSER, S., R. COLE, C. KALBFLEISCH a D. ROMASCANU. INTERNET ENGINEERING TASK FORCE (IETF). *Introduction to the Remote Monitoring (RMON) Family of MIB Modules: Request for Comments (RFC 3577)*. 2003. Dostupné z: http://www.ietf.org/rfc/rfc3577.txt

[22] WANG, L., X. ZHAO, D. PEI, R. BUSH, D. MASSEY, A. MANKIN, S. F. WU a L. ZHANG. Observation and analysis of BGP behavior under stress. In: *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment (IMW)*. New York, NY, USA: ACM, 2002, s. 183-195. DOI: 10.1145/637201.637231.

[23] WIMMER, G., R. PALENČÁR a V. WITKOVSKÝ. *Stochastické modely merania*. Bratislava: Grafické štúdio Ing. Peter Juriga, 2001, 115 s. ISBN 80-968-4492-X.

[24] Wireshark: Network protocol analyzer. *Wireshark* [online]. 2013 [cit. 2013-06-23]. Dostupné z: http://www.wireshark.org/

[25] WOLF, T., R. RAMASWAMY, S. BUNGA a Ning YANG. An Architecture for Distributed Real-Time Passive Network Measurement. In: *14th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. Washington, DC, USA: IEEE Computer Society, 2006, 335 - 344. DOI: 10.1109/MASCOTS.2006.11.

[26] ZSEBY, T., BOSCHI, N. BROWNLEE a B. CLAISE. INTERNET ENGINEERING TASK FORCE (IETF). *IP Flow Information Export (IPFIX) Applicability: Request for Comments (RFC 5472)*. 2009. Dostupné z: http://www.ietf.org/rfc/rfc5472.txt