Portál pre odborné publikovanie ISSN 1338-0087

Analýza QoS strímu pre MHP služby v IP sieťach v simulačnom prostredí Opnet

Kokoška Rastislav · Informačné technológie

01.09.2013

Cieľom tohto článku je poukázať na analýzu QoS strímu pre MHP služby v nestabilných IP sieťach v stimulačnom prostredí Opnet. Je zobrazený prehľad QoS kvality služieb, ich vlastnosti a spôsoby implementácie. Ponuka kvality služieb dostáva široký rozmer v IPTV službách pre komunikáciu s internetom a jej dostupnosťou ,šírky pásma, rýchlosti. Simulačný program opnet dáva možnosti modelovania sieti na základe parametrov kvality služieb.

1. Úvod

Trendom dnešnej doby je pre sieťových dizajnérov postaviť tzv. multiservisnú sieť, schopnú prenášať všetky typy komunikácie – hlas, dáta a video pomocou paketovej architektúry. Požiadavka po stále väčšej šírke pásma je neutíchajúca a v poslednej dobe sa ešte zintenzívňuje. Avšak zvýšená požiadavka na šírku pásma môže spôsobiť problémy s kvalitou, a to hlavne degradáciu časovo senzitívneho typu sieťovej prevádzky, akou je hlas. Hlasové pakety nemajú také isté výhody ako dátové, čo sa týka opätovného posielania v prípade straty paketu počas prenosu[1].

2. Kvalita služby

Kvalita služby (z angl. quality of services) je schopnosť poskytovať rôzne priority pre rôzne aplikácie, užívateľov, dátové toky alebo schopnosť garantovať určitú hodnotu výkonu pre dátový tok. Napríklad môže byť garantovaná požadovaná bitová rýchlosť, oneskorenie, pravdepodobnosť zahadzovania paketov alebo bitová chybovosť. Garantovanie kvality služby je dôležité v prípade, ak sieťová kapacita je nepostačujúca, špeciálne pre multimediálne aplikácie strímujúce v reálnom čase, ako napríklad prenos hlasu cez IP (VoIP), on-line hry a IP-TV, pretože tieto často vyžadujú pevnú prenosovú rýchlosť a sú citlivé na oneskorenie, ako v sieťach, kde je kapacita determinovaná zdrojom, napríklad v celulárnej dátovej komunikácii. QoS je požadovaná v sieťach bez zahltenia [2]. QoS funkcie poskytujú lepšie a viac predvídateľné sieťové služby tak, že:

- zaoberajú sa a riadia sieťové zahltenie tvarovaním sieťovej prevádzky.
- nastavujú prioritu sieťovej prevádzky naprieč sieťou.

2.1. Architektúra QoS

Konkrétne elementy QoS architektúry závisia od typu prenášaných informácií: hlas, dáta alebo video. Pre VoIP definuje QoS obmedzenia špecifické pre prenos hlasu, ako sú delay (oneskorenie), delay variation alebo aj jitter (časové chvenie), packet loss (strata paketov) a tiež echo [1]. Medzi reprezentatívnu metriku kvality služieb v počítačových sieťach radíme:

- koncové oneskorenie – doba medzi vyslaním paketu od zdroja a jeho doručením určenému príjemcovi
- kolísanie oneskorenia tzv. jitter- rozdiel v intervaloch medzi prijatými paketmi
- strata paketov tzv paket loss – podiel prijatých paketov a vyslaných paketov za jednotku času
- šírka pásma – prenosová kapacita, ktorá súvisí s priepustnosťou (objem úspešne prenesených dát za jednotku času) [3].

2.2. Modely zabezpečenia QoS

Riešenie ako dosiahnuť vyššiu úroveň služby prináša niekoľko spôsobov podpory podľa IETF(Internet Engineering Task Force). Konkrétne sa jedná o nasledujúce architektúry zabezpečujúce QoS v sieťach [3]:

- Integrated Services, IntServ
- Differentiated Services, DiffServ
- Multi-Protocol Label Switching
- Subnet Bandwidth Management [4].

2.2.1. Integrated Service

Model integrovaných služieb (intServ) sa snaží dodržať garantovanú úroveň obsluhy pre vybrané služby po celej trase prenosu. Aplikácia vyžaduje od siete, aby zabezpečila určitú úroveň parametrov prenosu, ktoré potrebuje na to aby pracovala správne. Aplikácia musí vedieť aká je charakteristika toku, ktorý generuje a signalizovať uzlom v sieti na celej trase prenosu [4]. Model IntServ podporuje dva rozdielne typy služieb: služba s riadenou záťažou – pre zaistenie spoľahlivého prenosu medzi dvoma bodmi riadením záťaže a garantovanú službu – pre garantované maximálne oneskorenie pri prenose v danom pásme [4].

2.2.2. Differentiated Services

Diferencované služby (DiffServ) predstavuje metódu, ktorá pomocou množiny klasifikačných nástrojov a mechanizmov pre prácu s frontami poskytuje široké možnosti pri zabezpečovaní kvality služby dátovým prenosom v sieti. Táto metóda je založená na tom, že okrajové smerovače klasifikujú rôzne druhy paketov prechádzajúcich cez sieť. Rôzne toky sa dajú klasifikovať na základe sieťovej adresy, protokolu, vstupného portu. Tok je tiež možné klasifikovať pomocou základných alebo rozšírených prístupových listov. Potom sa zaraďujú do tried. Každej triede sa priradí DiffServ hodnota (DSCP).

V jadre siete sú potom pakety znovu preposielané na základe nadefinovaného správania sa sieťových uzlov k toku s príslušnou hodnotou SCP. Keďže žiadna z metód (intServ a DiffServ) neponúka komplexné riešenie, využíva sa kombinovanie týchto

dvoch metód. Najnovší trend v zabezpečovaní kvality služby je zjednodušenie a automatizácia s ohľadom na jednoduchosť a schopnosť zabezpečiť garanciu kvality služby v IP sieťach. Technológie zabezpečujúce kvalitu služby ponúkajú množstvo možností a môžu byť využité pri výstavbe veľmi dômyselných sietí [4].

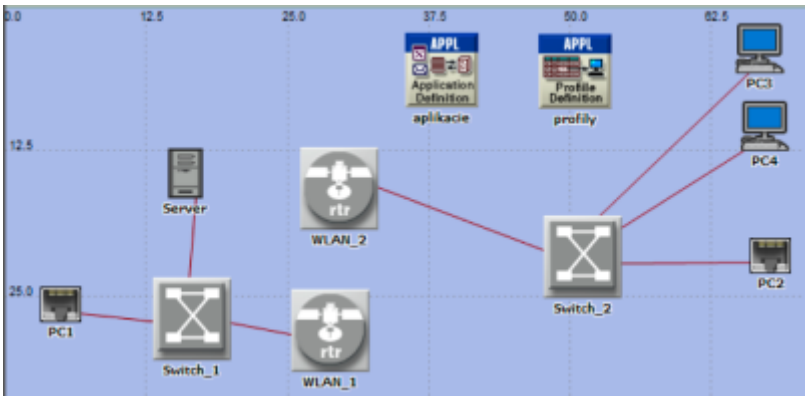
2.2.3. Mechanizmy zabezpečenia kvality služby

Pri zabezpečovaní kvality obsluhy dát sú používané rozličné nástroje ponúkané zariadeniami, ktoré sa podieľajú na riadení toku týchto dát cez sieť, do ktorých spadajú:

- Classification and marking
- Policing and shaping
- Congestion Management (manažment presýtenia siete)
- Congestion Avoidance (ochrana pred zahltením) [6].

3. Zostavenie simulovanej siete a prepojenie objektov

Narhovaná sieť využíva rozhranie SITL, ktoré umožňuje zobraziť streamované 3D video na prijímacej strane. Simulácia je doplnená video serverom a aplikáciami, ktoré podľa nastavenia zaťažujú bezdrôtový prenos. Na obr. 2 je znázornený návrh simulačnej siete.



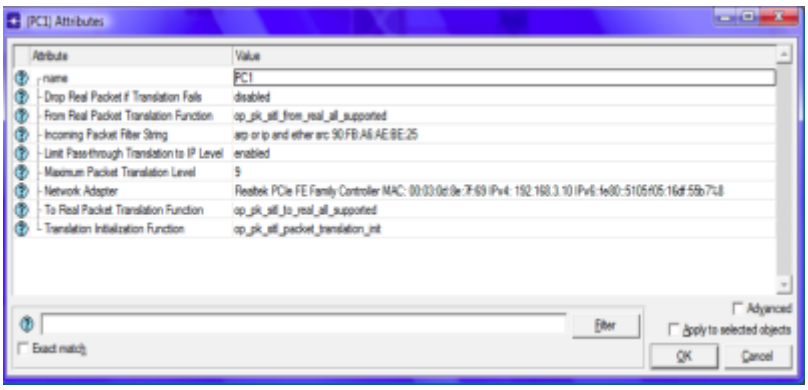
Obr. 2 Návrh simulačnej siete

Na Obr. 2, sa skladá sieť z dvoch rozhraní SITL (PC1 a PC2), pracovných staníc (PC3 a PC4), prepínačov (Switch_1 a Switch_2), bezdrôtových smerovačov (WLAN_1 a WLAN_2), video servera a objektov pre nastavenie aplikácií a profilov. Na rozhranie SITL PC1 je pripojený reálny počítač na ktorom je spustený program VLC. Program VLC je s verziou 2.0.5. PC1 streamuje 3D video pomocou protokolu HTTP na druhý reálny počítač, ktorý je pripojený na rozhranie SITL PC2. PC2 prijíma streamované 3D video tiež pomocou programu VLC.

Obr. 3 Reálne prepojenie počítačov

V module SITL na oboch stranách je dôležité nastaviť sieťovú kartu. Sú to sieťové karty

počítača na ktorom je spustený OM. Keďže notebooky majú len jednu sieťovú kartu, tak je potrebné dokúpiť druhú USB sieťovú kartu. Pri atribúte Incoming Packet Filter String je potrebné k predvolenej hodnote arp or ip, dosadiť MAC adresu sieťovej karty príkazom ether src a za tým MAC adresu v tvare XX:XX:XX:XX:XX:XX. Pre každé rozhranie je to MAC adresa počítača, na ktoré je počítač pripojený. Nastavenie filtra zabezpečí prenos paketov z príslušnej MAC adresy do simulácie [8]. Ukážka nastavenia je na obr.4.



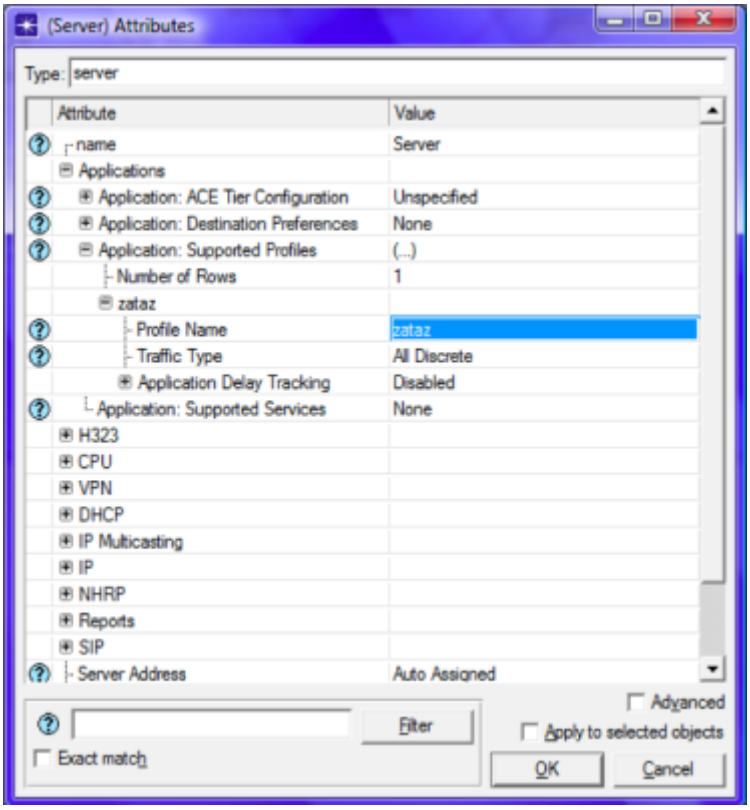
Obr. 4 Nastavenie atribútov pre modul SITL

Pri moduloch WLAN je dôležité nastaviť funkciu Access Point Functionality, kde pri WLAN_1 je táto funkcia povolená a pri WLAN_2 zakázaná. Potrebné je samozrejme nastaviť IP Routing Parameters, tzn. IP adresy rozhraní a smerovacie protokoly podľa tabuľky. Pri WLAN moduloch je možné meniť napr. prenosovú rýchlosť, prenosovú topológiu alebo vyrovnávaciu pamäť.

Device	Rozhranie	IP adresa	Maska podsiete	Predvolená brána
PC1	sieťová karta	192.168.3.11	255.255.255.0	192.168.3.1
PC2	sieťová karta	192.168.1.11	255.255.255.0	192.168.1.1
PC3	sieťová karta	192.168.1.12	255.255.255.0	-
PC4	sieťová karta	192.168.1.13	255.255.255.0	-
PC:OM	zabudovaná sieťová karta	192.168.3.10	255.255.255.0	-
	USB sieťová karta	192.168.1.10	255.255.255.0	-
WLAN_1	eternetový port	192.168.3.1	255.255.255.0	-
	WLAN rozhranie	192.168.2.2	255.255.255.0	-
WLAN_2	eternetový port	192.168.1.1	255.255.255.0	-
	WLAN rozhranie	192.168.2.1	255.255.255.0	-
Server	eternetový port	192.168.3.100	255.255.255.0	-

Na začiatok definujeme požadovaný počet aplikácií v atribúte Number of Rows. Zvolíme si žiadané aplikácie a zadáme každej meno. Je potrebné nastaviť pre tieto aplikácie profil. Po nastavení aplikácií si zvolíme počet profilov v ktorých budú umiestnené zvolené aplikácie. Po zadaní názvu profilu, môžeme každej konkrétnej aplikácií nastaviť čas spustenia aplikácie, čas trvania, čas opakovania prípadne počet opakovaní a ďalšie atribúty. Okrem pridelenia IP adresy serveru je potrebné povoliť funkciu na podporu aplikačných profilov (viď 5), kde si zvolíme podporované profily,

ktoré sme nastavili pred tým.



Obr. 5 Nastavenie podporovaných profilov aplikácií

V navrhovanej simulácií máme dve pracovné stanice s označením PC3 a PC4. Na každej z pracovných staníc je potrebné nastaviť IP adresy. Podobne ako pri nastavení servera je nutné povoliť podporu vytvorených profilov aplikácií . Počet pracovných staníc je ľubovoľný. Pri väčšom počte staníc, ktoré budú prijímať pakety zo servera bude aj zaťaženie siete väčšie. Vzhľadom na množstvo aplikácií a možnosti zostavenia siete akejkoľvek veľkosti je možné laborovať s rôznymi variantmi. DES sú parametre simulácie, ktoré musíme pred jej samotným spustením nastaviť. V našom prípade nesmieme zabudnúť na nastavenie hodnoty Real-time execution ration na hodnotu 1. Nastavíme ju v okne Configure/Run DES voľbou Execution→Advanced→ Kernel preferences v riadku Real-time execution ration na hodnotu 1.

Trvanie simulácie nastavíme primerane vzhľadom na dĺžku streamovaného 3D videa. Do celkového času trvania simulácie započítame aj niekoľko sekúnd potrebných na spustenie videostreamu na PC1 a potvrdenie prijímania streamu na PC2. Posledný krokom pred spustením simulácie je voľba štatistík, ktoré chceme počas simulácie sledovať a neskôr porovnávať. Po kliknutí pravého tlačidla myši na pracovnej ploche OM zvolíme možnosť Choose Individual Statistics, kde si vyberieme požadované štatistiky.

3.1. Výsledky simulácie prenosu 3D obsahu v grafoch.

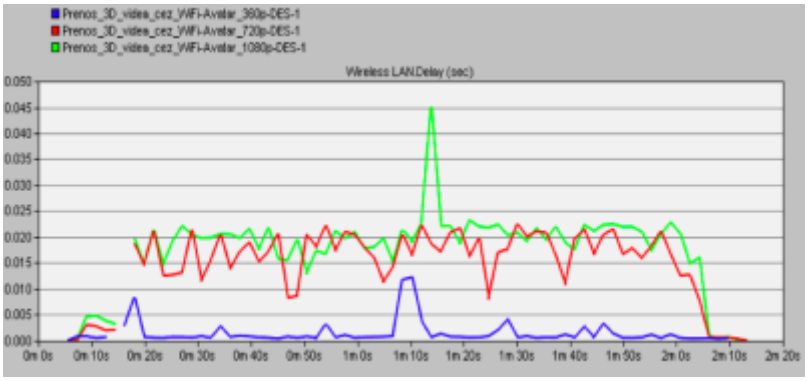
Každé 3D video malo rôznu kvalitu obrazu, konkrétne 360p, 720p a 1080p. V simulačných scenároch sme porovnávali správanie siete pri rôznych kvalitách video obsahu s dodatočným zaťažením pomocou aplikácií video konferencia, prezeranie obrázkov, databáza, FTP a email. Každý žáner bol v troch rôznych kvalitách, ako si môžeme všimnúť v prehľadnej tabuľke Tab. 2. Všetky ukážky sú vo formáte

MPEG4/AVC.

Názov 3D videa	Rozlíšenie (formát MPEG4/AVC)	I snímky		P snímky		Dĺžka sekvencie (min.)
		Max. veľkosť (kB)	Priemerná veľkosť (kB)	Max. veľkosť (kB)	Priemerná veľkosť (kB)	
Avatar (akčný)	1280x266	18,83	4,974	18,545	1,214	2:09
	1280x266	37,804	15,766	109,162	6,929	2:09
	1920x400	66,618	28,574	198,499	11,905	2:09
Ice Age 4 (animovaný)	640x360	39,372	12,953	9,639	2,429	2:18
	1280x720	124,553	39,867	33,414	8,8	2:18
	1920x1080	232,363	74,778	74,26	17,64	2:18

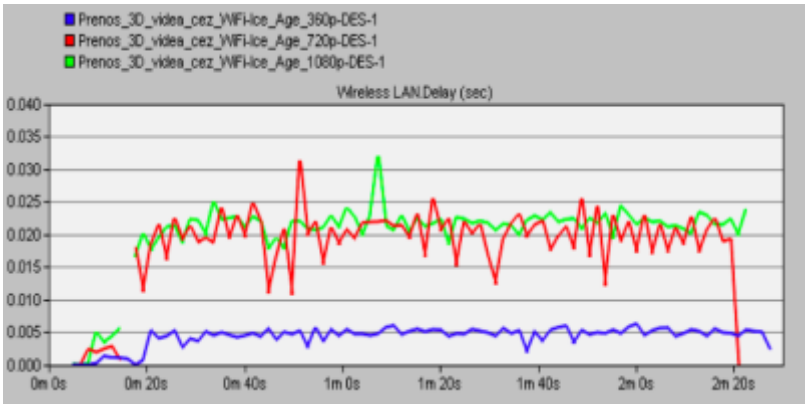
Tab. 2 Parametre prenášaných 3D sekvencií

Pri prenose 3D videosekvencií sme sledovali priepustnosť WLAN parametre prenosu počet prijatých a odoslaných paketov modulom SITL oneskorenie 3D videa počas celého prenosu cez WLAN. Prvý graf z testovanej 3D video sekvencie Avatar ukazuje oneskorenie pri rôznej kvalite prenášaného videa. Výsledky sú znázornené na obr. 6. kde vidieť, že oneskorenie je väčšie pri vyššej kvalite prenášaného videa. Špičkové hodnoty dosahujú 0.045 sekundy.

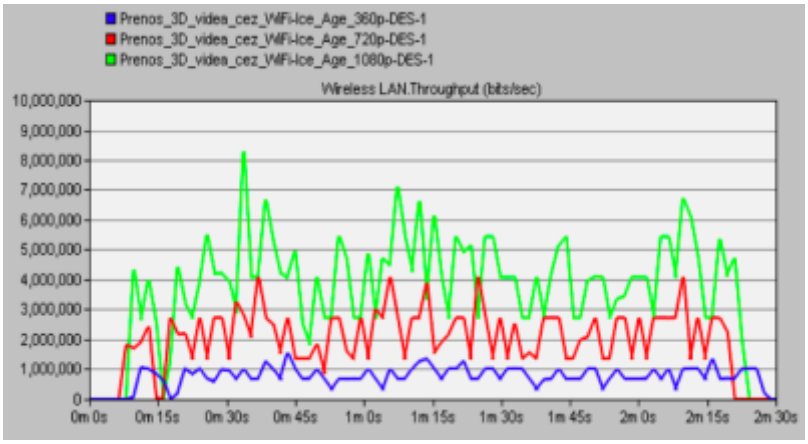


Obr. 6 Oneskorenie – Avatar

Testovanie 3D animovanej sekvencie Ice Age prebiehalo za rovnakých podmienok, ako pri predchádzajúcej sekvencií. Na obr.7 a obr.8 je porovnané oneskorenie a priepustnosť pri rôznej kvalite videa.



Obr. 7 Oneskorenie – Ice Age



Obr. 8 Priepustnosť – Ice Age

4. Záver

V tomto článku sme chceli poukázať na analýzu QoS strímu pre MHP služby v nestabilných IP sieťach. Bol znázornený spôsob implementácie kvality služieb jej vlastnosti. Kvalitu služieb je možné realizovať v simulačnom programe Opnet, ktorý umožňuje modelovanie, analýzu a vymodelovanie sietí. Taktiež je možné vytváranie vlastných modelov zariadení, protokolov, aplikácií, a parametrov QoS. Možno porovnávať vplyv rôznych technológií, modelovať rôzne typy prevádzky. Hlavnou doménou tohto simulačneho nástroja je rýchla a efektívna práca vďaka jeho grafickému prostrediu rozšírenej knižnici. Pri simulovaní namodelovanej siete je možne vidieť a zaznamenávať rôzne druhy štatistík. Po ukončení simulácie je možné výsledky zobraziť v grafoch a spracovať.

Literatúra

1. SMITKA, P.: Architecture design in IP telephony, http://diplomovka.sme.sk/zdroj/3224.doc
2. Quality of services, http://sk.wikipedia.org/wiki/QoS
3. ZAPLETAL, L.: Simulace modelu QoS v prostredí Opnet IT Guru, Fakulta elektrotechniky a komunikačných technológii ústav telekomunikácií, Brno, 2008
4. MAJERSKÝ, M.: Simulačný model siete Metro ethernet s MPLS chrbticovou sieťou v Opnet Modeler, Žilinská univerzita, Žilina, 2010
5. BOŽIK, M: Simulácia prenosu 3D videotokov pomocou programu Opnet Modeler, Technická univerzita v Košiciach, Fakulta elektrotechniky a informatiky, Košice, 2013
6. ZEMAN, O.: Modelování síťových aplikací a měření provozu v prostředí Opnet, Vysoké učení technické v Brně, Brno, pp. 2-6, 2006
7. Opnet Technologies, Inc., Opnet Modeler Documentation set., 2008
8. SENDREI, L.: H.264 Video prenos vo WLAN v prostredí Opnet Modeler, Technická univerzita v Košiciach, Fakulta elektrotechniky a informatiky, Košice, 2012

Spoluautorom článku je Ján Valiska, Katedra elektroniky a multimediálnych komunikácii, FEI TU Košice, Košice, Letná 9, 042 00 Košice