Semestrální práce z předmětu X36MTI
na téma:

Libor Bánovský

říjen 2007

1. Úvod

Tato práce by měla poskytnout ucelený pohled na technologii BitTorrentu. Obsahuje jak základní informace, které pomohou zorientovat se čtenáři, který o BitTorrentu nikdy neslyšel, tak informace pokročilejšího charakteru, jako je pohled na protokol, bezpečnost a vývoj pro BitTorrent. Obě skupiny by pak měla zajímat kapitola o legálnosti, protože „neznalost neomlouvá“.

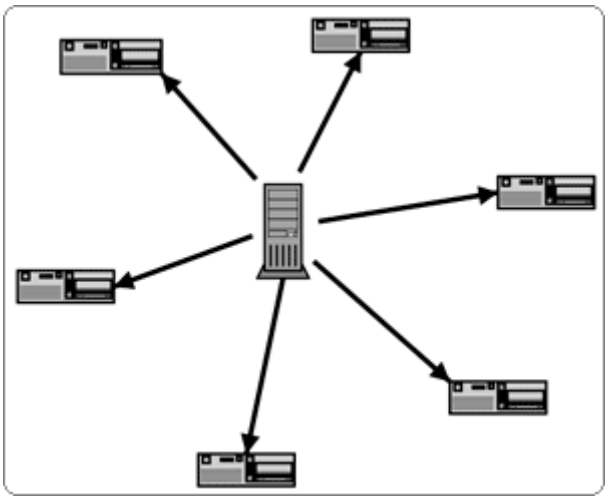
2. BitTorrent obecně

BitTorrent je distribuční protokol využívaný v sítích peer-to-peer, dále jen P2P, pro distribuci souborů. Název BitTorrent se ovšem vžil také pro pojmenování klientské aplikace, která tento protokol používá a také pro typ souborů s příponou `torrent`. Autorem je Bram Cohen, který ho představil světu v roce 2002. Referenční implementace je na psána v Pythonu a je uvolněna pod licencí BitTorrent Open Source Licence.

2.1. Klasický model sdílení souborů

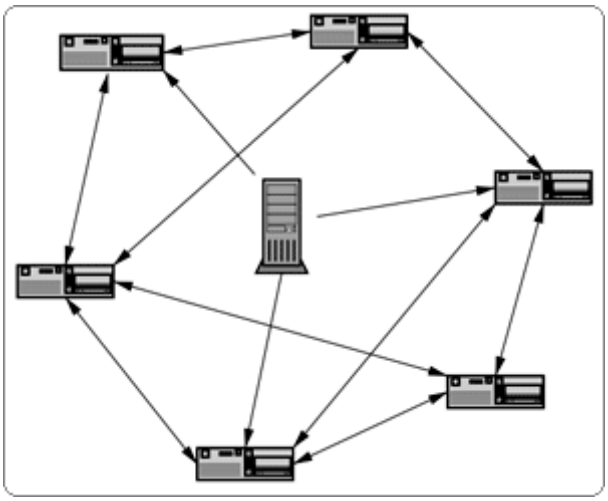
Sdílení souborů klasickou cestou předpokládá, že se každý klient připojuje pouze k serveru. To přináší následující problémy:

- Soubor se downloaduje delší dobu a tím pádem je během stahování k serveru současně připojeno více uživatelů.
- Zdroje serveru je nutné rozdělovat mezi více uživatelů - každý dostane menší díl CPU, paměti a přenosového pásma.
- Pokud se celý soubor nevejde to cache serveru, je nutné provádět mnoho diskových seek operací - v nejhorším případě jeden seek na každý odeslaný blok, což dále snižuje výkon.
- Velké soubory spotřebovávají zdroje ostatním službám na serveru.
- Největším problémem je potřeba velkého přenosového pásma. Nemilé je to zvláště v případě, pokud platíme za přenesené bajty.



2.2. BitTorrent model sdílení

Při distribuci pomocí BitTorrentu jsou soubory rozděleny klientem na menší bloky. Velikost resp. počet bloků lze nastavit. Každý klient může požádat kteréhokoliv jiného klienta, o jemu chybějící blok, a zároveň poskytuje ostatním svoje již kompletně stáhnuté bloky. Často klient může upřednostňovat méně se vyskytující bloky, nebo i bloky na začátcích souborů. Stahování přes BitTorrent je tím rychlejší, čím více klientů má již staženo celý soubor a poskytuje jej ostatním. Odpadá tak efekt „úzkého hrdla“ serveru.



3. Terminologie

torrent
: Je buď soubor `.torrent`, tedy soubor metadat o downloadu, nebo všechny soubory, které jsou jím popisovány.

soubor `.torrent`
: Obsahuje metadata o distribuovaných souborech. Obsahuje jména souborů, jejich velikosti a kontrolní součet jednotlivých bloků torrentu. Také obsahuje adresu trackeru.

seed
: Peer, který má kompletní kopii torrentu a stále nabízí upload. Čím více seedů je ve swarmu, tím větší bývá rychlost downloadu a také se zvyšuje šance na stažení kompletního souboru. Seedováním je torrent udržován v chodu.

peer
: Instance BitTorrent klienta běžícího na počítači. Obvykle je peerem nazýván ten, kdo nemá kompletně stažený torrent.

leech
- Je peer, který nemá kompletně stažený torrent. Když je download kompletní, leech se stává seedem
- Termín leech bývá také používán pro neslušného peera, který má velmi malý poměr uploadu/downloadu, nebo který opustí swarm hned po tom, co se stane seedem. Leeches obvykle spotřebovávají největší přenosové pásmo swarmu.

swarm
: Všichni peers, kteří sdílí torrent, se nazývají swarm. Například šest leeches a jeden seed je swarm (svazek) sedmi.

tracker
: Je HTTP nebo HTTPS služba, která zprostředkovává a režíruje spojení mezi klienty

(přechovává seznamy IP adres peerů), ale data přes něj netečou, ani nemá žádnou kopii torrentu. Odpovídá pouze na HTTP GET dotazy. Dotazy obsahují informace od klientů pomáhající trackeru udržovat přehled o stavu torrentu, odpověď obsahuje seznam peerů, takže se klient může podílet na torrentu (stahovat nebo šířit).

4. Stahování a sdílení

4.1. Stahování

K započetí stahování pomocí BitTorrentu jsou zapotřebí následující kroky:

- Nainstalovat BitTorrent klienta
- Prohlížet webu
- Kliknout na link .torrent souboru
- Nalézt kam požadovaný soubor uložit na disk
- Počkat až se dokončí stahování
- Ukončit klienta – do té doby sdílí stažená data

4.1.1. Získání metadat

Metadata jsou uložena v souboru s koncovkou .torrent. Tato metadata najdete na webové stránce spolu s upozorněním na možnost stažení souboru pomocí BitTorrentu. Je vhodné mít webbrowser nakonfigurován tak, aby podle koncovky nebo MIME typu automaticky spustil BitTorrent klienta. Metadata lze získat i jinou cestou (FTP, IRC, Email, ...) a je ovšem nutné na ně spustit BitTorrent klienta ručně.

4.1.2. Hledání chybějících bloků

Po získání a zpracování metadat začne BitTorrent klient hledat ostatní počítače stahující tentýž soubor. K jejich vyhledání slouží služba Tracker. URL této služby je uvedeno v položce announce v .torrent souboru. Existuje neoficiální rozšíření syntaxe 'announce-list', které umožňuje zadat seznam více Trackerů. Pokud je tracker nedostupný, nelze totiž soubor stáhnout.

Tracker je služba používající architekturu klient-server. Tracker komunikuje HTTP protokolem a obvykle běží na portu 6969. Úkolem služby Tracker je udržovat aktualizovaný seznam počítačů stahujících příslušný soubor. Tracker kromě toho shromažduje statistické informace o klientech (počet přenesených dat) a počítá downloady. Jeden Tracker může obsluhovat více .torrent souborů současně. Odhaduje se, že jeden Tracker zvládne okolo 10 000 klientů současně. Většina trackerů poskytuje po připojení web browserem různé doplňkové služby (statistika, chat, možnost hledání a stáhnutí .torrent souborů).

Klienti pravidelně ohlašují Trackeru svůj stav (started, stopped, completed), celkový počet přenesených bajtů (uploaded, downloaded), počet zbývajících bajtů (left). Nejdůležitějšími informacemi předávanými Trackeru jsou 20bajtové peer_id, IP adresa a číslo portu, na které jsou pro ostatní klienty k zastižení. Od Trackeru obdrží BitTorrent klient seznam několika ostatních a začne s nimi přímo komunikovat.

4.1.3. Přenost dat

V peer to peer síti BitTorrent existují dva typy uzlů: peer a seed. Rozdíl mezi těmito uzly není technický, ale spíše politický. Po technické stránce jsou oba dva naprosto shodné: používají stejný protokol a stejně se Trackeru ohlašují. Jediný rozdíl je ten, že seed vlastní kompletní kopii

souboru, zatímco peer nikoliv. Seedem se stává peer uzel automaticky v době, kdy má k dispozici kompletní stahovaný soubor. Pokud je spuštěn BitTorrent klient na již downloadovaný soubor, stane se seedem.

Myšlenka peer to peer sítě je založena na vzájemné spolupráci. Peer uzly se navzájem spojují a vyměňují si mezi sebou jednotlivé části souboru, a to nejlépe v poměru 1:1. Ty mně dáš jeden blok, co ještě nemám, a já ti za to dám jeden blok, co ty nemáš. Každý soubor je totiž předem rozdělen na bloky (obvykle 256K), jejichž SHA1 checksumy jsou známé z .torrent souboru.

Každý peer uzel se snaží připojit k rozumné míře (zhruba 10) ostatních uzlů. Po připojení si uzly navzájem vymění seznamy svých bloků. Uzel si tak může vybrat, o který blok požádá. V současné době se používají dvě strategie: náhodný výběr {random} a nejméně se vyskytující (rarest first) blok. Protože peer uzel nechce poskytovat své bloky zadarmo, začne nejprve vyměňovat své bloky za nějaké, které ještě nemá. Teprve potom, co nemá již nic na výměnu, dává semtam nějaké bločky ostatním zdarma, protože doufá, že od nich také něco dostane. Dávání bloků zdarma je nezbytné pro správnou funkci sítě -- odstranění dead-lock stavu. Uzel čas od času doluje z Trackeru seznam dalších uzlů.

Peer uzly si také mohou vymýšlet. Aby zvýšily svou šanci na získání bloků, mohou předstírat, že mají více bloků na výměnu než ve skutečnosti. V současné době se používají dvě metody podfuků: buďto se peer uzel na žádost o blok neobtěžuje nic poslat, nebo pošle náhodná data. Většina klientů tyto podfukáře rychle pozná a přestane dále komunikovat. V současné době neexistuje metoda, jak tyto uzly bonznout Trackeru. Při stahování delších souborů (ISO Image) se podvody nevyplácejí, při stahování MP3 to většinou projde, protože než to ostatní zjistí, máte již staženo.

Uzel typu seed je narozdíl od uzlu typu peer velice štědrý. Protože má všechno a nic nepotřebuje, dává zadarmo bločky komukoliv, kdo o ně požádá. Uzel typu seed se s výjimkou Trackeru nikam nespojuje, pouze čeká na příchozí spojení. Aby se zabránilo jejich přetížení, jsou seed uzly omezovány, a to jak počtem připojených peer uzlů, tak objemem přenesených dat za sekundu.

Pro zajištění úspěšného downloadu je žádoucí, aby byl vždy připojen alespoň jeden uzel typu seed. BitTorrent technologie umožňuje download i v případě tzv. distribuované kopie - klienti mají rozdílnou sadu bloků, která po složení dá celý soubor.

Aby bylo celé toto řešení dostatečně výkonné, je zásadní zvolit vhodný algoritmus pro výběr částic ke stahování. BitTorrent se řídí těmito pravidly:

- **Podle příslušnosti:** Do fronty se řadí částice příslušné jedinému bloku, až po jeho úplném stažení je možné začít stahovat částice dalšího bloku. Tato strategie vede k nejrychlejšímu přísunu celistvých bloků.
- **Podle vzácnosti:** Klient řadí do fronty takové částice, které má nejmenší počet ostatních klientů (jsou tedy nejvzácnější). Tím se zvýší pravděpodobnost, že bude mít co nabídnout ostatním klientům. Tato strategie je vhodná především na počátku života torrentu, kdy jsou data obvykle na jediném zdroji, protože klienti si co nejdříve vytvoří distribuovanou kopii dat a původní zdroj pak může být odpojen.
- **První blok náhodný:** Při začátku stahování nemají klienti žádná data, která by mohli posílat dalším klientům, je tedy žádoucí, aby se stáhl celý blok co nejdříve. Klienti respektující pouze pravidlo 2 by tedy čekali neúměrně dlouho na první blok (je vzácný, tudíž pro jeho přenos je menší šířka pásma uploadu), čímž by se distribuce dat zpomalila. První blok pro přenos je proto zvolen náhodně a až následující je volen strategií podle vzácnosti.

- **Mód dokončení:** Pokud je částice požadována po pomalém klientovi, musel by klient dlouho čekat na dokončení stahování. Ke konci stahování proto vyšle všem klientům, kteří mají příslušný blok, žádost o zaslání všech zbývajících částic. Po navázání prvního příjmu dané částice jsou ostatní žádosti zrušeny.

4.2. Sdílení

Pro začátek sdílení nějakého souboru jsou nutné následující kroky:

- Spuštění trackeru
- Spuštění web serveru, např. Apache
- Nastavení asociace přípony .torrent s mimetypem `application/x-bittorrent` na tomto serveru
- Vytvoření metadat (.torrent) obsahující kompletní popis sdílených dat a url trackeru
- Vložení těchto metadat na web server
- Přilinkování se na tato metadata z nějaké webové stránky
- Spuštění downloaderu, který má sdílená data

4.2.1. Vytváření torrentů

Soubor .torrent je malý binární soubor obsahující údaje o stahovaném souboru. Soubor metadat pro 690MB CD-ROM image je veliký zhruba 50 kB. Metadata jsou kodována pomocí tzv. bencoding (např. řetězec je uložen jako velikost:řetězec, integer jako ičísloe). Obsahuje následující údaje:

info: popis souboru torrentu. Jsou dvě možné formy:jedna pro případ 'single-file' torrentu bez adresářové struktury a druhá pro 'multi-file' torrent.

announce: url trackeru

announce-list: (volitelně) rozšíření od původní specifikace umožňující použití více trackerů

creation date: (volitelně) datum vytvoření, ve standardu unixového formátu (integer v sekundách od 1-Jan-1970 00:00:00 UTC)

comment: (volitelně) libovolný string

created by: (volitelně) jméno a verze programu použitého k vytvoření .torrent souboru

Informační část:

piece length: počet bitů v každém bloku

pieces: string obsahující 20-bytové SHA1 hashovací hodnoty

Informace pro single-file:

name: jméno souboru

length: velikost v bytech

md5sum: (volitelně) 32-znakový hexadecimální string odpovídající MD5 součtu souboru.

Informace pro multi-file:

name: jméno adresáře kam ukládat všechny soubory

files: seznam informací jednotlivých souborů obsahující následující informace:

length: velikost v bytech

md5sum: (volitelně) 32-znakový hexadecimální string odpovídající MD5 součtu

souboru.

path: seznam obsahující jeden nebo více znakových řetězců identifikujících cestu souboru. Např. pro cestu "dir1/dir2/file.ext" bude obsahovat řetězce "dir1", "dir2", and "file.ext". Toto bude benkódováno jako: *l''***4**:dir1'**4***:dir2'***8**:file.ext'**e***

Příklad úvodní textové části .torrent souboru:

```
d8: announce30: http://localhost:6969/announce7: comment30: NetBSD 1.6.2 for I386 - Disc 213: creation datei1078940925e4: infod6: lengthi690257920e4: name21: NetBSD-i386-1.6.2.ISO12: piece lengthi262144e6: pieces52680:
```

4.3. Specializace BitTorrentu

Kromě původního účelu se již také uvažuje i o jiném využití BitTorrent sítí. Jednou z možností je např. použití k vysílání televizních pořadů (TV-on-demand) při minimálních nákladech. Princip "sněhové koule", kdy se (v budoucnu) populární soubor od několika uživatelů šíří exponenciální řadou, samozřejmě televizním studiům neunikl. S vlnou oblíbeného pořadu, který si uživatel může stáhnout kdykoliv bude chtít, jde ruku v ruce samozřejmě i příslib příjmů z reklamy. Přitom podle internetových zdrojů náklady na distribuci 500GB dat v rámci sítě BitTorrent během jediného měsíce činily 4$. K tomuto účelu byla spuštěna služba BitTorrent DNA. Jedná se o komerční službu sloužící k šíření licencovaného multimediálního obsahu jako jsou filmy, hudba a tv programy. Spolu sní se objevil internetový obchod s videi licencovanými od hollywoodských studií pod záštitou bittorrent.com, který tuto distribuční technologii nyní nabízí jiným firmám.

4.4. Bezpečnost a omezení

BitTorrent neposkytuje uživateli anonymitu. Je totiž možné z trackeru zjistit ip adresu všech aktuálních účastníků swamu, dokonce i těch, kteří se v minulosti již odpojili.

Další ne dobrou vlastností je to, že není možné, ani dobré, nutit klienty, aby po stažení požadovaných dat zůstávali delší dobu seedy. To zapříčiňuje pomalé vymírání torrentu a velmi špatnou dostupnost starších a ne tolik populárních dat. Některé BitTorrent weby se této vlastnosti snaží zabránít tak, že monitorují poměr mezi uploadem a downloadem klienta a podle toho mu přidělují maximální rychlost downloadu. Ten, kdo urdžuje seedy po krátkou dobu, pak logicky není schopen dosáhnout rozumného downloadu, dokud svůj upload nezvýší. Následkem můžou být rychlosti stahování v mezích 1-10kB/s. Vyjímku mohou dostat pouze klienti připojení přes dial-up.

4.5. Legálnost

Problém legálnosti nabízeného obsahu trackery neřeší, protože matadata, která na jejich službu odkazují neobsahují žádný záznam o copyrightu nabízených dat. Je předpokládáno, že veškerý nabízený obsah je volně šířitelný, což se v praxi moc nedodržuje a mnoho trackerů muselo být z popudu protipirátských organizací jako je RIAA a MPAA uzavřeno.

V nynější době protipirátské organizace běžně využívají botů k monitorování torrentů a klientů k nim připojených, zda nesdílí nelegální obsah, pokud se taková činnost zjistí, je většinou odeslán mail providerovi o takovém jednání, ten pak buď zmíněného zákazníka odpojí nebo, a to se děje ve většině případů, takový mail maže. Nicméně již bylo několik lidí za šíření nelegálního obsahu odsouzeno, a toto jednání se sleduje.

5. Klienti

- **BitTorrent** – BitTorrent klient autora komunikačních protokolů BitTorrent. Jeho uživatelské rozhraní je jednoduché. Klient je napsán v Pythonu, a lze jej provozovat na řadě platforem včetně Windows, Linux a MacOSX.
- **Azureus** – Funkčně vyspělý multiplatformní opensource BitTorrent klient. Je napsán v Javě, takže funguje na většině současných operačních systémů. Ihned po instalaci je uživatelské rozhraní v češtině (ovšem některé nové funkce již přeloženy nejsou).
- **µTorrent** – mimořádně nenáročný na systémové zdroje, jeho celková velikost se pohybuje kolem 150 KiB. Uživatelské rozhraní je velmi podobné výše zmíněnému Azureu. Je napsaný v C++. Dostupný je prozatím pouze pro operační systémy Microsoft Windows
- **BitComet** – také nenáročný na systémové zdroje, napsaný v C++, dostupný pouze pro operační systémy Microsoft Windows
- **TorrenTopia** – spíše pro méně náročné uživatele. Zajímavý klient pro torrent soubory. Jako jeden z mála umožňuje změnu vzhledu. Neobsahuje oficiální český překlad. Výhodou je možnost vyhledávání torrentů pomocí vestavěného vyhledávače. Nevýhodou je, že neobsahuje pokročilé funkce, jako třeba blokování IP adres.
- **ABC** – Rychlý spolehlivý, méně funkcí, jednodušší alternativa k µTorrentu.
- **Tribler** – Tento klient je odvozený od ABC klienta, ale nabízí společenské sdílení. Nemusíte torrenty vyhledávat, vyberete je ze seznamu ostatních uživatelů. Pokud stahujete stejné torrenty jako jiný uživatel, v seznamu uvidíte jako první torrenty uživatele se stejnými zájmy (řazení podle doporučení = shoda zájmů).
- **RTorrent** – Konzolový klient pro unixové systémy napsaný v C++.
- **BitLord** – další pokročilý BitTorrent klient pro Windows.
- **KTorrent** – nenáročný BitTorrent klient pro Linuxové prostředí KDE, obsahuje například integrovaný vyhledávač, týdenní časovač objemu proudu dat, umožňuje zabezpečené stahování a filtr IP adres, výběr jednotlivých souborů ke stažení a jako všechny aplikace KDE je kompletně lokalizován.
- **Deluge** – klient napsaný v Pythonu a používající GTK+.

6. Vývoj

Původní specifikace BitTorrent protokolu je i nadále open source, nicméně nová verze protokolu je již uzavřená. Tento krok je zdůvodněn hlavně tím, že vznikalo mnoho klientů obsahujících malware. Druhou stranou mince se zdá ovšem tímto snaha zabránit širšímu okruhu programátorů vytvářet konkurence schopné klienty BitTorrent podporující. Vývoj pro BitTorren bude nadále možný pouze přes zveřejněné SDK.

7. Závěr

BitTorrent je velmi zajímavá služba, poskytující v optimálních případech výsledky nedosažitelné klasickou cestou, ovšem trpící také mnoha neduhy, jako je rychlá úmrtnost torrentů. Osobně jsem velice zvědav do jaké míry dojde ke komercializaci.

Vzhledem k efektivnosti šíření dat bych používání BitTorrentu doporučil každému, internet by byl rychlejší, svět krásnější :-)

8. Zdroje

Stránka Brama Cohena -	http://www.bitconjurer.org
Oficiální stánka BitTorrentu -	http://www.bittorrent.com
Wikipendie -	http://en.wikipedia.org/wiki/BitTorrent
	http://cs.wikipedia.org/wiki/BitTorrent
Root.cz -	http://www.root.cz/clanky/bittorrent-technologie
Bittorrent.webz.cz -	http://bittorrent.webz.cz