

Anonimowość w BitTorrentcie

Łukasz Jancewicz
2008

Zarys prezentacji

- BitTorrent
- Tribler
- Cooperative Download
- Privacy Mode

BitTorrent

- Najpopularniejszy obecnie protokół peer-to-peer
 - uTorrent
 - Azureus (Vuze)
 - Opera
- Kiedyś był na otwartej licencji
 - stąd...
- Komercyjne zastosowania!
 - Gry kupowane w Internecie
 - Patche do gier (WoW itp.)
- Prawdopodobnie największa zaleta: prostota

BitTorrent – jak działa?

- Plik .torrent – deskryptor pliku
 - Zestaw plików traktowany przez protokół jak jeden plik
- Podział na fragmenty (chunks)
 - Wielkość fragmentu dostosowana do rozmiaru pliku (ok. 512 kB)
- Strony przechowujące pliki .torrent
 - <http://www.thepiratebay.org/>
 - <http://www.mininova.org/>
 - <http://www.legaltorrents.com/>

BitTorrent – jak działa?

- Tracker – koordynator pobierania plików
 - Oddzielne dane dla każdego pliku .torrent
 - Wokół pliku tworzy się tzw. rój (*swarm*) – zbiór użytkowników, którzy go pobierają
- Klient BitTorrenta
 - kontaktuje się z trackerem, by uzyskać adresy IP i porty pozostałych użytkowników
 - Kontaktuje się bezpośrednio z innymi klientami, prosząc ich o konkretne części pliku
 - W tym czasie obsługuje prośby innych klientów

BitTorrent – jak działa?

- Nie można wysyłać wszystkim proszącym
 - Mechanizm dławienia (*choking*)
- Wysyłamy ustalonej liczbie klientów, którzy do tej pory okazali się najbardziej wdzięczni
 - Iterowany dylemat więźnia?
- Reputacja klienta liczona oddzielnie dla każdego roju (*swarm*)
 - Tracona po zakończeniu pobierania

BitTorrent a anonimowość

- Tracker ma listę adresów wszystkich pobierających
- Każdy użytkownik pobiera tę listę od trackera
- Rozszerzenia protokołu
 - PEx (Peer Exchange) – użytkownik wysyła innym informacje o użytkownikach
- Łatwo sprawdzić, czy użytkownik naprawdę pobiera plik
 - Wystarczy spróbować coś od niego pobrać lub coś mu wysłać

BitTorrent – inne problemy

- Fałszywe pliki
 - Brak ogólnego mechanizmu weryfikacji treści
- Reputacja „per swarm”
 - Ułatwia oszukiwanie, czyli pobieranie bez wysyłania

Tribler

- Wersja BitTorrenta na bazie BitTornado
- Warstwa społecznościowa
 - Przyjaciele
 - Rekomendacje
- Decentralizacja
 - Rozproszone przechowywanie deskryptorów
- Przyspieszenie
 - Cooperative Download
 - Reputacja na podst. ilości przesłanych danych
- Transmisje wideo

Tribler – założenia

- Komputery mają duże dyski
 - Klient przechowuje bardzo dużo informacji o strukturze sieci, plikach, użytkownikach, itp.
- Użytkownik rzadko pobiera plik
 - Jego łącze jest często niewykorzystywane
 - Kiedy już pobiera, chce to robić z pełną prędkością

Tribler – plany

- Privacy Mode
 - Anonimowość
- Uniezależnienie od trackerów
 - Rozproszone utrzymywanie rojów (*swarms*)

Po co anonimowość?

- Anonimowość == prywatność
- Nie każdy lubi, kiedy wszyscy mogą się dowiedzieć, co robi
- Treści:
 - Wstydlive
 - Nielegalne
 - Zdradzające tożsamość (filmy, dokumenty, etc.)

Stopnie anonimowości

- Niewykrywalne posiadanie i używanie programu
- Niemożliwość poznania pobieranych/udostępnianych treści
- Niepewność co do pobieranych/udostępnianych treści
- Można ukrywać udostępnianie bardziej, niż pobieranie
 - Sandstorm P2P
- Lepsza anonimowość \Leftrightarrow niższa wydajność

Anonimowość dziś

- Tor
 - <http://www.torproject.org>
 - Najlepsza obecnie sieć zapewniająca prywatność
 - Korzysta z dedykowanych serwerów na całym świecie
- I2P
 - <http://www.i2p2.de>
 - Opiera się na tunelowaniu przez „zwykłych” użytkowników
 - Brak mechanizmów zachęcających do pomocy

Ile anonimowości potrzebujemy?

- Polskie prawo karne:
 - Podejrzane 2 osoby
 - Żadna się nie przyznaje
 - Brak dodatkowych dowodów
 - Uniewinnienie obu podejrzanych
- Brak wyroków w prawie europejskim i amerykańskim w sprawach dotyczących wymiany plików

Plausible deniability

- Dwie różne czynności wyglądają z zewnątrz w ten sam sposób
- Jedna jest obciążająca, druga nie
- Kompromis między prywatnością a wydajnością
- Przykłady:
 - Oglądanie obrazka / czytanie zaszyfrowanej w nim wiadomości
 - Odbiorca pliku / serwer proxy

Tribler – Cooperative Download

- Jeśli wszyscy klienci pobierają ten sam plik od siebie nawzajem, to każdy pobiera z taką prędkością, z jaką wysyła
- ADSL – słabo
- Ale komputery często nic nie pobierają
 - Można to wykorzystać!

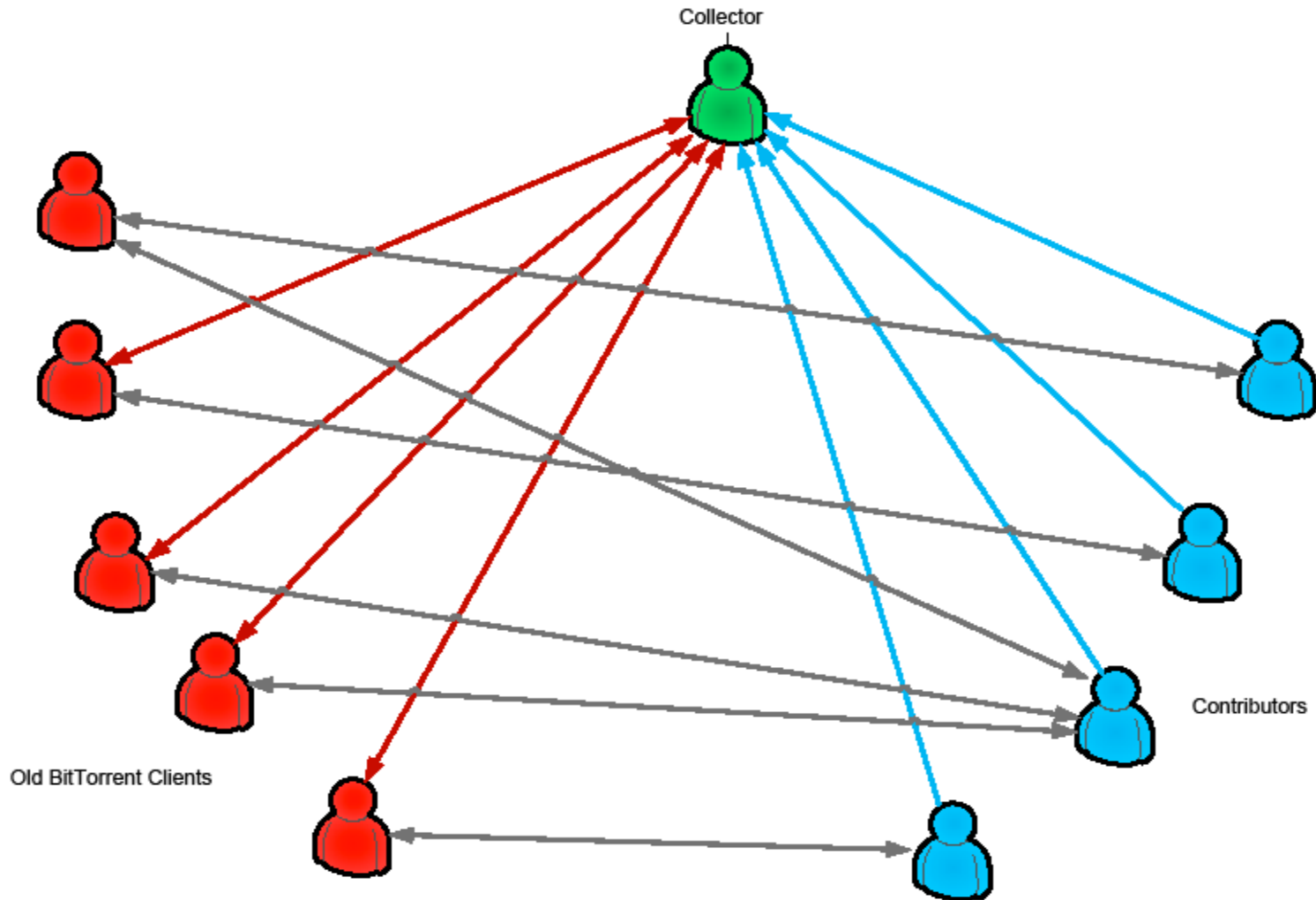
CoopDownload – opis

- Koordynator (odbiorca pliku) znajduje pomocników
- Pomocnicy pobierają od niego deskryptor pliku
- Zaczynają pobierać od innych użytkowników te części pliku, o które poprosi ich koordynator
- Dla pozostałych wyglądają jak zwykli użytkownicy, ale rozłączają się po zakończeniu pobierania przez koordynatora
- Sami nie zapisują sobie pobranych części (nie są zainteresowani tym konkretnym plikiem)

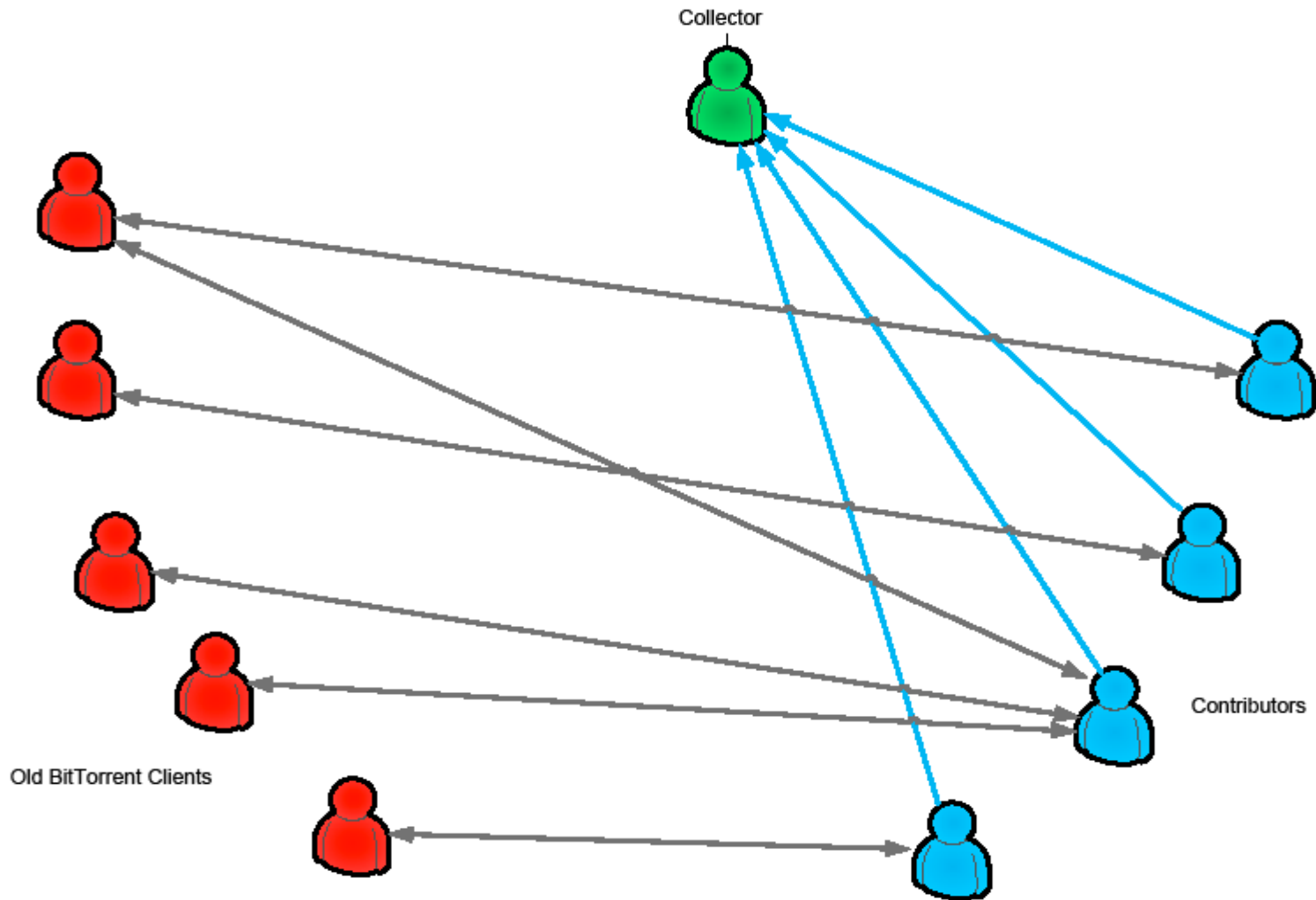
CoopDownload – wydajność

- Koordynator pobiera z pełną prędkością łączy
- Kompatybilne ze „starym” BitTorrentem
- Pomocnicy zyskują reputację
- Koordynator traci reputację u pomocników
 - Odbudowuje ją przez pomaganie im innym razem

CoopDownload – schemat



Krok ku anonimowości



Jednoelementowy tunel

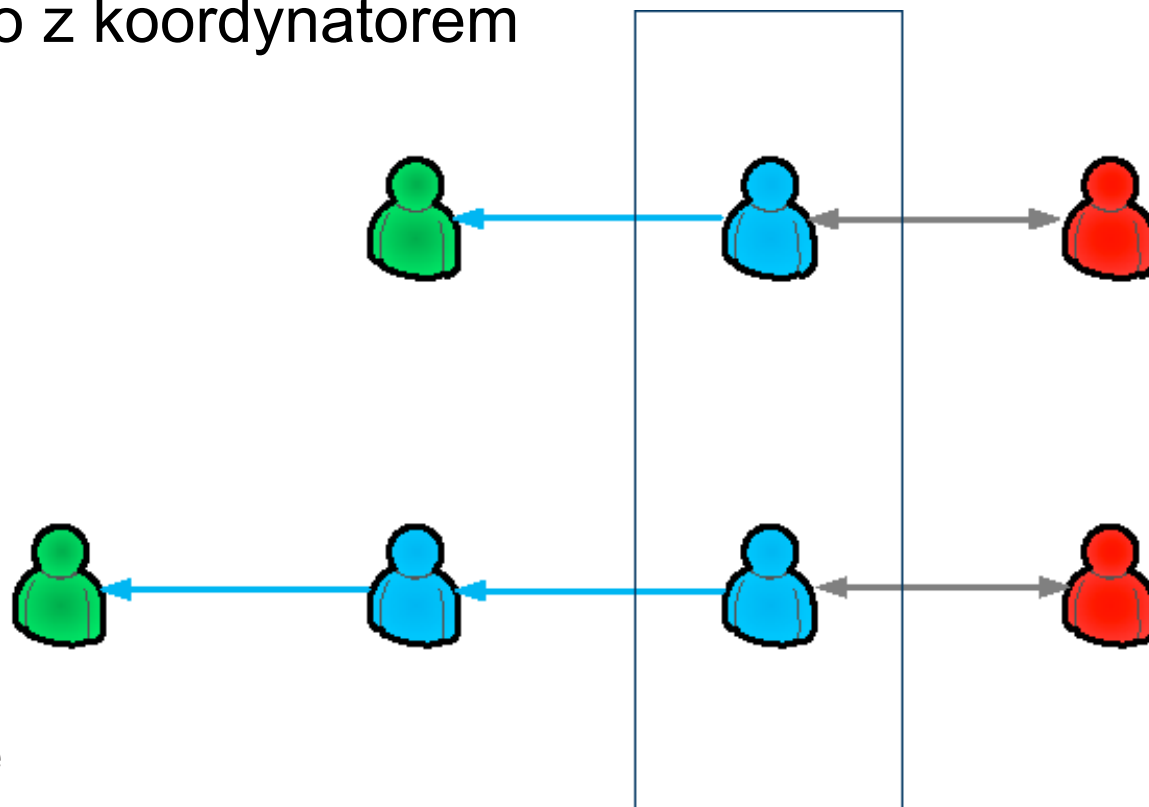
- Pobierający niewidoczny dla posiadacza pliku ani dla trackera
- Przy wystarczającej liczbie pomocników koordynator pobiera z pełną prędkością

Skąd brać pomocników?

- Przyjaciele
 - Ufamy im (?)
- Dowolni użytkownicy, którzy mają nieużywane łącze
 - Jak weryfikować ich wiarygodność?
 - Czy w ogóle trzeba to robić?

Przedłużenie tunelu

- Z pewnym prawdopodobieństwem pomocnik udaje koordynatora
 - Pomocnik nie jest pewien, czy kontaktuje się bezpośrednio z koordynatorem



Optymalizacja?

- Koordynator wcale nie musi rezygnować z bezpośredniego pobierania (!)
- Paranoid Mode ON/OFF

Co grozi pomocnikowi?

- Jeśli pożyczę samochód koledze, a on pojedzie obrabować bank, czy jestem odpowiedzialny?
 - Nie, ale czy to to samo, co pośredniczenie przy pobieraniu plików?
- Wi-Fi hijacking
 - Są wyroki uniewinniające
- Sprawa niemieckich routerów Tor
- A może pozwolić użytkownikowi filtrować, w czym chce pośredniczyć?

Autocenzura

- Anonimowość ułatwia przesyłanie treści nieakceptowanych przez zdecydowaną większość społeczeństwa
- „Democratic decloaking”
 - Użytkownicy mogą zgłaszać nieodpowiednie wg. nich treści
 - Wystarczająca liczba głosów przeciwko jednemu plikowi powoduje ujawnienie posiadacza
 - Na razie brak formalnego modelu
 - I nie wiadomo, czy tak naprawdę da się to zrobić
 - Ale byłoby fajnie 😊

Jak dobra jest anonimowość?

- Chaos
- Niepewność
- Niewiele poza tym
- Ale powinno wystarczyć!

- Można dodać szyfrowanie
 - Łatwe i nieciekawe

Inne problemy

- Anonimowość vs. reputacja
- Anonimowość vs. rekomendacje

Dziękuję za uwagę!

Pytania?