A Measurement Study of Attacks on BitTorrent Seeds

Autores: Prithula Dhungel, Xiaojun Hei, Di Wu, Keith W. Ross
Apresentado por: Edelberto Franco Silva

Publicado na ICC 2011

Abril, 2012

Agenda

Resumo

- Estudo de 2 modos de ataques em redes P2P (*peer-to-peer*).
- Ataque à semente inicial.
- Importância deste estudo:
  - no desenvolvimento de aplicações P2P altamente resistentes a ataques.
  - no entendimento das vulnerabilidades de sistemas baseados no BitTorrent.

Motivação

- Interesse em aplicações P2P mais resistentes a ataques.
- A indústria e os sistemas P2P.
- Abordagem:
  - testes em ambiente experimental.
  - validação dos resultados do ambiente experimental a partir de dados reais coletados por um Bittorrent modificado.
  - análise dos ganhos a partir de um modelo de fluidos simples.

Trabalhos Relacionados

- Análise das limitações do protocolo Bittorrent para *tit-for-tat*. Já em relação à segurança há poucos estudos.
- Como realizar ataques DDoS (*Distributed Denial of Service*) a qualquer *host* usando Bittorrent.

Ataques à semente inicial

- **Conceito principal:** diminuir a disseminação dos blocos referentes a *seed* incial.
- **Como funciona:** um atacante descobre que um *torrent* começou a ser distribuído e utiliza técnicas para "atrapalhar" (ou impedir) usuários reais de adquirir o conteúdo.
- **Tipos:** *bandwidth attack* e *connection attack*.

Bandwidth Attack

- Explora falhas do algoritmo de gerenciamento de *seed*.
- Sobrecarga do *upload* dos *peers*.
- Badwidth-first algorithm:
  - inicia o envio a 4 ou 5 *leechers* considerados melhores para a disseminação.
  - **leechers* melhores geralmente são aqueles com mais banda disponível para *download*.
  - de 30 em 30 segundos verifica se há um *leecher* melhor para trocar.

O ataque

- O atacante deve:
  - detectar que o *peer* está no estágio incial de disseminação da *seed*.
  - tentar ocupar continuamente o *peer*, sendo sempre escolhido como o melhor *leecher*.

Connection Attack

- 1 semente (*seed*) é igual a 50 *slots* de conexão.
- Ocupar o máximo de *slots*.
- Manter ocupado esses *slots*.

Metodologia

- Ambiente de ataque:
  - 1 semente = 1 arquivo.
  - 30 *leechers* legítimos.
  - 1 *tracker*.
  - *N* atacantes.
  - PlanetLab.
- O atacante:
  - cliente Bittornado 0.3.17.
  - recebe os blocos e não encaminha.
  - *leechers* autênticos com máximo de *upload* 48KB/s e 192KB/s de *download*.
  - atacantes com máximo de *upload* 10KB/s e 20KB/s de *download*.
- Análise do tráfego da *seed* em direção ao *leecher* e atacante com um Bittorrent modificado.
- Atacados seeds do Azureus 3.1.1, μTorrent 1.7.7 e Bittornado 0.3.17.

Modelo de fluido para *Badwidth Attack*

- Cenário I: favorece o leecher legítimo. ($b_A > b_L \geq u/n$)
- Cenário II: favorece o atacante. ($b_A \geq u/n > b_L$)

- u: banda para *upload*;
- n: número máximo de slots.

Type	File Size (MB)	Attacker				Leecher				Seed			
		Client	# of Attackers	b/w (KB/sec)		Client	# of Leechers	b/w (KB/sec)		Client	Unchoke Slots	Max Conn.	Up b/w (KB/sec)
				Up	Down			Up	Down				
b/w (I)	100	BT	40	u/l	u/l	BT	30	48	192	AZ	4	50	60/100/140
b/w (II)	100	BT	40	u/l	u/l	BT	30	20	40	AZ	4	50	500
Conn.	500	BT	800	10	20	BT	30	48	192	AZ	4	50	60/100/140
b/w (I)	500	BT	40	u/l	u/l	BT	30	48	192	BT	4	50	50/100/150
b/w (II)	100	BT	40	u/l	u/l	BT	30	20	40	BT	4	50	500
Conn.	500	BT	800	10	20	BT	30	48	192	BT	4	50	50/100/150
Combined	100	BT	800	u/l	u/l	BT	30	20	40	BT	4	50	500

- BT: Bittornado; AZ: Azureus; b/w: Bandwidth Attack;
- Conn: Connection Attack; I/II: Cenários e u/l: ilimitado.

Bandwidth Attack Azureus

Seed Uplink (KB/sec)	Avg Download Time w/o Attackers (mins)	Delay Ratio
60	36	2.24
60	36	2.58
100	35	1.37
100	35	1.45
140	34	1.08
140	34	1.04

TABLE II: Bandwidth Attack Results for Azureus (40 Attackers; 100 MB File; Leechers: 48 KB/sec & 192 KB/sec; Attackers: No Bandwidth Cap)

Mesmo com 40 atacantes e banda da *seed* $<$ 60KB/segundo, a razão do atraso $<$ 3.

Bandwidth Attack Azureus

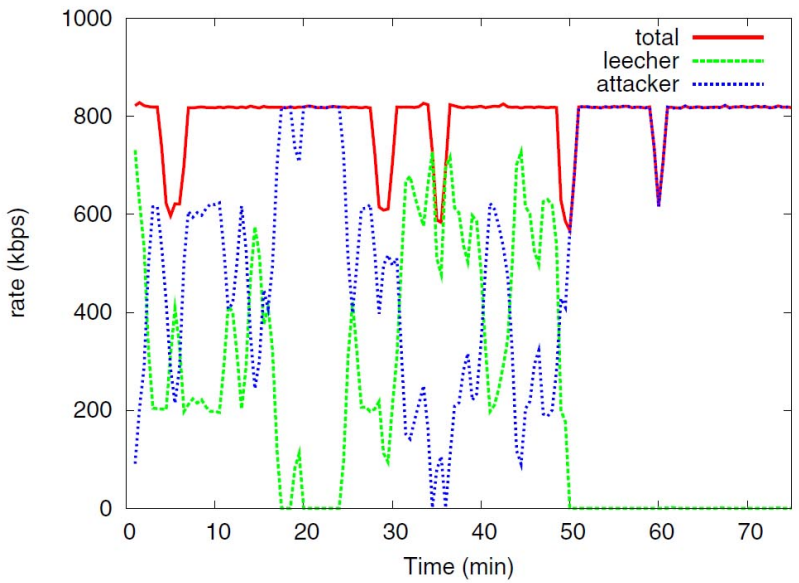

Fig. 1: Seed Bandwidth Distribution for Attackers and Leechers in an Azureus Bandwidth Attack

- Nem atacantes nem tão pouco *leechers* legítimos monopolizaram o *upload* da *seed*.
- Depois de 50min atacantes ocupam toda a banda da *seed*.
- Analisando o algoritmo de seleção: por conta da seleção otimista de *choke*, e cenário I, os *peers* têm a mesma chances, adicionando justiça a distribuição.

Bandwidth Attack Azureus

Seed Uplink (KB/sec)	Avg Download Time w/o Attackers (mins)	Delay Ratio
500	77	1.29
500	77	1.13

TABLE III: Bandwidth Attack Results for Azureus (40 Attackers; 100 MB File; Leechers: 20 KB/sec & 40 KB/sec; Attackers: No Bandwidth Cap)

- Cenário II.
- 40 atacantes com banda ilimitada e razão de atraso $< 1{,}5$.
- Porque o segundo critério do algoritmo de *seed* para *unchoke* é a quantidade de dados baixados.
- Escolhendo assim *leechers* legítimos de tempos em tempos.

Bandwidth Attack Bittornado

Seed Uplink (KB/sec)	Avg Download Time w/o Attackers (mins)	Delay Ratio
50	177	4.11
50	177	4.44
100	176	1.95
100	176	1.39
150	167	1.08
150	167	1.06

TABLE IV: Bandwidth Attack Results for BitTornado (40 Attackers, 500 MB File; Leechers: 48 KB/sec & 192 KB/sec; Attackers: No Bandwidth Cap)

- Cenário I.
- Ataque considerado ineficiente, com banda sendo compartilhada mais ou menos igual entre *leecher* e atacante.
- Considerado *upload* da *seed* $>$ 100KB/s.

Bandwidth Attack Bittornado

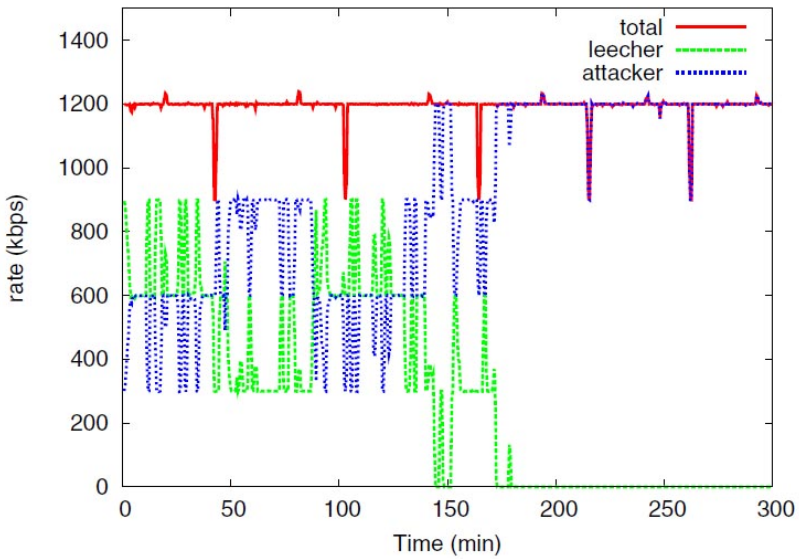

Fig. 2: Seed Bandwidth Distribution for Attackers and Leechers in a BitTornado Bandwidth Attack

- Cenário I.
- Considerados cenários com *upload* da *seed* = 150KB/s.
- Confirmando a boa distribuição pelo algoritmo de primeira *seed*, onde os *leechers* e atacantes brigam igualmente pelos *unchoke slots*.

Bandwidth Attack Bittornado

Seed Uplink (KB/sec)	Avg Download Time w/o Attackers (mins)	Delay Ratio
500	75	3.73
500	75	3.92

TABLE V: Bandwidth Attack Results for BitTornado (40 Attackers; 100 MB File; Leechers: 20 KB/sec & 40 KB/sec; Attackers: No Bandwidth Cap)

- Cenário II.
- Razão de atraso < 4.
- Observou-se que 3 de 4 *unchoke slots* eram ocupados por atacantes, e somente o *slot unchoke* otimista era ocupado ou por *leecher* legítimo ou por atacante.
- Mas, como *leecher* otimista tinha boa velocidade de *download*, não demorou muito para realizar o *download* do arquivo.

Bandwidth Attack - Conclusão

Bittornado e Azureus são muito resistentes a *bandwidth attack*.

Connection Attack Azureus

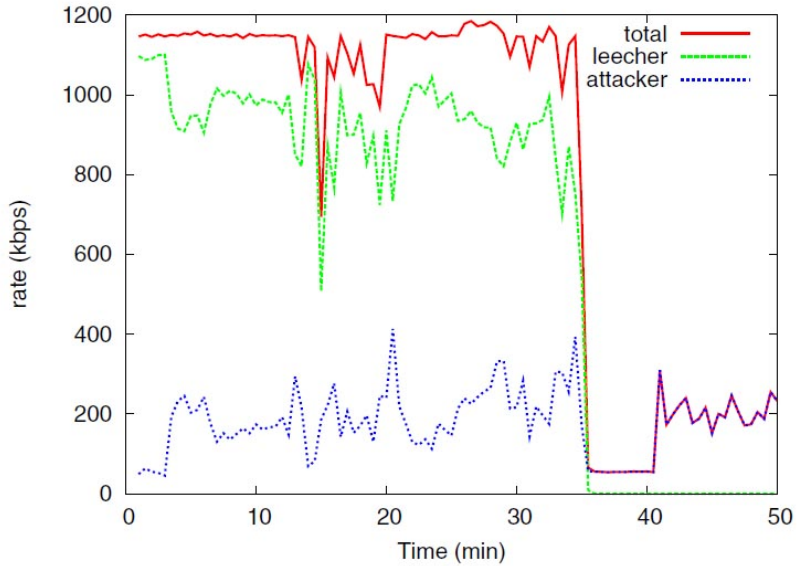

Fig. 3: Seed Bandwidth Distribution for Leechers and Attackers in an Azureus Connection Attack

- 50 *slots*. 5 ocupados pelos *leechers* legítimos (iniciados antes dos atacantes) e os 45 restantes ocupados pelos atacantes.
- *Upload* da *seed* = 140KB/s.
- Após 35min somente atacantes ocupando todos os *slots*.

Connection Attack Azureus

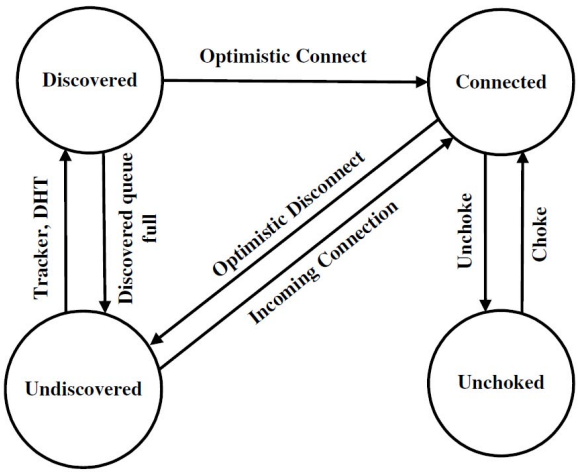

Fig. 4: State Diagram for Connection Management in Azureus

1. Premissa: todos os *slots* ocupados.
2. Lista "Discovered Peers", com os *peers* descobertos pelo *tracker*.
3. Se *slot* livre, então ocupa com o primeiro da lista, realizando o "Optimistic Connect".
4. A cada 30 segundos, se todos os *slots* ocupados, realiza "Optimistic Disconnect", que seleciona o *peer* mais antigo para entrar novamente. Também são desconectados aqueles com mais 5 minutos de conexão.
5. O segundo critério do algoritmo de seleção de *unchoke* auxilia os atacantes no momento em que baixaram menos dados.
6. Como *leechers* legítimos não podem ficar mais de 5min conectados, um a um são desconectados.

Connection Attack Bittornado

Seed Uplink (KB/sec)	Avg Download Time w/o Attackers (mins)	Delay Ratio
50	177	2.52
50	177	2.99
100	176	1.00
100	176	1.00
150	167	1.03
150	167	1.03

TABLE VI: Connection Attack Results for BitTornado (800 Attackers; 500 MB File; Leechers: 48 KB/sec & 192 KB/sec; Attackers: 10 KB/sec & 20 KB/sec)

- Cenário I.
- Mesmo com 800 atacantes, os 5 *leechers* legítimos iniciais conseguem ganhar os *unchoke slots*.
- Após baixá-los, redistribui para os 25 *leechers* legítimos.
- Ataque pouco eficiente.

Connection e Bandwidth Attack Bittornado

Seed Uplink (KB/sec)	Avg Download Time w/o Attackers (mins)	Delay Ratio
500	75	8.06
500	75	8.66

TABLE VII: Combined Bandwidth/Connection Attack Results for BitTornado (800 Attackers; 100 MB File; Leechers: 20 KB/sec & 40 KB/sec; Attackers: No Bandwidth Cap)

- Como o Bittornado não sofreu com ambos ataques, juntou-se os dois.
- Cenário II.
- *Delay ratio* quase 9.
- 3 de 4 *slots* da *seed* ocupados pelos atacantes (1 unchoke slot oportunista).
- Ganho no desempenho do ataque.

Considerações Finais

- Investigados 2 principais ataques à semente inicial.
- Utilizados os mais populares *seeds* (Azureus, μTorrent e Bittornado).
- Implementado no PlanetLab.
- Resultados mostram que Bittornado e Azureus são bem resistentes ao *Bandwith Attack*.
- A união dos ataques resulta em maior impacto.

Bibliografia: [ros, 2011]

 (2011).
A Measurement Study of Attacks on BitTorrent Seeds.

A Measurement Study of Attacks on BitTorrent Seeds

Autores: Prithula Dhungel, Xiaojun Hei, Di Wu, Keith W. Ross
Apresentado por: Edelberto Franco Silva

Publicado na ICC 2011

Abril, 2012