Attacks on BitTorrent Leechers

"A Meausrement Study of Attack on BitTorrent Leechers" by
Prithula Dhungel, Di Wu, Brad Schonhorst, Keith W. Ross

DELAIRE Jonathan - Université de Nice-Sophia Antipolis

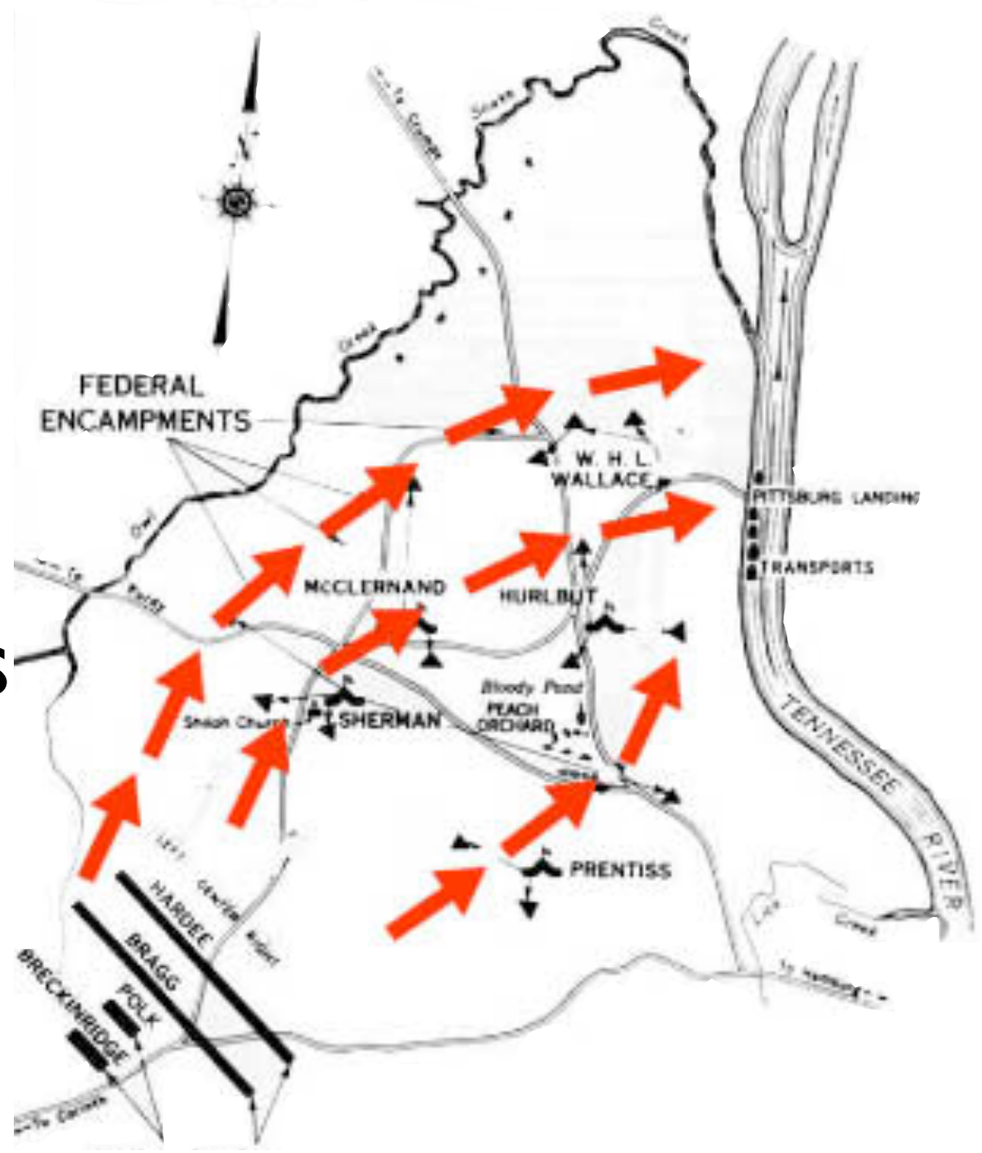
Plan

★Description

★The two Attacks

★Effectiveness of the Attacks

★Conclusion



Description

Problem?

★Illegal p2p content

★Hard to lawsuit user of bitTorrents

Solution?

★Impeding the user's download rate

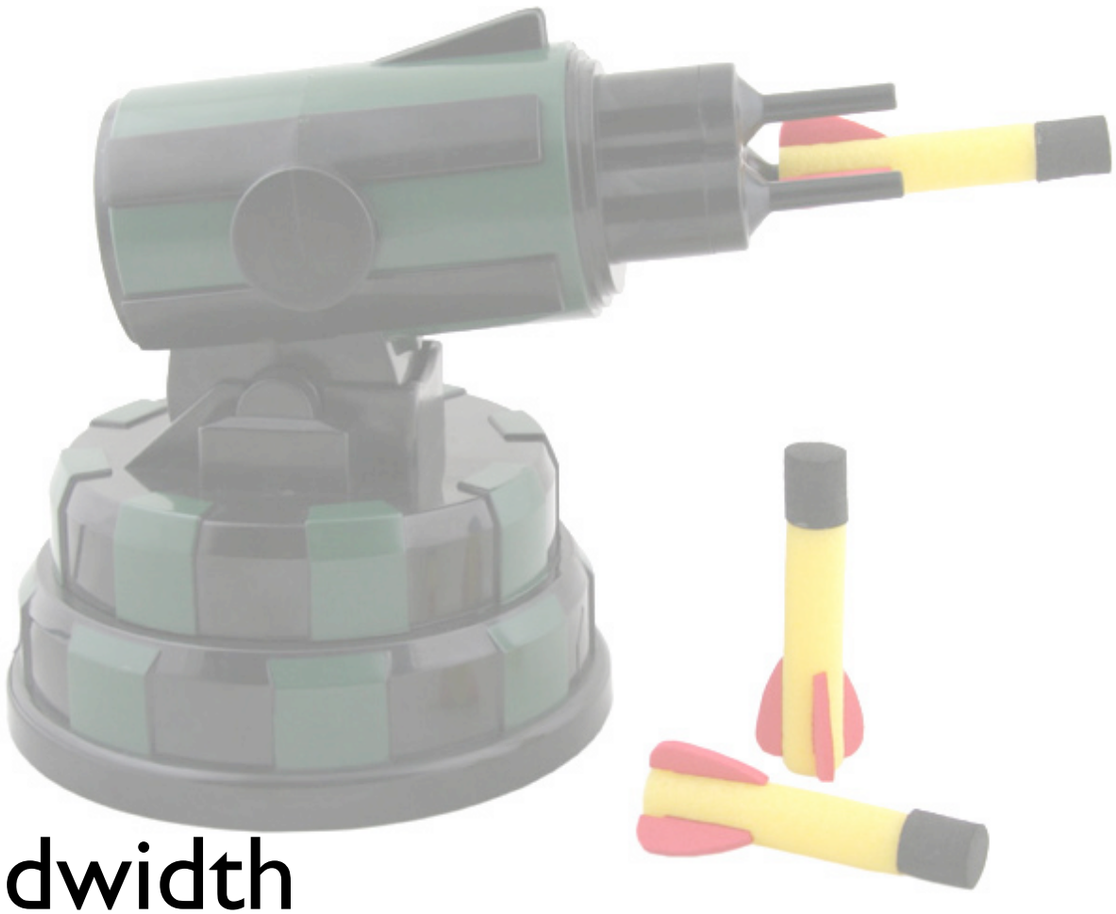
★Attacking the bitTorrent swarm

The two Attacks

Fake-Block Attack

Goal?

★Prolong the download



How?

★Wasting the peer's bandwidth

★Exploit the hash-check

★Can waste 256KB(piece size) of bandwidth with 16KB(block size)

The two Attacks

Uncooperative-Peer Attack

Goal?

★Prolong the download

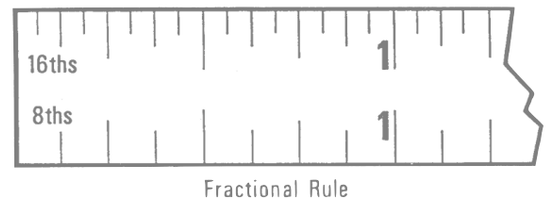
How?

★Exploit the protocol

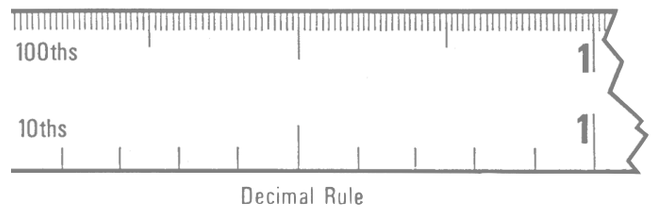
★"*Chatty peer attack*"

★Repeat handshake and bitmap request

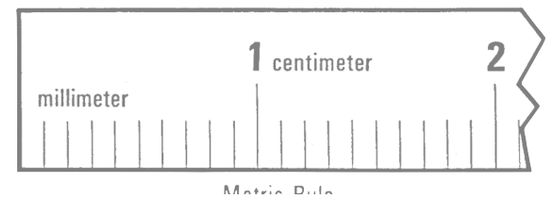
Effectiveness of the Attacks



Fractional Rule



Decimal Rule



Passive measurement

★Top UK chart/iTunes album

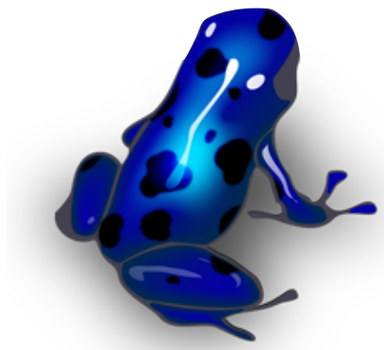
Wireshark

★TCP dumper

★Record all incoming/outgoing packet

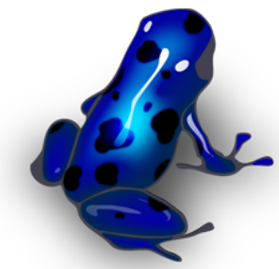
Packet-parser

★Identify the attack-type



Effectiveness of the Attacks

Passive measurement(108MB file)

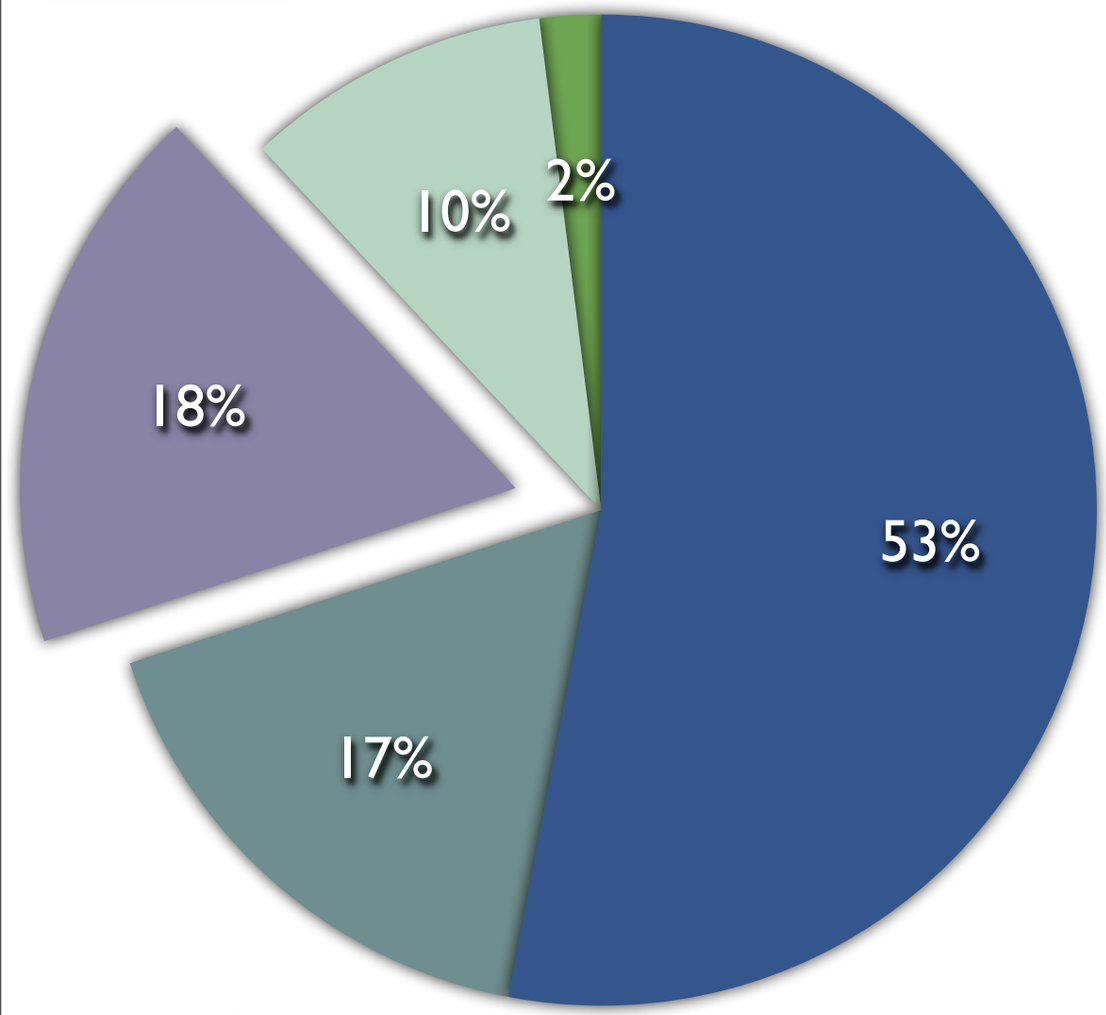


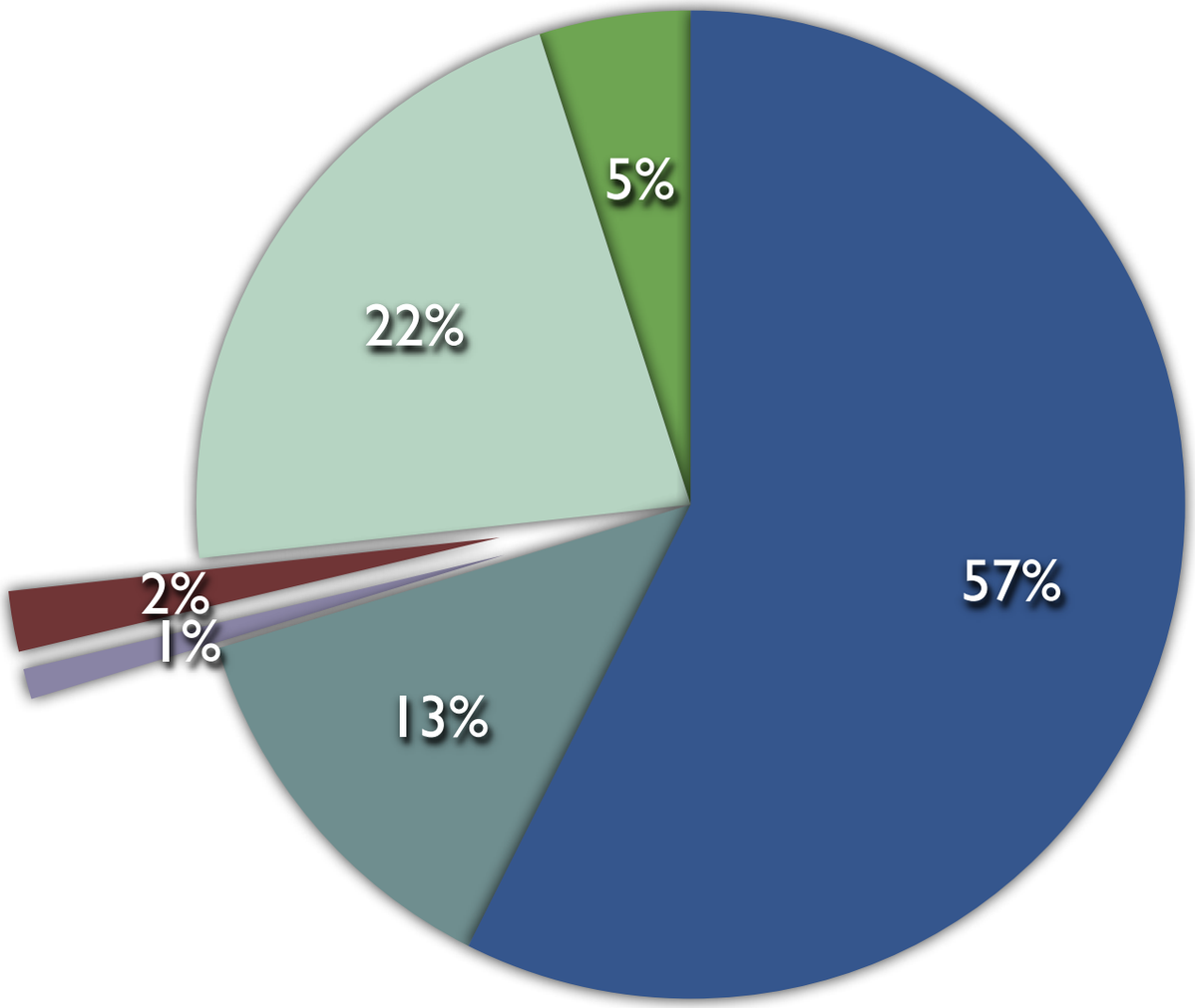
	Ethernet	DSL
w/ IP-filtering	15.52mins	19.98mins
w/o IP-filtering	20.99mins	25.88mins
Delay Ratio	35.2%	29.5%

	Ethernet	DSL
w/ IP-filtering	9.17mins	18.32mins
w/o IP-filtering	9.42mins	28.93mins
Delay Ratio	2.7%	57.9%

Effectiveness of the Attacks

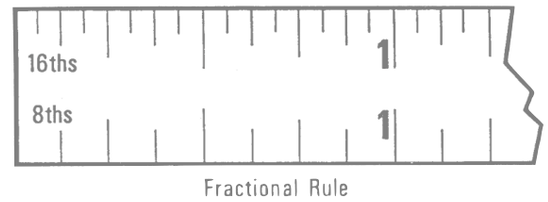
Passive measurement(108MB file)



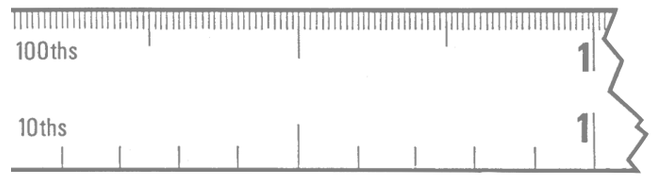


- No-TCP-connection Peers
- Chatty Peers
- Benevolent Peers
- No-BT-handshake Peers
- Fake-Block-Attack Peers
- Other Peers

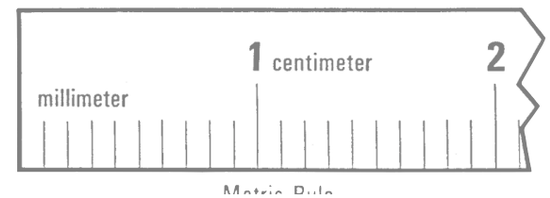
Effectiveness of the Attacks



Fractional Rule



Decimal Rule



Active measurement

★20 top box office movie

Crawler

★Generate a pool of Ip adress/port

★Gather ip-adress of a given torrent

★Use the peer-exchange feature if Azureus peers

Customized BitTorrent-client

★Detection of chatty/fake-block attack peers

Effectiveness of the Attacks

Results for chatty-peers

	Total Peers Crawled		Usefull Peers	Chatty Peers		
	Tracker	Gossip		Tracker	Gossip	IP from BL
Movie 1	116	864	54	0	27	26
Movie 2	633	206	152	0	7	7
Movie 3	144	158	93	0	0	0
Movie 4	16	407	17	0	2	0
Movie 5	29	1460	13	11	0	0
Movie 6	2356	3992	798	0	0	0
Movie 7	111	0	30	0	0	0
Movie 8	82	0	25	0	0	0

Effectiveness of the Attacks

Results for fake-block-peers

	Total Peers Crawled		Usefull Peers	Chatty Peers		
	Tracker	Gossip		Tracker	Gossip	IP from BL
Movie 1	104	2284	53	4	17	21
Movie 2	604	313	168	0	8	8
Movie 3	59	524	103	0	0	0
Movie 4	15	86	14	0	0	0
Movie 5	22	640	11	0	0	0
Movie 6	374	884	289	0	0	0
Movie 7	89	0	22	0	0	0
Movie 8	114	0	40	0	0	0

Conclusion

★Anti-P2P compagnis try to impede BitTorrent swarm

★Two type of attack

★Affect more broadand users

★Do not impede that much (not more than 50%....)

★But people don't bother since they mostly run overnight