

Gnutella protokollu täiustamine “mürgitajate” vastu  
ehk "Haamri olemasolul on kõik probleemid naela kujulised"

Meelis Roos

ATI seminar

5. juuni 2003

## Failijagamisvõrgud

- Tsentraalsed
  - \* Napster, ...
- Detsentraliseeritud
  - \* Kazaa, eDonkey, ..., Gnutella
  - \* Mojo Nation, BitTorrent
- Hea või halb – küsimus omaette

## Teenused võrgus

- Otsimine
- Failide hoidmine
- Failide transport
- Ühenduste vahendamine

## Liikluse optimeerimine

- Pakkimine – ainult juhtühendustele
- Sama faili eri koopiate ära tundmine
  - \* SHA1 räsüd on kujunemas failide primaarseks identifikaatoriks
- Sama faili tõmbamine korruga mitmest arvutist

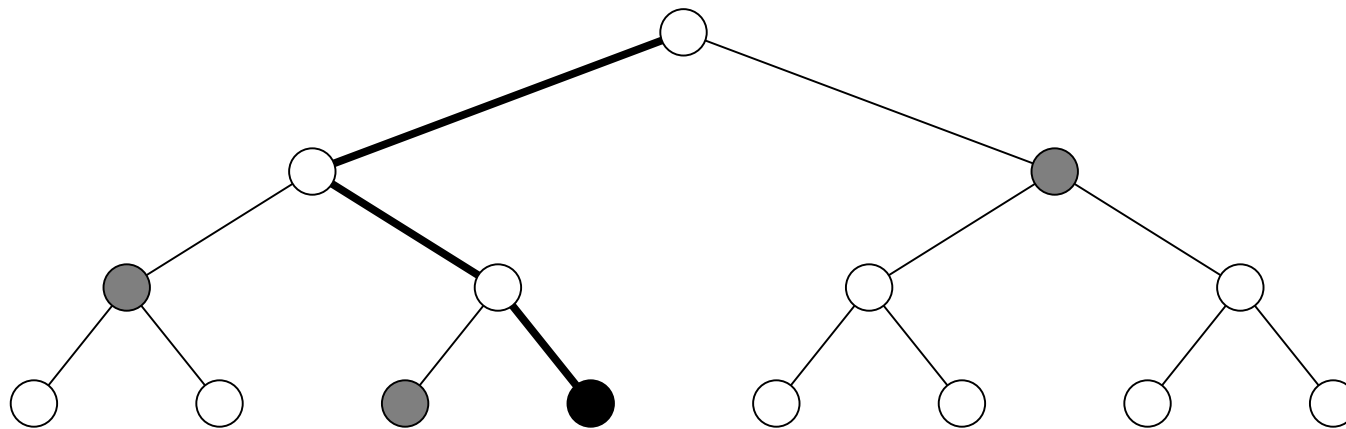
## Probleemid

- Skaleeruvus
- Aeglase ühendusega masinad on pudelikaelaks
- Tasakaal jagajate ja tõmbajate vahel
- "Mürgitamine"
  - \* Päringuvastuste tasemel
  - \* Faili sisu tasemel

## Lahendus failide sisu õigsuse tagamiseks

- Väikestest juppide ülekattumistest ei piisa
- Levitame koos päringu vastustega faili räsi
- Anname iga failijupiga kaasa tõestuse, et faili räsi sõltub sellest jupist
- Tõestus ei tohi kergesti võltistav olla
- Tõestus ei tohi liiga suur olla

# Merkle'i autentimispuud



## Rakendame autentimispuid Gnutellale

- Jagame faili fikseeritud pikkusega plokkideks (1M näiteks)
- Arvutame iga ploki räsi
- Ehitame räside baasil Merkle'i puu
- Puu tipp on faili uueks räsiks (lisaks SHA1-le)
- Iga ploki või plokivahemikuga paneb saatja kaasa autentimistee tipuni
- Saaja verifitseerib, kas ta saab andmeplokist ja autentimisteest sama räsi

## Hinnang lisaliiklusele

- 1M ploki ja 700M faili puhul tuleb autentimistee pikkuseks kuni 10 sammu
- Ühel sammul üks räsi – 160 baiti + ID → 200 baiti
- Kokku u. 2 KB lisa 1M kohta, alla 1%
- Plokkide jada puhul potentsiaalselt vähem (alampuude tõttu)
- Plokkide jada vajab kahe otsmise ploki autentimisteid

## Optimeerimine

- On olemas optimaalsemaid skeeme mingisse intervalli jäävate elementide autentimiseks
- Intervallajatemplid – sama probleem lahendatakse ajatemplite realiseerimiseks
- Intervallajatemplite linkimisskeem sobib ka meile vahemiku autentimiseks
- Konstandi 2 (2 nagu kaks ahelat) vähendamine 1.44 lähedale (asümptootiliselt)

## Probleemid

- Failisabade väiksed plokid
- SHA1 kasutuselevõtuks kulus üle aasta
- Palju konkureerivaid Gnutella parandusettepanekuid, raske oma "läbi suruda"
- Ehk kaovad "mürgitajad" niisamagi ära . . .