



Aalto-yliopisto
Perustieteiden
korkeakoulu

Peliteorian soveltaminen hajautettujen järjestelmien protokollasuunnittelussa

Riku Hyytiäinen

16.06.2014

Ohjaaja: *Harri Ehtamo*

Valvoja: *Harri Ehtamo*

Työn saa tallentaa ja julkistaa Aalto-yliopiston avoimilla verkkosivuilla. Muilta osin kaikki oikeudet pidätetään.

Sisältö

- ” Tausta
- ” Tavoitteet
- ” Rajaukset
- ” Tietolähteet/Aineistot
- ” Menetelmät/Työkalut
- ” Aikataulu

Tausta

- “ Tietojenkäsittelytieteessä usein ongelmia joihin voidaan soveltaa peliteoriaa
 - . Useita toimijoita, joiden toiminta riippuu toisista
- “ Esim. *Koordinoitu hyökkäys* . ongelma tai salaisuuden jakaminen
- “ Protokollaa suunnitellessa voi olla hyödyllistä tarkastella peliteorian näkökulmasta

Tavoitteet

- “ Määritellään sovellukseen tarvittavan Nashin tasapainon robustisuus
 - . Vahva Nashin tasapaino, koalition kestävä Nashin tasapaino ym.
- “ Selvitetään aiemmasta tutkimuksesta olemassa olevat protokollat
 - . Todistetaan Nashin tasapaino tai muu ehto
- “ Protokollan testaus simuloiden
 - . Testataan käytännössä

Rajaukset

- “ Salaisuuden jakaminen
 - . Salaisuuden pystyy laskemaan, mikäli tietää n kappaletta avainarvoja.
- “ Hajautettu laskenta
 - . Esim. Miljonäärin ongelma
- “ Synkroniset järjestelmät (ei asynkronisia)
 - . Toimijoilla on yhteinen kello ja jokaisella kuluu laskentaan yhtä kauan.

Tietolähteet ja työkalut

- ” Alan kirjallisuus
- ” Simulointiin Matlab

Aikataulu

- ” 4/14 . Aiheen valinta
- ” 5-8/14 . Työn kirjoittaminen
- ” 6/14 . Aiheen esittely
- ” 9/14 . Valmiin työn esittely