Aalto-yliopisto
Perustieteiden
korkeakoulu

Peliteorian soveltaminen hajautettujen järjestelmien protokollasuunnittelussa (valmiin työn esittely)

Riku Hyytiäinen

23.02.2015

Ohjaaja: *Harri Ehtamo*
Valvoja: *Harri Ehtamo*

Systeemianalyysin laboratorio

Tausta

- Protokollasuunnittelu on yksi tietojenkäsittelytieteen tutkimuskohde
- Mikä on protokolla?
  - Oxford English Dictionary:
    - "*A set of rules governing the exchange or transmission of data between devices.*"
- Esimerkiksi yksi internetin kulmakiviä, TCP-protokolla

Työn kuvaus

- Selvitetään kirjallisuudesta olemassa olevat protokollat
- Määritellään sovellutukseen tarvittavan Nashin tasapainon robustisuus
  - Vahva Nashin tasapaino, koalition kestävä Nashin tasapaino ym.
  - Näytetään Nashin tasapaino protokollalle
- Protokollan testaus simuloiden
  - Testataan käytännössä

Rationaalinen salaisuuden jakaminen

- Kassakaappi, jonka avaamiseen tarvitaan *n* kpl tunnuslukuja
- Tunnuslukuja jaetaan *m*:lle henkilölle ($m \geq n$)

- Henkilöiden hyötyfunktiot kuten seuraavalla kalvolla

- **Miten henkilöiden kannattaa jakaa tunnuslukuja keskenään, vai kannattaako?**

Protokolla pelinä

- Protokollan eri osapuolet pelaajia
- Pelaajilla hyötyfunktiot:
  - Pelaaja hyötyy enemmän, jos tämä saa kassakaapin auki kuin jos tämä ei saa kassakaappia auki
  - Mitä vähemmän on niitä, jotka saa kassakaapin auki, sitä parempi pelaajalle
- Peli koostuu kierroksista, joista kullakin jokainen pelaaja voi lähettää (tai olla lähettämättä) muille pelaajille viestejä

Deterministinen protokolla

- Päättyy äärellisen monen kierroksen jälkeen
- Rationaalisen pelaaja ei jaa informaatiota muille
  - Pelaajat tietävät varmuudella, milloin peli loppuu
  - Rationaalinen pelaaja ei jaa (hyödyllistä) informaatiota viimeisellä kierroksella
    - Kaikki strategiat, joissa pelaaja jakaa informaatiota viimeisellä kierroksella ovat dominoituja strategioita
      → Eliminoidaan nämä
  - Kaikki strategiat, joissa pelaaja jakaa informaatiota millään kierroksella voidaan eliminoida
- Tehdään protokollan päättymisajankohdasta satunnainen

Satunnaistettu protokolla

- Jaetaan tunnuslukuja 3 pelaajalle
- Kassakaapin avaamiseen tarvitaan 3 tunnuslukua
- Protokollan eteneminen:
  1. Jokainen pelaaja *i* arpoo satunnaisluvun c_i s.e. P(c_i = 1) = α ja $\mathrm{P}(c_i = 0) = 1 - \alpha$
  2. Lasketaan yhdessä $z = c_1 \oplus c_2 \oplus c_3$
  3. Jokainen kertoo muille oman tunnuslukunsa jos $z = 1$ ja $c_i = 1$
  4. Jos $z = 0$ tai tasan 1 pelaaja jakaa tunnuslukunsa muiden kanssa, niin kassakaappi nollataan, pelaajille jaetaan uudet tunnusluvut ja protokolla aloitetaan alusta
  5. Jos kohdan 4 ehto ei täyty, kaikki pelaajat saavat kassakaapin auki, tai joku on huijannut

     → Lopetetaan peli (Halpern et al., 2004)

Satunnaistettu protokolla - analyysi

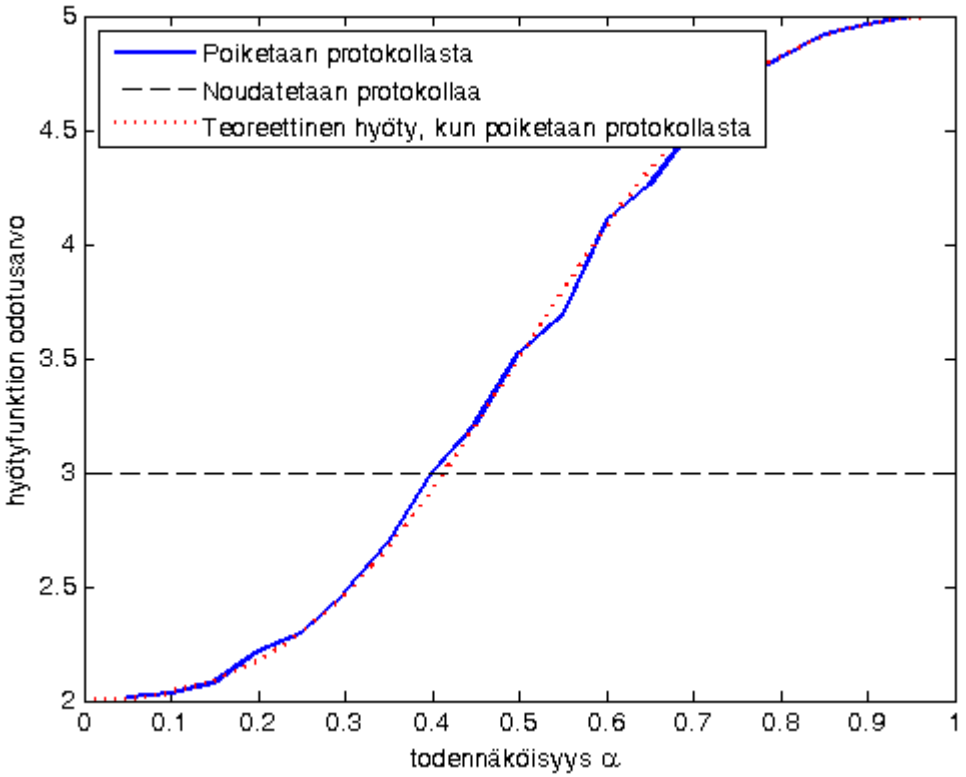
- **Kannattaako protokollasta poiketa?**
- Jos pelaaja ei osallistu z:n määrittämiseen, muut lopettavat
  - Ei kannata
- Kannattaako olla jakamatta oma tunnusluku, jos protokolla niin vaatii?
  - Pelaajan kuuluu jakaa tunnuslukunsa muille jos, $z = 1$ ja $c_i = 1$
  - Ei kannata, jos (1) pätee

$$\frac{\alpha^2}{(1-\alpha)^2+\alpha^2} u_i(\text{vain } i) + \frac{(1-\alpha)^2}{(1-\alpha)^2+\alpha^2} u_i(\text{ei kukaan}) < u_i(\text{kaikki}) \quad (1)$$

→ Parametri *α* pitää valita oikein

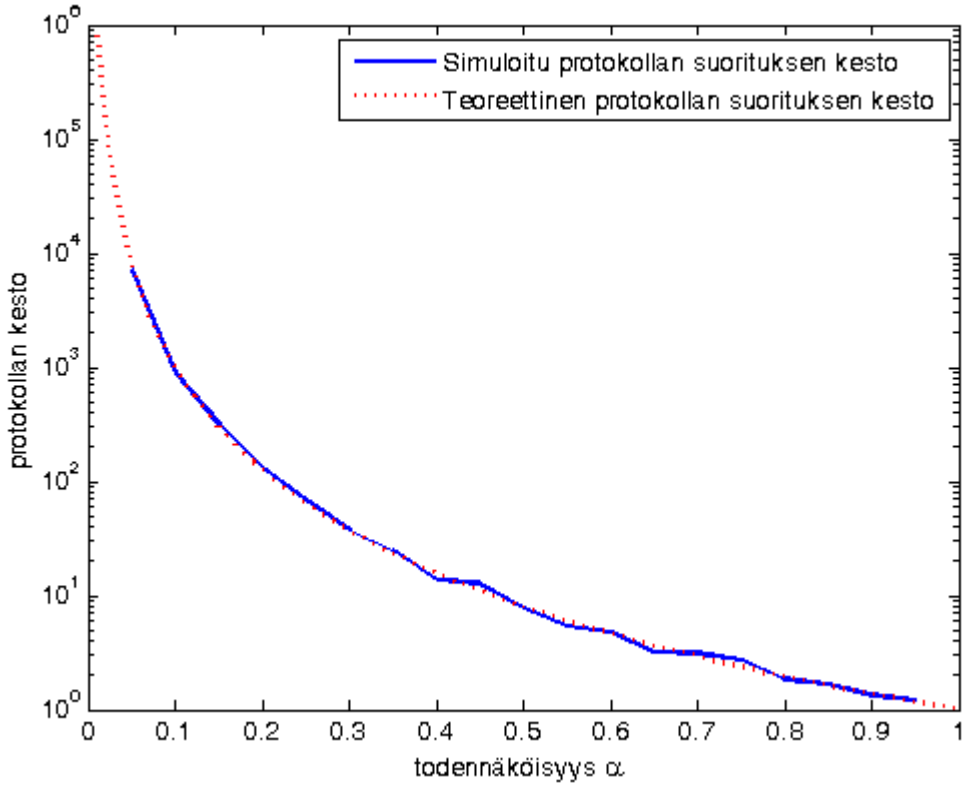
Simulointi – α:n valinta

- Valitaan α siten, että (1) pätee
  - $\alpha < 0.4$
- Hyötyfunktion odotusarvot määritetty Monte Carlo –simuloinnilla (N = 1000)



Simulointi – protokollan kesto

- Jos α on pieni, protokollalla kestää kauan päästä loppuun
  - Kannattaa valita mahdollisimman suuri α
- Protokollan kesto määritetty Monte Carlo –simuloinnilla (N = 100)



Simulointi – Nashin tasapaino

- Pelaajilla A, B ja C on kolme vaihtoehtoista toimintatapaa:
  1. Noudata protokollaa
  2. Älä ikinä jaa tunnuslukua muille
  3. Aina jaa tunnusluku muille
- Peliskenaario (A1,B1,C1), eli kaikki noudattavat protokollaa on koalition kestävä Nashin tasapaino (Bernheim et al., 1987)

C1

	B1	B2	B3
A1	**3, 3, 3**	1.8, 2.5, 1.8	3, 1.2, 3
A2	2.5, 1.8, 1.8	2, 2, 2	5, 1, 1
A3	1.2, 3, 3	1, 5, 1	1.3, 1.3, 4.7

C2

	B1	B2	B3
A1	1.8, 1.8, 2.5	2, 2, 2	1, 1, 5
A2	2, 2, 2	2, 2, 2	2, 2, 2
A3	1, 1, 5	2, 2, 2	1, 1, 5

C3

	B1	B2	B3
A1	3, 3, 1.2	1, 5, 1	4.7, 1.3, 1.3
A2	5, 1, 1	2, 2, 2	5, 1, 1
A3	1.3, 4.7, 1.3	1, 5, 1	3, 3, 3

Pelaajien hyödyn odotusarvo eri peliskenaarioissa

Tulokset

- Hyvällä protokollasuunnittelulla voidaan tehdä protokollasta poikkeamisesta epäedullista
  - Tässä voidaan hyödyntää peliteoriaa

- Käytännössä:
  - 3 osapuolen protokolla salaisuuden jakamiseen
    - Kaikkien osa-salaisuus on tarpeellinen
  - Protokollan noudattaminen on koalition kestävä Nashin tasapaino

Lähteet

- J. Halpern et al. Rational secret sharing and multiparty computation. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing,* pages 623-632. ACM, 2004
- D. Bernheim et al. Coalition-proof Nash Equilibria, I. Concepts. *Journal of Economic Theory,* 42(1):1-12, 1987