Riku Hyytiäinen

Peliteorian soveltaminen hajautettujen järjestelmien protokollasuunnittelussa

Perustieteiden korkeakoulu

Kandidaatintyö
Espoo 23.02.2015

Vastuuopettaja ja ohjaaja:

Prof. Harri Ehtamo

Aalto-yliopisto
Teknillinen korkeakoulu

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

AALTO-YLIOPISTO
PERUSTIETEIDEN KORKEAKOULU

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä: Riku Hyytiäinen

Työn nimi: Peliteorian soveltaminen hajautettujen järjestelmien protokollasuunnittelussa

Päivämäärä: 23.02.2015 Kieli: Suomi Sivumäärä:3+25

Tutkinto-ohjelma: Teknillinen fysiikka ja matematiikka

Vastuuopettaja: Prof. Harri Ehtamo

Tässä työssä perehdytään keinoihin hyödyntää peliteorian oppeja protokollasuunnittelun saralla. Työssä tutkitaan erityisesti rationaalista salaisuuden jakamista ja määritellään tähän käyttötarkoitukseen sopivan variaatio Nashin tasapainosta. Sopivaksi Nashin tasapainon variaatioksi protokollien hyvyyden tutkimiseen valitaan koalition kestävä Nashin tasapaino.

Työ keskittyy rationaaliseen salaisuuden jakamiseen, jota voidaan kuvailla esimerkillä kassakaappista, joka aukeaa syöttämällä tälle M kappaletta tunnuslukuja. Tunnuslukuja on toisaalta jaettu N:lle eri ihmiselle. Kanssakäymistä, jossa nämä eri ihmiset selvittävät toisiltaan tunnuslukuja, joilla kassakaapin voi avata, kutsutaan rationaaliseksi salaisuuden jakamiseksi. Soveltamalla peliteoriaa näytetään, ettei salaisuuden jakaminen onnistu äärellisessä ajassa päättyvällä protokollalla, mikäli eri osapuolet toimivat rationaalisesti ja hyötyvät siitä, etteivät muut saa salaisuutta selville. Kannustamalla eri osapuolia toimimaan sattumanvaraisesti saadaan kuitenkin aikaiseksi protokolla, josta rationaalinen pelaaja ei poikkea, mutta jonka kestolle ei voida asettaa ylärajaa.

Protokollan hyvyyden tutkimiseen työssä käytetään koalition kestävän Nashin tasapainon käsitettä. Koalition kestävä Nashin tasapaino on sellainen Nashin tasapaino, josta mikään koalitio ei pysty strategiaansa yhdessä muuttamalla parantamaan kaikkien jäsentensä hyötyfunktion odotusarvoa siten, että koalitio on keskenään tasapainossa. Lopuksi näytetään, että protokollan määrittelemä strategia on koalition kestävä Nashin tasapaino käyttäen Monte Carlo –simulaatiota.

Avainsanat: peliteoria, Nashin tasapaino, tietojenkäsittelytiede, protokollasuunnittelu, salaisuuden jakaminen

Sisältö

1 Johdanto

Nykypäivänä elämämme ovat päivä päivältä enemmän sidoksissa Internetiin, joka puolestaan toimii erilaisten protokollien varassa. Täten on tärkeää, että voimme luottaa järjestelmän toimivuuteen, vaikka jokin taho pyrkisi horjuttamaan sitä. Tietojenkäsittelytiede pyrkii protokollasuunnittelun kautta luomaan järjestelmiä, jotka kestävät jatkuvaa ja monipuolista käyttöä. Hajautetuissa järjestelmissä, eli järjestelmissä missä useampi taho pyrkii yhdessä suorittamaan jotakin tiettyä toimenpidettä, voi usein tulla vastaan tilanteita, jolloin eri osapuolet hyötyvät lopputuloksesta siten, ettei yhteistyö ole välttämättä hyödyllisin vaihtoehto toimijoille. Tällaisissa tilanteissa peliteoria on oivallinen näkökulma, josta tarkastella ongelmaa.

Tässä työssä selvitetään minkälaisia sovellutuksia peliteorialle on hajautettujen järjestelmien protokollasuunnittelun parissa. Työ on pääosiltaan kirjallisuuskatsaus ja sisältää kirjallisuudessa esitettyjen mallien havainnollista analyysia. Kappaleessa 2 esitellään lukijalle tarvittavat käsitteet ja menetelmät tietotekniikan alalta. Lisäksi esitellään muutamia tunnettuja ongelmia hajautettujen järjestelmien suunnittelun saralta, joiden avulla lopuksi perustellaan tarve hyödyntää peliteoriaa hajautettujen järjestelmien protokollasuunnittelussa. Kolmannessa kappaleessa esitellään ja perustellaan koalition kestävä Nashin tasapaino (*Coalition-Proof Nash Equilibrium*). Neljännessä kappaleessa käsitellään hajautettujen järjestelmien parissa esille tuleva salaisuuden jakamisen ongelma, ja selvitetään peliteorian keinoin koalition kestävän Nashin tasapainon saavuttava protokolla. Kappaleessa 5 laajennetaan salaisuuksien jakamisen ongelma yleiseksi monen osapuolen laskentaongelmaksi (*Multiparty Computation*). Lopuksi implementoidaan protokolla, jossa on koalition kestävä Nashin tasapaino pitäytyä protokollassa. Tutkitaan simuloiden tämän protokollan ominaisuuksia ja Nashin tasapainoja.

2 Tutkimusongelma

Tietojenkäsittelytiede

Tietojenkäsittelytiede tieteenalana tutkii tietotekniikkaan liittyviä ilmiöitä sekä ongelmia. Ongelmat liittyvät usein jonkin tietyn tehtävän, esimerkiksi optimointitehtävän ratkaisemiseen annettujen resurssien puitteissa. Tällöin tutkitaan ja kehitetään algoritmeja, eli yksityiskohtaisia ohjeistuksia siitä, kuinka annettu tehtävä tulee ratkaista, ja pyrkimyksenä on usein minimoida ajan ja muistin käyttötarve tai mahdollisesti eri laskentayksiköiden välisen kommunikaation tarve. Tietojenkäsittelytieteeseen kuuluu myös tärkeänä osana kryptografian ala. Kryptografia tutkii ja kehittää keinoja salata tietoa siten, että salauksen purkaminen on mahdollisimman vaikeaa ilman tiettyä käytettyyn salaukseen liittyvää avainta. Tämän kyseisen avaimen kanssa salauksen purkaminen tulisi puolestaan olla mahdollisimman helppoa.

Tämä työ keskittyy algoritmien tai salausten suunnittelun sijaan protokollasuunnitteluun, ja peliteorian soveltamiseen siinä. Protokollasuunnittelu sijoittuu loogisesti algoritmisuunnittelun ja kryptografian välimaastoon. Protokollalla tarkoitetaan yhteisiä sääntöjä siitä, kuinka eri osapuolten tulisi toimia käydessään viestinvaihtoa keskenään. Protokolla määrittelee kahden tai useamman koneen käymän "keskustelun"yksiselitteisesti siten, että kun kaikki osapuolet noudattavat annettua protokollaa, kaikki tarvittava informaatio välittyy toisille osapuolille. Protokollasuunnittelussa huomioitavia haasteita on muun muassa viestin välityksen epävarmuus, eli se, ettei lähetetty viesti aina välttämättä päädy perille vastaanottajalle, vaan jollakin todennäköisyydellä $p > 0$ viesti jää matkalle. Tämä voi johtua esimerkiksi jonkin komponentin rikkoutumisesta. Tässä työssä tutkittavissa protokollissa oletetaan myös, että "keskustelun"osapuolet saattavat poiketa annetusta protokollasta, tavoitellen omaa hyötyään. Tavoitteena on kehittää peliteoriaa hyödyntäen sellainen protokolla, jossa rikkomalla protokollan asettamia sääntöjä ei voi saada ylimääräistä etua.

Hajautetulla järjestelmällä tarkoitetaan sellaista järjestelmää, jossa useampi laskentayksikkö työskentelee yhdessä saavuttaakseen jonkin halutun lopputuloksen. Hajautetulla järjestelmällä voi saavuttaa monia toivottavia ominaisuuksia, kuten moninkertaisen laskentatehon tai oikein implementoituna lisätyn toimintavarmuuden. Hajautetun järjestelmän mukana tulevia haasteita on epävarmuus eri laskentayksiköiden toiminnasta, yksi tai useampi laskentayksikkö voi rikkoontua tai joutua esimerkiksi jonkin ulkopuolisen tahon kaappaamaksi. Hyvä hajautettu järjestelmä sietää osan laskentayksiköiden vikaantumisen. Tässä työssä tutkitaan protokollia, jotka kestävät yhden tai useamman laskentayksikön vikaantumisen.

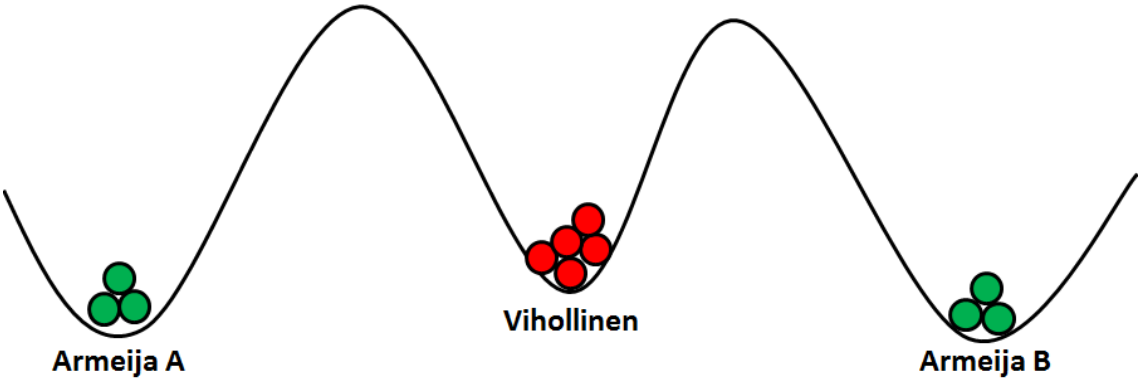
Tunnettuja ongelmia

Seuraavaksi perehdytään muutamaan tunnettuun protokollasuunnittelun ongelmaan. Tavoitteena on motivoida lukija protokollasuunnittelun tärkeydestä, sekä tuoda esiin ongelmia, joita hyvällä protokollasuunnittelulla pyritään ratkaisemaan.

Kenraalien probleema

Kahden kenraalin probleemana tunnettu ajatusleikki julkaistiin ensimmäistä kertaa vuonna 1975 E. A. Akkoyunlun, K. Ekanadhamin ja R. V. Huberin toimesta [2]. Tuolloin ajatusleikissä esiintyneet gangsterit suunnittelivat pankkiryöstöä ja pyrkivät sopimaan keskenään ryöstön yksityiskohdista. Tänä päivänä parhaiten tunnettuun kahden kenraalin probleeman muotoon ajatusleikin puki J. N. Gray vuonna 1978 [4].

Ajatusleikissä kahden armeijan kenraalit suunnittelevat hyökkäävänsä yhdessä yhteisen vihollisen kimppuun. Molemmat kenraalit tietävät, että vihollinen on ylivoimainen vastus kummallekin armeijalle yksinään, mutta jos kenraalien armeijat yhdistävät voimansa ja hyökkäävät samanaikaisesti vihollinen pystytään päihittämään. Kenraalien tulee siis sopia keskenään tarkka kellonaika, jolloin hyökkäys vihollisen kimppuun aloitetaan. Ongelmana on, että kenraalit armeijoineen ovat etäällä toisistaan ja voivat viestiä vain lähettien avulla. Lähetit eivät kuitenkaan ole täysin luotettavia viestin välittäjiä, vaan jollakin todennäköisyydellä $p > 0$ lähetti ei pääse perille vaan joutuu esimerkiksi vihollisen pidättämäksi. Tästä johtuen kenraali ei pysty ikinä olemaan varma, onko hänen lähettämänsä viesti päässyt perille vai ei. Asetelma on kuvattu kuvassa 1.



Kuva 1: Kenraalien probleema -ajatusleikin asetelma

Tarkastellaan tilannetta hieman tarkemmin esimerkin avulla. Oletetaan, että armeijan A kenraali päättää, että hyökkäys vihollista vastaan alkaa klo 19.00. Armeijan A kenraali lähettää lähetin viemään viestiä armeijan B kenraalille. Kumpikaan kenraali ei aloita hyökkäystä, ellei ole varma siitä, että toinen kenraali on tietoinen suunnitelmasta. Mikäli lähetti onnistuu toimittamaan viestin armeijan B kenraalille, viestin vastaanottanut kenraali lähettää vastavuoroisesti lähetin viestittämään armeijan A kenraalille, että hän on vastaanottanut tämän viestin. Jos tämä lähetti pääsee perille, armeijan A kenraali tietää, että toinen kenraali on vastaanottanut tämän viestin ja on tietoinen suunnitelmasta hyökätä klo 19.00. Toisaalta, armeijan B kenraali ei tiedä, onko kenraali A vastaanottanut tämän kuittausviestiä, joten kenraali A joutuu lähettämään lähetin kertomaan armeijan B kenraalille, että hän on vastaanottanut tämän kuittausviestin ja tietää, että armeija B on tietoinen suun-

nitelmasta hyökätä klo 19.00. Koska lähetti saattaa millä tahansa retkellään joutua vihollisen vangiksi, kumpikaan kenraali ei voi ikinä olla täysin varma, että toisella kenraalilla on sama informaatio kuin hänelläkin, ja että toinen kenraali on valmis aloittamaan hyökkäyksen sovittuun aikaan.

Voidaan osoittaa että yllä kuvattu viestittely jatkuu loputtomiin. Tehdään vastaoletus, että yllä kuvattu viestittely päättyy N:n viestin jälkeen tilanteeseen, jossa kumpikin kenraali tietää, että toinenkin kenraali on hyökkäämässä klo 19.00. Tällöin viimeinen viesti on ilmiselvästi kriittinen, koska viestittely päättyy siihen. Kuitenkin, jollakin nollasta poikkeavalla todennäköisyydellä viesti ei saavutakaan vastaanottajaa, joten jotta yhteinen tieto viestin saapumisesta määränpäähän saataisiin kaikille osapuolille, viimeisen viestin vastaanottaja joutuu lähettämään kuittausviestin takaisin alkuperäisen viestin lähettäjälle. Nyt viestejä joudutaan lähettämään $N + 1$ kappaletta. Tämä on ristiriidassa N:n viestin oletuksen kanssa ja viestiketju jatkuu siis loputtomasti.

Tästä ongelmasta opimme, kuinka yksinkertaisetkin ongelmat muuttuvat helposti monimutkaisiksi ja vaikeasti ratkaistaviksi kun viestin välityksessä esiintyy epävarmuutta.

Bysanttilainen sopimus

Tarkastellaan yllä kuvatun kahden kenraalin yleistettyä tapausta, jossa kenraaleja on useampia. Tällä kertaa viestit pystytään kuitenkin välittämään ilman epävarmuutta, mutta toisaalta kenraalit saattavat olla pettureita. Tällä kertaa ei myöskään ole selvää, että hyökkääjät voittaisivat siinä tapauksessa että he yhdistävät voimansa, vaan jokainen kenraali arvioi tilannetta omasta perspektiivistään ja informoi muita kenraaleita omasta arviostaan. Tämän jälkeen kenraalien pitäisi onnistua tekemään päätös hyökätäkö vai ei oman ja muiden kenraalien tekemien arvioiden perusteella, pitäen mielessä että yksi tai useampi kenraaleista saattaa olla petturi ja täten epäluotettava. Epäluotettava kenraali saattaa kertoa eri kenraaleille eriäviä arvioita ja pyrkiä täten saamaan osan kenraaleista hyökkäämään kun muut päättävät olla hyökkäämättä. Tätä asetelmaa pohti L. Lamport, R. Shostak ja M. Pease vuonna 1982 [6].

Bysanttilainen sopimus -protokollalla tarkoitetaan sellaista protokollaa, jossa yllä kuvatussa tilanteessa kaikilla rehellisillä kenraaleilla on lopulta sama informaatio ja jokainen kenraali tekee samalla informaatiolla saman johtopäätöksen hyökkäämisestä. Lisäksi bysanttilainen sopimus -protokollan tulee olla sellainen, jossa rehelliset kenraalit tekevät oikean johtopäätöksen hyökkäämisen suhteen jopa silloin, kun osa kenraaleista on pettureita. On todistettavissa, että mikäli kenraaleja on yhteensä $3m + 1$ kappaletta, bysanttilainen sopimus hyökkäyksestä saadaan aikaiseksi vain, jos pettureita on maksimissaan m kappaletta [7]. Mikäli pettureita on enemmän, nämä onnistuvat huijaamaan muita kenraaleja siten, että osa rehellisistä kenraaleista päättää hyökätä ja osa päättää olla hyökkäämättä.

Bysanttilaisen sopimuksen tapauksessa on havaittavissa piirteitä, joihin peliteoria voi ottaa kantaa. Tulkitaan kenraalit pelin pelaajiksi, joiden hyötyfunktiot riippuvat siitä, onko kyseinen kenraali rehellinen vai ei. Tällöin tilanne on tul-

kittavissa epätäydellisen informaation peliksi, sillä kenraalit eivät tiedä toistensa hyötyfunktioita.

Peliteorian soveltamisen tavoitteet

Tässä työssä formuloidaan hajautetussa järjestelmässä suoritettava toimenpide peliteoreettiseksi peliksi, ja pyritään muodostamaan protokolla, jossa Nashin tasapaino on noudattaa annettua protokollaa. Lisäksi huomioimme, että hajautetussa järjestelmässä useampi yksikkö voi toimia yhdessä jonkin tavoitteen saavuttamiseksi. Tätä varten laajennamme Nashin tasapainon käsitettä koalition kestäväksi Nashin tasapainoksi. Tällainen tasapainotila on tasapainossa, vaikka useampi pelaaja yhdessä pyrkisi sitä horjuttamaan.

3 Koalition kestävä Nashin tasapaino

Palautetaan ensimmäiseksi mieleen peliteorian peruskäsitteitä, mukaan lukien Nashin tasapaino. Jokaisessa pelissä on mukana pelaajia n kappaletta, merkitään näitä indeksoinnilla $i \in \{1, ..., n\} = N$. Merkitään pelaajan i valitsemaa strategiaa s_i, ja merkinnällä S_i joukkoa, josta pelaaja i voi strategiansa valita, eli $s_i \in S_i$. Lisäksi jokaisella pelaajalla on oma hyötyfunktio $u(...)$, joka riippuu pelaajan itse valitsemasta strategiasta sekä myös muiden pelaajien strategioista. Pelaajan i pelistä saama hyöty on siis $u_i(s_1, s_2, ..., s_{i-1}, s_i, s_{i+1}, ..., s_{n-1}, s_n)$. Peli voidaan määritellä eri pelaajien strategiajoukkojen sekä hyötyfunktioiden perusteella, $G = (S_1, ..., S_n; u_i, ..., u_n)$.

Jokin pelaajan i strategia s_i' on dominoitu, jos on olemassa jokin toinen pelaajan i strategia s_i'' siten, että riippumatta muiden pelaajien valitsemista strategioista, strategia s_i'' tuottaa pelaajalle i suuremman hyödyn kuin strategia s_i'. Strategia s_i'' dominoi strategiaa s_i' jos yhtälö (1) pätee:

$$u_i(s_1, ..., s_i', ..., s_n) < u_i(s_1, ..., s_i'', ..., s_n), \forall s_j \in S_j, j = 1, ..., i-1, i+1, ..., n. \quad (1)$$

Strategiavektori $\mathbf{s}^* = [s_1^*, ..., s_n^*]$ on Nashin tasapaino, jos yksikään pelaaja ei voi kasvattaa omaa hyötyään muuttamalla strategiaansa pois tasapainosta. Formaalisti voidaan määritellä Nashin tasapaino siten, että yhtälö (2) pätee kaikilla pelaajilla i:

$$u_i(s_1^*, ..., s_i, ..., s_n^*) \leq u_i(s_1^*, ..., s_i^*, ..., s_n^*), \forall s_i \in S_i. \quad (2)$$

Nashin tasapaino olettaa, etteivät pelaajat pysty kommunikoimaan ennen strategian valitsemista. Jokainen pelaaja joutuu siis valitsemaan strategiansa toisista pelaajista riippumattomasti. Monissa tilanteissa tätä oletusta ei kuitenkaan voi perustellusti tehdä. Tällöin voidaan ottaa käyttöön robustimpia tasapainokäsitteitä. Yksi tällainen on vahvan Nashin tasapainon käsite.

Oletetaan, että kaikki pelaajat pystyvät kommunikoimaan keskenään rajattomasti. Pelaajat pystyvät siis sopimaan keskenään, mitä strategiaa he tulevat pelaamaan. Pelaajien keskinäiset sopimukset eivät kuitenkaan ole sitovia, ja pelaajat voivat halutessaan poiketa keskenään sopimistaan strategioista. Vahva Nashin tasapaino on sellainen Nashin tasapaino, josta mikään mahdollinen pelaajien osajoukko eli koalitio ei voi parantaa jäsentensä hyötyfunktiota poikkeamalla tasapainosta. Strategiavektori $\mathbf{s}^*$ on vahva Nashin tasapaino jos ja vain jos kaikille mahdollisille pelaajien osajoukoille $J \subseteq N$ ja kaikille tämän osajoukon strategioille $\mathbf{s_J}$ pätee yhtälö (3). Merkitään pelaajaosajoukon J komplementtia $-J$.

$$\exists j \in J : u_j(\mathbf{s}^*) > u_j(\mathbf{s_J}, \mathbf{s}^*_{-\mathbf{J}}). \quad (3)$$

Käytännössä vahva Nashin tasapaino rajaa pois suuren osan tasapainotiloista. Tämä johtuu siitä, että vahvassa Nashin tasapainossa tarkasteltaville poikkeamille ei aseteta mitään ehtoja. Poikkeamat voivat olla minkälaisia tahansa, joten seurauksena kaikki vahvat Nashin tasapainot ovat välttämättä myös pareto-optimaalisia tiloja hyötyfunktioiden suhteen. Tällaisia tiloja ei välttämättä ole lainkaan ja useissa peleissä ei vahvaa Nashin tasapainoa ole olemassa.

Koalition kestävän Nashin tasapainon käsite kehitettiin vuonna 1987 B.D. Bernheimin ja B. Pelegin toimesta vahvan Nashin tasapainon rinnalle kuvastamaan tasapainoa, kun pelaajat voivat kommunikoida rajattomasti ennen strategiansa valitsemista [3]. Koalition kestävä Nashin tasapaino on sellainen tasapaino, josta mikään pelaajien osajoukko ei pysty yhteistuumin poikkeamalla parantamaan kaikkien koalition jäsenten hyötyfunktioiden arvoa, kun vaaditaan, että kaikki mahdolliset poikkeamat ovat itsessään koalition sisäisesti koalition kestävässä Nashin tasapainossa. Koalition kestävän Nashin tasapainon määritelmä on siis luonteeltaan rekursiivinen.

Määritellään koalition kestävä Nashin tasapaino formaalisti. Tarkastellaan n:n pelaajan peliä, jossa $u_i(...)$ ovat pelaajien hyötyfunktiot ja S_i on joukko strategioita, mistä pelaaja i voi strategiansa valita. Merkitään peliä merkinnällä $G(\mathbf{u}, S)$. Olkoon $\mathcal{J}$ pelaajien kaikkien aitojen osajoukkojen joukko, ja J yksi osajoukko. Toisin sanottuna, $J \in \mathcal{J}$ ja $J \subset N$. Merkitään jälleen osajoukon J komplementtia $-J$. Jos $n = 1$, eli pelaajia on pelissä vain yksi, $\mathbf{s}^*$ on koalition kestävä Nashin tasapaino, jos maksimoi pelaajan hyötyfunktion. Kahden tai useamman pelaajan koalition kestävää Nashin tasapainoa varten joudumme määrittelemään itsesäätelevän strategian käsitteen. Strategiavektori $\mathbf{s}^*$ on itsesäätelevä, jos kaikille pelaajien osajoukoille $J \in \mathcal{J}$, osajoukon J strategiavektori $\mathbf{s}^*_\mathbf{J}$ on koalition kestävä Nashin tasapaino pelissä $G/\mathbf{s}^*_{-\mathbf{J}}$. Merkinnällä $G/\mathbf{s}^*_{-\mathbf{J}}$ tarkoitetaan osajoukon J peliä, jossa osajoukon komplementin $-J$ strategiavektori $\mathbf{s}^*_{-\mathbf{J}}$ on lukittu. Toisin sanottuna, $G/\mathbf{s}^*_{-\mathbf{J}} = G(\{\hat{u}_j\}_{j\in J}; \{S_j\}_{j\in J})$, missä $\hat{u}_j = u_j(\mathbf{s}_\mathbf{J}, \mathbf{s}_{-\mathbf{J}}{}^*)$. Kahden tai useamman pelaajan pelissä, strategiavektori $\mathbf{s}^*$ on koalition kestävässä Nashin tasapainossa, mikäli $\mathbf{s}^*$ on itsesäätelevä eikä ole olemassa toista itsesäätelevää strategiavektoria $\mathbf{s}$ siten, että $u_i(\mathbf{s}) > u_i(\mathbf{s}^*)$, kaikilla $i = 1, ..., n$.

Tarkastellaan Bernheimin, Pelegin ja Whinstonin [3] käyttämää esimerkkiä. Esimerkillä havainnollistetaan Nashin tasapainon, vahvan Nashin tasapainon sekä koalition kestävän Nashin tasapainon eroavaisuuksia. Peli on esitetty taulukossa 1.

Taulukko 1: Esimerkki koalition kestävästä Nashin tasapainosta

	C₁		**C₂**	
	B₁	**B₂**	**B₁**	**B₂**
A₁	1,1,-5	-5,-5,0	-1,-1,5	-5,-5,0
A₂	-5,-5,0	0,0,10	-5,-5,0	-2,-2,0

Taulukossa 1 kuvatussa pelissä on kaksi Nashin tasapainoa, (A_2, B_2, C_1) sekä (A_1, B_1, C_2). Vahvan ja koalition kestävän Nashin tasapainon on oltava myös Nashin tasapainoja, riittää siis tarkastella pelin Nashin tasapainoja selvitettäessä pelin mahdollisia vahvoja ja koalition kestäviä Nashin tasapainoja. Tutkitaan ensiksi, ovatko pelin Nashin tasapainot myös vahvoja Nashin tasapainoja. Nashin tasapainossa (A_2, B_2, C_1) pelaajista A ja B koostuvan koalition molemmat osapuolet hyötyvät, jos molemmat vaihtavat strategiaansa, eli $(A_2, B_2) \to (A_1, B_1)$. Nashin tasapaino (A_2, B_2, C_1) ei siis ole vahva Nashin tasapaino. Nashin tasapainosta (A_1, B_1, C_2) puolestaan kaikista pelaajista A, B ja C koostuvan koalition kaikki jäsenet hyötyvät, jos kaikki vaihtavat strategiaansa, eli $(A_1, B_1, C_2) \to (A_2, B_2, C_1)$. Täten jälkimmäinenkään Nashin tasapaino ei ole vahva Nashin tasapaino. Voidaan

päätellä, ettei esimerkin pelissä esiinny vahvoja Nashin tasapainoja lainkaan.

Tutkitaan seuraavaksi, onko esimerkin pelissä koalition kestäviä Nashin tasapainoja. Tarkastellaan ensiksi ensimmäistä Nashin tasapainoa (A_2, B_2, C_1). Kuten huomattiin vahvaa Nashin tasapainoa tutkittaessa, Nashin tasapainosta (A_2, B_2, C_1) pelaajasta A ja B koostuvan koalition kummatkin osapuolet hyötyvät mikäli nämä vaihtavat strategiaansa $(A_2, B_2) \to (A_1, B_1)$. Tämän koalition strategiamuutoksesta seuraava tila on koalition keskinäisen pelin koalition kestävä Nashin tasapaino, kun pelaajan C strategia oletetaan kiinnitetyksi. Täten Nashin tasapaino (A_2, B_2, C_1) ei ole koalition kestävä Nashin tasapaino. Tarkastellaan seuraavaksi toista pelin Nashin tasapainoista (A_1, B_1, C_2). Tästä tilasta mikään pelaajien aidosta osajoukosta koostuva koalitio ei kykene strategiaansa yhdessä muuttamalla parantamaan jäsentensä hyötyfunktioiden arvoja. Täten (A_1, B_1, C_2) on koalition kestävä Nashin tasapaino.

4 Rationaalinen salaisuuden jakaminen

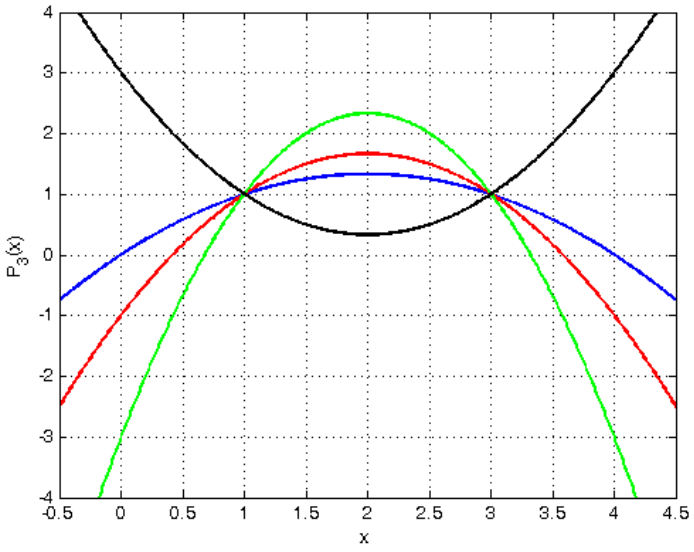
Tarkastellaan tässä kappaleessa erilaisia tapoja jakaa tai säilyttää jokin salainen tieto, esimerkiksi kryptografisen salauksen avainta. Kuvitellaan tilanne, jossa tahtoisimme tallettaa jonkin erityisen tärkeän ja salaisen tiedon itsellemme muistiin. Jos olemme huolestuneita vain tiedon vuotamisesta ulkopuoliselle, on tiedon tallentaminen yhdelle mahdollisimman turvalliselle palvelimelle todennäköisesti paras vaihtoehto. Toisaalta, jos olisimme huolestuneita kovalevyjen rikkoutumisesta ja tiedon häviämisestä, kannattavampaa olisi kopioida tietoa mahdollisimman monelle palvelimelle, jolloin todennäköisyys, että kaikki palvelimet hajoavat yhdenaikaisesti ja täten tieto häviäisi kokonaan saataisiin hyvin pieneksi.

Haetaan ratkaisu esitellylle kuvitteelliselle tilanteelle, jossa tahdomme tallettaa arkaluontoista mutta kuitenkin tärkeää tietoa siten, että ratkaisu on yllä käsiteltyjen ääriratkaisujen välimaastossa. Voimme toteuttaa tämän jakamalla salaisuutemme useampaan osaan, siten että näistä osa-salaisuuksista tai niiden osajoukosta voidaan koostaa alkuperäinen salattava tieto. Hieman formaalimmin aseteltuna, tahdomme jakaa salaisuuden n:ään osa-salaisuuteen siten, että varsinainen salaisuus saadaan koostettua vähintään k osa-salaisuuden avulla. Yksi tapa toteuttaa tämä on Shamirin kehittämä polynomeihin perustuva menetelmä [9].

Shamirin salaisuuden jakamiseen tähtäävässä menetelmässä generoidaan $k-1$-asteen polynomi $P_k(x) = a_0 + a_1x + ... + a_{k-1}x^{k-1}$, jonka kertoimet $a_i, i > 0$ ovat satunnaisesti arvottuja mutta arvo pisteessä $x = 0$, eli vakiotermi a_0 on itse jaettava salaisuus. Jakaaksemme salaisuuden useampaan osaan (n kpl), arvomme n kappaletta satunnaisia muuttujan x arvoja ja laskemme näitä vastaavat polynomin P_k arvot. Jokainen lukuparit $(x, P_k(x))$ toimii nyt menetelmän osa-salaisuutena ja jos tietää yhteensä k kappaletta osa-salaisuuksia, pystyy määrittämään alkuperäisen salaisuuden. Tämä seuraa siitä, että määritelläkseen $f-1$ -asteen polynomin yksiselitteisesti tarvitaan yhteensä k tunnettua pistettä. Esimerkiksi kuvassa 2 on esitetty useita kahden pisteen avulla määriteltyjä toisen asteen polynomeja, joilla kaikilla on eri vakiotermi. Kaikkien polynomien kuvaajat kulkevat kuitenkin pisteiden $(1, 1)$ ja $(3, 1)$ kautta. Toisen asteen polynomin yksikäsitteiseen määrittämiseen tarvitaan siis kolmas piste.

Osaamme nyt jakaa salaisuuden yksittäisiin osa-salaisuuksiin, joista jokainen on yksinään merkityksetön, mutta yhdessä k kappaletta osa-salaisuuksia määrittävät varsinaisen salaisuuden yksiselitteisesti. Tallennamme jokaiselle käytössämme olevalle palvelimelle talteen yhden osa-salaisuuden, ja myöhemmin voimme koostaa näistä osa-salaisuuksista uudestaan alkuperäisen salaisuuden. Mikäli tietoturvahyökkäyksen seurauksena joku onnistuisi saamaan yhden yksittäisen osa-salaisuuden selville, ei varsinainen salaisuus kuitenkaan paljastu hyökkääjälle. Toisaalta, mikäli yksi tai useampi palvelin rikkoontuu, voimme edelleen päätellä alkuperäisen salaisuuden, kunhan palvelimien lukumäärää $n > k$, missä k on tarvittavien osa-salaisuuksien lukumäärä.

Kun aikanaan tahdomme päästä käsiksi varsinaiseen salaisuuteen, pyydämme jokaista palvelinta toimittamaan meille oman osa-salaisuutensa. Ongelmana kuitenkin on, ettemme voi tässä vaiheessa tietää ovatko kaikki palvelimet luotetta-



Kuva 2: Useita kahdella pisteellä määriteltyjä 2. asteen polynomeja

via. Selvitetään seuraavaksi voiko sopivalla protokollalla taata sen, että pystymme päättelemään alkuperäisen salaisuuden vaikka yksi tai useampi palvelin lopettaa toiminnan. Palvelin voi lopettaa toiminnan laitteistorikon myötä, tai jos jokin ulkopuolinen taho on kaapannut palvelimen ja tahallaan jättää tietoa jakamatta, tavoitteenaan estää alkuperäisen salaisuuden selvittäminen muilta sekä saada itselleen selville alkuperäinen salaisuus.

Mallinnetaan tätä eri palvelimien välistä kommunikaatiota Halpernin ja Teaguen tapaan [5] pelinä, jossa jokainen palvelin on pelaaja, joka hyötyy ensisijaisesti siitä, että tämä saa selville salaisuuden. Toissijaisesti pelaajat hyötyvät siitä, ettei muut pelaajat saa salaisuutta selville. Pelaajien hyötyfunktioiden käyttäytymistä on kuvattu formaalisti yhtälöissä (4). Yhtälöissä (4) esiintyvä $\text{info}_i(\mathbf{s})$ saa arvon 1 jos pelaaja i kykenee koostamaan alkuperäisen salaisuuden kun pelaajat pelaavat strategioilla $\mathbf{s}$ ja 0 muulloin.

$$\begin{aligned}
\forall j, \text{info}_j(\mathbf{s}) = \text{info}_j(\mathbf{s}') &\quad\Rightarrow\quad u_i(\mathbf{s}) = u_i(\mathbf{s}') \\
\text{info}_i(\mathbf{s}) > \text{info}_i(\mathbf{s}') &\quad\Rightarrow\quad u_i(\mathbf{s}) > u_i(\mathbf{s}') \\
\left.\begin{array}{r} \text{info}_i(\mathbf{s}) = \text{info}_i(\mathbf{s}') \\ \forall j \neq i, \text{info}_j(\mathbf{s}) \leq \text{info}_j(\mathbf{s}') \\ \exists k \neq i, \text{info}_k(\mathbf{s}) < \text{info}_k(\mathbf{s}') \end{array}\right\} &\quad\Rightarrow\quad u_i(\mathbf{s}) > u_i(\mathbf{s}')
\end{aligned} \tag{4}$$

Peli etenee pelaajien osalta siten, että jokaisella kierroksella jokainen pelaaja joko lähettää, tai on lähettämättä oman osuutensa salaisuudesta muille. Lisäksi kaikki pelaajat lähettävät viestinsä jokaisella kierroksella samanaikaisesti. Pelaajat eivät siis voi havaita ensiksi toisen viestiä, ja tämän perusteella päättää lähettääkö itse viestin vai ei.

Deterministiset protokollat

Tarkastellaan peliä, joka kestää äärellisen määrän kierroksia. Tarkastellaan erityisesti pelin viimeistä kierrosta. Pelin viimeisellä kierroksella kukin pelin pelaaja i voi joko olla jo koostanut itselleen alkuperäisen salaisuuden, tai sitten ei. Tarkastellaan näitä kahta tilannetta erillään.

Pelaajan i on tehtävä päätös, jakaako oman osuutensa salaisuudesta muiden kanssa. Oletetaan ensin, että pelaaja i ei vielä kierrokseen k mennessä ole saanut selville alkuperäistä salaisuutta ja että jollakin todennäköisyydellä $0 \leq p_i \leq 1$ pelaaja i saa kierroksella k tietoonsa varsinaisen salaisuuden. Todennäköisyys sille, että pelaaja i saa selville alkuperäisen salaisuuden ei riipu siitä, jakaako hän oman salaisuutensa vai ei kierroksella k, koska muut pelaajat eivät kykene havainnoimaan pelaajan i päätöstä ennen kuin heidän tarvitsee tehdä oma päätöksensä. Toisaalta todennäköisyys sille, että jokin muu pelaaja saa selville alkuperäisen salaisuuden kierroksella k kasvaa, jos pelaaja i päättää jakaa oman salaisuutensa muiden pelaajien kanssa. Pelaajan i hyötyfunktion odotusarvo siis heikkenee, jos hän jakaa oman osuutensa salaisuudesta muiden kanssa kierroksella k.

Tarkastellaan seuraavaksi tilannetta, jossa pelaaja i tietää kierroksen k alussa alkuperäisen salaisuuden. Nyt pelaaja i ei enää kykene toimillaan parantamaan omaa hyötyfunktiotaan. Mikäli hän jakaa oman osuutensa salaisuudesta muille, pelaaja kasvattaa todennäköisyyttä sille, että jokin muu pelaaja saa salaisuuden selville kierroksella k. Täten pelaaja voi vain heikentää oman hyötyfunktionsa odotusarvoa lähettämällä oma osuutensa salaisuudesta muille kierroksella k.

Strategiat, joissa pelaaja i ei jaa omaa osuuttaan salaisuudesta dominoi siis aina strategioita, joissa pelaaja i jakaa oman osuutensa salaisuudesta muille kierroksella k. Induktiivisesti voidaan jatkaa samalla päättelyllä kierroksille $k-1$, $k-2$, aina ensimmäiselle kierrokselle asti. Ainoa strategia, joka ei ole dominoitu on siis strategia, jossa pelaaja i ei jaa omaa osuuttaan salaisuudesta kenellekään millään kierroksella. Koska tämä on ainoa strategia joka ei ole dominoitu, on tämä myös Nashin tasapaino.

Tutkitaan vielä, pystyykö jokin koalitio muuttamalla strategiaansa yhdessä parantamaan jäsentensä hyötyfunktiota. Mikäli yhdelläkin koalition jäsenistä on tiedossa kierroksen k alussa alkuperäinen salaisuus, ei koalitio pysty millään strategialla parantamaan kaikkien jäsentensä hyötyfunktiota. Tämä seuraa siitä, että jokaisen koalition jäsenen, joka tietää jo salaisuuden, hyötyfunktion odotusarvo heikkenee jos todennäköisyys sille, että jokin toinen pelaaja tietää salaisuuden kasvaa. Täten, jos koalitio yhdessä päättää poiketa Nashin tasapainosta ja jakaa omat osasalaisuutensa muille, kaikki koalition jäsenet, joilla on kierroksen k alussa salaisuus tiedossa, heikentävät oman hyötyfunktionsa odotusarvoa.

Entä pystyykö koalitio, jonka yksikään jäsen ei ole kierrokseen k mennessä saanut salaisuutta selville, parantamaan jokaisen jäsenensä hyötyfunktion arvoa poikkeamalla Nashin tasapainosta? Oletetaan, että salaisuus on jaettu osiin $\kappa - 1$ -asteen polynomin avulla. Tällöin koalitio pystyy parantamaan kaikkien jäsentensä hyötyfunktiota, jos koalition suuruus on suurempi kuin κ, eli $|\mathcal{C}| \geq \kappa$. Tämä johtuu siitä, että tällöin kaikki koalition jäsenet pystyvät päättelemään alkuperäisen

salaisuuden. Tästä seuraa suoraan, ettei strategia olla jakamatta ikinä omaa osuuttaan salaisuudesta ole vahva Nashin tasapaino. Poikkeama tasapainosta, jossa kaikki koalition jäsenet yhdessä paljastavat oman osasalaisuutensa ei kuitenkaan täytä koalition kestävää Nashin tasapainoa tarkasteltaessa tehtävän poikkeutuksen ehtoja, sillä jokainen koalition jäsen pystyy entisestään parantamaan oman hyötyfunktionsa arvoa jättämällä oma osuutensa salaisuudesta paljastamatta.

Strategia olla jakamatta kenellekään on siis Nashin tasapaino käytettäessä protokollaa, joka päättyy äärellisen määrän kierroksia jälkeen, jossa kukin osapuoli voi vapaasti päättää jakaako oman osuuden salaisuudesta vai ei ja pelaajien hyötyfunktiot noudattavat yhtälöiden (4) periaatteita. Halpern [5] ja Abraham [1] päätyvät samaan lopputulokseen ja toteavat myös, kuinka tällä asetelmalla ei ikinä päästä lopputulokseen, jossa joku saisi alkuperäisen salaisuuden selville. Tämä tarkoittaa käytännössä sitä, ettei sellaista determinististä protokollaa voi olla, joka päättyy äärellisessä ajassa ja jonka myötä salaisuuden jakaminen onnistuisi, kun eri osapuolten hyötyfunktiot ovat yhtälöiden (4) mukaiset ja osapuolet toimivat rationaalisesti.

Satunnaistetut protokollat

Deterministisen protokollan toimimattomuus kumpuaa siitä, ettei yhdelläkään pelaajalla ole syytä paljastaa omaa osuuttaan salaisuudesta viimeisellä kierroksella. Pelaaja tietää, ettei hän voi menettää mitään olemalla jakamatta omaa osuuttaan salaisuudesta. Tarkastellaan seuraavaksi protokollia, joissa tuomalla protokollan etenemiseen satunnaisuutta mukaan, voi pelaajille koitua haittaa siitä, että jättävät oman osuutensa salaisuudesta jakamatta.

Tarkastellaan samaa protokollaa ja peliä, jota Halpern käsitteli [5], ja jossa pelaajia on kolme ja salaisuus on jaettu heille kaikille siten, että kaikkien kolmen osuus tarvitaan salaisuuden koostamiseen. Lisäksi oletetaan, että pelaajilla on olemassa mekanismi, jolla he voivat arpoa satunnaislukuja, mutta vain siten etteivät pysty väärentämään lopputulosta. Muut pelaajat pystyvät siis näkemään arvotusta luvusta, onko se oikean satunnaislukugeneraattorin tuottama. Salaisuutta jaettaessa eri osapuolille on myös jaettu yhden osa-salaisuuden sijaan lista osa-salaisuuksia. Pelaajan i listan osa-salaisuus j on siis polynomin P_3^j arvo pisteessä x_i. Jokainen listalla oleva osa-salaisuus on siis osa-salaisuus yhteen polynomiin P_3^j. Toisaalta kaikkien polynomien vakiotermi on sama alkuperäinen salaisuus a_0.

1 Arvo luku c s.e. $P(c = 1) = \alpha$, $P(c = 0) = 1 - \alpha$
2 Jos $c = 1$, jaa listasi päälimmäinen osuus salaisuudesta muiden kanssa
3 Jos $c = 0$, lähetä arpomasi $c = 0$ muille tarkistettavaksi
4 Vastaanota muiden mahdollisesti jakamat osa-salaisuudet tai arvotut 0:t
5 Jos saat alkuperäisen salaisuuden koostettua, lopeta peli
6 Jos joku ei jakanut osa-salaisuuttaan, arpomaansa 0:aa tai jonkun jakama 0 oli väärennetty, lopeta peli
7 Poista päällimmäinen osuus salaisuudesta listaltasi
8 Palaa riville 1

Algorithm 1: Yksinkertainen satunnaistettu protokolla

Tarkastellaan protokollaa 1 peliteorian näkökulmasta. Oletetaan taas, että pelaajien hyötyfunktiot noudattavat yhtälöitä (4). Protokollan 1 pelaaja i arpoo todennäköisyydellä $1-\alpha$ c:n arvoksi 0. Muut pelaajat näkevät, että pelaaja i on arponut itselleen $c = 0$ eivätkä täten odota hänen jakavan omaa osa-salaisuuttaan muille. Tässä tilanteessa pelaajalla i ei ole mitään syytä poiketa protokollasta, vaan rationaalinen pelaaja noudattaa protokollaa. Toisaalta, todennäköisyydellä α pelaaja i arpoo itselleen satunnaisluvun $c = 1$. Nyt pelaajan i on tehtävä päätös, kannattaako hänen noudattaa protokollaa ja jakaa oma salaisuutensa, vai poiketa protokollasta. Jos pelaaja poikkeaa protokollasta, peli loppuu käynnissä olevalle kierrokselle, sillä muut pelaajat tulevat huomaamaan vilpin, ja lopettavat pelaamisen.

Tutkitaan hyötyfunktion odotusarvoa eri tilanteissa. Oletetaan, että jos pelaaja i noudattaa kaikkien muiden pelaajien kanssa protokollaa, kaikki saavat salaisuuden lopulta selville. Merkitään pelaajan i hyötyfunktion arvoa tuolloin u_i(kaikki). Jos pelaaja i ei noudata protokollaa, peli voi päättyä joko siten, ettei kukaan saa salaisuutta selville, tai pelkästään pelaaja i saa salaisuuden selville. Pelaaja i saa salaisuuden selville siinä tapauksessa, että molemmat muut pelaajat ovat arponeet satunnaisluvukseen $c = 1$. Tämän todennäköisyys on α^2. Muissa tapauksissa kukaan ei saa salaisuutta pelin loppuun mennessä selville ja todennäköisyys tämän toteutumiselle on $1 - \alpha^2$. Pelaajan i ei kannata poiketa protokollasta, jos tämän hyötyfunktion odotusarvo heikkenisi tästä. Toisin sanottuna, jos pelaajan i hyötyfunktio ja todennäköisyys α noudattavat yhtälöä (5), tällä ei ole syytä poiketa algoritmista missään vaiheessa protokollaa.

$$\alpha^2 u_i(\text{vain } i) + (1 - \alpha^2) u_i(\text{ei kukaan}) < u_i(\text{kaikki}) \tag{5}$$

Protokollan määrittelemä strategia on siis Nashin tasapaino, sillä yhdelläkään pelaajalla ei ole syytä poiketa tästä. Myöskään millään koalitiolla, jonka koko on 2 tai suurempi ei ole syytä poiketa protokollasta jättämällä omaa osa-salaisuuttaan jakamatta riippumatta arvonnan tuloksesta, sillä sen seurauksena kukaan ei saisi salaisuutta selville. Sen sijaan, jos kaikki kolme päättävät huolimatta arvottujen lukujen c arvoista jakaa toisilleen omat osa-salaisuutensa, jokainen koalition jäsen saa salaisuuden selville todennäköisyydellä $P = 1$. Tämä poikkeutus tasapainosta ei kuitenkaan täytä koalition kestävän Nashin tasapainoa tarkasteltaessa tehtävien poikkeu-

tusten ehtoja, sillä yksi pelaaja voi yksin edelleen parantaa oman hyötyfunktionsa arvoa jättämällä oman osa-salaisuutensa jakamatta muille. Tällä tavalla hän yksin saisi selville salaisuuden, mutta muut eivät. Vaikuttaisi siltä, että protokollan 1 määrittelemä strategia on Nashin tasapainon lisäksi myös koalition kestävä Nashin tasapaino, mutta ei kuitenkaan vahva Nashin tasapaino.

Protokollassa 1 on kuitenkin ongelma, jonka ylenkatsoimme analyysissämme olettamalla, että jokainen pelaaja saa salaisuuden selville lopulta, jos kaikki noudattavat protokollaa. Tämä ei kuitenkaan käytännössä pidä paikkaansa sillä, mikäli tasan kaksi arpovat satunnaislukunsa arvoksi $c = 1$ ja kolmas arpoo lukunsa arvoksi $c = 0$, pelaaja, joka arpoi satunnaisluvukseen $c = 0$ saa salaisuuden selville, kun muut eivät. Halpern [5] huomioi myös tämän, ja esitti toisen hieman monimutkaisemman kolmen pelaajan pelin sekä tämän perustana toimivan protokollaan. Tämä protokolla on esitetty kaaviossa 2. Protokollan kuvauksessa operaattorilla $\oplus$ tarkoitetaan eksklusiivista disjunktiota, eli XOR-operaattoria. Operaattorin $\oplus$ käyttäytyminen on kuvattu totuustaulussa 2.

Taulukko 2: XOR-operaattorin käyttäytyminen

A	**B**	**A** $\oplus$ **B**
1	1	0
1	0	1
0	1	1
0	0	0

1 Arvo luku c_i s.e. $P(c = 1) = \alpha$, $P(c = 0) = 1 - \alpha$
2 Arvo luku $c_{(i,+)}$ s.e. $P(c = 1) = 1/2$, $P(c = 0) = 1/2$
3 Laske luku $c_{(i,-)} = c_i \oplus c_{(i,+)}$
4 Lähetä luku $c_{(i,+)}$ pelaajalle i^+ ja luku $c_{(i,-)}$ pelaajalle i^-
5 Vastaanota luku $c_{(i^-,+)}$ pelaajalta i^- ja luku $c_{(i^+,-)}$ pelaajalta i^+
6 Laske ja lähetä luku $c_{(i^+,-)} \oplus c_i$ pelaajalle i^-
7 Vastaanota luku $c_{((i^+)^+,-)} \oplus c_{i^+} = c_{(i^-,-)} \oplus c_{i^+}$ pelaajalta i^+
8 Laske $z = c_{(i^-,-)} \oplus c_{i^+} \oplus c_{(i^-,+)} \oplus c_i = c_{(i^-,-)} \oplus c_{(i^-,+)} \oplus c_{i^+} \oplus c_i = c_{i^-} \oplus c_{i^+} \oplus c_i$
9 Jos $z = 1$ ja $c_i = 1$, lähetä oman listasi päälimmäinen osuus salaisuudesta muiden kanssa
10 Vastaanota muiden mahdollisesti lähettämät osuudet salaisuudesta
11 Jos $z = 1$ ja $c_i = 1$, mutta vastaanotit tasan yhden osa-salaisuuden, joku on poikennut protokollasta – lopeta peli
12 Jos $z = 1$ ja $c_i = 0$, mutta et vastaanottanut yhtään osa-salaisuutta, joku on poikennut protokollasta – lopeta peli
13 Jos saat salaisuuden koostettua, lopeta peli
14 Poista päällimmäinen osuus salaisuudesta listaltasi
15 Palaa riville 1

Algorithm 2: Korjattu kolmen pelaajan satunnaistettu protokolla

Tutkitaan protokollaa 2 ja selvitetään, missä vaiheessa pelaajalla i voisi olla syytä poiketa protokollasta. Jos pelaaja i jättää jonkin luvuista lähettämättä protokollan vaiheissa 4 tai 6, muut pelaajat havaitsevat pelaajan i vilpin, ja lopettavat pelin kesken. Näissä vaiheissa pelaajan i kannattaa siis joka tapauksessa lähettää jokin viesti protokollan mukaisesti. Tarkastellaan, voiko pelaaja i huijata molemmat muut lähettämään omat osuutensa salaisuudesta siten, että molemmat kanssapelaajat laskevat z:n arvoksi 1 tasan silloin kun molempien arpoma luku $c_j = 1$ ja muulloin $z = 0$. Yhtälöissä (6) on esitetty kaavat, joilla pelaajat i^+ ja i^- laskevat z:n arvon.

$$\begin{aligned} i^+ : &\quad z_{i^+} = (c_{(i,-)} \oplus c_{i^-}) \oplus c_{(i,+)} \oplus c_{i^+} \\ i^- : &\quad z_{i^-} = (c_{(i^+,-)} \oplus c_i) \oplus c_{(i^+,+)} \oplus c_{i^-} \end{aligned} \tag{6}$$

Pelaaja i voi huijata valitsemalla muille lähettämänsä $c_{(i,-)}$, $c_{(i,+)}$ ja $(c_{(i^+,-)} \oplus c_i)$ mielivaltaisesti. Jotta huijaamisesta olisi hyötyä, tulisi nämä luvut valita siten, että molemmat kanssapelaajat laskevat z:n arvoksi yksi tarkalleen silloin kun molempien $c_j = 1$. Koska pelaaja ei kuitenkaan tiedä muiden yhtälöissä (6) esiintyvien lukujen arvoja ei tämä voi valita lähettämiään arvoja siten, että huijaus onnistuisi. Pelaaja i^+ saadaan laskemaan z:n arvoksi 1, kun sekä c_{i^+} että c_{i^-} ovat 1, lähettämällä protokollan vaiheessa 4 $c_{(i,+)}$ ja $c_{(i,-)}$ siten, että näistä tasan yksi on arvoltaan 1. Tällöin pelaaja i^+ laskee z:n arvoksi 1 myös silloin, jos sekä c_{i^+} että c_{i^-} ovat 0. Pelaaja i ei siis voi huijata valitsemalla lähettämiensä lukujen arvoja mielivaltaisesti.

Tutkitaan vielä, voiko yksittäinen pelaaja hyötyä poikkeamalla protokollasta vaiheessa 9 olemalla lähettämättä omaa osuuttaan salaisuudesta vaikka protokollan mukaan hänen pitäisi. Oletetaan taas, että mikäli pelaaja ei poikkea protokollasta, niin kaikki pelaajat saavat salaisuuden lopulta selville. Tällä kertaa, jos kaksi kolmesta arpovat satunnaisluvukseen $c_i = 1$, kukaan ei lähetä osuuttaan salaisuudesta toisille, eli samaa ongelmaa kuin protokollassa 1 ei tällä kertaa ole. Pelaajan i hyötyfunktion arvo hänen pelatessa protokollan mukaisesti on siis u_i(kaikki). Pelaajan i on järkeä poiketa protokollasta vain, jos $z = 1$ ja jos arpomansa $c_i = 1$. Tällöin poikkeamalla protokollasta voi olla kaksi eri seurausta, joko $c_{i^+} = c_{i^-} = 1$, molemmat muut pelaajat jakavat oman osa-salaisuutensa ja pelaaja i saa yksinään salaisuuden selville, tai vaihtoehtoisesti $c_{i^+} = c_{i^-} = 0$, kukaan ei jaa osa-salaisuuttaan ja peli päättyy kun molemmat muut pelaajat huomaavat pelaajan i huijanneen jättämällä lähettämättä omaa osuuttaan. Lasketaan näille kahdelle eri skenaariolle ehdolliset todennäköisyydet.

$$
\begin{aligned}
P(c_{i^+}=1, c_{i^-}=1 | v=1, c_i=1) &= \frac{P(v=1, c_i=1 | c_{i^+}=1, c_{i^-}=1) P(c_{i^+}=1, c_{i^-}=1)}{P(v=1, c_i=1)} \\
&= \frac{P(v=1 | c_i=1, c_{i^+}=1, c_{i^-}=1) P(c_{i^+}=1, c_{i^-}=1, c_i=1)}{P(v=1 | c_i=1) P(c_i=1)} \\
&= \frac{P(c_{i^+}=1) P(c_{i^-}=1) P(c_i=1)}{(P(c_{i^+}=0, c_{i^-}=0) + P(c_{i^+}=1, c_{i^-}=1)) P(c_i=1)} \\
&= \frac{P(c_{i^+}=1) P(c_{i^-}=1)}{P(c_{i^+}=0, c_{i^-}=0) + P(c_{i^+}=1, c_{i^-}=1)} \\
&= \frac{\alpha^2}{(1-\alpha)^2 + \alpha^2}
\end{aligned}
$$

$$
\begin{aligned}
P(c_{i^+}=0, c_{i^-}=0 | v=1, c_i=1) &= \frac{P(v=1, c_i=1 | c_{i^+}=0, c_{i^-}=0) P(c_{i^+}=0, c_{i^-}=0)}{P(v=1, c_i=1)} \\
&= \frac{P(v=1 | c_i=1, c_{i^+}=0, c_{i^-}=0) P(c_{i^+}=0, c_{i^-}=0, c_i=1)}{P(v=1 | c_i=1) P(c_i=1)} \\
&= \frac{P(c_{i^+}=0) P(c_{i^-}=0) P(c_i=1)}{(P(c_{i^+}=0, c_{i^-}=0) + P(c_{i^+}=1, c_{i^-}=1)) P(c_i=1)} \\
&= \frac{P(c_{i^+}=0) P(c_{i^-}=0)}{P(c_{i^+}=0, c_{i^-}=0) + P(c_{i^+}=1, c_{i^-}=1)} \\
&= \frac{(1-\alpha)^2}{(1-\alpha)^2 + \alpha^2}
\end{aligned}
$$

Eri skenaarioiden todennäköisyyksiä johtaessa voidaan huomata, ettei eri skenaarioiden toteutuminen riipu pelaajan i satunnaisluvun todennäköisyysjakaumasta, vaan pelkästään muiden pelaajien satunnaislukujen c_j todennäköisyysjakaumista. Pelaaja i ei siis voi parantaa oman hyötyfunktionsa odotusarvoa muuttamalla oman satunnaislukunsa todennäköisyysjakaumaa. Rationaalinen pelaaja i ei poikkea protokollasta ellei tämän hyötyfunktion odotusarvo parane protokollasta poikkeamisen myötä. Mikäli pelaajan hyötyfunktio u_i ja satunnaisluvun c generoinnissa käytetty todennäköisyys α noudattavat epäyhtälöä (7), protokollan 2 määrittelemä strategia on Nashin tasapaino.

$$
\frac{\alpha^2}{(1-\alpha)^2 + \alpha^2} u_i(\text{vain } i) + \frac{(1-\alpha)^2}{(1-\alpha)^2 + \alpha^2} u_i(\text{ei kukaan}) < u_i(\text{kaikki}) \tag{7}
$$

Protokollan määrittelemä strategia on siis Nashin tasapaino, mutta tutkitaan vielä, onko kyseinen strategia myös koalition kestävä Nashin tasapaino tai jopa vahva Nashin tasapaino. Jälleen, jos kaikki kolme pelaajaa päättävät poiketa tasapainosta jakamalla omat osa-salaisuutensa muille riippumatta arvottujen satunnaislukujen arvosta, niin kaikki kolme saavat salaisuuden selville. Tämä ei kuitenkaan nyt paranna kenenkään hyötyfunktion arvoa, sillä kaikki saavat salaisuuden selville joka tapauksessa. Pienempien koalitioiden ei kannata poiketa protokollasta, koska silloin

he eivät pysty missään tilanteessa parantamaan omien hyötyfunktioidensa arvoja. Jos koalitio, jonka koko on 2 päättää olla jakamatta omia osuuksiaan salaisuudesta, kukaan ei saa salaisuutta selville. Toisaalta jos molemmat jakavat salaisuutensa riippumatta arvottujen satunnaislukujen arvosta, he eivät itse välttämättä saa salaisuutta selville, mutta kolmas pelaaja saa salaisuuden varmuudella selville. Protokollaan määrittelemä strategia on siis koalition kestävä Nashin tasapaino.

5 Monitaholaskenta

Monitaholaskennalla (*multiparty computation*) tarkoitetaan laskentaa, jossa yhden laskentayksikön sijaan useampi palvelin tai muu yksikkö yhdessä suorittavat jonkin annetun protokollan mukaisesti laskutoimituksia. Suorittamalla laskentaa useammassa laskentayksikössä samanaikaisesti, voidaan laskenta-aikoja pienentää merkittävästi. Tässä kappaleessa keskitymme kuitenkin monitaholaskentatehtäviin, joissa jokaisella laskennan osapuolella on oma syöte, ja laskennan on tarkoitus tuottaa jokin lopputulos eri osapuolten syötteistä.

Erityisesti tutkimme seuraavaksi sellaisia tilanteita, joissa eri osapuolet tahtovat suorittaa jonkin laskutoimituksen yhdessä kaikkien syötteillä, mutta pelaajat eivät kuitenkaan tahdo paljastaa omaa syötettään muille. Yksi esimerkki tällaisesta pulmasta on miljonäärien ongelma, jossa kaksi tai useampi miljonääriä tahtovat selvittää kuka on heistä rikkain. Miljonäärit eivät kuitenkaan tahdo paljastaa toisilleen oman omaisuutensa arvoa. Tämä on mahdollista toteuttaa, kuten Yao näytti vuonna 1982 [11].

Kaikille funktioille tällainen laskenta ei kuitenkaan ole mahdollista. Shoham ja Tennenholtz [10] määrittelivät funktioiden luokan, jonka kaikkien funktioiden tulokset voidaan laskea, kun käytössä on yhteinen luotettava laskentayksikkö, jokainen osapuoli tahtoo ensisijaisesti saada lopputuloksen laskettua, ja toissijaisesti puolestaan jokainen pelaaja pyrkii estämään tiedon välittymisen muille. Shoham ja Tennenholtz nimittivät tätä funktioden luokkaa *Non-cooperative computable* (NCC) nimellä. Vain tähän luokkaan kuuluvia funktioita on järkevää pyrkiä ratkomaan monitaholaskennalla, jossa jokainen osapuoli tavoittelee omaa etuaan.

Monitaholaskennan suhteen päästään vastaaviin tuloksiin kuin salaisuuden jakamisenkin kanssa, kun tarkkaillaan protokollaa, joka päättyy äärellisessä ajassa. Määritellään eri osapuolille hyötyfunktiot samassa hengessä kuin salaisuuden jakamisen yhteydessä (4). Tällä kertaa mallinnetaan tieto yhden salaisuuden sijaan useaksi atomiseksi "tiedonjyväseksi" $\mathcal{I}_0, \mathcal{I}_1, \mathcal{I}_2, ..., \mathcal{I}_m$. Joukko $\text{info}_i(\mathbf{s})$ on kaikkien pelaajan i tietämien $\mathcal{I}$ joukko kun osapuolet käyttävät strategioita $\mathbf{s}$.

$$\begin{aligned}
\forall j, \text{info}_j(\mathbf{s}) = \text{info}_j(\mathbf{s}') &\quad\Rightarrow\quad u_i(\mathbf{s}) = u_i(\mathbf{s}') \\
\left.\begin{array}{r} \text{info}_i(\mathbf{s}) \supseteq \text{info}_i(\mathbf{s}') \\ \forall j \neq i, \text{info}_j(\mathbf{s}) \subseteq \text{info}_j(\mathbf{s}') \end{array}\right\} &\quad\Rightarrow\quad u_i(\mathbf{s}) \geq u_i(\mathbf{s}') \\
\left.\begin{array}{r} \exists j \neq i, \text{info}_j(\mathbf{s}) \subset \text{info}_j(\mathbf{s}') \\ \forall k \neq j, \text{info}_k(\mathbf{s}) = \text{info}_k(\mathbf{s}') \\ u_j(\mathbf{s}) < u_j(\mathbf{s}') \end{array}\right\} &\quad\Rightarrow\quad u_i(\mathbf{s}) > u_i(\mathbf{s}')
\end{aligned} \tag{8}$$

Hyötyfunktio (8) on pohjimmiltaan hyvin samanlainen aiemmin käsitellyn hyötyfunktion kanssa. Hyötyfunktioon vaikuttaa pelkästään eri pelaajilla oleva informaatio. Mikäli pelaaja i tietää enemmän tai yksi tai useampi muista pelaajista tietää vähemmän, pelaajan i hyötyfunktion arvo ei ainakaan heikkene. Toisaalta, jos jokin muut pelaaja saa uutta informaatiota, jonka myötä hänen hyötyfunktionsa arvo paranee, pelaajan i hyötyfunktion arvo heikkenee.

Tarkastellaan äärellisessä ajassa päättyvää protokollaa, jossa määritetään eri pelaajien syötteiden perusteella jokin lopputulos. Protokolla päättyy ajanhetkellä k.

Eri osapuolet voivat lähettää viestejä toisilleen aina jokaisella kierroksella. Oletetaan että tällaisia kierroksia on k ajanhetkeä kestävässä pelissä k kappaletta. Tarkastellaan viimeistä kierrosta k. Mikäli protokollan mukaan jonkin pelaajan tulisi lähettää toisille pelaajille jotakin informaatiota $\mathcal{I}$ tällä kierroksella, rationaalinen pelaaja jättää kyseisen viestin lähettämättä, sillä tämän myötä hänen oman hyötyfunktionsa arvo voi vain heiketä. Lähettäjänä hän ei voi vastaanottaa mitään uutta informaatiota, mutta sen sijaan informaation vastaanottajat voivat hyötyä tästä viestistä. Tämä puolestaan laskee lähettäjän hyötyfunktion odotusarvoa. Näin voidaan päätellä, ettei yksikään rationaalinen osapuoli lähetä protokollan viimeisellä kierroksella kenellekään viestejä.

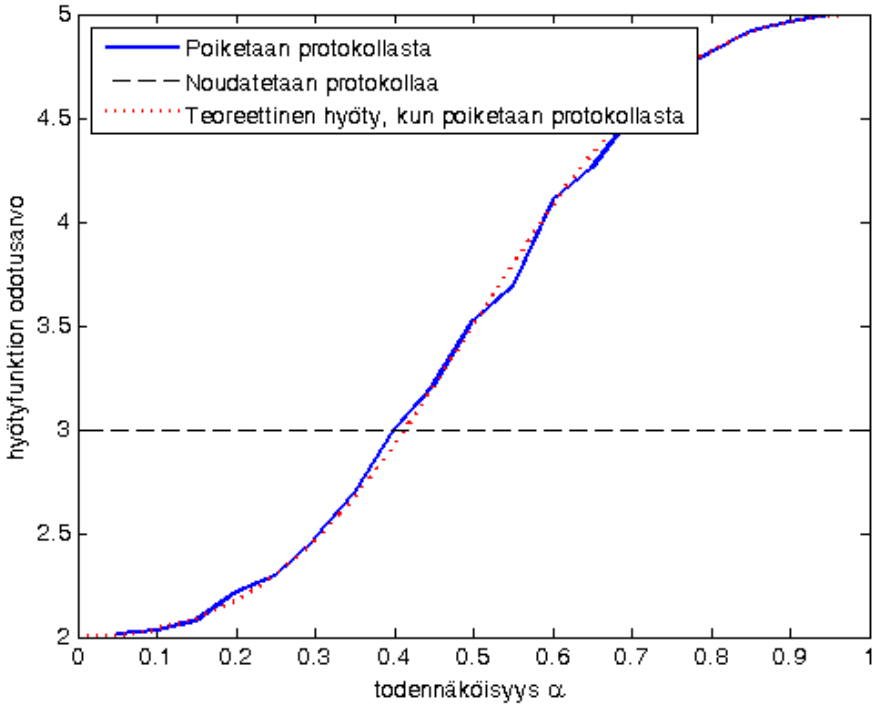
Voimme tarkastella aiempia kierroksia $k-1$, $k-2$ ja niin edelleen samaan tapaan kuin tarkastelimme rationaalisten osapuolien toimintaa viimeisellä kierroksella k. Näin päädymme lopulta lopputulokseen, ettei yksikään rationaalinen osapuoli protokollassa lähetä koko protokollan aikana yhtään ainutta viestiä. Samaan tapaan kuin deterministisen salaisuuden jakamisen suhteen, voimme myös päätellä, että tämä strategia olla noudattamatta protokollaa on itse asiassa koalition kestävä Nashin tasapaino. Tästä voimme johtaa vastaavan johtopäätöksen kuin deterministisen salaisuuden jakamisenkin suhteen, ettei ole olemassa sellaista protokollaa, joka päättyy äärellisessä ajassa ja jota rationaalinen osapuoli noudattaisi.

6 Tulokset

Tutkitaan kappaleessa 4 esitettyä kolmen osapuolen satunnaistettua protokollaa salaisuuden jakamiseen simuloimalla sitä. Näytämme simuloimalla, että protokollan noudattaminen on tosiaan koalition kestävä Nashin tasapaino, eikä rationaalinen pelaaja tästä täten poikkea. Käytetään simuloimiseen numeeriseen laskentaan tarkoitettua Matlab-ohjelmistoa.

Voidaksemme simuloida protokollan toimintaa ja eri pelaajille koituvia hyötyjä, meidän täytyy valita pelaajille sopiva hyötyfunktio. Kappaleen 4 analyysissä oletimme, että hyötyfunktio noudattaa epäyhtälöitä (4). Valitaan pelaajille 1, 2 ja 3 hyötyfunktiot, jotka noudattaa näitä epäyhtälöitä. Valitaan hyötyfunktioksi funktio (9), missä $\text{info}_i(\mathbf{s})$ saa arvon 1, jos pelaaja i pystyy protokollan päättyessä selvittämään alkuperäisen salaisuuden ja muulloin funktio saa arvon 0. Nyt hyötyfunktio saa pienimmän mahdollisen arvon 0, jos kaikki muut paitsi pelaaja i saa alkuperäisen salaisuuden selville. Paras mahdollinen hyöty 5 saavutetaan jos pelkästään pelaaja i saa salaisuuden selville. Mikäli kaikki saavat salaisuuden selville on hyötyfunktion arvo $u_i = 3$, ja jos kukaan ei saa salaisuutta selville hyötyfunktion arvo on $u_i = 2$.

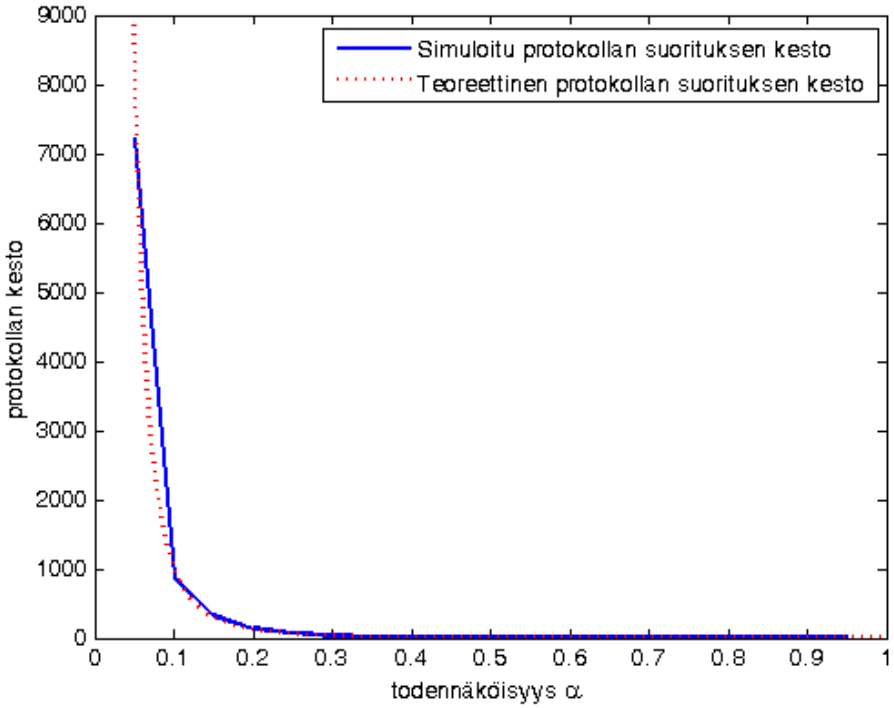
$$u_i(\mathbf{s}) = 2 + 3\text{info}_i(\mathbf{s}) - \sum_{j \in \{1,2,3\} \setminus i} \text{info}_j(\mathbf{s}) \tag{9}$$



Kuva 3: Hyötyfunktion odotusarvo kun jätetään osuus salaisuudesta jakamatta protkollan kohdassa 9.

Protokollaa varten täytyy vielä määrittää protokollaan parametri α. Parametri α kuvastaa todennäköisyyttä, jolla pelaaja arpoo itsellensä satunnaisluvun arvoksi 1, ja täten vaikuttaa suoraan siihen, kuinka usein pelaajien tulisi protokollan mukaan jakaa muille oma osa-salaisuutensa. Aiemmin johdimme pelaajan hyötyfunktion ja parametrin α välistä suhdetta kuvaavan epäyhtälön (7), jonka tulee toteutua, jotta rationaalinen pelaaja ei poikkea protokollasta. Tutkitaan Monte Carlo -simuloinnilla, millä parametrin α arvoilla tämä epäyhtälö pätee. Kuvassa 3 on kuvattu pelaajan hyötyfunktion odotusarvon kehittymistä kun pelaaja poikkeaa protokollasta olemalla jakamatta omaa osa-salaisuuttaan ja parametrin α arvoa muutetaan, sekä verrattu tätä pelaajan hyötyfunktion odotusarvoon, kun pelaaja noudattaa protokollaa.

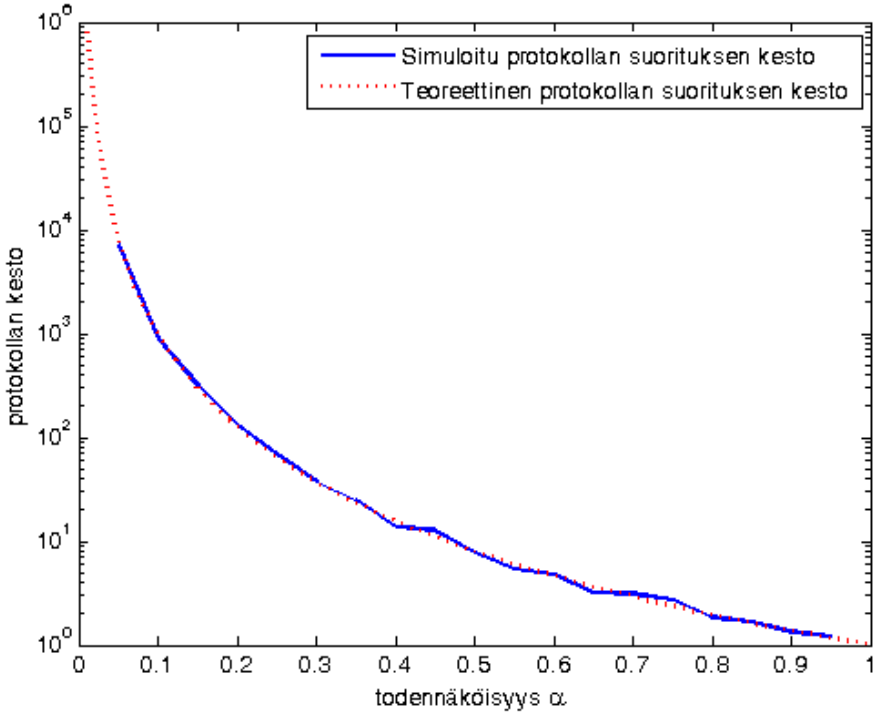
Tarkastelemalla kuvaa 3 näemme, kuinka pelaajan hyötyfunktion odotusarvo tämän poiketessa protokollasta on parametrin α suhteen aidosti kasvava. Tämä on järkevää, sillä hyvin pienillä todennäköisyyksillä α, on hyvin epätodennäköistä, että molemmat muut pelaajat arpoisivat satunnaisluvuikseen $c = 1$. Se, että molemmat muut pelaajat arpovat satunnaisluvun $c = 1$ on kriteeri sille, että protokollasta poikkeava pelaaja saa selville salaisuuden. Tämä johtuu siitä, että vain silloin muut pelaajat jakavat protokollasta poikkeavalle pelaajalle omat osa-salaisuutensa ennen kuin huomaavat, että pelaaja poikkeaa protokollasta eikä jaa omaa osa-salaisuuttaan vaikka tämän pitäisi.



Kuva 4: Protokollan kesto eri parametri α arvoilla.

Kun todennäköisyys α lähenee nollaa, protokollasta poikkeavan pelaajan hyötyfunktion odotusarvo lähenee arvoa, jonka pelaajan hyötyfunktio saa, kun kukaan pelaajista ei saa salaisuutta selville. Toisaalta, mitä suuremmaksi todennäköisyys

α kasvaa, sitä todennäköisempää on, että molemmat muut pelaajat arpovat satunnaisluvukseen $c = 1$ ja jakavat omat osa-salaisuutensa protokollasta poikkeavalle pelaajalle. Tästä seuraa se, että hyötyfunktio lähenee maksimia, eli hyötyä kun vain protokollasta poikkeava saa salaisuuden selville. Kuvasta voidaan silmämääräisesti arvioida, että jotta rationaalinen pelaaja ei poikkeaisi protokollasta, parametrin α arvon tulee olla pienempi kuin 0.4. Jos todennäköisyyttä α lasketaan tästäkin pienemmäksi protokollasta poikkeamisesta saadaan entistä kannattamattomampaa.



Kuva 5: Protokollan kesto eri parametri α arvoilla.

Mielivaltaisen pieneksi emme kuitenkaan voi todennäköisyyttä α asettaa, koska α:n lähestyessä nollaa protokollan kesto kasvaa rajusti. Mikäli kaikki osapuolet noudattavat protokollaa, protokolla päättyy kun kaikki osapuolet arpovat satunnaisluvukseen $c = 1$. Koska jokainen arpoo satunnaislukunsa toisistaan riippumattomasti, ja todennäköisyys että yhden pelaajan satunnaisluku saa arvon 1 on α, todennäköisyys että jokainen kolmesta arvotusta satunnaisluvusta saa arvon 1 samanaikaisesti on α^3. Protokollan päättymisajankohta noudattaa siis eksponenttijakaumaa, parametrilla $\lambda = \alpha^3$ ja täten protokollan päättymiseen tarvitaan keskimäärin $1/\alpha^3$ kierrosta. Kuvissa 4 ja 5 on kuvattu protokollan päättymiseen tarvittavien kierrosten lukumäärät kun parametria α muutetaan. Kuvassa 5 protokollan kesto on kuvattu logaritmisella asteikolla.

Kuvista 4 ja 5 voimme päätellä, että α kannattaa asettaa mahdollisimman suureksi, mikäli tahdomme protokollamme toimivan sujuvasti. Toisaalta parametrin α tulee olla riittävän pieni, ettei protokollasta poikkeamisesta tule kannattavaa. Valitaan lopulta α:n arvoksi 0.3. Tällä parametrin arvolla protokollan noudattamisen

pitäisi olla selvästi siitä poikkeamista kannattavampaa, mutta toisaalta protokolla ei vaadi liikaa aikaa päättyäkseen.

Määritetään kaikkien kolmen osapuolen hyötyfunktioiden odotusarvot erilaisissa peliskenaarioissa Monte Carlo -menetelmällä. Pelaajilla on kolme eri toimintavaihtoehtoa. Joko pelaaja noudattaa protokollaa (vaihtoehto 1), poikkeaa protokollasta eikä ikinä jaa muille omaa osa-salaisuuttaan (vaihtoehto 2) tai poikkeaa protokollasta ja aina jakaa oman osa-salaisuutensa muille (vaihtoehto 3). Monte Carlo -simulointien tulokset on nähtävillä taulukossa 3. Monte Carlo -simulaatioissa hyötyfunktioiden odotusarvot määritettiin toistamalla protokolla 100000 kertaa. Parametrin α arvo simuloinneissa oli 0.3.

Taulukko 3: Pelaajien hyötyfunktioiden odotusarvot

		$\mathbf{C_1}$	
	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$
$\mathbf{A_1}$	$3, 3, 3$	$1.8, 2.5, 1.8$	$3, 1.2, 3$
$\mathbf{A_2}$	$2.5, 1.8, 1.8$	$2, 2, 2$	$5, 1, 1$
$\mathbf{A_3}$	$1.2, 3, 3$	$1, 5, 1$	$1.3, 1.3, 4.7$

		$\mathbf{C_2}$	
	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$
$\mathbf{A_1}$	$1.8, 1.8, 2.5$	$2, 2, 2$	$1, 1, 5$
$\mathbf{A_2}$	$2, 2, 2$	$2, 2, 2$	$2, 2, 2$
$\mathbf{A_3}$	$1, 1, 5$	$2, 2, 2$	$1, 1, 5$

		$\mathbf{C_3}$	
	$\mathbf{B_1}$	$\mathbf{B_2}$	$\mathbf{B_3}$
$\mathbf{A_1}$	$3, 3, 1.2$	$1, 5, 1$	$4.7, 1.3, 1.3$
$\mathbf{A_2}$	$5, 1, 1$	$2, 2, 2$	$5, 1, 1$
$\mathbf{A_3}$	$1.3, 4.7, 1.3$	$1, 5, 1$	$3, 3, 3$

Tarkastelemalla taulukkoa 3 huomataan, että peliskenaario (A_1, B_1, C_1), eli skenaario jossa kaikki pelaajat noudattavat protokollaa on Nashin tasapaino. Tarkemmalla tarkastelulla voidaan huomata, että kyseinen peliskenaario on myös koalition kestävä Nashin tasapaino. Huomioitavaa on myös, että peliskenaariot, joissa vähintään kaksi osapuolta poikkeaa tasapainosta olemalla jakamatta muille omaa osa-salaisuuttaan ovat myös Nashin tasapainoja.

7 Yhteenveto

Työssä tutustuttiin aluksi pinnallisesti tietojenkäsittelytieteeseen, sekä sen erääseen tutkimuskohteeseen, protokollasuunnitteluun. Lukijalle perusteltiin peliteorian soveltamisen mielekkyys alalla. Seuraavaksi selvitettiin käyttötarkoitukseen sopiva Nashin tasapainon variaatio. Perinteinen Nashin tasapaino todettiin turhan löyhäksi, kun tarkastelukohteena on tietokoneverkko, jossa useampi osapuoli voi tehdä yhteistyötä jonkin tavoitteen saavuttamiseksi. Toisaalta vahva Nashin tasapaino rajaa turhan suuren osan mielenkiintoisista tasapainoista pois. Todettiin, että koalition kestävä Nashin tasapaino on sopiva kompromissi perinteisen Nashin tasapainon ja vahvan Nashin tasapainon välissä ja sopii sovellettavaksi protokollien hyvyyden tutkimiseen.

Työssä todettiin, ettei ole mahdollista suunnitella sellaista protokollaa salaisuuden jakamiseen tai ylipäänsä monitaholaskentaan, joka päättyy äärellisen monen kierroksen jälkeen ja jota rationaalinen osapuoli noudattaisi. Mikäli on tiedossa, että protokolla päättyy tietyn kierroksen jälkeen, rationaalinen pelaaja ei missään vaiheessa protokollan suoritusta jaa lainkaan informaatiota muille osapuolille. Kuitenkin, mikäli protokollan kesto muutetaan satunnaiseksi, voidaan osapuolia kannustaa osallistumaan tiedonvaihtoon.

Aiemmasta kirjallisuudesta selvitettiin jo olemassa olevia satunnaistettuja protokollia. Näitä analysoituamme tulimme tulokseen, että näissä protokollan noudattaminen on koalition kestävä Nashin tasapaino, kunhan osapuolten hyötyfunktiot noudattavat tehtyjä oletuksia (4). Analyysin paikkansapitävyys tarkistettiin simuloimalla protokollan toimintaa. Simuloinnin tulokset vastasivat teoreettisen analyysin tuloksia. Kirjallisuudesta selvittämämme protokolla kolmen osapuolen salaisuuden jakamiseen on siis sellainen, että rationaalinen pelaaja ei poikkea siitä, sillä protokollan noudattaminen on koalition kestävä Nashin tasapaino.

Tässä työssä käsiteltiin pitkälti vain salaisuuden jakamiseen liittyviä protokollia. Salaisuuden jakaminen on vain yksi tietty ongelma, johon protokollasuunnittelu pyrkii löytämään ratkaisuja. Peliteoriaa voisi jatkotutkimuksissa soveltaa laajemmalti muihinkin vastaaviin ongelmiin. Lisäksi käsittelimme vain yksinkertaista kolmen osapuolen asetelmaa salaisuuden jakamisessa. Tässä työssä selvitettyä kolmen osapuolen salaisuuden jakamiseen koalition kestävän Nashin tasapainon tarjoavan protokollan voisi jatkotutkimuksissa laajentaa useamman osapuolen salaisuuden jakamiseen. Myös salaisuuden selvittämiseen tarvittavien osa-salaisuuksien määrää voisi varioida.

Viitteet

[1] Ittai Abraham, Danny Dolev, Rica Gonen, and Joe Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In *Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, pages 53–62. ACM, 2006.

[2] E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber. Some constraints and tradeoffs in the design of network communications. *SIGOPS Oper. Syst. Rev.*, 9(5):67–74, November 1975.

[3] B Douglas Bernheim, Bezalel Peleg, and Michael D Whinston. Coalition-proof nash equilibria i. concepts. *Journal of Economic Theory*, 42(1):1–12, 1987.

[4] J.N. Gray. Notes on data base operating systems. In R. Bayer, R.M. Graham, and G. Seegmüller, editors, *Operating Systems*, volume 60 of *Lecture Notes in Computer Science*, pages 393–481. Springer Berlin Heidelberg, 1978.

[5] Joseph Halpern and Vanessa Teague. Rational secret sharing and multiparty computation. In *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, pages 623–632. ACM, 2004.

[6] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Trans. Program. Lang. Syst.*, 4(3):382–401, July 1982.

[7] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *Journal of the ACM (JACM)*, 27(2):228–234, 1980.

[8] A. Rubinstein. Finite automata play the repeated prisoner's dilemma. *Journal of Economic Theory*, 1986.

[9] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[10] Yoav Shoham and Moshe Tennenholtz. Non-cooperative computation: Boolean functions with correctness and exclusivity. *Theoretical Computer Science*, 343(1):97–113, 2005.

[11] Andrew C Yao. Protocols for secure computations. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 160–164. IEEE, 1982.