Kvanttikommunikaatioverkkojen mallinnus satunnais- sekä skaalavapaissa verkkomalleissa

Pro Gradu
Turun yliopisto
Fysiikka
2025
LuK Helmi Pajamäki
Tarkastajat:
Dos. Johannes Nokkala
Prof. Jyrki Piilo

TURUN YLIOPISTO
Fysiikan laitos

Pajamäki, Helmi Kvanttikommunikaatioverkkojen mallinnus satunnais- sekä skaalavapaissa verkkomalleissa

Pro Gradu, 83 s., 3 liites.
Fysiikka
Heinäkuu 2025

Kvanttikommunikaatioverkot on suunniteltu mahdollistamaan informaation siirto käyttäjien välillä kvanttitilojen välityksellä. Yksi niiden keskeisimmistä sovelluksista on kvanttikryptografia ja kvantti-avainten jakamiseen pystyvät (eng. *Quantum Key Distribution*, QKD) verkot, joita hyödynnetään erityisesti kryptografisten avainten turvalliseen jakamiseen ja niiden kautta viestien salaamiseen. Tämän vuoksi kvanttikommunikaatioverkot muodostavat aktiivisen ja nopeasti kehittyvän tutkimuskohteen. Kirjallisuudessa on esitetty useita mallinnusmenetelmiä kvanttikommunikaatioverkoille, joista tärkeitä ovat Waxman-malli sekä Barabási-Albert -malli, joka edustaa skaalavapaita verkkoja. Näissä malleissa noodit sijoitetaan verkkoon satunnaisesti, mutta verkkojen rakenteet eroavat: skaalavapaissa verkoissa linkit muodostetaan dynaamisesti suosien korkean asteen linkkejä, kun taas Waxman-mallissa linkit generoidaan staattisesti, sille ominaisen todennäköisyysjakauman perusteella.

Reaalimaailman verkkojen, kuten sähköverkkojen, mallinnuksessa noodien maantieteelliset sijainnit ovat keskeisiä, sillä tällaisissa verkoissa noodit keskittyvät usein tiettyihin keskuksiin, jolloin nooditiheys on epähomogeenisesti jakautunut. Tässä opinnäytetyössä analysoitiin ja vertailtiin sekä olemassa olevia (Waxman- ja Barabási–Albert) verkkomalleja että opinnäytetyötä varten kehitettyä uutta mallia. Uudessa mallissa noodit lisätään verkkoon iteratiivisesti siten, että uusien noodien koordinaatit painottuvat lähelle jo olemassa olevia noodikeskittymiä. Lisäksi linkkien muodostumiseen vaikuttaa noodien välinen etäisyys.

Työn teoreettisessa osuudessa tarkasteltiin kvanttikommunikaatioverkkojen perusteita sekä niiden mallinnusperiaatteita. Käytännön osiossa suoritettiin simulaatioita Python-kielellä eri verkkomalleille. Verkkojen ominaisuuksia visualisoitiin ja analysoitiin sekä verrattiin toisiinsa. Kehitetyn mallin osalta havaittiin parametrien vaikutuksesta muodostuvan alueita, joilla ei ole lainkaan noodeja, sekä useita selkeitä keskittymiä. Tämä tekee mallista varteen otettavan vaihtoehdon olemassa oleville verkkomalleille.

Asiasanat: QKD, Waxman-malli, skaalavapaa malli, kvanttikommunikaatioverkko

Sisällys

Johdanto

Ensimmäiset kaupalliset kommunikaatioverkot olivat puhelinverkkoja, joissa operaattorit yhdistivät tulevat puhelut vastaanottajalle. Tunnetuin kommunikaatioverkko Internet on hyvä esimerkki siitä, miten paljon yhteiskunta hyödyntää kommunikaatioverkkoja [5].

Klassiset salausalgoritmit perustuvat suurten lukujen tekijöihin jakamiseen[30], mikä on laskennallisesti raskas prosessi ja yleisesti klassisilla tietokoneilla murtamaton [30]. Kvanttitietokoneilla sekä -algoritmeilla klassiset salausalgoritmit ovat kuitenkin murrettavissa, kvanttitietokoneiden tuoman laskutehon kasvun ansiosta[30]. Kvanttikryptografian salausalgoritmien toiminta perustuu kvanttimekaniikan ominaisuuksiin, kuten lomittumiseen sekä kloonauksenkieltolauseeseen, mikä tekee niistä kvanttitietokoneiden kestäviä. Kryptografinen vaatimus on, että lähetetty viesti ei ole saavutettavissa muille kuin lähettäjälle ja vastaanottajalle, vaikka käytetty kanava olisi epäluotettava [30, 40].

Kvanttikommunikaatioverkkojen toiminta perustuu kvanttimekaniikan malleihin ja ne hyödyntävät kommunikaatiossa mm. kubitteja sekä tilojen lomittumista [16]. Niiden tärkeimpiä sovelluksia ja sen vuoksi tutkituimpia aloja ovat QKD-verkot, jotka jakavat kryptografisia avaimia sekä lomittumista hyödyntäen fotoneita informaation vaihtoon [20, 25]. QKD-verkkojen tavoitteena on välittää informaatiota lähettäjän ja vastaanottajan (yleisesti kirjallisuudessa Alice ja Bob) välillä ilman, että ulkopuolinen taho (Eve) voi saada informaatiota Alicen ja Bobin jakamista kubiteista muuttamatta niiden tilaa. Alice ja Bob voivat uhrata osan jakamistaan kubiteista ja verrata saamiaan tuloksia keskenään varmistaakseen ettei avain ole muuttunut salakuuntelun tai hälyn seurauksena [24]. Kvanttikommunikaatioverkot koostuvat noodeista, joissa kubitteja varastoidaan ja joiden välillä kommunikaatio tapahtuu kvanttikanavia (eng. *quantum channel*) pitkin [9]. Alicen ja Bobin välillä on kaksi informaatiokanavaa: kvanttikanava kubittien jakamiseen, sekä klassinen

informaatiokanava, jota Alice ja Bob voivat käyttää avainten vertailuun [11].

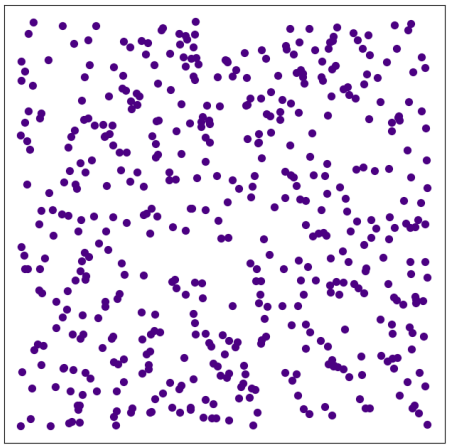
Kommunikaation pullonkaulana kaukaisten noodien välillä toimii kanavan virhetaajuus, joka skaalautuu kanavan pituuden mukaan. Kvanttikommunikaatiossa virheen mahdollisuus mittauksissa skaalautuu eksponentiaalisesti kanavan pituuteen kommunikaation tapahtuessa hälyisten kanavien kautta. Kvanttikommunikaatioverkkojen suurimpia ongelmia ovatkin hälystä aiheutuva tarkkuuden (eng. *fidelity*) pieneneminen sekä fotonin absorboitumisen muuttuminen todennäköisemmäksi etäisyyden kasvaessa. Tällöin kubitti ei pääse ikinä vastaanottajalle. Tämä rajoittaa etäisyyttä, jolle informaatio voidaan välittää. Näiden ongelmien ratkaisuksi on esitetty mm. kvanttitoistimia [9]. Ennen viestien lähettämistä Alice ja Bob ovat jakaneet EPR-parin, jonka tilat ovat lomittuneet keskenään ja jota voidaan käyttää kvanttitoistimissa kubittien jakamiseen. Myös useammat reitit verkossa lähde- ja vastaanottajanoodin välillä helpottavat kommunikaatiota ja tekevät siitä turvatumpaa.

Kvanttikommunikaatioverkkojen teoreettinen huipputaso saadaan summaamalla lähde- ja vastaanottajanoodien välisen leikkauksen kapasiteetit. Leikkaus koostuu noodiparin väillä olevien polkujen linkeistä, joilla kapasiteetti on pienin ja jotka tällöin toimivat pullonkaulana kommunikaatiolle. Näiden kapasiteettien teoreettinen yläraja on PLOB-raja, joka riippuu etäisyydestä [28]. Tämän päivän huipputaso läpäisevyydelle optisessa kuidussa on $10^{-0,02dB/km*d}$ välimatkalle d. Rakennettuja kvanttiverkkoja sijaitsee esim. Bostonissa (DARPA)[15], Tokiossa[37], Wienissä (SECOQC) [29] ja Hefeissä[12] sekä Beijing-Shanghaissa kvanttirunkoverkko, joka hyödyntää satelliittilinkkejä maassa olevien linkkien yhdistämiseen, saavuttaen jopa 2000 km välimatkaan informaation jakamiseen, kun taas optisiin kuituihin nojaavien verkostojen, joihin suurin osa rakennetuista kvanttiverkoista kuuluu, suurin saavutettavissa oleva välimatka on noin 100 km [25, 31].

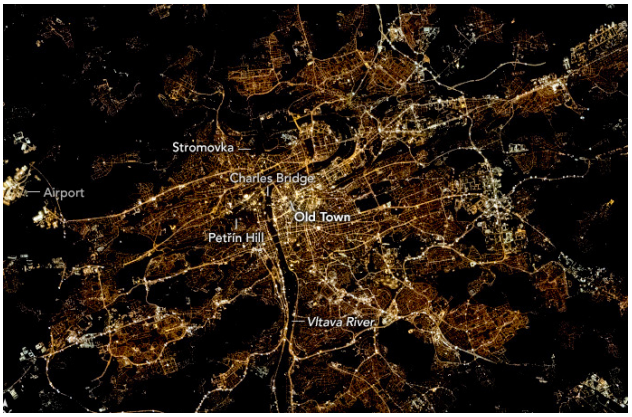
Verkkojen paremmuutta voidaan verrata vertaamalla esim. niiden leikkauksia eli

montako reittiä on päätenoodien välillä, linkkien läpäisevyyksiä, erityisesti ketjujen minimiläpäisevyyksiä sekä verkkojen kapasiteetteja, jotka kertovat kuinka paljon kubitteja verkko pystyy siirtämään päätenoodilta toiselle rajatussa ajassa. Myös niiden alttiutta virheille sekä maksimikommunikaatioetäisyyttä voidaan verrata keskenään [9][16]. Kirjallisuudessa tärkeitä verkkomalleja kvanttikommunikaatioverkkojen mallintamiseen ja käsittelyyn ovat Waxman- sekä skaalavapaa malli, joista tunnetuin on Barabási-Albert -malli. Waxman-verkkomallit ovat satunnaisverkkomalleja, joissa verkon noodit sijoitetaan satunnaisesti alueelle ja niiden välille luodaan linkit todennäköisyydellä, joka riippuu noodien etäisyydestä. Waxman-mallin verkoissa astejakauma noudattaa Poisson-jakaumaa [23]. Alunperin Erdös-Renyi -mallin verkkoja käytettiin kaikkien, myös reaalimaailman verkkojen, kuvaamiseen sillä niiden asteiden uskottiin noudattavan satunnaisverkkomallien mukaisesti Poisson jakaumaa. Kuitenkin mm. Internetin astejakaumaa tutkittaessa huomataan, että sen astejakauma noudattaa potenssilakia. Tämä pätee myös useille muille realimaailman verkoille. Ensimmäisenä mallin potenssilakia noudattaville verkoille loi Price 70-luvulla ja nykyään paljon tutkitun mallin loivat Albert-László Barabási ja Reka Albert 1990-luvulla.[23] He ottivat käyttöön termin skaalavapaa verkko kuvaamaan verkkoja, jotka ilmentävät potenssilain mukaista astejakaumaa [4]. Malli on nimetty skaalavapaaksi, koska sen asteiden arvot eivät noudata tiettyä skaalaa, vaan ne voivat saada hyvin paljon suuruusluokaltaan eriäviä arvoja [22]. Skaalavapaat verkot rakentuvat dynaamisesti noodi kerrallaan. Lisätty noodi yhdistetään muihin verkon noodeihin linkittämällä ne m muuhun noodiin, jossa todennäköisyys linkin muodostumiselle riippuu olemassa olevan noodin asteluvusta (eng. *degree*). Lisätyille noodeille määritetään satunnaiset koordinaatit, jolloin verkkojen noodien asettelu muistuttaa kuvassa 1a olevaa tasajakautumaa.[23]

Kuitenkin useat reaalimaailman verkot, esimerkiksi sähköverkot, jotka noudattavat astejakaumissaan potenssilakia, eivät ole tasajakautuneita koordinaattiensa



(a) Tasajakautuneet noodit



(b) Kuva: NASA's Earth Observatory[21]. Yöllinen kuva Prahasta, astronautin kuvaamana.

Kuva 1: Tasajakautuneita noodeja (waxman- ja skaalavapaa malli) sekä Prahan valojen muodostama verkosto yöllä kuvattuna. *(https://earthobservatory.nasa.gov/images/151557/prague-at-night)*

suhteen. Niissä voidaan havaita suurempia ryhmittymiä, kuten kuvasta 1b nähdään. Kuva on NASA's Earth Observatory :n omistama yöllinen kuva Prahasta, astronautin kuvaamana. Siinä voidaan nähdä selkeitä kirkkaampia keskittymiä kaupungin keskustassa, sekä pienempiä ryhmittymiä asuinalueilla. Tässä opinnäytetyössä on tarkoituksena tutustua Waxman- ja skaalavapaisiin verkkomalleihin, niiden laajan suosion vuoksi, sekä verrata niiden ominaisuuksia työtä varten kehitettyyn satunnaisverkkomalliin. Tätä mallia kehitettäessä pyrittiin potenssilain mukaiseen astejakaumaan, jotta se vastaisi reaalimaailman verkkoja sekä noodien sijoittumiseen siten että verkkoon syntyy selkeitä keskittymiä sekä täysin noodivapaita alueita, jotta verkon rakenne vastaisi kuvan 1b rakennetta. Tutkielman rakenne on seuraava: teorialuvussa käsitellään kvanttimekaniikkaa ja verkkoteoriaa pääpiirteittäin, jotta niiden avulla voidaan syventyä kvanttikommunikaatioverkkoihin ja erityisesti Waxman- ja skaalavapaseen malliin. Luvussa kaksi käsitellään simulaatioiden oletamuksia ja vakioita sekä kuvaillaan mallien rakentumista, sekä teoriassa käsitellyille, että tutkielmassa kehitetylle mallille. Luvussa kolme esitetään saadut tulokset ja

verrataan malleja toisiinsa, jonka jälkeen tutkielman päätelmät kootaan viimeisessä luvussa.

1 Teoria

Tässä kappaleessa käsitellään kvanttikommunikaatioverkkojen kannalta olennaista teoreettista taustatietoa. Ensin käsitellään kvanttimekaniikkaa sekä verkkoteoriaa olennaisilta osin, jonka jälkeen perehdytään kvanttikommunikaatioverkkoihin.

1.1 Kvanttimekaniikka

Kvanttimekaniikka on yksi modernin fysiikan kulmakiviä, johon pohjaavat kvantti-informatiikan lisäksi mm. kvanttioptiikka, kvanttikenttäteoria sekä kvanttikemia. Tässä kappaleessa kvanttimekaniikkaa lähestytään kvantti-informatiikan kannalta tärkeiden ominaisuuksien kautta, kuten mm. lomittumisen ja kubittien, sekä niiden seurauksena ilmenevien ominaisuuksien, kuten kloonauksen kieltolauseen, kautta. Kappaleen matemaattinen käsittely ja teoria vastaa kirjojen [18] ja [38] teoriaa.

1.1.1 Kubitti

Klassisesti informaation välityksessä käytetään hyväksi bittejä, jotka voivat saada joko arvon 0 tai 1. Informaation välittäjinä toimivat tilat, jotka ovat myös nimetty arvoin 0 ja 1. Sen sijaan kvanttimekaanisten systeemien tilaa kuvataan kubiteilla, jotka voivat olla edeltävien tilojen lisäksi kahden tilan superpositiossa. Näitä tiloja voidaan kuvata (Diracin notaatiota käyttäen) aaltofunktiolla ψ

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1}$$

jossa α,$\beta \in \mathbb{C}$. Kertoimille α ja β pätee $|\alpha|^2+|\beta|^2 = 1$. Jos kubitilla halutaan kuvata klassista tilaa, voidaan toinen kertoimista asettaa nollaksi, mutta muulloin kubitin tila on näiden kahden superpositio.

1.1.2 Lomittuminen

Kubitteja voidaan yhdistää myös useamman kubitin systeemeiksi, jotka voivat olla joko lomittuneita (eng. *entangled*) tai separoituvia. Hilbertin avaruus $\mathcal{H}$ koko systeemille saadaan tensoritulolla sen alisysteemeistä $\mathcal{H}_l$, $\mathcal{H} = \otimes_{l=1}^{n} \mathcal{H}_l$. Superposition seurauksena, voidaan koko systeemin tila kirjoittaa muotoon:

$$|\psi\rangle = \Sigma_{l_n} c_{l_n} |\boldsymbol{i}_n\rangle, \tag{2}$$

jossa $\mathbf{i}_n = i_1,...i_n$ on multi-indeksi[1] ja

$$|\boldsymbol{i}_n\rangle = |i_1\rangle \otimes ,,, \otimes |i_n\rangle$$

[17].

Tilan kuvaamiseen voidaan käyttää esimerkiksi elektronin spiniä, koska sillä on kaksi mahdollista arvoa (ylös tai alas). Kuvataan seuraavaksi esimerkin avulla lomittumista kahden elektronin systeemissä. Merkitään elektronien tiloja seuraavasti:

$$|\psi\rangle_1 = a\,|\uparrow\rangle_1 + b\,|\downarrow\rangle_1 \tag{3}$$

$$|\phi\rangle_2 = c\,|\uparrow\rangle_2 + d\,|\downarrow\rangle_2, \tag{4}$$

jossa kertoimet a,b,c ja d on normalisoitu eli

$$|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1, \tag{5}$$

ja jossa alaindeksit merkitsevät kyseessä olevaa elektronia. Jos siis mitataan elektronien spiniä z-suunnassa, on neljä mahdollista mittaustulosta:

$$|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle \text{ ja } |\downarrow\downarrow\rangle. \tag{6}$$

Pareissa ensimmäinen nuoli merkitsee ykköselektronin spiniä ja jälkimmäinen elektronin kaksi spiniä. Tällöin tilojen superpositio voidaan kirjoittaa

$$|\psi\rangle = \frac{1}{2}|\uparrow\uparrow\rangle + \frac{1}{2}|\uparrow\downarrow\rangle + \frac{1}{2}|\downarrow\uparrow\rangle + \frac{1}{2}|\downarrow\downarrow\rangle. \tag{7}$$

[1]Huomautuksena, että yleisesti tilaa ei voida kirjoittaa alisysteemien tilojen tensoritulona, $|\psi\rangle \neq |\psi_1\rangle \otimes ,,, \otimes |\psi_n\rangle$,

Koska elektronien tilat ovat toisistaan riippumattomia, ovat tilat kuten yllä oleva esimerkki separoituvia eikä elektronien välillä ole lomittumista. Separoituville tiloille voidaan määrittää kertoimien a, b, c ja d arvot ilman riippuvuutta muihin kertoimiin. Esimerkiksi tila:

$$|\psi\rangle = ac\,|\uparrow\uparrow\rangle + ad\,|\uparrow\downarrow\rangle + bc\,|\downarrow\uparrow\rangle + bd\,|\downarrow\downarrow\rangle \tag{8}$$

on mahdollista kirjoittaa kahden alitilan tulona

$$|\psi\rangle_1\,|\phi\rangle_2 = (a\,|\uparrow\rangle_1 + b\,|\downarrow\rangle_1) \times (c\,|\uparrow\rangle_2 + d\,|\downarrow\rangle_2). \tag{9}$$

Lomittuneille tiloille on mahdotonta löytää kertoimien arvoja, joilla olisi mahdollista kirjoittaa tila kahden muun tilan tuloksi. Esimerkiksi tilalle

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\,|\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}\,|\downarrow\downarrow\rangle\,, \tag{10}$$

on mahdotonta löytää kertoimien a, b, c ja d arvoja samoin kuin aiemmin olleelle separoituvalle tilalle. Toisin sanoen tilan kaksi elektronia ovat lomittuneet, sillä niille ei voida löytää erillisiä tilavektoreita[2].

Käytännössä siis, jos Alica ja Bob jakaisivat kaavan (11) mukaisen lomittuneen tilan, on molemmilla 50% todennäköisyys kumpaankin mittaustulokseen, spin ylös sekä spin alas. Kuitenkin jos Alice mittaa oman elektroninsa tilan ja saa tulokseksi $\uparrow$, tietää hän myös Bobin elektronin olevan samassa tilassa.

Bellin tilat

Yksi esimerkki lomittuneesta tilasta on niin kutsuttu EPR (Einstein-Podolsky-Rosen) pari tai toiselta nimeltään Bellin tila. EPR-pareilla viitataan Alicen ja Bobin tai viereisten noodien keskenään jakamaan joukkoon lomittuneita kubitti pareja,

[2]Toisin sanoen lomittuneille elektroneille ei voida löytää erillisiä puhtaita tiloja. Puhdas tila on kvanttitila, joka voidaan esittää kantavektoreiden summana: $|\psi\rangle = \sum_i c_i\,|i\rangle$, jossa c_i on vakio ja tila $|i\rangle$ on kantavektori.

jotka ovat maksimaalisen lomittuneessa tilassa, jolloin molemmat tilat ovat yhtä todennäköisiä. Nämä tilat muodostavat kannan neliulotteisessa Hilbertin avaruudessa [24]:

$$\begin{aligned} |\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\ |\Phi^-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \\ |\Psi^-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned} \tag{11}$$

Kloonauksen kieltolause

Eräs kvantti-informaation ja -laskennan kannalta olennainen teoria on kloonauksenkieltolause (eng. *no-cloning theorem*). Se vastaa kysymykseen, onko kvanttitilojen kloonaus mahdollista, johon vastaus nimestäkin päätellen on ei. Kloonauksen kieltolause mahdollistaa QKD:n käytön salausavaimien jakamiseen. Tilojen kloonaamisen mahdottomuus on olennainen osa avainten jakamista ja mahdollistaa tiedon siitä onko joku ollut avainten jaon välissä ja vaikuttanut avaimina käytettävien kubittien tilaan.

Kuvitellaan kvanttikone, jolla on kaksi muistipaikkaa A ja B. Muistipaikkaan A on tallennettu tuntematon, mutta puhdas kvanttitila $|\psi\rangle$ ja se halutaan kopioida paikkaan B, joka on alkutilassa $|s\rangle$, joka oletetaan myös puhtaaksi. Kone on siis tilassa

$$|\psi\rangle \otimes |s\rangle$$

ja se halutaan saattaa jollain unitaarioperaatiolla tilaan, jossa molemmissa muistipaikoissa on sama tila:

$$|\psi\rangle \otimes |s\rangle \rightarrow U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle .$$

Tutkitaan seuraavaksi kahta kloonattavaa tilaa $|\psi\rangle$ ja $|\phi\rangle$. Molemmille voidaan kirjoittaa unitaarioperaatio:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\phi\rangle \otimes |s\rangle) = |\phi\rangle \otimes |\phi\rangle .$$

Ottamalla sisätulo näistä yhtälöistä saadaan:

$$\langle\psi| |\phi\rangle = (\langle\psi| |\phi\rangle)^2.$$

Yhtälölle $x = x^2$ on kuitenkin vain kaksi ratkaisua, x=0 tai x=1 eli joko molemmat tilat ovat samoja tai ne ovat ortogonaalisia keskenään. Tällöin kloonauskone pystyisi kopioimaan ainoastaan ortogonaalisia tiloja, eli yleinen kvanttikloonauskone on mahdoton [24].

1.1.3 Kvanttiteleportaatio

Lomittumisen erikoisin käyttö on ehkä kvanttiteleportaatio. Siinä yhden hiukkasen, joka on Alicella, tila siirretään Bobin hiukkaselle, ilman että kumpikaan saa informaatiota kyseisestä tilasta. Prosessissa siis siirretään kubitin tila toiselle, eikä hiukkanen itsessään vaihda paikkaa. Teoriassa Alice ja Bob voivat myös olla kuinka kaukana tahansa, ilman, että se vaikuttaa teleportaatioon.

LOCC

Kvantti-informaatiossa tietoa jaetaan kahden osapuolen välillä, johon voidaan hyödyntää mm. kvanttitoistimia. Ne käyttävät kvanttiteleportaatiota sekä lokaaleja mittauksia ja kvanttioperaatioita informaation jakamiseen. Tämän lisäksi osapuolten voidaan sallia kommunikoida klassisesti mitä tahansa klassista dataa, esimerkiksi jakamalla mittaustuloksiaan. Lokaalien mittausten sekä klassisen kommunikaation yhdistelmää kutsutaan LOCC:ksi, joka on lyhenne englanninkielisistä sanoista *local*

operations and classical communication. [13] Esimerkiksi kuvassa 5 esitetyssä lomittumisen tislauksessa hyödynnetään LOCC:a: ensin Alice ja Bob lokaalisti suorittavat CNOT operaatioita sekä mittauksia omiin kubitteihinsa, jonka jälkeen he klassisesti kommunikoivat mittaustuloksensa [24].

Kvantti-informaatiossa voidaan hyödyntää kvanttitoistimia informaation välittämiseen, mutta tämä asettaa vaatimukseksi aiemmin käsitellyn kloonaamisen kieltolauseen. Tällöin ei voida hyödyntää signaalin vahvistusta tai luoda kopioita tiloista, jolloin jokaista tuntemattoman kubitin jakamista voidaan yrittää vain kerran. Näiden rajoitusten seurauksena verkostojen kvanttikanavien tulisi olla hälyttömiä, luotettavia ja niiden tulisi pystyä viestimään yhtä laajalle kuin klassiset verkot, jotta kubitit voidaan saada noodilta toiselle luotettavasti. Kvanttiteleportaatiolla tämä voidaan saavuttaa. Verkoilla tämä tarkoittaa, että noodien välille tulee muodostaa jaettu lomittunut pari, joka voidaan kuluttaa siihen, että kubitti voidaan jakaa LOCC:a hyödyntäen. [2, 13, 25]

Kvanttiteleportaation havainnoimiseksi kuvitellaan, että Alice ja Bob ovat jakaneet lomittuneen EPR-parin keskenään siten että kummallakin on parin toinen kubitti. Alicella on hallussaan myös kubitti $|\psi\rangle$, jonka tilaa Alice ei tiedä. Tavoite on jakaa $|\psi\rangle$ Bobille klassista kommunikaatiota hyödyntäen. Tiivistettynä Alice vuorovaikuttaa oman EPR-parinsa jaettavan kubitin kanssa ja sen jälkeen mittaa kaksi hallussaan olevaa kubittia, saaden tulokseksi joko 00, 01, 10 tai 11. Hän jakaa informaation saamastaan tuloksesta Bobille ja tuloksesta riippuen Bob suorittaa jonkun neljästä operaatiosta omalle EPR-parilleen. Näin Bob saa alkuperäisen tilan $|\psi\rangle$, mutta Alicen ja Bobin jakama EPR-pari kuluu operaatiossa. Matemaattisesti jaettava tila voidaan esittää:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

jossa α ja β ovat tuntemattomia vakioita. Jos otetaan EPR-pareista esimerkiksi ylin

yhtälöistä 11, voidaan esittää alkutila muodossa:

$$\begin{aligned}|\psi_0\rangle &= |\psi\rangle\,|\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)].\end{aligned}$$

Alice vuorovaikuttaa oman puolensa EPR-paria jaettavan kubitin kanssa[3]

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)],$$

minkä jälkeen Alice saattaa ylemmän kubitin superpositioon[4]

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)],$$

joka voidaan uudelleen ryhmitellä:

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}[&|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) \\ &+ |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)].\end{aligned}$$

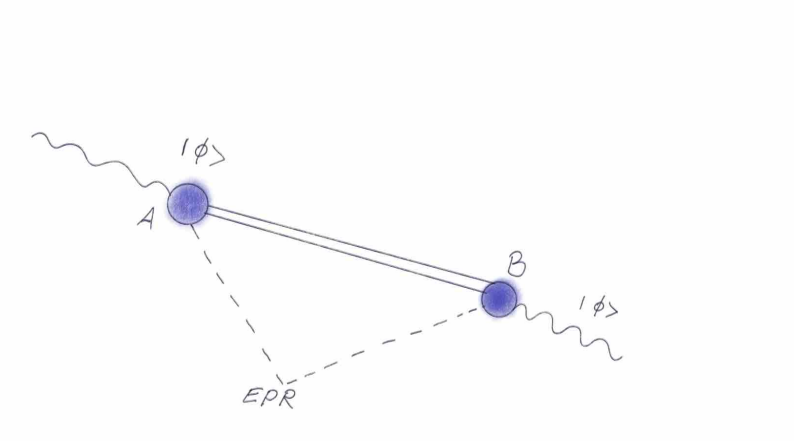
Tämä voidaan jakaa helposti termeihin, joista nähdään Alicen kubitin ja Bobin kubitin tilat, eli esimerkiksi jos Alice saa mittaustulokseksi tilan $|00\rangle$, on Bobin kubitti tilassa $\alpha\,|0\rangle + \beta\,|1\rangle$, joka on alkuperäisen jaettavan kubitin tila. [24]

Kuvassa 2 on esitetty kvanttiteleportaation ajatus yksinkertaisesti. Alice ja Bob jakavat EPR-parin keskenään ja Alice vuorovaikuttaa oman puolensa parista kvanttitilan $|\phi\rangle$ kanssa ja jakaa saamansa tuloksen klassisesti, joka on esitetty kahdella rinnakkaisella viivalla. Saadun tuloksen perusteella Bob suorittaa tietyn operaation omalle puolikkaalleen EPR-parista, joka tuottaa halutun kvanttitilan. Tämä kuitenkin kuluttaa Alicen ja Bobin aiemmin jakaman EPR-parin, eikä sitä voida käyttää uudelleen kvanttiteleportaatioon.

Lomittumisen jakaminen

[3]Kvanttipiirissä tämä tapahtuu "cnot-portin avulla.

[4]Tämä tapahtuu kvanttipiirissä Hadamard-portin avulla.



Kuva 2: Kvanttiteleportaatio: Alice (A) ja Bob (B) ovat aiemmin jakaneet keskenään EPR parin. Alice vuorovaikuttaa oman EPR parin puolikkaansa kvanttitilan $|\phi\rangle$ kanssa ja jakaa tuloksen klassista kommunikaatiota hyödyntäen Bobin kanssa. Bob suorittaa operaation omalle EPR parin osalleen saamansa tiedon mukaisesti ja saa tuloksena alkuperäisen kvanttitilan.

Kvanttikommunikaatiossa lomittumisen jakaminen on olennainen osa linkkien luomista kaukaisempien noodien välille. Se vähentää välinoodien tarvetta yhdistämällä noodit suoraan, mutta johtaa usein heikompaan puhtauteen noodien välillä.

Lomittumisen jakamisen (eng. *entanglement swapping*) havainnoimiseksi tutkitaan kahta kubittiparia. Ensimmäinen pari muodostuu kubiteista A ja B ja toisen parin muodostavat kubitit C ja D. Alisysteemien tilat voidaan kirjoittaa:

$$|\phi\rangle_{AB} = \sqrt{p_0}\,|00\rangle_{AB} + \sqrt{p_1}\,|11\rangle_{AB}\,,$$
$$|\phi\rangle_{CD} = \sqrt{p'_0}\,|00\rangle_{CD} + \sqrt{p'_1}\,|11\rangle_{CD}\,,$$

jossa p_i:t ovat tilojen todennäköisyyksiä. Tällöin kaikkien neljän kubitin tilaksi saa-

daan:

$$\begin{aligned}|\Phi\rangle &= |\phi\rangle_{AB}\,|\phi\rangle_{CD}\\ &= \sqrt{p_0 p_0'}\,|0000\rangle_{ABCD} + \sqrt{p_0 p_1'}\,|0011\rangle_{ABCD} + \sqrt{p_1 p_0'}\,|1100\rangle_{ABCD}\\ &+ \sqrt{p_1 p_1'}\,|1111\rangle_{ABCD}\,,\end{aligned}$$

joka voidaan uudelleen järjestellä siten, että kubitit A ja D sekä kubitit B ja C kirjoitetaan yhdessä:

$$\begin{aligned}|\Phi\rangle = \sqrt{p_0 p_0'}\,|00\rangle_{AD}\,|00\rangle_{BC} + \sqrt{p_0 p_1'}\,|01\rangle_{AD}\,|01\rangle_{BC} + \sqrt{p_1 p_0'}\,|10\rangle_{AD}\,|10\rangle_{BC}\\ + \sqrt{p_1 p_1'}\,|11\rangle_{AD}\,|11\rangle_{BC}\,.\end{aligned} \tag{12}$$

Jotta voidaan tehdä mittauksia kubitteihin BC, tarvitaan neljän tilan ortonormaalikanta. Tähän voidaan käyttää edellä mainittuja Bellin tiloja (11). Huomataan, että kubittien BC tilat voidaan kirjoittaa Bellin tilojen avulla, esimerkiksi $|00\rangle_{BC} = \frac{|\Phi^+\rangle_{BC} + |\Phi^-\rangle_{BC}}{\sqrt{2}}$. Nyt yhtälö (12) voidaan kirjoittaa uudelleen muotoon:

$$\begin{aligned}|\Phi\rangle = \sqrt{p_{\Phi^+}}\,|\varphi^+\rangle_{AD}\,|\Phi^+\rangle_{BC} + \sqrt{p_{\Phi^-}}\,|\varphi^-\rangle_{AD}\,|\Phi^-\rangle_{BC}\\ + \sqrt{p_{\Psi^+}}\,|\phi^+\rangle_{AD}\,|\Psi^+\rangle_{BC} + \sqrt{p_{\Psi^-}}\,|\phi^-\rangle_{AD}\,|\Psi^-\rangle_{BC}\,,\end{aligned} \tag{13}$$

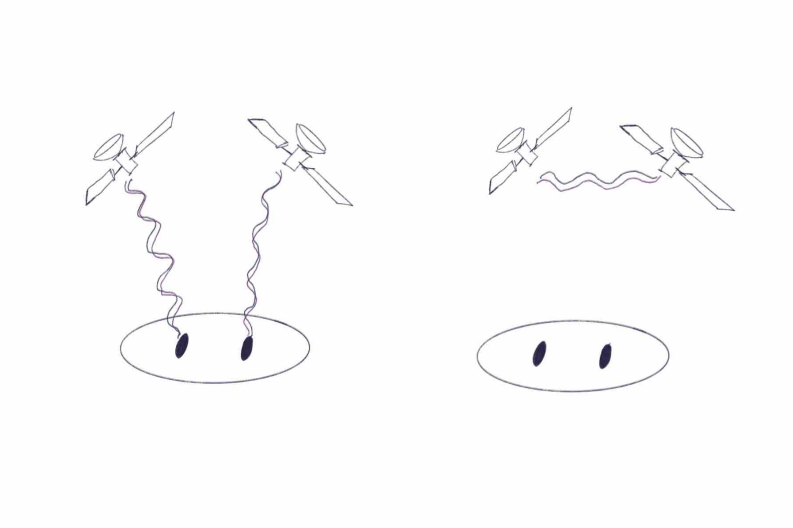
josta voidaan määrittää kubittien AD mahdolliset tulokset:

$$\begin{aligned}|\varphi^+\rangle_{AD} &= (\sqrt{p_0 p_0'}\,|0\rangle_A\,|0\rangle_D + \sqrt{p_1 p_1'}\,|1\rangle_A\,|1\rangle_D)/\sqrt{2p_{\Phi^+}}\\ |\varphi^-\rangle_{AD} &= (\sqrt{p_0 p_0'}\,|0\rangle_A\,|0\rangle_D - \sqrt{p_1 p_1'}\,|1\rangle_A\,|1\rangle_D)/\sqrt{2p_{\Phi^-}}\\ |\phi^+\rangle_{AD} &= (\sqrt{p_0 p_1'}\,|0\rangle_A\,|1\rangle_D + \sqrt{p_0' p_1}\,|1\rangle_A\,|0\rangle_D)/\sqrt{2p_{\Psi^+}}\\ |\phi^-\rangle_{AD} &= (\sqrt{p_0 p_1'}\,|0\rangle_A\,|1\rangle_D - \sqrt{p_0' p_1}\,|1\rangle_A\,|0\rangle_D)/\sqrt{2p_{\Psi^-}}\end{aligned} \tag{14}$$

ja jossa mahdolliset todennäköisyydet ovat:

$$\begin{aligned}p_{\Phi^+} &= p_{\Phi^-} = \frac{p_0 p_0'}{2} + \frac{p_1 p_1'}{2}\\ p_{\Psi^+} &= p_{\Psi^-} = \frac{p_0 p_1'}{2} + \frac{p_0 p_1'}{2}.\end{aligned} \tag{15}$$

Yhtälöistä (14) nähdään, että tilat A ja D, jotka olivat alunperin separoituvia ovat nyt lomittuneita keskenään. [43]



Kuva 3: Lomittumisen jakaminen: Ensin molemmat satelliitit jakavat lomittuneen kubittiparin kahden maassa olevan aseman kanssa. Kun maassa oleviin kubitteihin tehdään mittaus, projisoituu niiden satelliittien kanssa jakama lomittuminen satelliittien välille.

Kuvassa 3 kuvataan lomittumisen jakaminen kahden satelliitin välillä. Alussa molemmat satelliitit jakavat erilliset lomittuneet tilat maassa olevien asemien kanssa. Satelliittien välillä ei ole lomittunutta tilaa. Maassa olevat asemat tekevät yhteisen mittauksen soveltuvassa kannassa pariin, joka muodostuu molempien lomittuneiden parien maassa olevista puolista. He kommunikoivat klassisesti saamansa tuloksen satelliittien kanssa, jolloin niiden hiukkasten välille syntyy lomittuminen. Tämä tilanne on esitetty kuvassa 3 oikealla.

1.1.4 Lomittumisen tislaus

Kvanttikommunikaatiossa lomittumisen tislaus yhdessä kvanttiteleportaation kanssa mahdollistaa virhevapaan kommunikaation hälyisten kanavien kautta. Lomittumisen tislaus on tarpeellista, jos haluamme tavoitella mahdollisimman korkeita kapasiteetteja verkon noodien välillä.

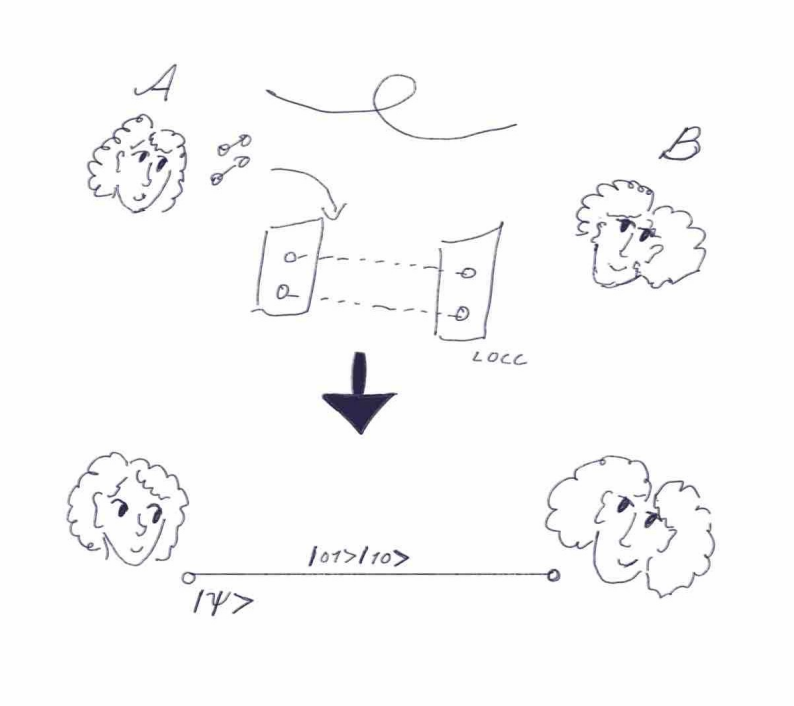
Lomittumisen tislauksella (eng. *Entanglement distillation or purification*) tar-

koitetaan prosessia, jossa suurempi määrä N hälyisiä (eng. *noisy*)[5] ja sekoittuneita tiloja muutetaan jollain todennäköisyydellä pienemmäksi määräksi maksimaalisen lomittuneita puhtaita tiloja (Bellin tiloja). Hälyiset tilat saadaan luotua esimerkiksi jakamalla hälyisen kanavan kautta useita lomittuneiden tilojen osia. Saadut tilat käsitellään paikallisesti klassista kommunikaatiota hyödyntäen (LOCC), jolloin saadaan vähemmän, mutta tarkkuudeltaan suurempia tiloja. Kun samoja protokollia toistetaan tarpeeksi, saadaan lopulta maksimaalisen lomittuneita tiloja. Lomittumisen tislaukseen on useita protokollia, joista jokainen operoidessaan N kopioon hälyisistä tiloista tuottaa $M \leqslant N$ kappaletta puhdistettuja tiloja. [10, 13]

Kuvassa 4 kuvataan lomittumisen tislauksen hyödyntämistä kvanttikommunikaatiossa. Ensin Alice lähettää maksimaalisen lomittuneen tilan kvanttikanavaa pitkin Bobille. Koska kanava on hälyinen, on Bobille saapuva alisysteemi maksimaalisen lomittunut ja sekoittunut. Alice toistaa tämän toiselle tai vielä useammalle kubitti parille. Alice ja Bob suorittavat omiin kubitteihinsa lokaaleja mittauksia ja kommunikoivat saamansa tulokset klassisesti toisilleen, hyödyntäen puhdistusprotokollaa. Erilaisia puhdistusprotokollia on esitelty alempana. Lopulta Alice ja Bob päätyvät kuvassa 4 alhaalla esitettyyn tilanteeseen, jossa he ovat luoneet maksimaalisesti lomittuneen tilan, jota he voivat hyödyntää teleportaatiokanavana.

On olemassa useita erilaisia puhdistusprotokollia, jotka poikkeavat mm. siinä mitä tiloja ne pystyvät puhdistamaan, tehokkuudessa sekä siinä moneenko kopiotilaan ne operoivat. Puhdistus protokollat voidaan jakaa suodatusprotokolliin (eng. *filtering protocols*), toistoprotokolliin (eng. *recurrence protocols*), tiivistämis- ja jalostusprotokolliin (eng. *hashing and breeding protocols*), sekä $N \to M$ protokolliin [14]. Käsitellään seuraavaksi muutamia esimerkkejä lomittumisen tislauksesta eri puhdistusprotokollilla.

[5]Häly on seurausta kvanttitilan vuorovaikutuksesta ympäristön kanssa, joka muuttaa tilaa epätoivotusti.



Kuva 4: Lomittumisen tislaus: Alice jakaa Bobille useamman maksimaalisesti lomittuneen tilan osia, joihin syntyy hälyä jakamisen seurauksena. Alice ja Bob muuttavat puhdistusprotokollia käyttäen hälyiset ja sekoittuneet tilat yhdeksi maksimaalisen lomittuneeksi tilaksi, jota he voivat käyttää hälyttömänä kanavana kvanttiteleportaatioon.

Suodatusprotokollat

Suodatusprotokollat operoivat kopioon yhdestä sekoittuneesta tilasta ja koostuvat paikallisista suodatusmittauksista[6]. Tilaan sovelletaan siis sarja paikallisia mittauksia, siten että saatava tila σ on lomittuneempi kuin alkuperäinen tila ρ. Suodatusprotokollia voidaan soveltaa seuraavan laisiin tiloihin:

$$\rho = F\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + (1-F)\left|00\right\rangle\left\langle 00\right|,$$

jossa $\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(\left|01\right\rangle + \left|10\right\rangle)$. Operaatiot paikallisella operaattorilla $O = \sqrt{\epsilon}\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|$, joka johtaa epänormalisoituun tilaan:

$$\rho' = F\epsilon\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + (1-f)\epsilon^2\left|00\right\rangle\left\langle 00\right|. \tag{16}$$

Tarkkuus uudelle tilalle voidaan kirjoittaa:

$$F' = F\epsilon/[F\epsilon + (1-F)\epsilon^2].$$

Huomataan, että epsilonin lähestyessä nollaa, lähestyy tarkkuus ykköstä. Kuitenkin tällöin myös halutun tilan todennäköisyys lähestyy nollaa. Suodatusprotokollat ovatkin hyvin rajatuissa tilanteissa käytännöllisiä.[14]

BBPSSW protokolla

Bennett et al. [6] luoma puhdistusprotokolla, joka mahdollistaa yhden maksimaalisesti lomittuneen tilan luomisen useista sekoittuneista tiloista ρ, kunhan tarkkuus F jollekin maksimaalisesti lomittuneelle tilalle täyttää ehdon $F > 1/2$. Ensin sekoittunut tila ρ saatetaan depolarisoituun Wernerin tilaan:

$$\begin{aligned} W_F =& F\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{1-F}{3}\left|\Psi^+\right\rangle\left\langle\Psi^+\right| \\ &+ \frac{1-F}{3}\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \frac{1-F}{3}\left|\Phi^-\right\rangle\left\langle\Phi^-\right|. \end{aligned}$$

[6]Esim. heikot mittauksista, joihin kuuluvat mm. paikalliset operaatiot ancillaan ja Neumann mittaukset ancillasta. Ancilla on kvanttipiirissä ylimääräisistä kubiteista muodostuva osa, johon voidaan tehdä operaatioita ilman informaatiokatoa[24].

Tämän jälkeen tilaan sovelletaan rotaatioita sekä CNOT-operaatioita[7]. Tämän jälkeen tilat mitataan paikallisesti sekä tulokset kommunikoidaan klassisesti. Tislaus tuottaa tiloja, joiden tarkkuus F' määräytyy alkuperäisten tilojen mukaan:

$$F' = \frac{F^2 + [(1-F)/3]^2}{F^2 + 2F(1-F)/3 + 5[(1-F)/3]^2},\ F' > F.$$

[6, 14]

Kuvassa 5 on esitetty Bennett et al. protokollan toimintaa yksinkertaisesti. Siinä Alice ja Bob muuttavat kaksi heikommin lomittunutta paria yhdeksi lomittuneemmaksi pariksi, hyödyntäen CNOT operaatioita. He mittaavat kohdeparin 0/1 kannassa ja kommunikoivat klassisesti saamistaan tuloksista. Jos saadut tulokset vastaavat, on saatu pari lomittumiseltaan parempi kuin alkuperäinen. Muutoin tislaus toistetaan uudelleen, kunnes päästään haluttuun lopputulokseen [26].

PSBZ protokolla

Jos Alice ja Bob haluaisivat jakaa keskenään maksimaalisesti lomittuneita kubitti-/fotonipareja, tilassa:

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B),$$

jossa alaviitteet A ja B viittaavat Alicen ja Bobin fotoneihin/kubitteihin. Ennen puhdistusta parit ovat sekoittuneessa tilassa

$$\begin{aligned}\rho_{AB} =& F\,|\Phi^+\rangle_{AB}\langle\Phi^+| + (1-F)\,|\Psi^+\rangle_{AB}\langle\Psi^+| \\ |\Psi^+\rangle_{AB} =& \frac{1}{\sqrt{2}}(|H\rangle_A |V\rangle_B + |V\rangle_A |H\rangle_B).\end{aligned}$$

Tällöin Alicen ja Bobin jakamaan tilassa on halutun maksimaalisesti lomittuneen tilan lisäksi epätoivottu osa, joka on sekoittuneessa tilassa. Tila voidaan kirjoittaa neljän puhtaan tilan todennäköisyyksien sekoituksena, jotka on esitetty taulukossa I.

[7]Kvanttipiireissä tämä toteutetaan CNOT-porteilla

Taulukko I: Puhtaiden tilojen todennäköisyydet

F^2	$\|\Phi^+\rangle\|\Phi^+\rangle$
$F(1-F)$	$\|\Phi^+\rangle\|\Psi^+\rangle$
$F(1-F)$	$\|\Psi^+\rangle\|\Phi^+\rangle$
$(1-F)^2$	$\|\Psi^+\rangle\|\Psi^+\rangle$

Protokollan tavoitteena on saattaa systeemi tilaan, jossa tasan yksi fotoni on jokaisessa spatiaalisessa tilassa, jolloin taulukon I keskimmäiset tapaukset voidaan hylätä, sillä ne eivät johda tällaisiin tiloihin. Tällöin voidaan kirjoittaa uusi operaattori muotoon:

$$\rho' = F' \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + (1-F') \left|\Psi^+\right\rangle\left\langle\Psi^+\right|,$$

jossa tarkkuus F' voidaan kirjoittaa:

$$F' = \frac{F^2}{F^2 + (1-F)^2} > F, F > \frac{1}{2}.$$

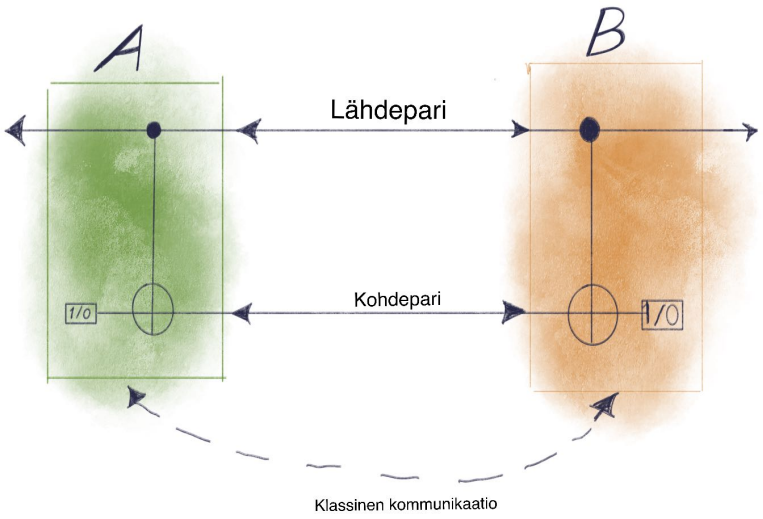
[26]

1.2 Verkkoteoria

Verkkoteoria tutkii noodien (eng. *node* tai *vertex*) ja linkkien (eng. *link* tai *edge*) avulla esimerkiksi sosiaalisissa tieteissä ihmisten välisiä suhteita tai biologiassa lajien suhteita toisiinsa. Kvantti-informaatiossa verkkoteoriaa käytetään informaation välittämiseen. Verkkoteorian kappaleen matemaattinen käsittely noudattaa Newmanin kirjaa *Networks: An Introduction*[23].

1.2.1 Graafit

Verkostot, tai graafit, joka on matemaattisessa kirjallisuudessa yleisempi nimitys, ovat joukosta noodeja ja linkkejä koostuvia rakenteita. Matemaattisempi määritystapa graafille on sen järjestäminen pariksi $G = (V, E)$, jossa V on joukko noodeja



Kuva 5: Lomittumisen tislaus BBPSSW protokollalla. Alice ja Bob muuttavat kaksi heikommin lomittunutta paria yhdeksi lomittuneemmaksi pariksi, hyödyntäen CNOT operaatioita. He suorittavat mittauksen kohdeparin ja kommunikoivat klassisesti saamansa tulokset. Jos saadut tulokset vastaavat, on saatu pari lomittumiseltaan parempi kuin alkuperäinen. Jos tulokset eivät vastaa, tislaus toistetaan uudelleen, kunnes päästään haluttuun lopputulokseen.

ja E:

$$E \subseteq \{\{i,j\}|i,j \in V\}, i \neq j, \tag{17}$$

on näiden välillä oleva joukko linkkejä. Yleisesti graafin noodien lukumäärää merkitään n:llä ja linkkien lukumäärää kirjaimella m. Noodeille on määritetty aste k (eng. *degree*) kuvaamaan moneenko muuhun noodin graafissa se on yhdistettynä linkillä eli montako naapuria sillä on. Kun kaikkien noodien aste tiedetään, voidaan laskea keskimääräinen aste, joka on noodien asteiden keskiarvo. Graafille voidaan myös määrittää astejakauma, joka kertoo, montako tietyn asteista noodia graafissa on. Astejakauma kuvaa graafin muotoa ja esimerkiksi kertoo, onko siinä paljon keskusnoodeja (eng. *hubs*).

Keskusnoodi on graafin noodi, jolla on korkea aste ja joka on yleensä graafille tärkeä, sillä sen poistaminen saattaa erottaa graafin useaksi erilliseksi verkoksi. Klusterit (eng. *clusters*) ovat noodijoukkoja, jotka ovat kytkeytyneet keskenään.

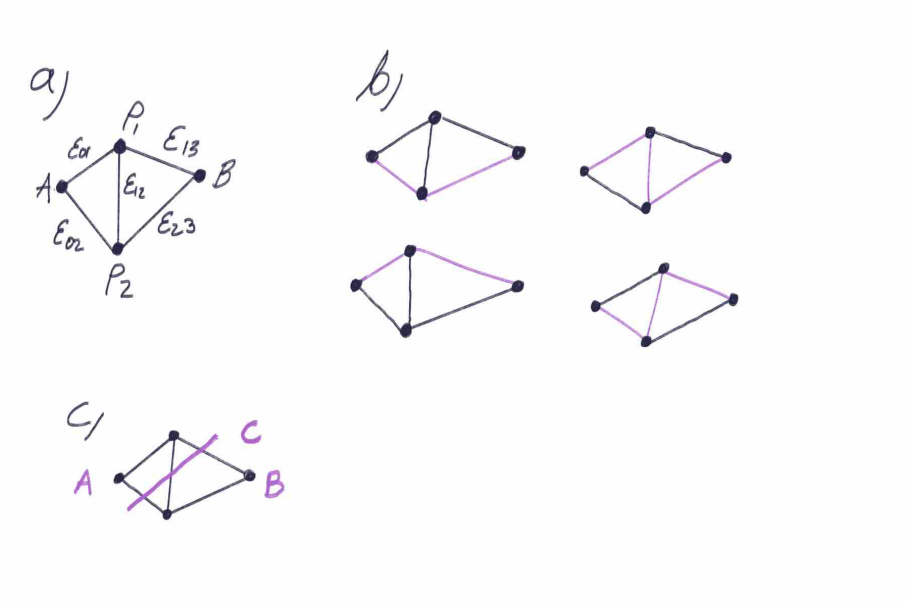
Kvanttikommunikaatioverkoissa verkkojen noodit kuvaavat kvanttitoistimia tai kvanttitietokoneita ja linkit valokuitukaapeleita niiden välillä.

Leikkausjoukko

Kahden noodin välillä verkossa on yleensä useita mahdollisia reittejä. Osa näistä reiteistä jakaa linkkejä keskenään ja vain osa mahdollisista poluista on erillisiä toisistaan. Näistä erillisistä poluista voidaan valita yksittäiset linkit, jotka leikkaamalla noodipari ei enää ole yhteydessä toisiinsa. Tätä linkkien joukkoa kutsutaan leikkausjoukoksi (eng. *cut set*).[23]

Kuvassa 6 on esitetty salmiakkigraafi (a), sen noodien A ja B välillä olevat mahdolliset reitit (b) sekä yksi mahdollinen leikkausjoukko C (c), joka eristää noodit A ja B.

Kvanttikommunikaatiossa kahden noodin välinen minimileikkausjoukko kuvaa



Kuva 6: Salmiakkigraafi sekä sen noodien A ja B väliset mahdolliset reitit esitetty kohdassa (b). Kohdassa (c) on esitetty yksi mahdollinen leikkaus noodien A ja B välillä.

hyvin noodien välisen kommunikaation maksimitehoa, sillä jos otetaan leikkausjoukon linkit kerrottuna niiden kapasiteeteilla ja summataan, saadaan melko hyvä arvio kokonaiskapasiteetista ja sitä kautta maksimaalista nopeutta informaation välitykselle luotettavasti.

Vierusmatriisi

Noodien i ja j välistä linkkiä voidaan merkitä parina (i,j), ja graafin linkit voidaan kerätä listaksi. Listoja käytetään usein esim. tietokoneilla graafin rakenteen tallentamiseksi, mutta matemaattisesti tehokkaampi tapa käsitellä niitä on vierusmatriisi (eng. *adjacency matrix*). Vierusmatriisi kuvaa graafin rakennetta ja noodien välisiä suhteita. Vierusmatriisi **A** määritellään seuraavasti:

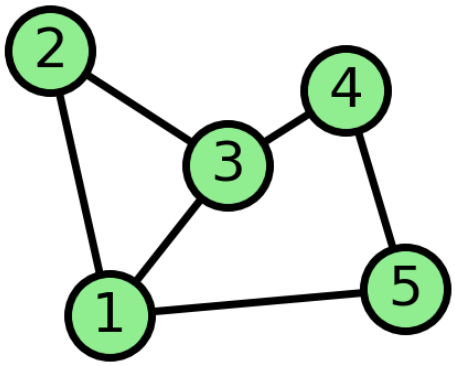
$$A_{ij} = \begin{cases} 1 \text{ jos noodit } i \text{ ja } j \text{ jakavat linkin,} \\ 0 \text{ muulloin,} \end{cases}$$

Matriisin diagonaalilla on siis noodin itsensä kanssa muodostamat linkit, mutta tä-

män tutkielman aikana ne yleisesti oletetaan nolliksi.[8] Graafin linkeille voidaan antaa myös painotettuja arvoja, kuvaamaan mm. kahden noodin välistä virtausta tai esimerkiksi etäisyyttä. Tällöin matriisin alkiot saavat linkin painoarvon arvokseen.

Esimerkiksi kuvan 7 yksinkertainen graafi voidaan esittää vierusmatriisin avulla:

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$



Kuva 7: Yksinkertainen viiden noodin graafi

1.2.2 Satunnaisverkkomallit

Satunnaisverkoissa (eng. *random network*) verkkojen ominaisuudet ovat yleisesti satunnaisia, lukuun ottamatta yksittäistä ominaisuutta, jotka on verkolle asetettu, esimerkiksi astejakauma tai linkkien muodostuminen. Satunnaisverkkoihin viitataan usein matemaattisesti $G(n, m)$ mallin verkkoina. Satunnaisverkot ovat kokonaisuus

[8]Myös matriisin alkiot voisivat saada suurempia arvoja kuin yksi, jos noodien välillä olisi useampi linkki, mutta näitä tapauksia ei tutkielmassa käsitellä.

verkkoja, joilla on samat ominaisuudet, esimerkiksi noodien ja linkkien lukumäärän suhteen, joiden joukosta valitaan/arvotaan verkko.

Satunnaisverkoille voidaan määrittää todennäköisyys $P(G)$ kaikkien verkkojen yli, siten että:

$$P(G) = \frac{1}{\Omega},$$

jossa Ω on kaikkien mahdollisten verkkojen lukumäärä. Satunnaisverkoille voidaan määrittää keskimääräisiä arvoja esimerkiksi asteelle $< k >= 2m/n$. Kaikkein yksinkertaisimmassa ei triviaalissa verkossa eli Erdős-Rényi mallin verkossa valitaan noodien lukumäärä sekä kiinteä todennäköisyys niiden välisille linkeille, mutta muutoin verkon ominaisuudet ovat satunnaisia. Erdős-Rényi mallia kutsutaan myös $G(n, p)$ malliksi tai $G(n, m)$ malliksi[9]. Tässä työssä keskitytään $G(n, p)$ malliin, sillä sen ominaisuudet ovat helpompia käsitellä matemaattisesti. $G(n, p)$ on kokonaisuus verkostoja, josta jokainen yksittäinen graafi esiintyy todennäköisyydellä

$$P(G) = p^m(1-p)^{\binom{n}{2}-m},$$

jossa m on linkkkien lukumäärä. Todennäköisyys saada graafi jossa on tasan m kappaletta linkkejä on

$$P(m) = \binom{\binom{n}{2}}{m} p^m (1-p)^{\binom{n}{2}-m},$$

jolloin linkkien lukumäärän keskiarvoksi saadaan

$$\langle m \rangle = \sum_{m=0}^{\binom{n}{2}} mP(m) = \binom{n}{2} p.$$

Asteen keskiarvoksi voidaan tällöin määrittää:

$$\begin{aligned} \langle k \rangle =& \sum_{m=0}^{\binom{n}{2}} \frac{2m}{n} P(m) \\ =& \frac{2}{n}\binom{n}{2} p = (n-1)p. \end{aligned}$$

[9] $G(n, m)$ mallissa on kiinteä noodien ja linkkien lukumäärä, mutta näiden sijoittuminen verkkoon on satunnaista, kuitenkin niin, että noodiparin välilä voi olla vain yksi linkki.

Erdős-Rényi mallille voidaan määrittää todennäköisyysjakauma seuraavasti: aloitetaan määrittämällä todennäköisyys p_k jolla tietty noodi on yhdistetty tasan k:n toiseen noodiin, määrittämällä todennäköisyydelle Taylorin sarja ja tämän jälkeen muodostamalla todennäköisyysjakauman kaava. Matemaattisesti: Todennäköisyys noodin linkittymiselle tasan k:n toiseen noodiin:

$$p_k = \binom{n-1}{k} p^k (1-p)^{n-1-k}.$$

Noodien lukumäärän n lähestyessä ääretöntä, p $= \frac{c}{n-1}$ lähestyy nollaa, jossa $c = \langle k \rangle$. Voidaan kirjoittaa:

$$\begin{aligned} ln[(1-p)^{n-1-k}] =& (n-1-k) ln(1 - \frac{c}{n-1}) \\ \cong& -(n-1-k)\frac{c}{n-1} \cong -c, \end{aligned}$$

joka voidaan uudelleen kirjoittaa

$$(1-p)^{n-1-k} = e^{-c}.$$

Viimein voidaan johtaa suurelle n:n arvolle

$$p_k = \frac{(n-1)^k}{k!} (\frac{c}{n-1})^k e^{-c} = e^{-c}\frac{c^k}{k!},$$

joka on Poisson-jakauman todennäköisyysfunktio, minkä takia Erdős-Rényi mallin graafeista käytetään joskus myös nimitystä Poisson-satunnaisgraafi. [23]

Tästä hieman monimutkaisempi satunnaisverkkomalli on Waxman-malli[42], jossa noodien sijoittuminen on satunnaista, mutta näiden väliset linkit riippuvat etäisyydestä [23]. Jokainen noodipari on yhdistetty linkillä todennäköisyydellä

$$\Pi(x, x') = \beta e^{-d/\alpha L}, \tag{18}$$

jossa d on noodien etäisyys, L on suurin mahdollinen etäisyys parin välillä ja α on vakio, siten että $\alpha L = 226$ km[10] [45]. Vakiot α ja β voivat molemmat saada arvoja

[10]Tämä arvo huippuluokan optisissa kuiduissa.

nollan ja yhden välillä eli $0 < \alpha \leqslant 1$, joka kuvaa linkin muodostumisen herkkyyttä etäisyyteen ja $0 < \beta \leqslant 1$ kontrolloi linkkien tiheyttä [19]. Voidaan valita, että noodit sijoittuvat satunnaisesti alueen $\Omega_R = [0, R] \times [0, R]$, jolloin suurin mahdollinen etäisyys $L = \sqrt{2}R$. Myös Waxman-mallin verkkojen astejakauma (eng. *degree distribution*) noudattaa Poisson-jakaumaa, samoin kuin edellä käsitellyssä Erdős-Rényi mallissa.[35]

Useimmat reaalimaailman verkot eivät kuitenkaan noudata astejakaumaltaan Poisson-jakaumaa. Vuonna 1999 Albert-Làszlò Barabàsi sekä Rèka Albert esittelivät mallinsa skaalavapaille (eng. *scale-free*) verkoille[3], joita kutsutaan heidän mukaansa myös Barabàsi-Albert-verkoiksi[11]. Barabàsi-Albert-verkoissa noodit lisätään yksitellen ja niistä luodaan c kappaletta linkkejä olemassa oleviin noodeihin, suosien sellaisia noodeja, joiden aste on ennestään suuri. Tämän seurauksena minkään noodin aste verkossa ei voi olla pienempi kuin c. Korkean asteen noodien suosiminen voidaan toteuttaa lisäämällä linkit noodien välille todennäköisyydellä $\Pi(k_i) = k_i/\Sigma_j k_j$, jossa verrattavan noodin aste jaetaan koko verkon noodien asteiden summalla [4, 8]. Verkkojen astejakaumat noudattavat potenssilakia (eng. *power law*) eli $P(k) \sim k^{-\gamma}$, kuten myös useimmat reaalimaailman verkot. Vakio k on noodin aste. Esimerkiksi internetin astejakauma voidaan esittää muodossa

$$p_k = Ck^{-\alpha},$$

jossa vakio C=e^c. Vakio α saa yleensä arvoja väliltä $2 \leqslant \alpha \leqslant 3$, mutta myös hieman suuremmat ja pienemmät arvot ovat myös mahdollisia joillain verkoilla. [3, 23]

Verkoissa, joissa noodit ovat vahvasti kytkeytyneet toisiinsa[12], voidaan verkon kapasiteetissa havainnoida raja-arvo tiheydessä, jonka alapuolella kapasiteetti no-

[11]Ennen Barabàsia ja Albertia potenssilain mukaisesti jakautunutta mallia tutki Price 60- ja 70-luvvulla, mutta Pricen malli käsittelee suunnattuja verkkomalleja, jossa linkit ovat yhden suuntaisia. Barabàsi-Albert-malli on tunnetumpi ja se kuvaa verkkoja, joissa linkit välittävät informaatiota molempiin suuntiin, mikä tekee siitä kommunikaatioverkkoja tutkittaessa käytännöllisemmän.

[12]Esimerkiksi Waxman-verkoissa sekä Erdős-Rényi -mallissa.

peasti romahtaa lähes nollaan. Rajan yläpuolella kahden noodin välinen kapasiteetti kommunikaatiolle ei yllättäen useimmiten riipu etäisyydestä, johtuen niiden välillä olevista useista poluista. Vähemmän kytkeytyneillä verkoilla, kuten skaalavapailla verkoilla, kapasiteetti on riippuvainen etäisyydestä. [45]

1.3 Kvanttikommunikaatioverkot

Kvanttikommunikaatioverkot ovat verkkoja, joissa fotonit toimivat informaation, kryptografisten avainten sekä lomittumisen välittäjinä. Verkot voidaan jakaa karkeasti kahteen osaan: saavutettavissa oleviin verkkoihin, joita vastaavat enimmäkseen QKD verkot sekä teoreettisiin verkkoihin, joita vastaavat kvantti-informaatio verkot. Viime vuosina tämä raja on kuitenkin hämärtynyt ja mm. NISQ verkot ovat yleistyneet.[25]

Kvanttikommunikaatioverkot koostuvat noodeista, joissa kubitteja varastoidaan ja joiden välillä kommunikaatio tapahtuu kvanttikanavia[13] (eng. *quantum channel*) pitkin. Kommunikaation pullonkaulana kaukaisten noodien välillä toimii kanavan virhetaajuus, joka skaalautuu kanavan pituuden mukaan. Kvanttikommunikaatiossa virheen mahdollisuus mittauksissa skaalautuu eksponentiaalisesti kanavan pituuteen kommunikaation tapahtuessa hälyisten kanavien kautta. Etäisyyden kasvu johtaa siihen, että fotonin välitys ilman että se absorboituu vaatii useampia yrityksiä[14] ja vaikka fotoni pääsee perille, sen tarkkuus (eng. *fidelity*) pienenee eksponentiaalisesti. Tämä rajoittaa etäisyyttä, jolle informaatio voidaan välittää. Näiden ongelmien ratkaisuksi on esitetty mm. kvanttitoistimia.[9]

Kvanttitoistimet

Klassisessa kommunikaatioteoriassa toistimia (eng. *repeater*) käytetään heikke-

[13]Kvanttikanavat vastaavat linkkejä verkkoteoriassa.

[14]Vaadittujen yritysten määrä kasvaa eksponentiaalisesti etäisyyden suhteen.

nevän signaalin vahvistamiseen sekä palauttamiseen alkuperäiseen muotoon. Toistimet sijoitetaan kanavan sopiviin kohtiin, jotta signaali pysyy hyvänä. Klassisten toistimien ideaan pohjautuen voidaan kvanttikommunikaatiossa käyttäää avuksi kvanttitoistimia.[36] Kvanttikommunikaation tapauksessa kanava jaetaan N osaan, joiden välissä on liitospisteinä apunoodeja. Tämän jälkeen luodaan N kappaletta EPR pareja, jossa tarkkuus viereisten noodien välillä on F. Osien lukumäärä N valitaan siten, että tarkkuus on välillä $F_{min} < F \lesssim F_{max}$[15]. Kun EPR-pari ollaan saatu luotua, sitä voidaan käyttää kvantti-informaation siirtämiseen. Parit voidaan yhdistää toisiinsa noodeissa tehtävillä Bell mittauksilla ja välittämällä klassisesti saadut mittaustulokset. Valitettavasti parien yhdistäminen laskee niiden välistä tarkkuutta, sillä käytetyt epätäydelliset operaatiot lisäävät hälyä. Jos kaikki parit yhdistetään, tippuu kanavan tarkkuus alle minimi arvon F_{min}, kun etäisyys d on pitkä. Ainoa tapa välttää tämä on olla yhdistämättä kaikkia pareja, siten että yhdistetyille pareille $L \ll N$ tarkkuus on yli minimi arvon $F_L > F_{min}$. [9]

Aiemmin käsiteltyjen standardipuhdistusprotokollien sijaan referenssissä [9] esitetyssä sisäkkäisessä puhdistusprotokollassa (eng. *nested purification protocol*) parit yhdistetään ja puhdistetaan saman aikaisesti, minkä seurauksena lomittumisen luomiseen kulunut aika skaalautuu polynomiaalisesti ja vaadittujen materiaali resurssien määrä liitospistettä kohden skaalautuu logaritmisesti etäisyyden suhteen. Oletetaan, että $N = L^n$, jollekin kokonaisluvulle n. Ensin kaikki parit yhdistetään L välein eli kaikissa muissa liitospisteissä, paitsi alkupisteessä, sekä sen jälkeen L välein olevissa $C_L, C_{2L}, ,,,, C_{N-L}$ liitospisteissä. Tällöin saadaan N/L paria, joiden pituus on L ja joilla on jokaisella oma tarkkuus. Näiden parien puhdistukseen tarvitaan tietty määrä M kopiota, jotka luodaan rinnakkaisesti alkuperäisten lomittuneiden

[15]Suurin mahdollinen tarkkuus F_{max} kertoo, kuinka puhtaaksi tila on mahdollista saada, mitä kuitenkin rajoittaa käytettyjen puhdistus protokollien epätäydellisyys. F_{min} on tarkkuuden minimi arvo, jonka puhdistus protokollat vaativat toimiakseen, mutta joka on mahdotonta saavuttaa etäisyyden d kasvaessa.

parien kanssa. Tämän jälkeen kopioiden avulla puhdistetaan sekä määritetään väleille $A\&\ C_L$, $C_L\ \&\ C_{2L}$ jne tarkkuus $\geqslant F_1$[16]. Vaadittujen kopioiden määrä riippuu alkuperäisestä tarkkuudesta, siitä paljonko tarkkuus muuttuu parien yhdistämisessä sekä puhdistus protokollan tehokkuudesta. Tällöin vaadittujen parien määrä on $(LM)^2$. Prosessia voidaan toistaa yhdistämällä jälleen L paria ja niin edelleen, kunnes kanavan alku- ja loppupiste on saatu yhdistettyä. Lopullisen parin etäisyys tällöin on N ja tarkkuus $\geqslant F_1$. Alkeisparien kokonaismäärä R on $(LM)^n$, joka voidaan ilmaista myös

$$R = N^{log_L M+1},$$

josta voidaan nähdään vaadittujen resurssien kasvavan logaritmisesti etäisyyden kasvaessa.[9]

1.3.1 QKD verkot

QKD eli kvanttiavainten jako (eng. *Quantum Key Distribution*) verkot ovat todistetusti kryptografisesti turvallisia verkkoja, joita voidaan käyttää viestien lähettämiseen julkisesti, vaikka kaikki verkon noodit eivät olisikaan luotettavia [20, 24]. QKD verkot eroavat suuresti perinteisistä tietoliikenneverkoista, sillä verkon rakenteelta ja linkeiltä vaaditaan QKD tyypillisiä ominaisuuksia [20]. QKD verkoille ominaisia rajoituksia ovat etäisyydestä riippuva hälyn ja epätarkkuuden kasvu sekä se, kuinka nopeasti verkon noodit pystyvät luomaan kryptografisia avaimia. Usein QKD verkoilla käytetään maksimaalisen turvallisuuden takaamiseksi viestien salaamiseen viestien kanssa yhtä pitkiä avaimia ja jotka käytetään vain kerran, mikä lisää verkkojen rajoitteisuutta.[25]

QKD:n perusideana on, että salakuuntelija Eve ei voi saada informaatiota Alicen jakamista kubiteista ilman, että hän vaikuttaa niiden tilaan. Kun Bob vastaan ot-

[16] F_1 on alkuperäinen tarkkuus.

taa Alicen lähettämät kubitit, he voivat uhrata osan jaetusta avaimesta ja vertailla tuloksia keskenään, varmistaen samalla kuinka paljon tilat ovat muuttuneet salakuuntelun tai kanavan meluisuuden seurauksena. [24]

Eve ei voi saada tietoa epäortogonaalisista tiloista, ilman että hän aiheuttaa häiriötä tiloihin. Tämän todistamiseksi voidaan tutkia kahta epäortogonaalista kvanttitilaa $|\psi\rangle$ ja $|\varphi\rangle$. Eve koittaa saada näistä informaatiota vuorovaikuttamalla ancillalla, joka on muodostettu standardi tilaan $|u\rangle$, tilojen kanssa. Jos oletetaan, että Even mittaus ei vaikuta tilohin, saadaan:

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle$$
$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle|v'\rangle.$$

Jotta Eve saisi jotain informaatiota alku tiloista, pitäisi $|v\rangle$ ja $|v'\rangle$ erota. Kuitenkin, koska sisätulon on säilyttävä unitaarisessa muunnoksessa:

$$\langle v|v'\rangle\langle\psi|\varphi\rangle = \langle u|u\rangle\langle\psi|\varphi\rangle$$
$$\langle v|v'\rangle = \langle u|u\rangle = 1.$$

Tästä nähdään, että $|v\rangle$ ja $|v'\rangle$ on oltava identtiset, Jos Eve siis haluaisi jotain informaatiota alkuperäisistä kvanttitiloista, olisi hänen häirittävä ainakin toista tiloista.[24]

Ensimmäinen QKD protokolla oli Bennettin ja Brassardin vuonna 1984 esittelemä neljän tilan menetelmä, joka jaetaan kahteen pariin. Alice valitsee $(4 + \delta)$n - bitin pituisen satunnaisen datan sekä yhtä pitkän satunnaisbittijonon b. Tämän jälkeen hän muuttaa jokaisen data kubitin joko kantaan $|0\rangle, |1\rangle$ jos vastaava b:n arvo on 0 tai kantaan $|+\rangle, |-\rangle$, jos vastaava b: bitti on 1. Alice lähettää saamansa tuloksen Bobille, joka mittaa saamansa kubitit X tai Z kannassa[17] satunnaisesti. Alice jakaa myös alkuperäisen b:n Bobille. Alice ja Bob hylkäävät biteistä ne, jotka Bob

[17] X kanta on $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ ja Z kanta on $|0\rangle, |1\rangle$ kanta.

mittasi eri kannassa kuin mihin Alice ne valmisteli alunperin ja vertaavat osaa jäljellejääneistä, varmistaakseen ettei Eve ole salakuunnellut ja sen myötä vaikuttanut tiloihin tai ettei melun vaikutuksesta tilat ole muuttuneet matkalla. Jäljelle jääneistä biteistä Alice ja Bob saavat salausavaimen, jota he voivat hyödyntää salattujen viestien jakamiseen.[24]

QKD verkkojen katsotaan usein koostuvan kolmesta kerroksesta: Kvanttikerros, jossa avain luodaan, avaintenkäsittelykerros, jossa avainten turvallisuus tarkistetaan ja avaimet tallennetaan käyttöä varten sekä kommunikaatiokerros, jossa avaimia käytetään turvalliseen datan siirtoon. Verkoille syntyy myös joitain ominaisuuksia ja vaatimuksia niiden QKD luonteen takia:

- Avaintenjakonopeus (eng. *key rate*), joka kertoo millä nopeudella linkki pystyy luomaan avain materiaalia viestien salaamista sekä purkamista varten. Tämä suoraan vaikuttaa siihen, kuinka paljon noodi pystyy ottamaan vastaan sekä lähettämään informaatiota. Esimerkiksi vuonna 2002 rakennettu DARPA QKD verkko saavuttaa noin 400 bps nopeuden 10 kilometrin matkalle, kun taas vuonna 2007 rakennettu SECOQC verkko saavuttaa maksimissaan 3.1 kbps nopeuden 33 kilometrin matkalle. Paras nopeus on kuitenkin saavutettu Tokion 2009 rakennetussa QKD verkossa, joka pystyy 304 kbps nopeuteen 45 kilometrin matkalla. Vuosien saatossa avaintenjakonopeus on parantunut esimerkiksi detektorien ja optisten komponenttien kehittyessä [20].

- QKD verkon linkkejä rajoittaa maksimi pituus, jolla linkit pystyvät välittämään informaatiota turvallisesti. Tätä rajoittaa muun muassa kubitteina käytettyjen fotonien absorboituminen sekä sironta, jotka aiheutuvat ympäristön ja epätäydellisten linkkien tuomasta hälystä [20].

- Koska QKD verkkojen suurin hyöty on niiden turvallisuus, joten on tärkeää, että verkon noodit ovat turvallisia ja suojaavat niihin tallennettuja avaimia.

Verkkojen on oltava myös sitkeitä (eng. *robust*) hyökkäyksiä yksittäisiä noodeja vastaan, mutta myös uusien noodien lisäämistä kohtaan [20].

- Avainten luonti on kallista ja usein avain materiaalia on vähäisesti käytettävissä. Tämän takia on tärkeää, että resursseja käytetään mahdollisimman vähän, mutta kuitenkin niin että viestien salaus säilyy [20].

Kommunikaatio QKD verkkojen yli on suuresti etäisyyden rajoittamaa. Erityisesti häviöllisten bosonisten kanavien kautta tapahtuvassa kommunikaatiossa on rajoituksena kanavan kapasiteetti (eng. *capacity*). Varsinkin toistimettomilla verkoilla, häviöllisille kanaville suurin saavutettavissa oleva kapasiteetti on niin kutsutun PLOB (Pirandola-Laurenza-Ottaviani-Bachi) rajan rajoittama:

$$C(\eta) = -\log_2(1-\eta), \tag{19}$$

joka on suunnilleen 1.44η, kun $\eta \ll 1$. Kaavassa η on läpäisevyys (eng. *transmissivity*)[18]. Moderneille optisille kuiduille on yleisesti käytössä $\eta = 10^{-\gamma d/10}$, jossa $\gamma = 0.2$ dB/km [25, 28]. Jos kanava koostuu useammista linkeistä ja noodeista, muodostuu rajoittavaksi tekijäksi linkeistä se, jonka läpäisevyys on pienin, jolloin koko kanavan läpäisevyys on [28]

$$\eta_{P_t} = \min_{e \in P_t} \eta_e. \tag{20}$$

QKD verkoille on ehdotettu useita eri malleja, kuten:

- Luotettujen noodien verkko (eng. *trusted-node networks*), ovat verkkoja, jossa salausavain voidaan jakaa pidemmälle kuin viereisille noodeille, mutta tällöin jokaisen noodin reitillä tulee olla luotettava [33].

- Luotettavat toistin verkot (eng. *trusted repeater QKD network*) on luotettujen noodien verkon rinnakkaistapaus, jossa noodit ovat toistimia [20].

[18] Läpäisevyys on välityksestä selvinneiden fotonien osuus.

- Osittain luotettavat (eng. *partially trusted*) verkot ovat verkkoja, joissa osa noodeista on luotettavia ja osa ei. Yksi esimerkki osittain luotettavista verkoista ovat satelliitti QKD verkot (eng. *satellite QKD*), joissa osa verkon noodeista on satelliitteja. Satelliitit mahdollistavat suurempien verkkojen olemassaolon ja voivat esimerkiksi toimia välinoodeina kaupungeissa olevien verkkojen välillä [33].

- Turvallisuus ilman luotettuja toistimia (eng. *Security without Trusted Repeaters*): Luotettavien toistimien vaatimusta voidaan helpottaa esim. käyttämällä mittauslaitteistosta riippumatonta QKD:tä (eng. *measurement device independent (MDI) QKD*), kvanttitoistimilla tai turvautumalla useisiin reitteihin [20].

Ideaaliset kvanttikommunikaatioverkot

Ideaalisilla verkoilla viitataan kvanttikommunikaatiossa verkkoihin, jotka ovat ominaisuuksiltaan ideaaliset ja joissa esimerkiksi hälyn määrä oletetaan minimaaliseksi tai olemattomaksi. Myös QKD verkkoja tutkittaessa, niiden QKD luonne tuo mukanaan heikkouksia, joista reaalimaailman verkot kärsivät.

Epäideaaliset verkot kärsivät:

- Hälystä (eng. *noise*): Kvanttikommunikaatioverkoissa häly on ympäristön aiheuttamaa epätoivottua häiriötä tai epätäydellisyyttä, joka vaikuttaa kubittien ja lomittuneiden kubittiparien tarkkuuteen (eng. *fidelity*) sekä QKD verkoissa turvallisuuteen[20, 24, 34]. Häly voi esiintyä eri muodoissa kvanttikommunikaatioverkoissa, mm:

  - Dekoherenssi (eng. *decoherence*) kuvaa ilmiötä, jossa kvanttitilat menettävät ominaisuuksiaan vaikuttaessaan ympäristön kanssa, esimerkiksi lomittumisen katoaminen fotonin vuorovaikuttaessa ympäristön kanssa.[24,

38]

  - Fotonien absorboituminen sekä sironta, jotka optisten kuitujen vuorovaikutuksesta fotonin kanssa. Tämä johtaa informaation katoamiseen ja nostaa mahdollisten virheiden mahdollisuutta. Tästä ilmiöstä käytetään myös nimitystä vaiheen vaimennus (eng. *phase damping*, joka kuvaa kvanttiinformaation häviötä ilman että menetetään energiaa.[24]

- Ulkopuolisesta vaikutuksesta ja salakuuntelusta aiheutuvasta muutoksesta lähetettyihin tiloihin, joka näkyy virhetaajuudessa[34].

Reaalimaailman verkot ovat kuitenkin alttiita häviöille, sillä parhaimmatkin valokuitukaapelit eivät ole täydellisiä. Nämä verkot ovat edelleen ideaalisia, jos niillä ei esiinny muita rajoituksia [44]. Myös kommunikaatioverkkojen QKD luonne tuo joitain heikkouksia ja rajoitteita. Osa näistä on käsitelty jo aiemmin QKD verkkoja käsitellessä, mutta muita epäideaalisten QKD verkkojen heikkouksia ovat mm.:

- Hyökkäykset QKD verkkoihin: Kvantti hakkerointi (eng. *quantum hacking*) on uudempi tutkimuksen ala, joka tutkii mahdollisia hyökkäys tapoja QKD verkkoihin sekä ratkaisuja hyökkäyksiin. Esimerkiksi detektoreiden sokaisu hyökkäyksissä (eng. *detector blinding attacks*) hyökkääjä estää detektoreita havaitsemasta niihin saapuvia fotoneita ja pakottaa ne kertomaan haluamistaan havainnoinneista.[11]

- Tämänhetkisen teknologian tuomat heikkoudet: vaikka kvanttitoistimia on tutkittu paljon, ovat ne käytännössä nykyteknologian saavuttamattomissa. Erityisesti niiden vaatimat kvanttimuistit ovat vielä vahvasti teoriatasolla.[20] Myös kvanttikanavina käytettävät optiset kuidut eivät ole ideaalisia ja voivat aiheuttaa hälyä reaaliverkoissa.

Ideaalisissa verkoissa nämä ongelmat kuitenkin oletetaan ratkaistuiksi tai että ne

eivät vaikuta verkkoihin. Ongelmia pyritään korjaamaan mm. virheenkorjaus protokollilla (eng. *error correction protocol*) [11, 34].

Kvanttikommunikaatioverkkojen päästä päähän kapasiteetti

Usein kommunikaatioverkoissa on useita reittejä noodiparien välillä, mitä pystytään kuvaamaan aiemmin käsitellyllä leikkausjoukolla. Jos Alice ja Bob viestisivät vain yksittäisen linkki ketjun kautta, saadaan ketjun päästä-päähän kapasiteetti läpäisevyydeltään pienimmän linkin mukaan. Kun otetaan huomioon useat mahdolliset reitit noodien välillä, saadaan kapasiteetti summaamalla jokaisen reitin pienimmän läpäisevyyden linkkien kapasiteetit, sillä läpäisevyydeltään pienin linkki toimii pullonkaulana kommunikaatiossa.

Jotta voidaan päästä PLOB-rajan ylittäviin tuloksiin, täytyy verkostossa ottaa käyttöön kvanttitoistimet. Ne kykenevät sekä klassisiin että kvanttioperaatioihin, mikä mahdollistaa myös LOCC:n käytön kommunikaatiossa. Kaikissa ideaalisissa tilanteissa, joissa toistimet ovat käytössä, PLOB rajan rikkomiseksi täytyy selvittää myös päästä-päähän kapasiteetit (eng. *end-to-end capacities*) kubittien lähettämiselle (eng. *transmitting*), ebittien jakamiselle sekä salausavainten generoimiselle.

Tarkastellaan Alicea **a** ja Bobia **b**, jotka ovat lineaarisen ketjun N päissä, joka koostuu kvanttitoistimista $\mathbf{r}_1$,...,$\mathbf{r}_N$. Jokaisella toistimella on rekisteri, jota voidaan kasvattaa tulevilla systeemeillä ja kutistaa lähtevillä systeemeillä. Ketju on $N + 1$ kvanttikanavan yhdistämä $\{\mathcal{E}\}_i = \{\mathcal{E}_0,...,\mathcal{E}_i,...,\mathcal{E}_N\}$, joiden läpi systeemejä välitetään. Tämä tarkoittaa, että jos Alice lähettää systeemin toistimelle $\mathbf{r}_1$, tämä välittää systeemin toistimelle $\mathbf{r}_2$ ja niin edelleen, kunnes viimein systeemi lähetetään Bobille.[19]

[19]Huomaa, että koska suuntaamattomilla linkeillä voidaan systeemejä lähettää molempiin suuntiin, jolloin voi olla tilanne jossa keskellä oleva toistinnoodi saa systeemin molemmista suunnista. Systeemeille yleensä tämän takia määritetään suunnat, joissa informaatio siirtyy joko eteen- tai taaksepäin.[27]

Viestittäessä ketjun päästä päähän, kutakin kvanttikanavaa käytetään tasan kerran. Oletetaan, että ketju päät pyrkivät jakamaan bittejä, jotka voivat olla joko ebittejä tai salaisia kubitteja. Yleisin kvanttijakoprotokolla (eng. *quantum distribution protocol*) $\mathcal{P}_{chain}$ sisältää tiedonsiirtoa, joka hyödyntää adaptiivista LOCC:ia kaikkien osapuolten välillä eli lokaaleja operaatioita noodeissa, sekä klassista kommunikaatiota toistimien sekä päätepisteiden välillä. Ennen ja jälkeen tiedonsiirron noodit päivittävät ja optimoivat rekisterinsä LOCC:a hyödyntäen. Kun ketjua on adaptiivisesti käytetty n kertaa, jakavat päätepisteet keskenään tilan, joka koostuu nR_n kohde bitistä, jossa R_n on asymptoottinen nopeus. Asymptoottinen nopeus $\lim_n R_n$ voidaan optimoida kaikkien protokollien $\mathcal{P}_{chain}$ yli, jolloin voidaan määrittää kaksisuuntainen kapasiteetti ketjulle $\mathcal{C}(\{\mathcal{E}_i\})$. Jos oletetaan, että kaksisuuntainen klassinen kommunikaatio on käytettävissä, molemmilla kubiteilla ja ebiteillä toistimilla avustettu kapasiteetti $\mathcal{C}$ vastaa lomittumisen jakamisen kapasiteettia (ebitit) tai kvanttikapasiteettia (kubitit). [27]

Verkostot useimmiten ovat monimutkaisempia kuin yksinkertaisia ketjuja, sillä useammat reitit Alicen ja Bobin välillä tekevät kommunikaatiosta tehokkaampaa. Tällöin Alice valmistelee M tilaa, jotka hän lähettää M:lle naapuri noodille verkossa. Nämä lähettävät tilat eteenpäin, kunnes kaikki tilat saapuvat Bobille. Esimerkiksi salmiakkigraafissa (esitetty kuvassa 6), Alice lähettää tilat noodeille (eli kvanttitoistimille) $\mathbf{p}_1$ ja $\mathbf{p}_2$, jota merkitään

$$\mathbf{a} \rightarrow \{\mathbf{p}_1, \mathbf{p}_1\}.$$

Tämän jälkeen toistin $\mathbf{p}_1$ kommmunikoi Bobin kanssa,

$$\mathbf{p}_1 \rightarrow \mathbf{p}_2,$$

ja toistin $\mathbf{p}_2$ kommunikoi Bobin sekä toistimen $\mathbf{p}_1$ kanssa,

$$\mathbf{p}_2 \rightarrow \{\mathbf{p}_1, \mathbf{b}\}.$$

Verkon jokaista linkkiä käytetään tasan kerran. Tätä prosessia kutsutaan verkoston hukuttamiseksi (eng. "*flooding*") tietokoneverkoissa.

Yleisissä kvanttihukutusprotokollissa $\mathcal{P}_{flood}$, verkosto alustetaan LOCC operaatioilla, jonka jälkeen Alice lähettää tilat kaikille naapuri toistimille. Tämän jälkeen suoritetaan uudet LOCC operaatiot kaikissa toistimissa, jonka jälkeen tilan saaneet toistimet kommunikoivat naapureidensa kanssa. Tätä jatketaan, kunnes jokainen Bobin naapuri noodi on kommunikoinut kerran Bobin kanssa. Kun hukuttaminen on toistettu n kertaa protokollaa $\mathcal{P}_{flood}$ käyttäen, voidaan määritellä verkon kapasiteetille arvo $\mathcal{C}^m(\mathcal{N})$. Lopulta verkon kapasiteetin ylärajaksi voidaan kirjoittaa:

$$\mathcal{C}^m(\mathcal{N}) \leqslant \min_C \mathcal{C}^m(C),$$

jossa

$$\mathcal{C}^m(C) := \sum_{(x,y)\in C} \mathcal{C}(\mathcal{E}_{xy})$$

on leikkauksen kokonaiskapasiteetti. [27]

Monimutkaisemmissa verkoissa useamman reitin kapasiteetti saadaan siis summaamalla mahdollisten reittien kapasiteetit. Yhden reitin kapasiteetin määrittää sen "heikoin lenkki"eli linkeistä se, jonka transmittiivisyys ja sitä kautta kapasiteetti on pienin.

2 Simulaatiot

Simulaatioissa käsiteltiin erilaisia kvantti-informatiikan verkkomalleja ja niiden ominaisuuksia. Simulaatioilla pyrittiin mallintamaan sekä kirjallisuudessa paljon käsiteltyjä Waxman- ja skaalavapaa (Barabási-Albert) verkkoja, että työhön kehitettyä mallia ja vertailemaan näiden ominaisuuksia. Itsekehitetyssä mallissa pyrittiin mallintamaan kommunikaatioverkkoja, joissa huomioitiin noodien maantieteellinen sijainti osana verkon rakentumista.

Koska sekä klassiset kommunikaatio verkot kuten internet sekä kvanttikommunikaatioverkot rakentuvat optisista kuitukaapeleista, joissa fotonit toimivat informaation välittäjinä, mallinnettaessa linkkien ominaisuuksien oletetaan vastaavan huippuluokan optisten kuitujen ominaisuuksia. Linkkien pituudet ovat kilometreinä. [45]

Optisissa kuiduissa informaation välittäjinä toimivat fotonit ovat alttiita hälylle, minkä seurauksena pelkästään optisia kuituja hyödyntäen pystytään viestimään vain noin 100 km matkalla. Tämän takia verkon noodien mielletään mallintavan kvanttitoistimia, jotka mahdollistavat kommunikaation pidemmälle. [36]

2.1 Python

Simuloinnit toteutettiin Python-ohjelmointikielellä, Visual Studio -ympäristössä ja koodin toteutuksessa hyödynnettiin NetworkX-, Matplotlib-, Seaborn- ja NumPy-kirjastoja. NetworkX-kirjasto on kompleksisten verkkojen rakenteen, ominaisuuksien ja dynamiikoiden kuvaamiseen ja käsittelyyn luotu Python kirjasto. Seaborn-, NumPy- ja Matplotlib kirjastoja käytettiin datan matemaattiseen käsittelyyn sekä saatujen tulosten esittämiseen kuvaajien muodossa.

Mallien ominaisuuksien käsittelyn helpottamiseksi verkoille määritettiin vierus-, etäisyys- ja minimileikkausmatriisit sekä kapasiteetilla painotettu vierusmatriisi.

Matriiseista luodut jakaumien kuvat on esitetty Mathplotlib- ja Seaborn- kirjastojen avulla. Kuvissa joissa data on esitetty histogrammina ja siihen on sovitettu kuvaaja, on sovitus tehty Seabornin histplot-funktiolla. Tällöin kuvaaja on approksimaatio jakaumasta. Tästä poikkeus on epähomogeenisen mallin jakaumille tehdyt sovitukset, joissa on käytetty Scipyn stats-moduulia, sekä sen normaalijakauma, log-normaalijakauman ja potenssilain mukaisen jakauman funktioita. Funktioita hyödynnettiin jakaumien muodon määrittämisessä, näitä jakaumia on listattu Tuloksia-kappaleen alaluvussa Vertailu.

2.2 Oletukset

Verkkojen rakennetta kuvataan graafilla. Koska kvanttikommunikaatioverkkojen noodeilla on maantieteellinen sijainti, määritettiin jokaiselle noodille koordinaatit (**x, y**) -koordinaatistoon. Mallintamisen yksinkertaistamiseksi, oletetaan että jokaiselle linkille noodien etäisyys $\sqrt{(\mathbf{x}-\mathbf{x}')^2+(\mathbf{y}-\mathbf{y}')^2}$ ja niiden välisen kanavan pituus *D(**x**, **x**')* ovat samat. Waxman- sekä skaalavapaan mallin graafien noodeille valitaan koordinaatit satunnaisesti

$$\Omega \equiv [0,R] \times [0,R],$$

laatikosta, jonka pinta-ala on R^2. Tällöin suurin mahdollinen etäisyys kahden noodin välillä $L = \sqrt{2}R$. [43]

Waxman- ja skaalavapaa verkkomalleja varten tehdyt oletukset pohjaavat lähteessä [45] esiteltyihin, huipputeknologiaa edustaviin valokuituverkkoihin.

Linkit noodien välillä mallintavat bosonisia kanavia, joissa transmissiivisyys, joka kuvaa kanavan häviöllisyyttä, saadaan kaavasta

$$\eta = 10^{-\gamma D(x,x')}, \tag{21}$$

ja jossa huipputason valokuitukaapelissa γ on 0,2 dB/km.

Toisin kuin klassisessa kommunikaatiossa, kvantti-informatiikassa siirtonopeus jokaiselle linkille on kanavan häviöllisyyden rajoittama. Tätä siirtonopeutta kuvataan kanavan kapasiteetilla, jonka yläraja on PLOB-raja:

$$\mathcal{C}_E(E_{x,x'}) = -\log_2(1-\eta) = -\log_2(1-10^{-\gamma D(x,x')}) \tag{22}$$

riippumatta energiasta. Noodeille voidaan määrittää kapasiteetilla painotettu aste summaamalla noodiin liittyneiden linkkien kapasiteetit eli

$$\mathcal{C}_N(x) = \sum_{x' \in \mathcal{N}(x)} \mathcal{C}_E(E_{x,x'}). \tag{23}$$

Tällöin päästä päähän kapasiteetti noodi parille saadaan ratkaistua selvittämällä niiden välisen minimileikkauksen. Leikkaus noodien x ja x' välillä on joukko linkkejä, joiden poistaminen katkaisee yhteyden niiden välillä. Kapasiteetti päätenoodien välillä on tällöin niiden välinen linkkien kytkeytyvyys (eng. *"edge connectivity"*)

$$\mathcal{C}(x, x') = \min_{U_{x,x'}} \mathcal{C}_U(U_{x,x'}) \equiv \min_{U_{x,x'}} \sum_{E_{y,y'} \in U_{x,x'}} \mathcal{C}_E(E_{y,y'}).$$

[45].

Verkkomallien ominaisuuksia eri parametreillä on esitetty kuvissa Tuloksia -kappaleessa. Kullakin parametrikombinaatiolla on generoitu yksi verkko, jonka ominaisuuksia analysoidaan. On huomionarvoista, että satunnaisverkkojen luonteesta johtuen eri simulointikerroilla verkon ominaisuudet voivat vaihdella, vaikka parametrit pysyisivät samoina. Tämä voi johtaa näennäisiin eroihin eri verkkomallien välillä tai satunnaisvaihtelu saattaa peittää joitain eroja ominaisuuksissa. Koska eri malleja on tutkittu ja verrattu toisiinsa useilla parametrikombinaatioilla, oletetaan että satunnaisuuden vaikutus jää vähäiseksi verrattuna mallien ja parametrien välisten erojen suuruuteen.

Waxman-malli

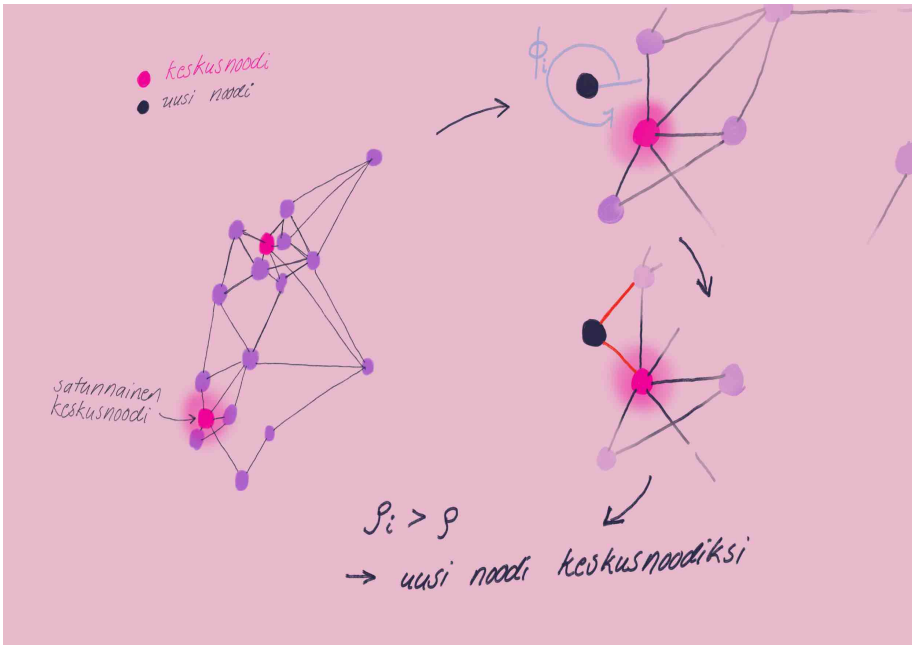
Waxman-mallissa noodit sijoitetaan satunnaisesti laatikko alueeseen, jonka jälkeen niiden välille luodaan linkit todennäköisyydellä

$$\Pi(x, x') = \beta e^{-D(x,x')/\alpha L},$$

jossa $D(x, x')$ on etäisyys noodien välillä, L on suurin mahdollinen etäisyys laatikossa ja α on vakio, joka valittiin vastaamaan amerikkalaista huippuvalokuituoptiikkaa, jolloin $\alpha L = 226$ km [45]. Beta saa arvoja väliltä $0 < \beta \leqslant 1$ ja kontrolloi linkkien tiheyttä, useimmiten β:n arvoksi valitaan 1.

Skaalavapaa malli

Skaalavapaassa mallissa verkko rakentuu dynaamisesti: kun jokainen noodi x lisä-



Kuva 8: Epähomogeeniselle mallille uuden noodin lisääminen verkkoon. Pinkit noodit ovat keskusnoodeja, joista valitaan yksi satunnaisesti verrattavaksi noodiksi uudelle, tumman siniselle, noodille. Uudelle noodille määritetään kulma, joka määrittää mihin suuntaan keskusnoodista nähden uusi noodi lisätään. Tämän jälkeen uudesta noodista lisätään uudet m_i linkkiä lähimpiin noodeihin. Uudelle noodille annetaan satunnainen lukuarvo väliltä (0,1) ja jos tämä luku ylittää annetun raja arvon ρ, lisätään uusi noodi keskusnoodien joukkoon.

tään verkkoon, se liitetään m:n toiseen jo olemassa olevaan noodiin verkossa[20]. Noodeille myös määritetään satunnaiset koordinaatit $R\times\ R$ laatikossa. Todennäköisyys sille, että noodi *x'* yhdistyy lisättyyn noodiin x on verrannollinen sen nykyiseen asteeseen *c(x')* sekä kääntäen verrannollinen noodien väliseen etäisyyteen *D(x,x')*:

$$\Pi(x, x') \propto \frac{c(x')}{D(x, x')}.$$

Epähomogeeninen malli

[20]Kuitenkaan lisättävien linkkien lukumäärä ei voi ylittää verkossa jo olevien noodien lukumäärää.

Simulaatioihin kehitettiin myös uusi satunnaisverkkomalli. Mallin tavoitteena oli kehittää verkko, jonka noodit eivät ole tasaisesti jakautuneet $R \times R$ laatikkoon[21], vaan verkkoon syntyy selkeästi nooditiheydeltään suurempia alueita sekä noodeja, joiden aste on verrattain korkea. Malli myös nimettiin tämän ominaisuuden mukaan, sillä sen noodit ovat epähomogeenisesti jakautuneet verkkoon.

Epähomogeenisen mallin uuden noodin lisäys on esitetty kuvassa 8. Siinä ensin arvotaan jokin keskusnoodeista (kuvassa pinkit noodit), määritetään uuden noodin kulma, joka määrää suunnan keskusnoodista, johon uusi noodi (kuvassa tummansininen) lisätään. Tämän jälkeen uudesta noodista lisätään m_i uutta linkkiä olemassa oleviin lähimpiin noodeihin. Lopuksi uudelle noodille annetaan satunnainen lukuarvo väliltä (0,1) ja tämän ylittäessä annetun raja arvon ρ, lisätään uusi noodi keskusnoodien joukkoon.

Mallissa parametrin n verran noodeja lisätään dynaamisesti verkkoon ja niistä yhdistetään linkit lähimpiin olemassa oleviin noodeihin. Noodi lisätään etäisyydelle r, joka noudattaa puolinormaalijakaumaa[22] ja lisättyä noodia verrataan yhteen verkossa jo olevaan noodiin. Noodeja, joihin uusia noodeja verrataan, nimitettiin simulaatiossa keskusnoodeiksi. Keskusnoodit tallennettiin erilliseen listaan, alkaen ensimmäisestä noodista, jonka jälkeen jokaisen lisätyn noodin kohdalla arvottiin, lisätäänkö se keskusnoodeihin. Yhtenä parametrina työssä käytettiin herkkyysrajaa ρ[23], joka määrittää kuinka todennäköisesti noodi lisätään keskusnoodiksi. Tämä toteutettiin arpomalla satunnaisluku väliltä [0, 1) ja jos tämä luku ylitti annetun raja-arvon, lisättiin noodi keskusnoodiksi. Uusia noodeja siis verrataan satunnaiseen

[21]Mallista kehitettiin myös versio, jossa aluetta johon noodit lisätään ei rajoitettu, vaan noodit lisättiin vapaasti satunnaiselle etäisyydelle keskusnoodista

[22]Normaalijakauma on jatkuva todennäköisyysjakauma, joka kuvaa satunnaismuuttujan saamia reaalilukuarvoja. Sen todennäköisyyden tiheysfunktioon $f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, jossa μ on jakauman odotusarvo/keskiarvo ja σ^2 on varianssi [41]. Puolinormaalijakauma on positiivisille reaaliluvuille soveltuva todennäköisyysjakauma, jonka tiheysfunktio on: $f(x) = \frac{\sqrt{2}}{\sigma\sqrt{\pi}} e^{-\frac{x^2}{2\sigma^2}}$ [39].

[23]Herkkyysrajalle ρ voidaan antaa arvoja välillä [0, 1), oletusarvoksi ρ:lle asetettiin 0.99.

keskusnoodiin.

Lisätylle noodille määritettiin myös suunta/kulma ϕ. Ensimmäiselle noodille arvottiin kulma ϕ_0 satunnaisesti väliltä $[0,\ 2\pi)$ sekä satunnaiset koordinaatit (textbfx, $\mathbf{y}$), joiden arvot ovat väliltä $(0,\ R)$. Seuraavia kulmia ϕ verrattiin edellisen lisätyn noodin kulmaan, jota käytettiin normaalijakauman odotusarvona. Jakauman keskihajonnaksi valittiin 0.1. Uusien noodien koordinaatit saatiin seuraavasti:

$$x_i = x + r * \cos(\phi)$$

$$y_i = y + r * \sin(\phi).$$

Noodienkertyminen reunoille estettiin arpomalla uusi kulma väliltä $[0,\ 2\pi)$, jos edellinen noodi oli liian lähellä reunaa[24]. Koska rajatussa laatikossa lisätyt noodit saattoivat saada koordinaatteja laatikon ulkopuolelta, hylättiin tapaukset, joissa noodi olisi lisätty laatikon ulkopuolelle ja arvottiin tällöin uusi etäisyys ja kulma noodille.

Uudesta noodista lisättävien linkkien lukumäärä m_i noudattaa normaalijakaumaa, jonka odotusarvo on parametri m ja keskihajonta 0.5. Lisättäviä linkkejä oli kuitenkin aina vähintään yksi ja lisättävien linkkien lukumäärä ei voinut ylittää verkossa jo olevien noodien lukumäärää. Uudet linkit lisättiin lähimpiin m_i noodiin.

2.3 Verkkojen vertailuissa käytetyt ominaisuudet

Eri verkkomallien vertailun helpottamiseksi, määritetään kaikille verkoille useita jakaumia kuvaamaan mallien ominaisuuksia.

Astejakauma

Ensimmäiseksi jokaiselle verkolle määritetään vierusmatriisi, jossa alkio $A_{i,j}$ on yksi, jos noodien i ja j välillä on linkki ja nolla muutoin. Jokaisen rivin summa on vastaavan noodin aste:

$$c_i = \Sigma_j A_{ij}.$$

[24]Herkkyydeksi reunan läheisyydelle valittiin 5 % laatikon särmästä.

Nämä asteet esitetään astejakaumina etäisyyden suhteen. Verkoille määriteettiin myös kapasiteetilla painotetut astejakaumat, joissa jokainen noodien välinen linkki on kerrottu sen asteella ja summattu samoin kuin astejakaumassa.

Etäisyysjakauma

Verkon rakenteen tutkimiseksi kaikille verkoille muodostetaan etäisyysmatriisit, joissa alkio $D_{i,j}$ on noodien i ja j välinen etäisyys (x,y)-koordinaatistossa, laskettuna:

$$D_{ij} = \sqrt{\Delta x_{ij}^2 + \Delta y_{ij}^2}.$$

Etäisyydet esitetään tiheysfunktiona, jossa y-akselilla on esiintymistodennäköisyys kullekin x-akselilla olevalle etäisyyden arvolle.

Kapasiteettijakauma

Koska kommunikaation kannalta yksi tärkeimpiä verkon ominaisuuksia on sen kapasiteetti, määritetään verkoille kapasiteettimatriisi etäisyys- ja vierusmatriisin avulla, jossa linkeille lasketaan etäisyydestä riippuva ideaalikapasiteetti PLOB-rajan mukaisesti, kaavasta:

$$C(D_{ij}) = -\log_2(1 - 10^{-\frac{\gamma \times D_{ij}}{10}}),$$

jossa gamma on huippuluokan valokaapelien mukainen[25].

Koska noodien välillä voi olla useita polkuja, määritettiin jokaisen noodiparin välille maksimikapasiteetti useaa riippumatonta polkua käyttäen, summaamalla jokaisen polun pienimmän[26] kapasiteetin linkkien kapasiteetit yhteen. Tämä vastaa alla käsiteltävää minimileikkausta, jota hyödyntäen määritettiin noodiparien väliset maksimikapasiteetit, jotka esitetään etäisyyden funktiona Tuloksia-kappaleessa.

[25] $\gamma = 0{,}2$

[26] Pienimmän kapasiteetin linkki on pullonkaula kommunikaatiolle polulla.

Minimileikkausjakauma

Toinen kommunikaation kannalta tärkeä ominaisuus verkoissa on sen noodien väliset minimileikkaukset. Verkoille määritettiin minimileikkausmatriisit, joissa laskettiin minimileikkausten arvot eri noodiparien *(i,j)* välillä ja joissa linkit painotettiin niiden kapasiteeteilla. Verkoille määritettiin minimileikkausmatriisit NetworkX kirjastoa hyödyntäen. Minimileikkaus kahden noodin välillä kuvaa suurinta mahdollista kapasiteettia tiedonsiirrolle noodista toiseen. NetworkX:n minimum_cut_value() -funktio käyttää maksimivirtauksen minimileikkausteoriaa eli minimileikkauksen kapasiteetin arvo vastaa maksimivirtauksen virtausarvoa [1]. Minimileikkausjakauma esitettiin minimileikkausten tiheysfunktiona.

Minimileikkaus ja painotettu aste

Noodiparien välistä minimileikkausta verrataan myös parin painotetun asteen minimiin eli verrataan noodiparien painotettuja asteita ja valitaan niistä pienempi. Näiden kuvaajat esitetään samassa kuvassa, jotta voidaan verrata niiden yhtenevyyttä. On huomion arvoista, että kapasiteetilla painotettujen asteiden minimin kuvaaja asettaa ylärajan minimileikkausten kuvaajalle. Kuvaajien erotessa suuresti, on verkossa noodien välillä pienemmän kapasiteetin linkki, joka muodostaa pullonkaulan kommunikaatiolle ja joka aiheuttaa minimileikkauksen pienemmät arvot verrattuna painotettuun asteeseen. Kuvaajat eivät voi sijoittua toisinpäin, sillä se tarkoittaisi, että verkossa siirretään enemmän informaatiota kuin päätenoodista voi lähteä tai mitä toinen päätenoodi voi vastaanottaa.

Jokaiselle verkolle luotiin myös NetworkX-kirjastolla graafi, johon tallennettiin verkon noodit koordinaatteineen sekä linkit kapasiteetteineen, verkkojen rakenteen kuvaamiseksi.

3 Tuloksia

Tässä kappaleessa esitetään eri verkkomalleille saatuja tuloksia, miten ne vertautuvat toisiinsa, sekä mitkä ominaisuudet tekevät mallista hyvän.

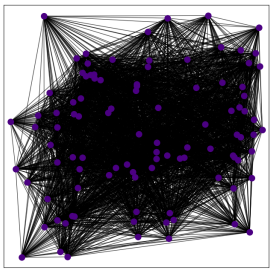
3.1 Waxman-malli

Waxman-mallin simulointi toteutettiin teoria kappaleen mukaisesti. Waxman-mallin tutkimiseksi luotiin $R \times R$ laatikko (R:n arvoilla 200 ja 600), johon lisättiin N noodia (100 ja 200) satunnaisin koordinaatein. Noodien etäisyyksien avulla laskettiin verkolle todennäköisyysmatriisi, jossa todennäköisyydet linkille tiettyjen noodien välillä laskettiin kaavalla 18. Verkkoon arvottiin todennäköisyysmatriisista linkit noodien välille. Verkoista on esimerkkejä kuvassa 9, joista voidaan nähdä noodien ja niiden välille luotujen linkkien levittyneen tasaisesti laatikon sisään.

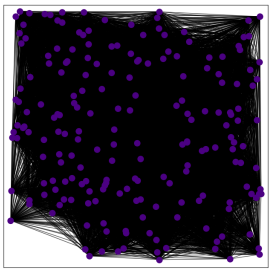
Waxman-mallin kuvaamiseksi tutkittiin sen statistisia ominaisuuksia, luomalla kuvaajat esittämään verkkojen eri jakaumia. Etäisyysjakauma, astejakauma, todennäköisyysjakauma ja kapasiteettijakauma on esitetty vastaavasti kuvissa 10, 11 ja 13.

Waxman-mallin astejakauma noudattaa Poisson-jakaumaa, mikä näkyy erityisesti suuremmilla noodien määrillä, kuten kuvassa 11b. Tämä vastaa myös *Zhuang et al.* tuloksia lähteessä [45]. Astejakaumille luotiin myös kapasiteetilla painotetut jakaumat, jotka on esitetty kuvissa 12.

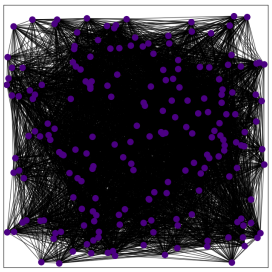
Myös saadut etäisyysjakaumat noudattavat Poisson-jakaumaa, kuten nähdään kuvista 10. Samassa kuvassa on myös esitetty vastaavien verkkojen todennäköisyyksien kuvaajia. Todennäköisyyskuvaajissa on esitetty mahdolliset todennäköisyydet linkin syntymiselle ja y-akselilla linkkien lukumäärä, joilla kyseinen todennäköisyys linkin syntymiselle esiintyy. Suuremmissa laatikoissa, joissa noodien tiheys on pienempi ja noodien väliset etäisyydet ovat suurempia, on todennäköisyysjakauma selkeästi pienille todennäköisyyksille painottunut, kuten kuvassa 10f. Voidaan havai-



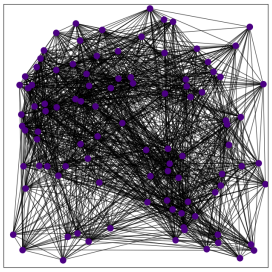
(a) Verkko, jossa N=100 ja R=200.



(b) Verkko, jossa N=200 ja R=200.



(c) Verkko, jossa N=200 ja R=600.



(d) Verkko, jossa N=100 ja R=600.

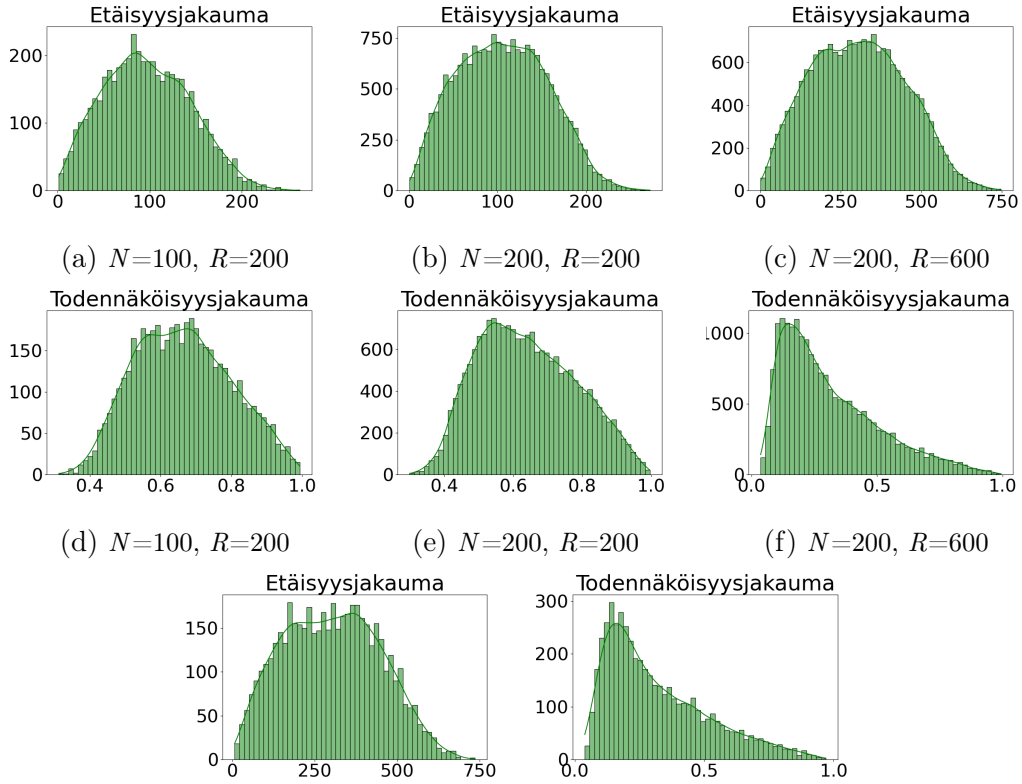
Kuva 9: Esimerkkiverkkoja eri noodi määrillä ja laatikoiden särmillä.

ta tämän vaikuttavan myös astejakaumaan, sillä suuremmilla muuttujan R arvoilla voidaan havaita pienempiä asteiden maksimiarvoja.

Esimerkkejä kapasiteettijakaumasta eri noodi määrillä sekä laatikon koilla on esitetty kuvassa 13. Vertaamalla kuvia 13a ja 13d voidaan nähdä, että laatikon särmän ollessa pienempi, linkkien pituudet ovat keskimäärin lyhyempiä, minkä seurauksena kapasiteetit pienemmissä laatikoissa ovat suurempia. Pienemmässä laatikossa nooditiheyden ollessa suurempi, on myös hajonta kapasiteeteissa pienempää, mikä näkyy kuvaajan tasaisuudessa. Vertaamalla kuvia 13a ja 13b voidaan nähdä, että noodien määrän ja sen myötä myös tiheyden kasvaessa, maksimikapasiteetti verkossa on suurempi ja yleisesti kapasiteettien arvot ovat suurempia. Maksimi etäisyydet noodien välillä eivät suuresti muutu noodien määrän muuttuessa. Nooditiheyden kasvu johtaa myös pienempään hajontaan kapasiteetin kuvaajassa.

Verkoista luotiin myös versiot, joissa linkkien väri ja vahvuus kuvaa sen kapasiteettia, jotta verkon rakenteesta on helpompi löytää korkeamman kapasiteetin linkit. Näitä on esitetty kuvassa 14. Esimerkiksi kuvien 14b ja 14c verkkoja vertaamalla voidaan nähdä, että pienemmillä R:n arvoilla kapasiteetit saavat suurempia arvoja, mikä näkyy sinisten linkkien suurempana määränä. Tämä on seurausta lyhyistä linkkien pituuksista, kapasiteetin etäisyysriippuvuudesta johtuen. Kun laatikon sivu on 200, käytettiin rajana tummemmille linkeille kapasiteetin arvoa 1 ja laatikossa, jonka sivu on 600, käytettiin rajana tummemmille linkeille kapasiteetin arvoa 0.2. Jos laatikon koko pidetään vakiona ja noodien määrää eli nooditiheyttä kasvatetaan, lyhyiden linkkien ja sen myötä sinisten suuren kapasiteetin linkkien määrä myös kasvaa.

Minimileikkausjakaumia on esitetty kuvassa 15. Vertaamalla esimerkiksi kuvia 15b ja 15a, voidaan nähdä, että minimileikkaus saa arvoja laajemmalta alalta, kun noodien määrää laatikossa kasvatetaan. Nähdään myös, että pienemmässä laatikossa minimileikkauksen arvot ovat suurempia, esimerkiksi vertaamalla kuvia 15d ja

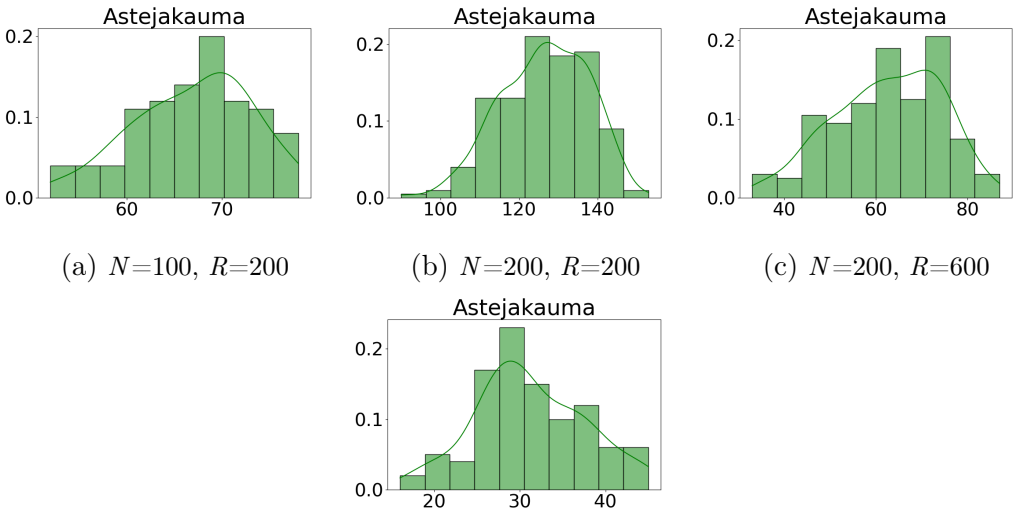


(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N=100, R=200 (e) N=200, R=200 (f) N=200, R=600

(g) N=100, R=600 (h) N=100, R=600

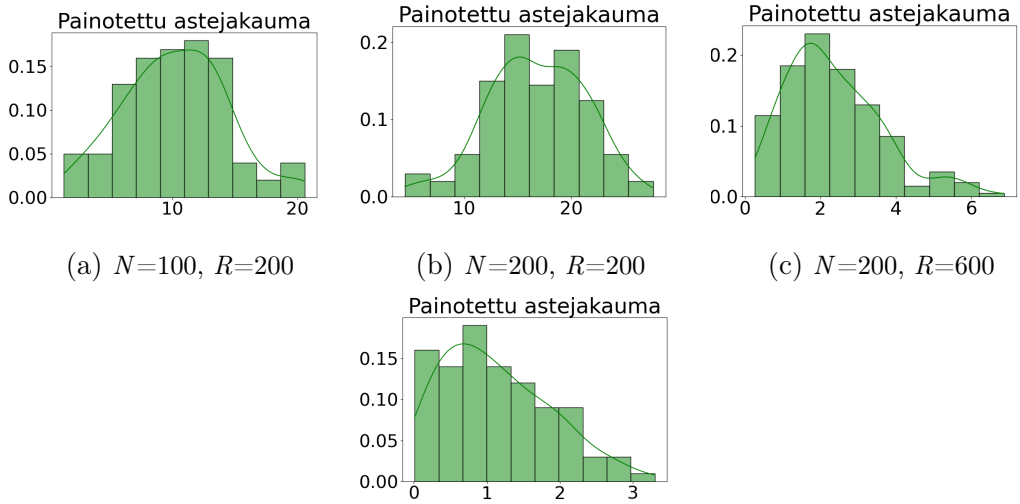
Kuva 10: Etäisyysjakaumia Waxman-mallin verkoista sekä niitä vastaavat linkkien muodostumisen todennäköisyysjakaumat.



(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N=100, R=600

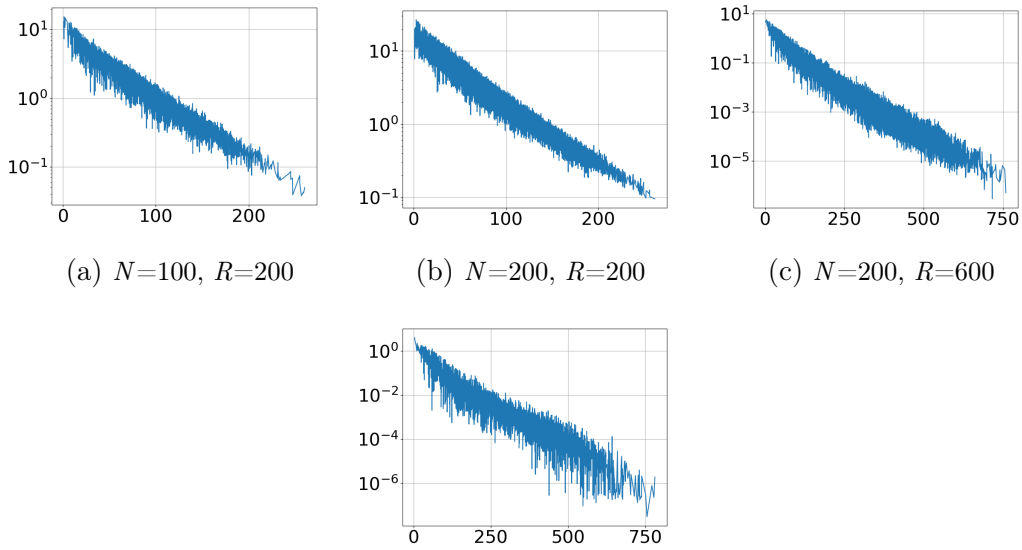
Kuva 11: Astejakaumia Waxman-mallin verkoista.



(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N=100, R=600

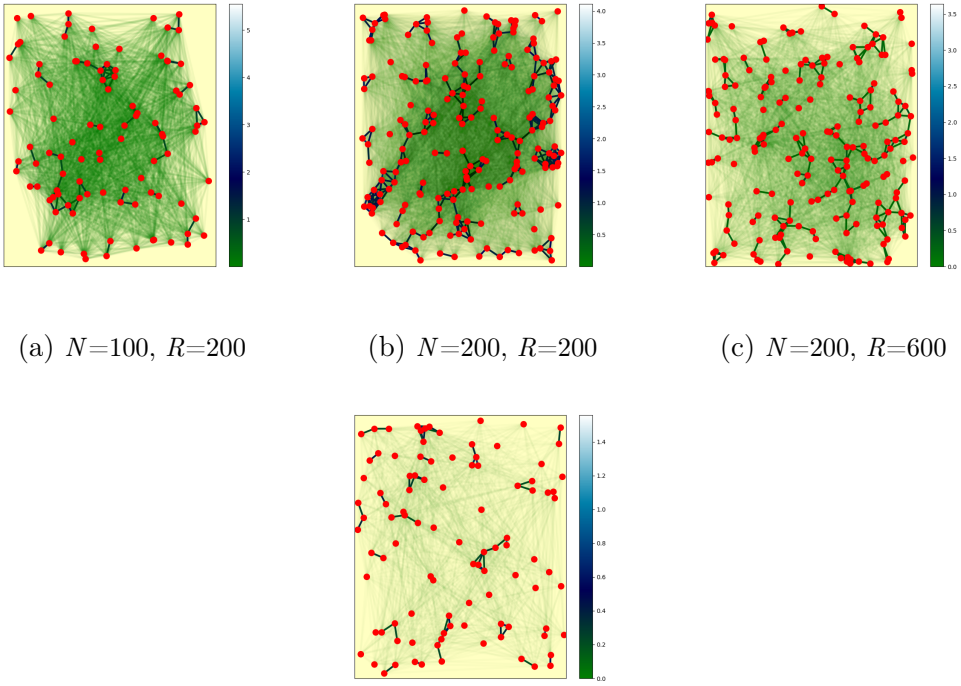
Kuva 12: Astejakaumia Waxman-mallin verkoista.



(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N=100, R=600

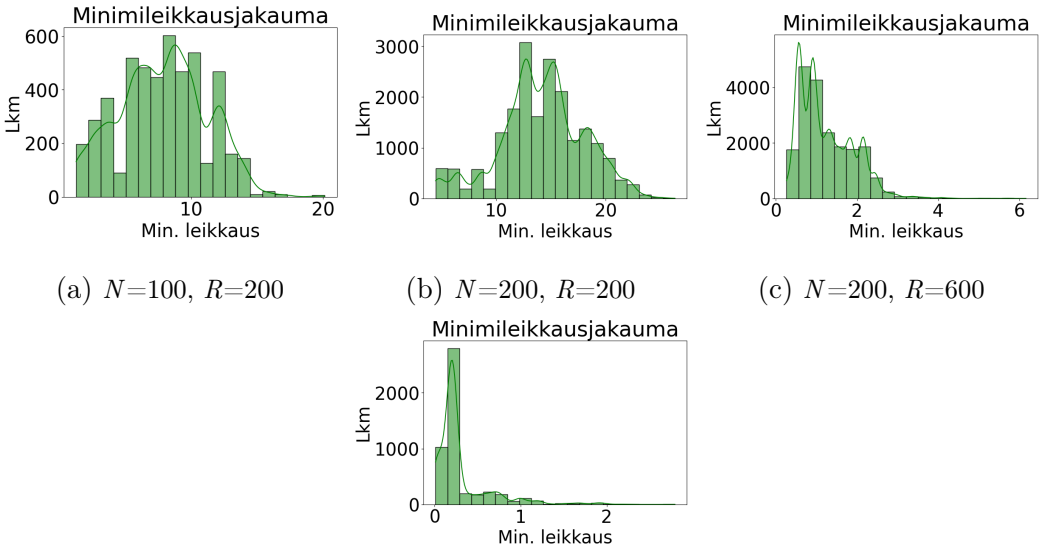
Kuva 13: Kapasiteettijakaumia Waxman-mallin verkoista. Jakaumissa kapasiteetin arvo on esitetty etäisyyden funktiona.



(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N=100, R=600

Kuva 14: Esimerkkiverkkoja eri noodi määrillä ja laatikoiden särmillä, joissa linkkien väri riippuu kapasiteetista. Tummat ja sinisemmät linkit ovat korkeamman kapasiteetin linkkejä. Kun laatikon särmä on 200, käytettiin rajana tummemmille linkeille 1 ja laatikossa, jonka sivu on 600, käytettiin rajana tummemmille linkeille 0.2 kapasiteetin arvoa.



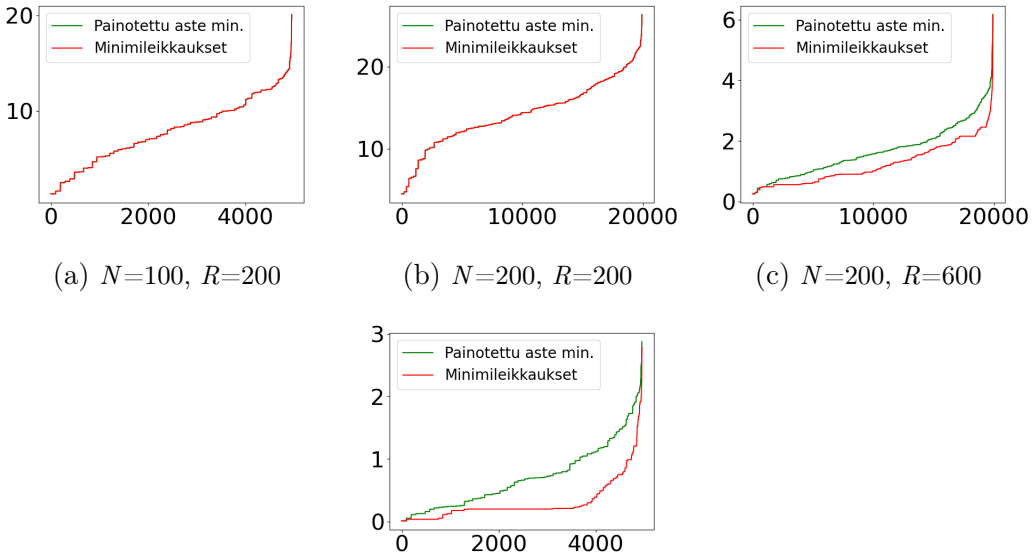
(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N on 100 ja R on 600.

Kuva 15: Minimileikkausjakaumia Waxman-mallin verkoista.

15a. Tämä on seurausta pienemmistä etäisyyksistä noodien välillä, joka johtaa suurempaan todennäköisyyteen linkeille. Nooditiheyden ollessa suuri eli kun noodien lukumäärä n on suuri ja laatikon särmä R on pieni, muistuttaa minimileikkausjakauma Poisson-jakaumaa ja minimileikkausten arvot ovat suurempia. Nooditiheyden pienetessä on jakauma vahvasti pienille arvoille painottunutta.

Mutta kuinka hyvin asteiden minimi ennustaa minimileikkausta? Tämän tutkimiseksi verrattiin asteiden minimiä, eli pääte noodien kapasiteetilla painotetun asteen minimiä, samojen noodien välisen minimileikkauksen arvoon. Tuloksia on esitetty kuvassa 16. Jokaiselle noodille määritettiin kapasiteetilla painotettu aste kaavasta 23 ja päätenoodien painotettujen asteiden arvoja verrattiin ja otettiin niiden minimi. Näitä arvoja verrattiin päätenoodien väliseen minimileikkaukseen. Kuvista 16 nähdään, että näiden arvot ovat hyvin lähellä toisiaan, mikä on oletettavissa Waxman-mallille, sillä noodien asteilla ja linkkien pituuksilla ja sitä kautta kapasiteeteilla on taipumus olla lähellä toisiaan, mikä näkyy myös verkkojen aste- ja etäisyysjakaumissa. Kuvia 16b ja 16c vertaamalla voidaan todeta, että laatikon kasvaessa minimileikkauksen ja asteiden minimin kuvaajat eroavat enemmän kuin pie-



(a) N=100, R=200 (b) N=200, R=200 (c) N=200, R=600

(d) N=100, R=600

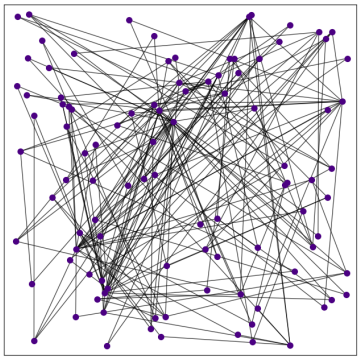
Kuva 16: Minimileikkauksia ja kapasiteetilla painotettuja asteita Waxman-mallin verkoissa.

nemmällä laatikon särmällä. Tällöin noodien välinen minimileikkaus saa pienempiä arvoja kuin noodien painotettujen asteiden minimi, erityisesti kuvaajien keskellä, mikä on seurausta noodien pienemmästä tiheydestä, joka tuottaa verkkoon heikomman kapasiteetin omaavia pitkiä linkkejä, jotka toimivat pullonkaulana. Toisaalta noodien lukumäärän kasvaessa, ovat kuvaajien arvot lähempänä toisiaan, kuten voidaan nähdä kuvista 16d ja 16c. Tämä on Waxman-mallille hyvin ominaista, koska molemmissa tapauksissa linkkien pituudet ovat lyhyempiä arvojen ollessa lähellä toisiaan, joka seuraa kapasiteetin sekä linkkien todennäköisyyden etäisyysriippuvuudesta.

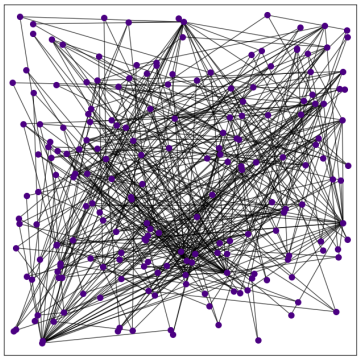
3.2 Skaalavapaa malli

Skaalavapaalle mallille simulaatiot toteutettiin Teoria- sekä Simulaatiot- kappaleiden mukaisesti. Mallin vertailtavuuden takaamiseksi tutkittiin verkoa sekä sen ominaisuuksia laatikoiden särmillä R (200 ja 600), noodien määrillä N (100 ja 200) sekä lisättävien linkkien lukumäärillä m (2 ja 3).

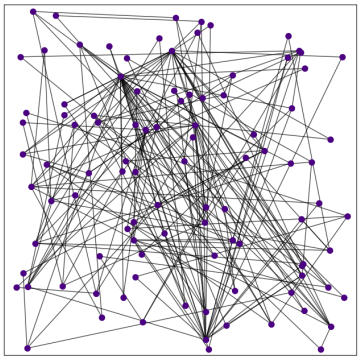
Kuvissa 17 on esitetty Barabási-Albert mallilla luotuja skaalavapaita verkko-



(a) $n = 100$, $m = 2$ ja $R = 200$.

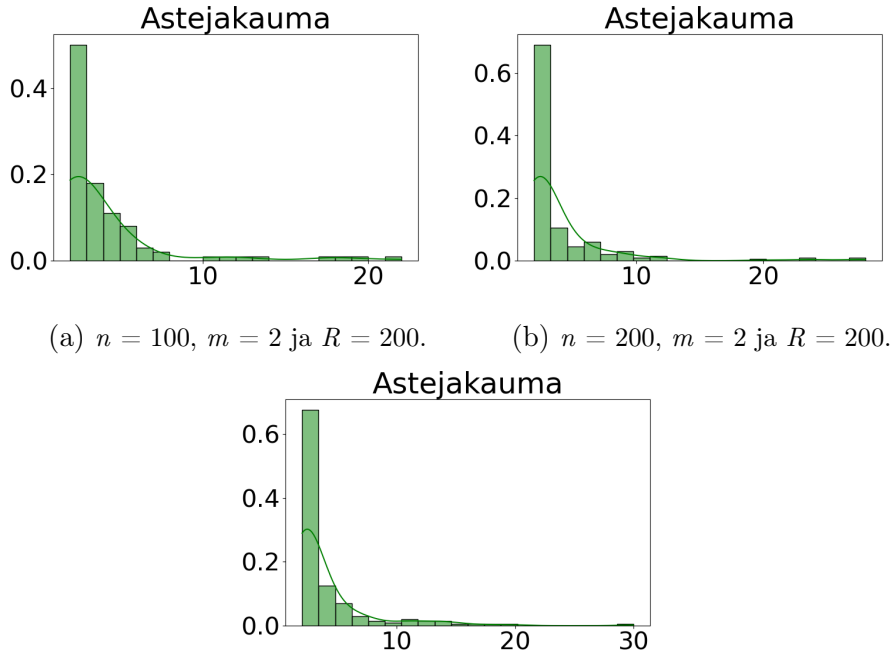


(b) $n = 200$, $m = 2$ ja $R = 200$.



(c) $n = 100$, $m = 2$ ja $R = 600$.

Kuva 17: Skaalavapaan mallin verkkoja, eri muuttujilla.



(a) $n = 100$, $m = 2$ ja $R = 200$.

(b) $n = 200$, $m = 2$ ja $R = 200$.

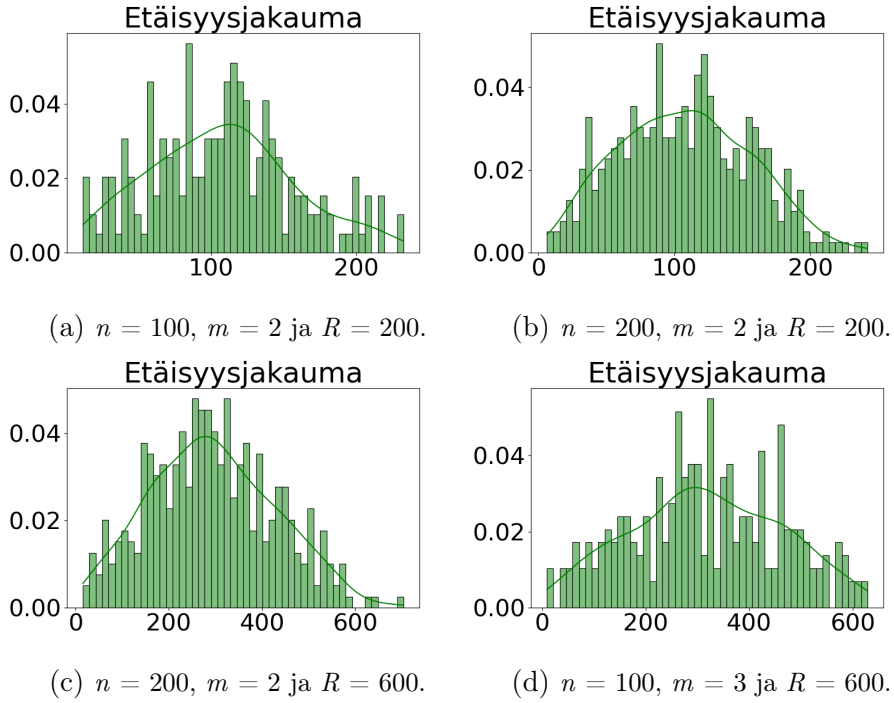
(c) $n = 200$, $m = 2$ ja $R = 600$.

Kuva 18: Skaalavapaan mallin astejakaumia, joissa x-akselilla esitetty mahdolliset asteet ja y-akselilla näiden todennäköisyys, eri muuttujien arvoilla.

ja. Erityisesti suuremmilla noodimäärillä voidaan nähdä selkeitä suuremman asteen noodeja, joista on luotu useita linkkejä muista noodeista. Tämä voidaan nähdä vertaamalla verkkoja 17a ja 17b. Noodien voidaan nähdä levittyneen tasaisesti laatikkoon ja myös korkeamman asteen noodit sijaitsevat satunnaisissa kohdissa verkkoa.

Kuten Teoria kappaleessa todettiin, noudattaa skaalavapaan mallin astejakauma potenssilakia. Tämä voidaan todeta myös kuvista 18, joissa erityisesti suurilla noodimäärillä, kuten kuvassa 18b, jakauma painottuu pieneille asteille ja skaalavapaalle mallille ominaisesti omaa pitkän hännän. Astejakauman käyttäytyminen vastaa myös kirjallisuudessa havaittua [45]

Kuvista 19 voidaan nähdä, että verkkojen etäisyysjakauma noudattaa vahvasti Poissonjakaumaa, mikä on seurausta noodien koordinaattien satunnaisuudesta. Jakaumassa voidaan havaita paljon vaihtelua rinnakkaisten etäisyyksien välillä, mutta jakaumalla havaitaan kuitenkin yksittäinen huippu. Laatikon koko vaikuttaa odote-



(a) $n = 100$, $m = 2$ ja $R = 200$.

(b) $n = 200$, $m = 2$ ja $R = 200$.

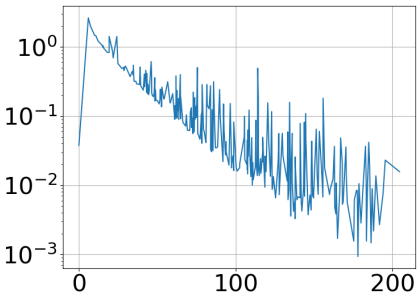
(c) $n = 200$, $m = 2$ ja $R = 600$.

(d) $n = 100$, $m = 3$ ja $R = 600$.

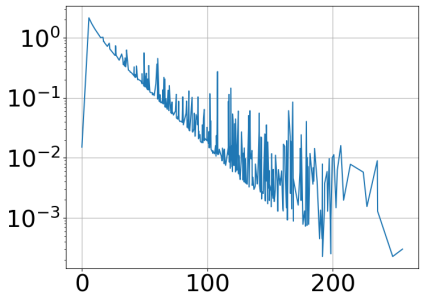
Kuva 19: Skaalavapaan mallin etäisyysjakaumia eri muuttujien arvoilla.

tusti noodien maksimietäisyyksiin, muttei jakauman muotoon, mikä voidaan nähdä kuvista 19b ja 19c. Noodien lukumäärn lisäys havaitaan jakaumissa suurempina esiintyminä yksittäisille etäisyyksille, linkkien lukumäärän kasvaessa.

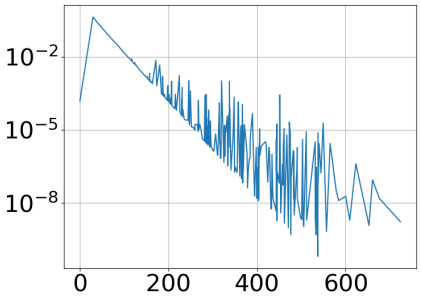
Skaalavapaiden verkkojen kapasiteetteja noodien etäisyyden suhteen on esitetty kuvassa 20. Kuvaajista havaitaan pienten muutosten etäisyyksissä aiheuttavat suurta vaihtelua kapasiteeteille saatavissa arvoissa ettäisyyksien ollessa suuria. Kuvaajien alussa esiintyvä piikki on seurausta noodien satunnaisesta asettelusta laatikkoon, joka aiheuttaa tilanteita, joissa noodit ovat lähellä toisiaan, mutta niiden välillä ei ole linkkejä, ja kommunikaatio tapahtuu jonkin kaukana olevan noodin kautta. Kuvista voidaan nähdä, että laatikon kasvaessa etäisyydet noodein välillä kasvavat ja verkoissa esiintyvien linkkien kapasiteetit saavat pienempiä arvoja. Koska kapasiteetti on etäisyydestä riippuva, suurimmat erot kapasiteettien kuvaajissa on eri särmän pituuksien välillä ja pienimmät kapasiteetin arvot saadaankin pienillä nooditiheyksillä.



(a) $n = 100$, $m = 3$ ja $R = 200$.

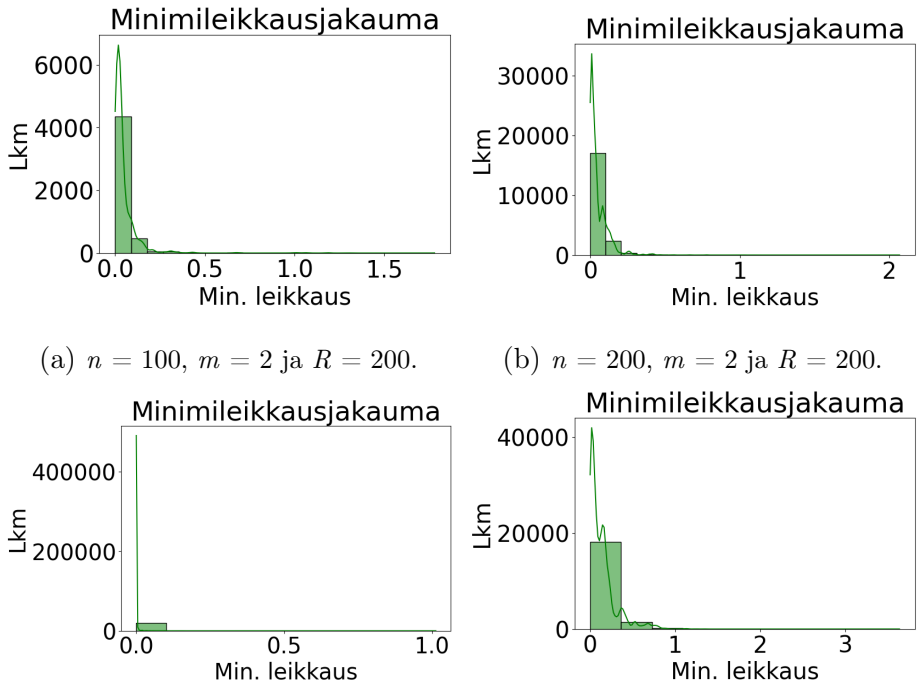


(b) $n = 200$, $m = 2$ ja $R = 200$.



(c) $n = 100$, $m = 3$ ja $R = 600$.

Kuva 20: Skaalavapaan mallin kapasiteettijakaumia. Jakaumissa kapasiteetin arvo on esitetty etäisyyden funktiona.



(a) $n = 100$, $m = 2$ ja $R = 200$.

(b) $n = 200$, $m = 2$ ja $R = 200$.

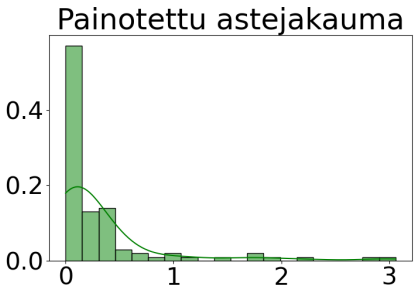
(c) $n =200$, $m = 3$ ja $R = 600$.

(d) $n =200$, $m = 3$ ja $R = 200$.

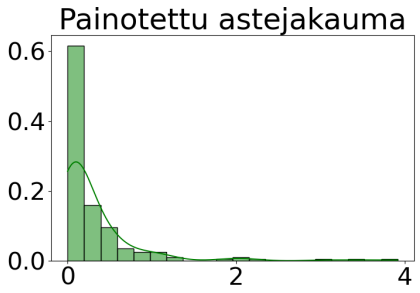
Kuva 21: Skaalavapaan mallin minimileikkausjakaumia eri muuttujien arvoilla.

Verkkojen kapasiteetilla painotettujen asteiden jakaumat noudattavat potenssilakia, mikä on odotettavissa astejakauman potenssilaki käyttäytymisen seurauksena. Näitä jakaumia on esitetty kuvissa 22. Myös minimileikkaukset skaalavapaalla mallilla noudattavat potenssilain mukaista jakaumaa, kuten voidaan nähdä kuvista 21. Kuvissa esitetty minimileikkauksen arvot tiheysfunktioina. Suurin osa minimileikkauksista on pieniä, mikä on seurausta skaalavapaan mallin ominaisuudesta keskittää linkit muutamaan keskusnoodiin, jolloin tähän noodiin vievän linkin leikkaamalla saadaan useimmat noodit erotettua muista verkon noodeista, erityisesti pienilä m:n arvoilla, kuten kuvassa 21a. Myös suurella R:n arvolla minimileikkauksen arvot ovat erityisen keskittyneitä jakauman alkupäähän.

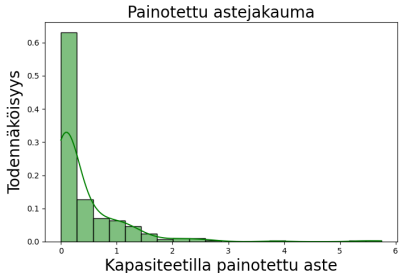
Kuvissa 23 on esitetty skaalavapaan verkon minimileikkauksia sekä kapasiteetilla painotetun asteen minimejä. Voidaan nähdä, että jokaisen verkon kuvaajat poikkeavat hieman toisistaan erityisesti painotetun asteen arvojen kasvaessa. Erot ovat suu-



(a) $n = 100$, $m = 2$ ja $R = 200$.

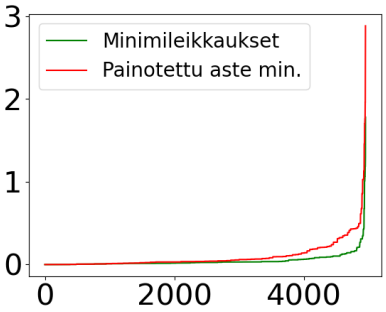


(b) $n = 200$, $m = 2$ ja $R = 200$.

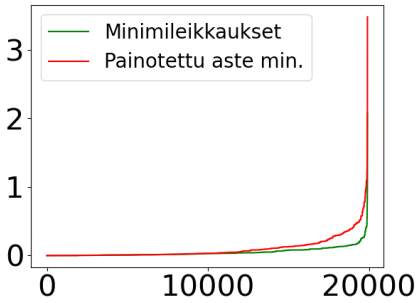


(c) $n = 300$, $m = 2$ ja $R = 200$.

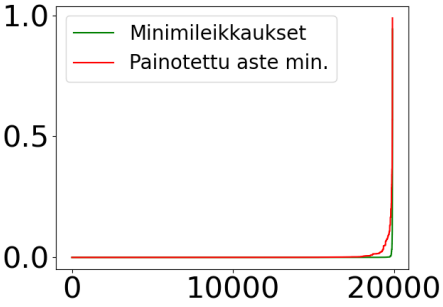
Kuva 22: Skaalavapaan mallin kapasiteetilla painotettuja astejakaumia.



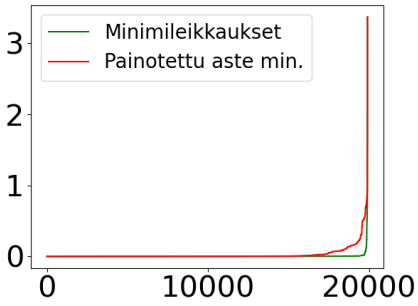
(a) $n = 100$, $m = 2$ ja $R = 200$.



(b) $n = 200$, $m = 2$ ja $R = 200$.



(c) $n = 200$, $m = 2$ ja $R = 600$.



(d) $n = 200$, $m = 4$ ja $R = 600$.

Kuva 23: Skaalavapaan mallin minimileikkaus sekä kapasiteetilla painotetun asteen minimi.

rempia muuttujan m arvon kasvaessa, mikä voidaan nähdä vertaamalla kuvia 23c ja 23d. Kuvista nähdään, että suurimmalle osalle satunnaisia noodipareja sekä minimileikkaus että painotettujen asteiden minimi ovat hyvin pieniä, mutta joillain noodipareilla arvot ovat isompia. Tämän voidaan olettaa johtuvan skaalavapaan mallin ominaisuudesta keskittää linkkejä yksittäsille noodeille, joilla minimileikkauksien arvot ovat suurempia.

3.3 Epähomogeeninen malli

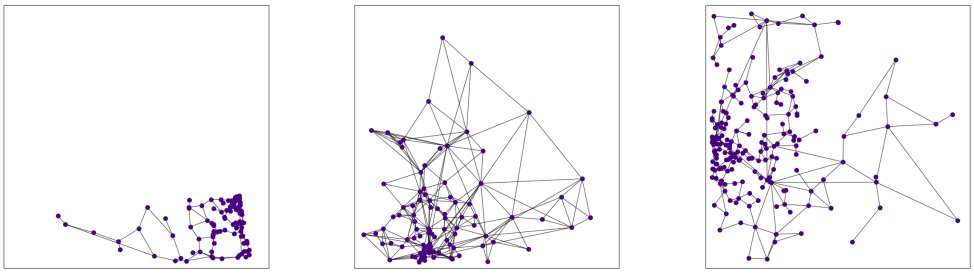
Epähomogeenisen satunnaisverkkomallin simulointi toteutettiin Simulaatiot kappaleen mukaisesti. Mallin tutkimiseksi luotiin sen mukaisia verkkoja laatikon särmän R arvoilla (200 ja 600), noodien n määrillä (100 ja 200), eri herkkyysrajoilla ρ (0.99 ja 0.999), sekä eri linkkien määrän odotusarvoilla m (2,3 ja 4). Joitain verkon ominaisuuksia tutkittiin myös isommilla noodimäärillä, mutta minimileikkauksien laskeminen verkoille kävi raskaaksi noodien lukumäärän kasvaessa, mikä rajoitti minimileikkausten vertailua.

Noodit lisättiin yksitellen verkkoon ja lisätessä niistä luotiin linkit osaan olemassa olevista noodeista. Valmiita verkkoja on esitetty kuvassa 24. Kuvista voidaan nähdä, että noodit eivät ole levittäytyneet tasaisesti alueelle, vaan verkkoon syntyy keskuksia, joissa noodien tiheys on suurempi kuin muualla verkossa sekä täysin noodivapaita alueita. Kuvia 24a ja 24c vertaamalla voidaan nähdä, että kun m, R ja ρ pidetään samoina ja noodien lukumäärää n kasvatetaan, täyttyy verkko tasaisemmin ja tyhjäksi jäävä alue on pienempi. Oletettavasti tämä on seurausta korkeasta ρ:n arvosta, jonka seurauksena keskusnoodien määrä on pienempi noodien lukumäärän ollessa pienempi, jolloin noodit keskittyvät harvempiin keskuksiin. Herkkyysrajan vaikutus verkon rakenteeseen voidaan nähdä myös kuvissa 24g ja 24f, joiden ominaisuudet ovat ρ:n arvoja lukuunottamatta samat. Tällöin suuremmalla ρ:n arvolla muodostetussa verkossa noodit ovat tiheämmin yhdessä keskuksessa, toisin kuin ρ:n

arvoa laskettaessa, jolloin noodit ovat levittäytyneet laajemmalle ja voidaan havaita, että verkkoon syntyy useampi nooditiheydeltään suurempi keskittymä. Tälläisiä keskittymiä esiintyi pienemmillä noodimäärillä, jos raja-arvoa ρ laskettiin tai jos korkealla raja-arvolla noodien lukumäärää kasvatettiin, kuten kuvissa 24i ja 24h. Koska ρ on raja-arvo yksittäisen noodin lisäämiselle keskusnoodiksi, on loogista, että pienillä noodimäärillä rajan täytyy olla pienempi, jotta jokin noodi lisätään keskusnoodiksi mahdollistaen usean keskuksen syntymisen. Linkkien odotusarvon muutos vaikutti enimmäkseen linkkien määrään noodien välillä, muttei muutoin verkon rakenteeseen, mikä voidaan nähdä kuvista 24c ja 24e. On huomionarvoista, että joillain muuttujien arvoilla verkko ei lähtenyt levittymään, kuten kuvassa 24a. Tämä on suurilta osin seurausta pienistä noodimääristä sekä korkeasta ρ:n arvosta, jolloin kaikki noodit keskittyvät yhden keskusnoodin lähelle.

Kun kaikki noodit ja linkit oli lisätty verkkoon, laskettiin kaikkien noodien väliset etäisyydet ja niitä hyödyntäen linkkien yhdistämille noodipareille kapasiteetit, samoin kuin Waxman-mallin verkoissa. Lisäksi verkon noodeille määritettiin asteet. Verkkojen etäisyysjakaumia on esitetty kuvaissa 25. Verkon etäisyysjakaumat ovat vahvasti jakauman alkuun painnottuneita, erityisesti raja-arvon ρ ollessa korkea sekä noodien lukumäärän ollessa pieni, esimerkiksi kuvassa 25d. Kuitenkin kun ρ:ta kasvatetaan, saa jakauma arvoja pienemmältä alalta, kuten kuvassa 25e. Linkkien odotusarvon m kasvattaminen tasoittaa jakaumaa, kuten nähdään kuvista 25a ja 25d. Myös laattikon särmän R muutoksen vaikuttavat jakauman leveyteen, sillä suuremmassa laatikossa pidemmät linkit ovat mahdollisia. Erityisen mielenkiintoista on huomata kuvassa 25f olevan jakauman kaksi huippua. Jos tätä verrataan vastaavan verkon kuvaan 24h, nähdään huippujen olevan seurausta kahdesta keskittymästä, joiden välillä esiintyy linkkejä.

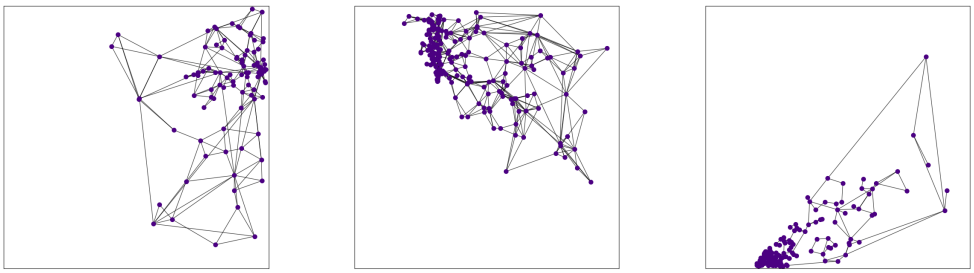
Kuvasta 26 nähdään mallin mukaisten verkkojen astejakaumien painottuneen jakauman alkupäähän, vaikkakin myös suurien asteiden noodeja löytyy. Astejakauma



(a) $n = 100$, $m = 2$, raja = 0.999 ja $R = 200$.

(b) $n = 100$, $m = 4$, raja = 0.99 ja $R = 200$.

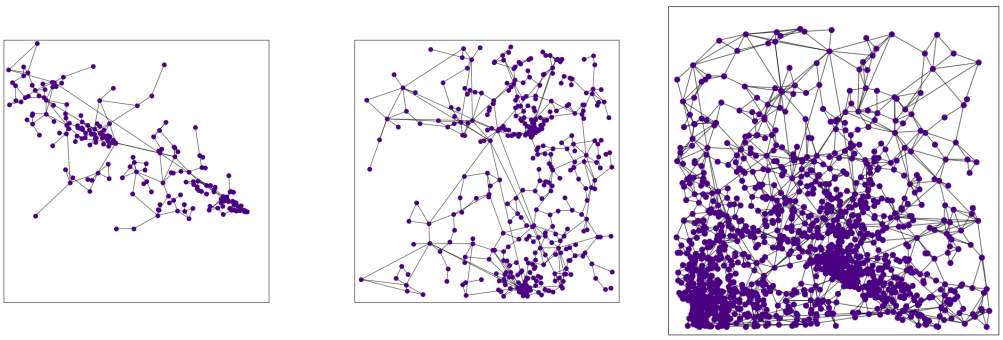
(c) $n = 200$, $m = 2$, raja = 0.999 ja $R = 200$.



(d) $n = 100$, $m = 3$, raja = 0.99 ja $R = 600$.

(e) $n = 200$, $m = 4$, raja = 0.999 ja $R = 200$.

(f) $n = 200$, $m = 2$, raja = 0.999 ja $R = 600$.

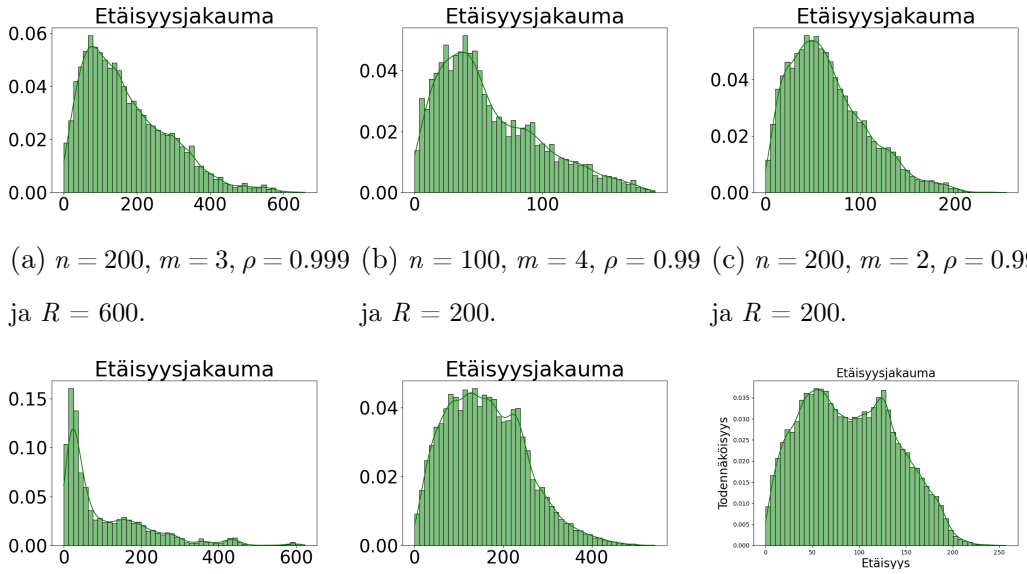


(g) $n = 200$, $m = 2$, raja = 0.99 ja $R = 600$.

(h) $n = 400$, $m = 2$, raja = 0.99 ja $R = 200$.

(i) $n = 1500$, $m = 3$, raja = 0.999 ja $R = 200$.

Kuva 24: Epähomogeenisen verkkomallin mukaisia verkkoja eri muuttujilla.

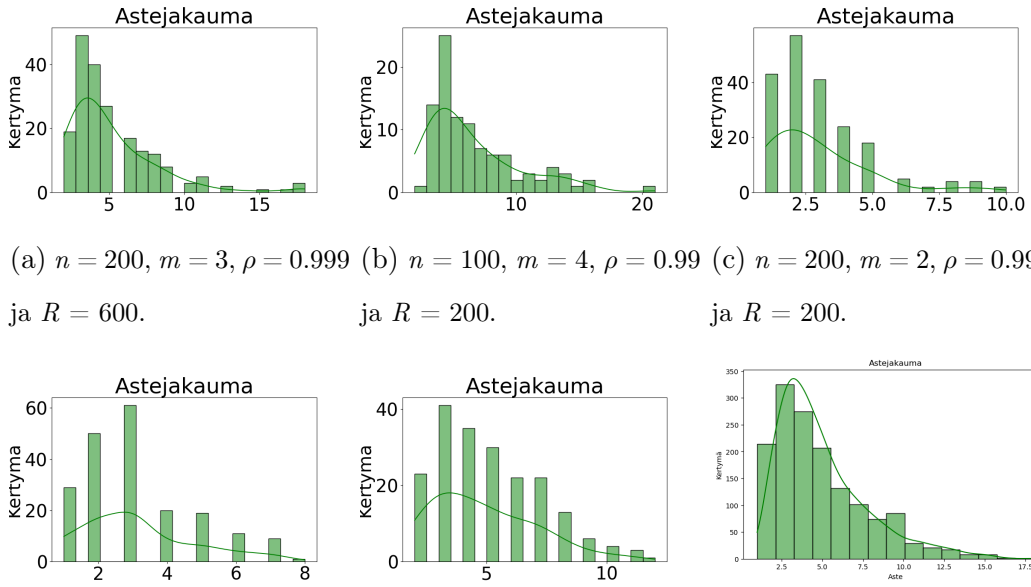


(a) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$. (b) $n = 100$, $m = 4$, $\rho = 0.99$ ja $R = 200$. (c) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 200$.

(d) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 600$. (e) $n = 200$, $m = 3$, $\rho = 0.99$ ja $R = 600$. (f) $n = 400$, $m = 2$, $\rho = 0.99$ ja $R = 200$.

Kuva 25: Epähomogeenisen verkkomallin mukaisia etäisyysjakaumia eri muutujien arvoilla.

on vahvasti painottunut pienille asteille ja erityisesti raja-arvon ollessa suuri ($\rho = 0.999$) sekä noodien lukumäärän kasvaessa, astejakauma muistuttaa enemmän log-normaalijakaumaa. Jakauman muoto määritettiin Scipyn tilastollisilla funktioilla, sovittamalla astejakauman histogrammiin eri jakaumien mukaisia kuvaajia ja niistä parhaiten jakaumaa kuvaava oli log-normaalijakauma. Laatikon koko ei juurikaan vaikuta verkon astejakaumaan. Sen sijaan herkkyysraja ρ vaikuttaa jakauman muotoon, kuten kuvissa 26e ja 26a. Pienemmällä ρ:n arvolla jakauman häntä jatkuu pidemmälle, mikä on oletettavissa, sillä vähemmän noodeja on mahdollisina keskuksina ja syntyy yksittäisiä noodeja, joilla on korkea aste. Linkkien odotusarvon m nostaminen nostaa verkossa olevien linkkien määrää, mikä näkyy kuvaajan pidempänä häntä. Noodien lukumäärän n muutokset vaikuttavat jakauman kertymien suuruuteen, sekä kasvattavat hieman maksimiasteiden arvoja. Tämä on seurausta kasvaneesta noodi- sekä linkkitiheydestä, sekä näistä johtuvasta keskusnoodien asteen kasvusta, joka johtaa pidempään häntään jakaumissa.



(a) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$.

(b) $n = 100$, $m = 4$, $\rho = 0.99$ ja $R = 200$.

(c) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 200$.

(d) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 600$.

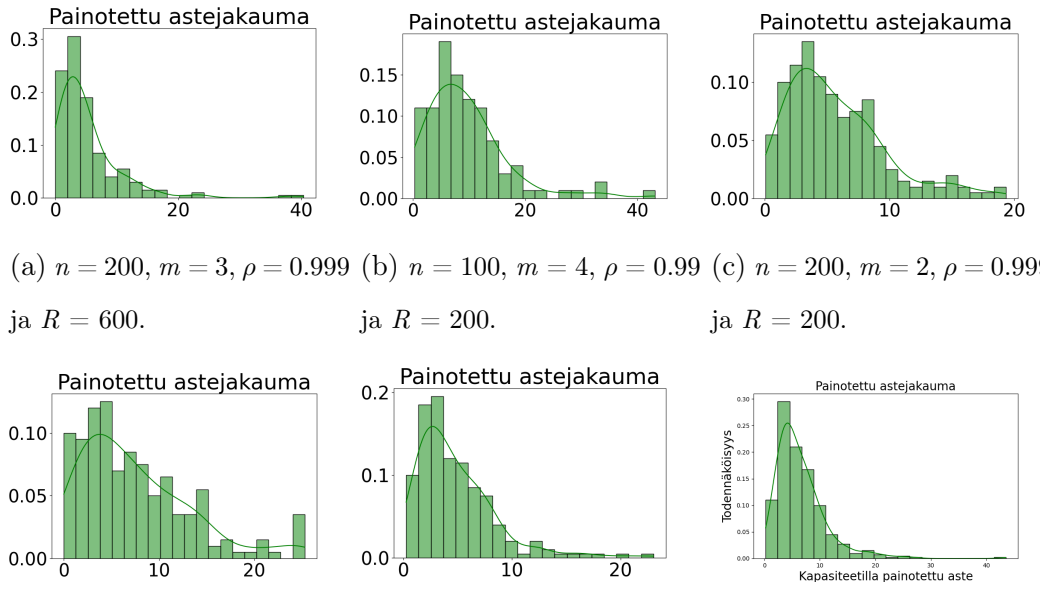
(e) $n = 200$, $m = 3$, $\rho = 0.99$ ja $R = 600$.

(f) $n = 1500$, $m = 3$, $\rho = 0.99$ ja $R = 600$.

Kuva 26: Epähomogeenisen verkkomallin mukaisia astejakaumia.

Verkolle määritettiin myös kapasiteetilla painotetut asteet, joiden jakaumia on esitetty kuvissa 27. Kun niitä verrataan astejakaumiin kuvassa 26, painottuvat asteiden arvot vielä selkeämmin jakauman alkupäähän. Toisaalta alkupäässä arvot jakautuvat tasaisemmin asteiden välille, kuten nähdään esimerkiksi kuvia 26b ja 27b vertaamalla.

Verkon kapasiteetteja on esitetty kuvassa 28. Kaikille jakaumille havaitaan suurempaa vaihtelua kapasiteetin arvoissa etäisyyden kasvaessa noodien välillä. Laatikon koon kasvaessa maksimietäisyydet noodien välillä kasvavat, mikä johtaa pienempiin minimikapasiteetteihin verkossa. Herkkysrajan ρ suuremmilla arvoilla verkko synnytti pienemmälle alueelle keskittyneitä verkkoja, mikä näkyy jakaumien etäisyyksissä, maksimietäisyyden kommunikaatiolle jäädessä pieneksi varsinkin noodien lukumäärän n ollessa pieni, esimerkiksi kuvassa 28a. Noodien lukumäärä n vaikuttaa verkon nooditiheyteen, joka yleensä lyhentää yksittäisten linkkien pituuksia, joka parantaa verkon kapasiteettia. Muuttujan m arvo vaikuttaa verkossa olevien link-



(a) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$.

(b) $n = 100$, $m = 4$, $\rho = 0.99$ ja $R = 200$.

(c) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 200$.

(d) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 600$.

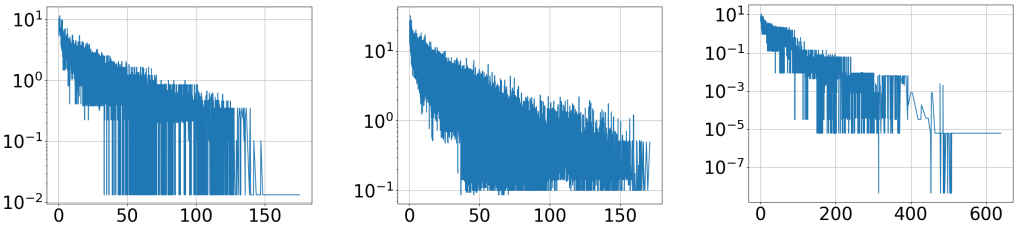
(e) $n = 200$, $m = 3$, $\rho = 0.99$ ja $R = 600$.

(f) $n = 400$, $m = 2$, $\rho = 0.99$ ja $R = 200$.

Kuva 27: Epähomogeenisen verkkomallin mukaisia, kapasiteetilla painotettuja astejakaumia.

kien määrään, jolloin linkkitiheys ja mahdollisten polkujen määrä verkossa kasvaa, joka johtaa suurempaan kapasiteettiin noodiparien välillä. Toisaalta suurilla noodimäärillä kuten kuvassa 28d noodiparin päästä päähän kapasiteetin arvo saattaa vaihdella paljonkin eri noodiparien välillä, joka johtaa hyvin paksuun jakaumaan.

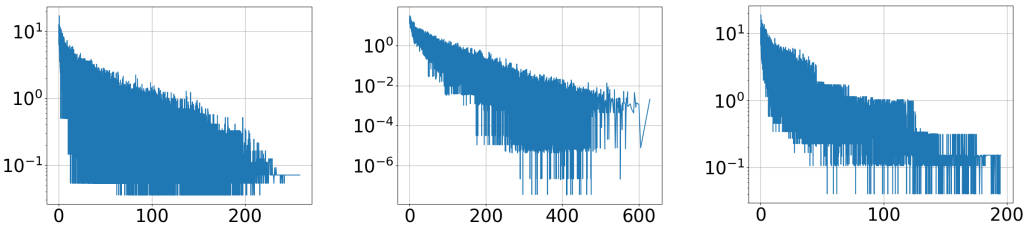
Kuvassa 29 on esitetty mallin minimileikkauksia. Kuten astejakaumatkin, ovat minimileikkausjakaumat hyvin painottuneita jakauman alkupäähän ja noudattavat likimain log-normaalijakaumaa. Raja-arvon ρ ollessa pieni, tämä painottuminen on vahvempaa, mikä nähdään mm. kuvasta 29c. Myös noodien lukumäärän n kasvaessa jakauman painottuminen on selkeämpää. Muuttujat R sekä m vaikuttavat minimileikkausten arvojen suuruuteen, m:n pienemmillä arvoilla minimileikkausten arvot ovat pienempiä (nähtävissä kuvista 29d ja 29e) ja pienellä R:n arvolla minimileikkaukset saavat tasaisemmin arvoja jakaumassa, kuten voidaan nähdä kuvista 29b ja 29e.



(a) $n = 100$, $m = 2$, $\rho = 0.999$ ja $R = 200$.

(b) $n = 200$, $m = 3$, $\rho = 0.99$ ja $R = 200$.

(c) $n = 100$, $m = 2$, $\rho = 0.99$ ja $R = 600$.

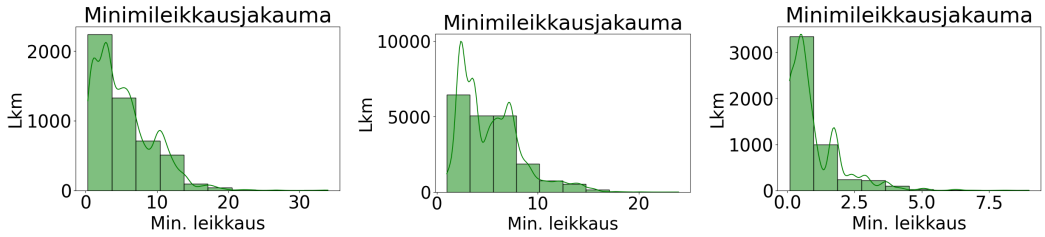


(d) $n = 400$, $m = 2$, $\rho = 0.99$ ja $R = 200$.

(e) $n = 200$, $m = 4$, $\rho = 0.999$ ja $R = 600$.

(f) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 200$.

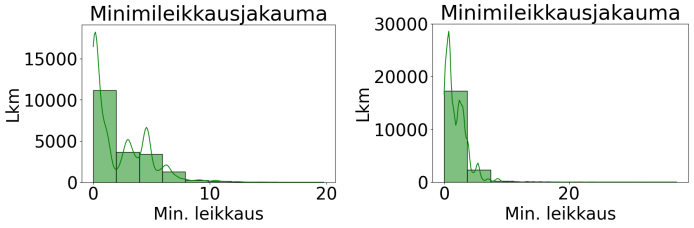
Kuva 28: Epähomogeenisen verkkomallin mukaisia kapasiteetin kuvaajia. Jakaumissa kapasiteetin arvo on esitetty etäisyyden funktiona.



(a) $n = 100$, $m = 4$, $\rho = 0.99$ ja $R = 200$.

(b) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 200$.

(c) $n = 100$, $m = 2$, $\rho = 0.99$ ja $R = 600$.

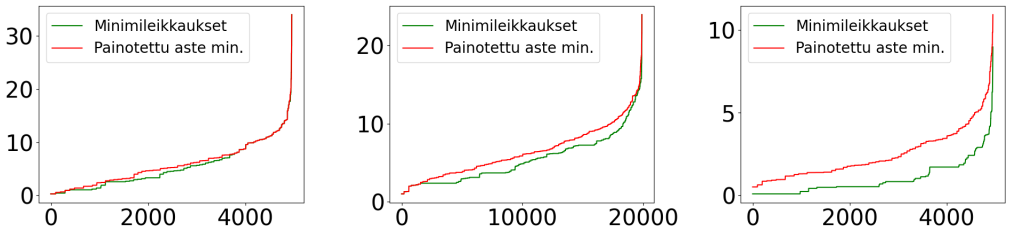


(d) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 600$.

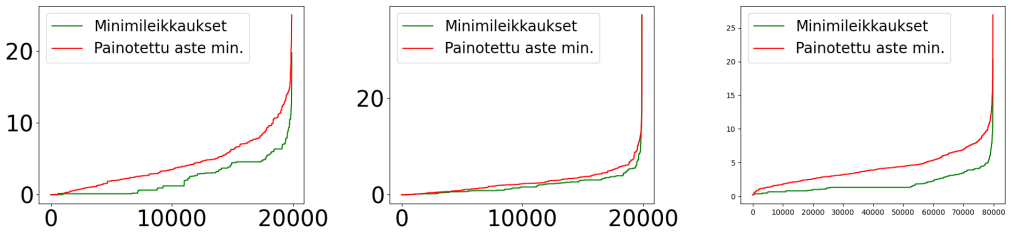
(e) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$.

Kuva 29: Epähomogeenisen verkkomallin mukaisia minimileikkausjakaumia eri muuttujien arvoilla.

Minimileikkauksia sekä kapasiteetilla painotettujen asteiden minimejä on esitetty kuvissa 30. Selkein ero kuvaajien välillä riippuu m:n arvoista, sillä pienillä arvoilla kuvaajat eroavat paljon ja vastaavat toisiaan ainoastaan pienimmillä ja kaikkein suurimilla minimileikkauksen sekä painoetun asteen minimin arvoilla, mutta m:n kasvaessa ne saavuttavat lähes vastaavat kuvaajat. Tämä on nähtävissä kuvista 30d ja 30e. Myös raja-arvon ρ muutokset vaikuttavat hieman kuvaajien vastaavuuteen, mutta havaittavat erot ovat pieniä. Muuttujan R arvot vaikuttavat kuvaajien muotoon, siten että suuremmilla R:n arvoilla kuvaajat mallintavat eksponentiaalista kasvua ja R:n pienetessä kuvaajat loivenevat ja arvot ovat tasaisemmin jakautuneita. Noodien lukumäärä n vaikuttaa odotettavasti minimileikkausten sekä painotettujen asteiden maksimiarvoihin, sillä mitä enemmän noodeja verkossa on, sitä enemmän linkkejä verkkoon syntyy. Muuttujan n muutokset eivät kuitenkaan vaikuta kuvaajien vastaavuuteen toistensa kanssa.



(a) $n = 100$, $m = 4$, $\rho = 0.99$ ja $R = 200$. (b) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 200$. (c) $n = 100$, $m = 2$, $\rho = 0.99$ ja $R = 600$.

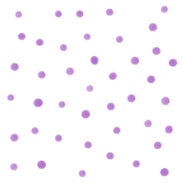
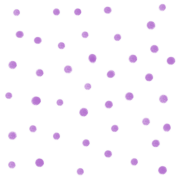
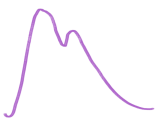
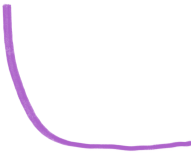
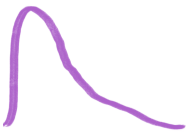
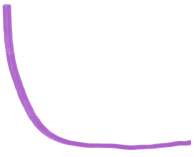
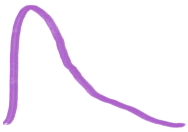


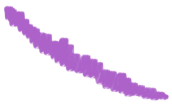
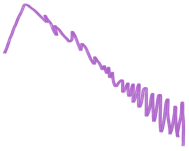
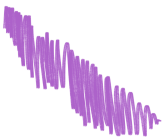
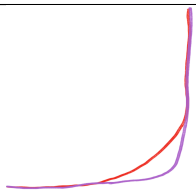
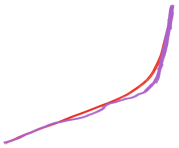
(d) $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 600$. (e) $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$. (f) $n = 400$, $m = 2$, $\rho = 0.99$ ja $R = 200$.

Kuva 30: Minimileikkauksia sekä painotettujen asteiden minimejä eri muuttujien arvoilla epähomogeenisen mallin verkoissa.

3.4 Vertailu

Tässä kappaleessa vertaillaan kirjallisuudesta tunnettujen verkkomallien, Waxman- ja skaalavapaa (Barabási-Albert), ominaisuuksia ja rakennetta työtä varten kehitettyyn epähomogeeniseen verkkomalliin. Tarkastelun kohteena ovat erityisesti aste- ja etäisyysjakauma, sekä mallien kapasiteetit ja minimileikkaukset, sillä ne kuvaavat kvanttikommunikaatioverkkojen topologista rakennetta ja suorituskykyä.

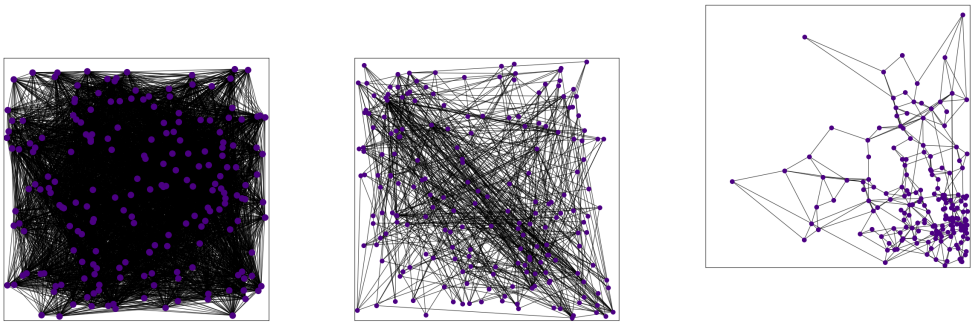
Ominaisuudet	Waxman	Skaalavapaa	Epähomogeeninen
Nooditiheys	 homogeeninen	 homogeeninen	 epähomogeeninen, useita keskuksia
Etäisyysjakauma	 normaalijakauma	 normaalijakauma	 log-normaali, useita huippuja
Astejakauma	 Poisson	 potenssilaki	 log-normaali
Minimileikkaus	 normaalijakauma	 potenssilaki	 log-normaali

Kapasiteetti	 lineaarinen, suuria arvoja	 lineaarinen, pieniä arvoja	 lähes lineaarinen, suuria arvoja
Minimileikkaus ja painotettu aste	 vastaavat hyvin, melko suuria arvoja	 vastaavat melko hyvin, pieniä arvoja	 vastaavat melko hyvin, suuria arvoja

Taulukko II: Verkkomallien ominaisuuksia.

Kuvassa 31 on esitetty eri mallien verkkoja soveltuvilta osin samoilla muuttujilla. Kuvista 31a ja 31b voidaan nähdä, että verkkojen noodit ovat tasaisesti jakuatuneet laatikon alueelle, toisin kuin epähomogeenisessä mallissa kuvassa 31c, jossa noodien sijainti on painottunut. Taulukossa 3.4 on esitetty kunkin verkkomallin ominaisuuksia tiiviisti.

Kuten aiemmissa kappaleissa todettiin, noudattavat Waxman-mallin astejakauma Poisson jakaumaa ja skaalavapaan mallin astejakauma potenssilakia. Skaalavapaa malli tuottaa odotetusti raskaan hännän omaavan jakauman, jossa muutama noodi hallitsee suurta osaa yhteyksistä. Tämä voi olla haaste kvanttikommunikaatioverkoissa, joissa resurssien keskittäminen harvoihin noodeihin voi johtaa pullonkauloihin ja heikompaan vikasietoisuuteen. Waxman-malli puolestaan tuottaa Poisson jakauman, mikä näkyi selvästi suppeampana astejakauman vaihteluna. Epähomogeenisen mallin astejakauma sijoittui näiden väliin: sen arvot ovat jakautuneet hajautetummin kuin skaalavapaalla mallilla, mikä vähentää pullonkaulaefektiä, mutta



(a) Waxman-malli, $n = 200$ ja $R = 600$.

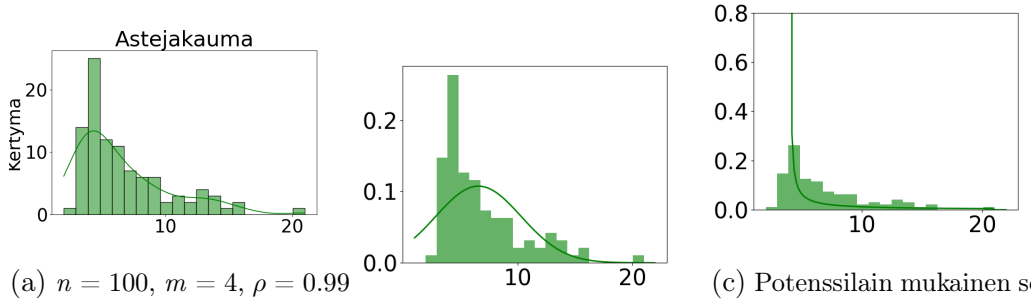
(b) Skaalavapaa malli, $n = n = 200$, $m = 3$ ja $R = 600$.

(c) Epähomogeeninen malli, $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$.

Kuva 31: Eri malleilla simuloituja verkkoja, joissa laatikon koko sekä noodien lukumäärä pidetty samoina vertailun helpottamiseksi.

mahdollistaa samalla tehokkaamman verkon läpäisevyyden korkean asteen noodien kautta. Työtä varten kehitetylle mallille astejakauma on näiden jakaumien välimaastosta, kuten nähdään kuvasta 32. Astejakauma on vahvasti painottunut pienille asteille ja erityisesti raja-arvon ollessa suuri ($\rho = 0.999$) tai noodien lukumäärän kasvaessa, astejakauma muistuttaa skaalavapaan mallin jakaumaa.

Waxman-mallilla sekä skaalavapaalla mallilla etäisyysjakaumat noudattavat selkeästi satunnaisjakaumaa, mikä on seurausta noodien satunnaisesta sijoittelusta alueelle. Tällöin verkoissa syntyy joitain lyhyitä sekä pitkiä linkkejä, mutta suurin osa linkeistä on keskipitkiä. Tämä eroaa suuresti rakennettujen kommunikaatioverkkojen rakenteesta, joissa jakauma on painottunut lyhyisiin linkkeihin ja joissa pitkiä linkkejä on vain vähän. Kuvasta 33 voidaan nähdä, että epähomogeenisen mallin etäisyysjakauma eroaa selkeästi Waxman- sekä skaalavapaan mallin jakaumista, sillä sen jakauma laskee nopeasi ensimmäisten arvojen jälkeen. Tämän on seurausta mallin rakenteesta, joka suosii tiettyjä verkon noodeja, joiden lähelle uudet noodit sijoittuvat. Mallin mukaisten verkkojen etäisyydet ovat suppeammalla hajonnalla kuin Waxman- tai skaalavapaan mallin verkkojen etäisyydet. Epähomogeeni-

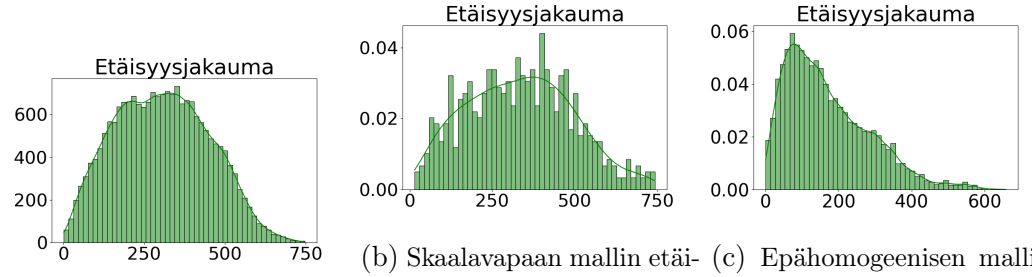


(a) $n = 100$, $m = 4$, $\rho = 0.99$ ja $R = 200$.

(b) Poisson mallin sovitus.

(c) Potenssilain mukainen sovitus.

Kuva 32: Epähomogeenisen mallin astejakauma eri jakaumien mukaisilla sovituksilla. Poisson jakauma vastaa Waxman-mallin jakaumaa ja skaalavapaata mallia vastaa potenssilakijakauma.



(a) Waxman-mallin etäisyysjakauma, $n = 200$ ja $R = 600$.

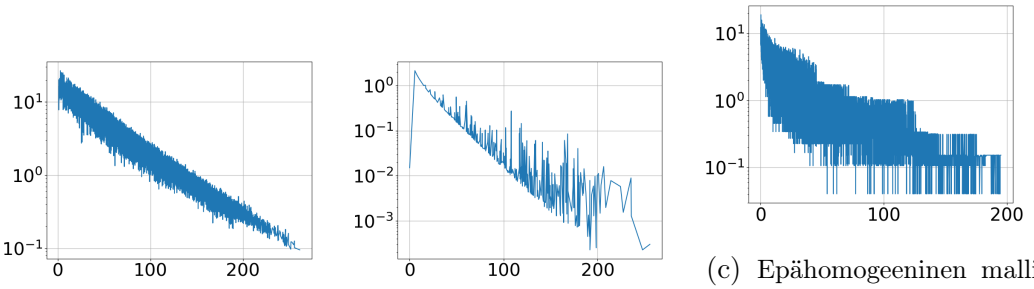
(b) Skaalavapaan mallin etäisyysjakauma, $n = 200$, $m = 3$ ja $R = 600$.

(c) Epähomogeenisen mallin etäisyysjakauma, $n = 200$, $m = 3$, $\rho = 0.999$ ja $R = 600$.

Kuva 33: Etäisyysjakaumat Waxman-, skaalavapaalle sekä epähomogeeniselle mallille. Kaikissa noodien lukumäärä sekä laatikon koko pidetty samana.

selle mallille havaittiin myös jakauman kaksi huippua, kun verkossa esiintyi kaksi keskittymää. Tällaista käyttäytymistä ei havaittu muilla mallilla. Lyhyet etäisyydet verkoissa ovat kommunikaation kannalta edullisia, sillä kapasiteetti linkeissä on etäisyydestä riippuva.

Kaikille verkkomalleille on esitetty esimerkki kapasiteetinkuvaajat kuvassa 34. Vaikka kaikissa verkoissa on soveltuvilta osin käytetty samoja muuttujia, esim. noodien lukumäärä ja laatikon koko ovat kaikissa vastaavat, on kuvaajissa selkeitä eroja. Waxman-mallin kuvaaja 34a on logaritmisella asteikolla lähes suora ja vaihtelu pienten etäisyyden vaihteluiden suhteen on myös pientä, mikä johtaa kapeahkoon



(a) Waxman-malli, $n = 200$ ja $R = 200$.

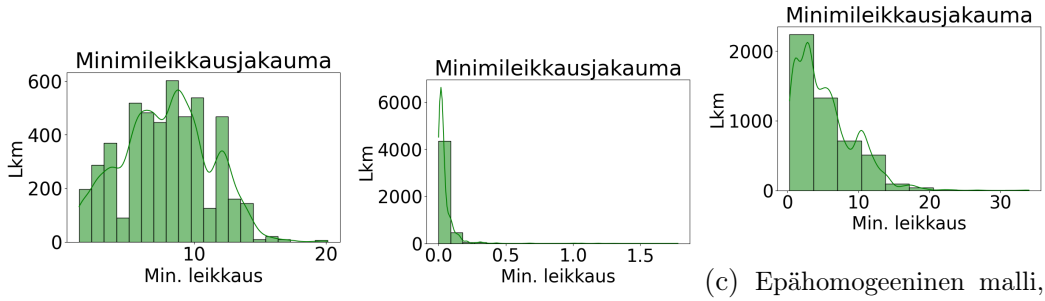
(b) Skaalavapaa malli, $n = n = 200$, $m = 2$ ja $R = 200$.

(c) Epähomogeeninen malli, $n = 200$, $m = 2$, $\rho = 0.999$ ja $R = 200$.

Kuva 34: Eri malleille kapasiteetin kuvaajia, kun muuttujat on pidetty soveltuvilta osin samoina vertailun helpottamiseksi.

kuvaajaan. Waxman-verkon kapasiteetit saavat melko hyviä arvoja ja pienimmät kapasiteetit ovat luokkaa 10^{-1}. Skaalavapaalla mallilla 34b kapasiteettijakaumalla voidaan havaita huomattavasti enemmän vaihtelua, varsinkin suurilla etäisyyksillä. Myös kapasiteettien suurin ja pienin arvo ovat selkeästi pienempiä kuin Waxman-mallissa sekä työhön kehitetyssä mallissa. Epähomogeenisessä mallissa 34c kapasiteetin arvot vaihtelevat suunnilleen samalla välillä kuin Waxman-mallin kuvaajassa, mutta maksimietäisyys jää pienemmäksi. Tämän on seurausta Waxman- sekä skaalavapaan verkon noodien sijoittelun satunnaisuudesta, minkä seurauksena suurimmat etäisyydet noodien välillä verkossa ovat $\sqrt{2}R$ luokkaa, kun epähomogeenisessä mallissa yksittäisten noodien väliset etäisyydet ovat lyhyempiä, noodien painottuessa toistensa lähelle niitä verkkoon lisätessä. Epähomogeeninen malli ei myöskään sijoittele noodeja koko laatikkoon, mikä selittää lyhyemmät maksimietäisyydet. Työhön kehitetyn mallin jakaumassa esiintyy paljon vaihtelua pienillä etäisyyden muutoksilla.

Eri malleille on esitetty minimileikkausjakaumia kuvissa 35. Kuvia vertaamalla voidaan havaita skaalavapaan mallin minimileikkausjakauman olevan hyvin painottunut pienille arvoille ja sen jakauman selvästi noudattavan potenssilakia, ku Waxman-mallilla minimileikkausten arvot ovat tasaisemmin jakautuneet ja jakau-



(a) Waxman-malli, $n = 100$ ja $R = 200$.

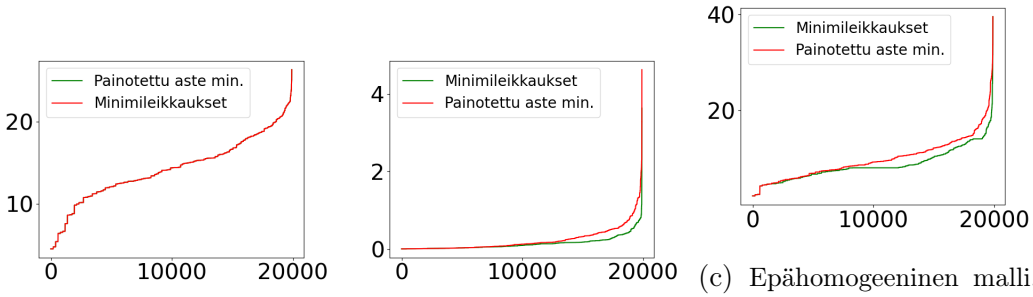
(b) Skaalavapaa malli, $n = n = 100$, $m = 4$, $\rho = 0.99$ ja 100, $m = 2$ ja $R = 200$.

(c) Epähomogeeninen malli, $R = 200$.

Kuva 35: Eri malleille minimileikkausjakaumat, kun muuttujat on pidetty soveltuvilta osin samoina vertailun helpottamiseksi.

ma muistuttaa Poisson-jakaumaa, vaikka senkin arvot ovat painottuvat jakauman alkuun. Waxman-mallin minimileikkausten maksimiarvot ovat suurempia kuin skaalavapaalla mallilla. Epähomogeenisella mallillakin jakauma painottuu alkupään pieniin arvoihin ja sen jakauma muistuttaa myös vahvasti log-normaalijakaumaa, mutta toisin kuin skaalavapaalla mallilla, sille havaitaan myös yksittäisiä suuria minimileikkauksen arvoja. Kommunikaation kannalta korkeat minimileikkauksen arvot ovat hyviä, sillä silloin verkko on hyvin yhdistynyt ja yksittäisten linkkien katkaiseminen ei katkaise yhtä helposti kommunikaatiota verkon eri noodien välillä ja verkko sietää paremmin ulkoisia hyökkäyksiä.

Myös mallien minimileikkausten sekä kapasiteetilla painotettujen asteiden minimien kuvaajia vertaamalla voidaan nähdä, että skaalavapaan mallin arvot ovat selkeästi pienempiä kuin Waxman- tai epähomogeenisella mallilla. Työhön kehitetty malli saavuttaa Waxman-malliakin suuremman maksimiarvon minimileikkauksille sekä painotettujen asteiden minimeille, mutta sen kuvaajat eivät vastaa toisiaan yhtä hyvin kuin Waxman-mallin kuvaajat. Skaalavapaalla mallillakin voidaan huomata kuvaajien vastaavan toisiaan suuremmalta alalta kuin epähomogeenisella mallilla. Muodoltaan epähomogeenisen mallin kuvaajat ovat Waxman-mallin ja skaalavapaan mallin välimuoto, sillä skaalavapaan mallin kuvaajat kasvavat ekspo-



(a) Waxman-malli, $n = 200$ ja $R = 200$.

(b) Skaalavapaa malli, $n = n = 200$, $m = 3$ ja $R = 200$.

(c) Epähomogeeninen malli, $n = 200$, $m = 3$, $\rho = 0.99$ ja $R = 200$.

Kuva 36: Eri malleille minimileikkaukset sekä kapasiteetilla painotettujen asteiden minimi esitetty kuvaajissa, muuttujat on pidetty soveltuvilta osin samoina vertailun helpottamiseksi.

nentiaalisesti, kun Waxman-mallilla kuvaajat lähestyvät lineaarista. Epähomogeenisen mallin kuvaajat alkuun mallintavat lineaarista kasvua, mutta tekevät hypyn eksponentiaaliseen kasvuun suurilla arvoilla.

4 Yhteenveto

Kvanttikommunikaatioverkkoja tarvitaan turvalliseen tiedonsiirtoon, erityisesti kvanttisalausta (QKD) varten. Ne tarjoavat kvanttimekaniikkaan perustuvaa tietoturvaa, jota ei voida murtaa klassisilla laskentamenetelmillä [30]. Verkkojen avulla voidaan rakentaa esimerkiksi kansallisia tai kansainvälisiä kvanttiverkkoja, jotka yhdistävät kvanttilaskimia tai suojaavat kriittistä infrastruktuuria tietomurroilta [32].

Tässä opinnäytetyössä pyrittiin mallintamaan kvanttikommunikaatioverkkoja sekä luomaan malli, joka huomioi reaalimaailman verkoille ominaisen maantieteellisen sijainnin. Epähomogeenisella mallilla havaittiin syntyvän useita noodikeskuksia, joka näkyi myös esimerkiksi etäisyysjakauman useana huippuna. Tämä viittaa siihen, että verkon rakenne ei keskity vain yhden noodin ympärille kuten skaalavapaassa mallissa, vaan jakaa informaatiovirran usean keskuksen kautta. Tällöin yksittäisen

noodin ylikuormittumisen riski pienenee, mikä parantaa verkon vikasietoisuutta [7]. Tällaista ilmiötä ei havaittu muilla malleilla.

Epähomogeenisen mallin rakenne synnyttää kuitenkin myös rajotteita kommunikaatiolle, sillä verkkoon syntyy täysin noodivapaita alueita, joihin kommunikaatio ei onnistu, toisin kuin Waxman- ja skaalavapaalla mallilla. Malli kuitenkin pyrkii matkimaan reaalimaailman verkkoja, joissa tällaisten noodivapaiden alueiden voidaan mieltää esittävän esimerkiksi vesistöjä, joissa ei oletettavasti esiinnykään kommunikaatiota. Toisaalta malli voi antaa ideoita kvanttikommunikaatioverkkojen kasvusta, sillä tämän hetkiset reaalimaailman verkot ovat hyvin pieniä, esimerkiksi DARPA-verkko Bostonissa on muutamasta noodista koostuva verkko [15].

Kvanttikommunikaatioverkon käytännöllisyyden kannalta tärkeää on myös niiden rakenteellinen kestävyys, joka näkyy korkeina minimileikkauksen arvoina. Minimileikkausten arvot painotettiin linkkien kapasiteeteilla. Suurilla minimileikkausten arvoilla verkko säilyttää toimintakykynsä, vaikka yksittäisiä linkkejä poistettaisiin käytöstä esimerkiksi hyökkäyksin. Työhön kehitetty malli tuottaa muihin malleihin verrattain korkeita minimileikkauksen arvoja, mikä tekee siitä kestävän linkkien poistolle, kuten nähtiin Tuloksia-kappaleen Vertailu-alaluvussa.

Yksi kvanttikommunikaatioverkkojen tehokkuuden mittari on verkon kapasiteettijakauma. Noodiparit pystyvät hyödyntämään useita polkuja kommunikaatioon, mikä kasvattaa päästä-päähän kapasiteettia, minkä takia useat reitit ja niiden kautta suuret minimileikkauksen arvot ovat hyviä ominaisuuksia kommunikaatioverkoille. Korkea kapasiteetti saavutetaan myös lyhyillä linkkien pituuksilla, koska kapasiteetti on vahvasti etäisyydestä riippuva. Työhön kehitetty malli suosii vahvasti lyhyitä linkkejä, mikä nostaa verkoilla esiintyviä kapasiteetteja.

Epähomogeenisen mallin etuja onkin sen ominaisuus suosia lyhyitä linkkejä, joka johtaa korkean kapasiteetin linkkeihin. Tämän seurauksena myös minimileikkaukset, painotettuna kapasiteetilla, ovat suuria. Toisaalta mallin heikkous on laatikkoon jää-

vät tyhjät alueet, joissa ei ole noodeja. Tätä haittaa ei kirjallisuuden malleilla esiinny, niiden noodien levittäytyessä tasaisesti laatikkoon. Toisaalta näillä malleilla linkit ovat pidempiä, minkä takia niiden kapasiteetin ja seurauksena myös minimileikkaukset ovat pienempiä. Epähomogeenisen ja Waxman-mallin etuja ovat myös verrattain suuret maksimikapasiteetit, mikä toisaalta kuuluu skaalavapaan mallin heikkouksiin.

Tulevaisuudessa epähomogeenistä mallia voisi koittaa jatkokehittää muokkaamalla mallia siten, että sille voi antaa halutun noodivapaan alueen, mikä helpottaisi oikeiden maantieteellisten verkkojen suunnittelua ja mallinnusta sekä kokeilemalla linkkien lisäyksen muokkaamista saman kaltaiseksi kuin skaalavapaassa mallissa. Tällä hetkellä linkit lisätään lähimpiin noodeihin, mutta voisi olla hyvä tutkia myös miten malli käyttäytyy jos linkit lisättäisiin asteeltaan suurimpiin noodeihin. Työhön kehitettä malli voisi myös vertailla olemassa oleviin kvanttikommunikaatioverkkoihin, joiden noodeilla on maantieteellinen sijainti ja vertailla kuinka hyvin malli vastaa näitä.

Yhteenvetona voidaan todeta, että työtä varten kehitetty malli tarjoaa kompromissin kapasiteetin ja verkon rakenteellisen tehokkuuden välillä. Se hyötyy sekä topologisesta joustavuudesta että optimaalisesta kapasiteetista ja minimileikkauksista, mikä tekee siitä varteenotettavan vaihtoehdon käytännön kvanttikommunikaatioverkkojen suunnittelussa ja simuloinnissa.

A Työssä käytetty koodi

Kvanttikommunikaatioverkko mallien simuloimiseksi ja analysoimiseksi kirjoitettiin koodia, jossa jokaiselle mallille oli omat luokkarakenteensa. Koodi löytyy osoitteesta https://github.com/helpaja/Quantum-communication-networks/tree/cb009b14dcac3a850ae9299e93080008cf496571.

B AI:n käyttö

Tässä opinnäytetyössä on hyödynnetty OpenAI:n luomaa ChatGPT-4o mallia auttamaan työtä varten luodun koodin tarkistamisessa. ChatGPT-4o mallia käytettiin huolimatomuusvirheistä, kuten kirjoitusvirheistä sekä dimensioiden eriparisuudesta johtuvien ongelmien paikantamiseen ja ratkaisemiseen. Dimensioiden eriparisuus toi ongelmia matriiseihin kohdennetuissa laskuissa, esimerkiksi matriisien kertolasku vaatii, että matriisien dimensiot vastaavat. Dimensio-ongelmia ratkaistaessa erityistä huolellisuutta käytettiin fysikaalisten ominaisuuksien säilyttämiseksi.

Viitteet

[1] Networkx, 10 2024. URL https://networkx.org/documentation/stable/reference/algorithms/generated/networkx.algorithms.flow.minimum_cut_value.html#networkx.algorithms.flow.minimum_cut_valuehttp://conference.scipy.org.s3-website-us-east-1.amazonaws.com/proceedings/scipy2008/paper_2/full_text.pdf.

[2] A. Acín, J. I. Cirac, and M. Lewenstein. Entanglement percolation in quantum networks. *Nature Physics*, 3(4):256–259, 2007.

[3] A.-L. Barabási and R. Albert. Emergence of scaling in random networks. *science*, 286(5439):509–512, 1999.

[4] A.-L. Barabási. *Network Science*. Cambridge, 7 2016. ISBN 9781107076266.

[5] R. Bassoli, H. Boche, C. Deppe, R. Ferrara, F. H. P. Fitzek, G. Janssen, and S. Saeedinaeeni. *Quantum Communication Networks*, pages 1–11. 2021. doi: 10.1007/978-3-030-62938-0_1.

[6] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical review letters*, 76(5):722, 1996.

[7] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang. Complex networks: Structure and dynamics. *Physics reports*, 424(4-5):175–308, 2006.

[8] P. Bonacich and P. Lu. *12. Scale-Free Networks*, pages 117–136. Princeton University Press, 12 2012. doi: 10.1515/9781400842452-015.

[9] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[10] D. Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43 (9):4237–4251, 2002.

[11] P. Chan, I. Lucio-Martínez, X. Mo, and W. Tittel. Quantum key distribution. *arXiv preprint arXiv:1111.4501*, 2011.

[12] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, et al. Metropolitan all-pass and inter-city quantum communication network. *Optics express*, 18(26):27217–27225, 2010.

[13] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter. Everything you always wanted to know about locc (but were afraid to ask). *Communications in Mathematical Physics*, 328:303–326, 2014.

[14] W. Dür and H. J. Briegel. Entanglement purification and quantum error correction. *Reports on Progress in Physics*, 70(8):1381, 2007.

[15] C. Elliott. The darpa quantum network. In *Quantum Communications and cryptography*, pages 91–110. CRC Press, 2018.

[16] M. Epping, H. Kampermann, and D. Bruß. Large-scale quantum networks based on graphs. *New Journal of Physics*, 18(5):053036, 2016.

[17] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865–942, 2009.

[18] P. Kok. *A First Introduction to Quantum Physics*. Springer International Publishing, 2018. ISBN 978-3-319-92206-5. doi: 10.1007/978-3-319-92207-2.

[19] A. Lakhina, J. W. Byers, M. Crovella, and I. Matta. On the geographic location of internet resources. *IEEE Journal on Selected Areas in Communications*, 21: 934–948, 8 2003. ISSN 0733-8716. doi: 10.1109/JSAC.2003.814667.

[20] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, et al. Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41, 2020.

[21] Nasa. Nasa earth observatory, 7 2023. URL https://earthobservatory.nasa.gov/images/151557/prague-at-night.

[22] M. E. Newman. Power laws, pareto distributions and zipf's law. *Contemporary physics*, 46(5):323–351, 2005.

[23] M. E. J. Newman. *Mathematics of networks*, pages 109–167. Oxford University Press, 3 2010. doi: 10.1093/acprof:oso/9780199206650.003.0006.

[24] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 6 2012. ISBN 9781107002173. doi: 10.1017/CBO9780511976667.

[25] J. Nokkala, J. Piilo, and G. Bianconi. Complex quantum networks: a topical review. *Journal of Physics A: Mathematical and Theoretical*, 2024.

[26] J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger. Entanglement purification for quantum communication. *Nature*, 410(6832):1067–1070, 2001.

[27] S. Pirandola. End-to-end capacities of a quantum communication network. *Communications Physics*, 2(1):51, 2019.

[28] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):15043, 2017.

[29] A. Poppe, M. Peev, and O. Maurhart. Outline of the secoqc quantum-key-distribution network in vienna. *International Journal of Quantum Information*, 6(02):209–218, 2008.

[30] C. Portmann and R. Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94(2):025008, 2022.

[31] J. Qiu et al. Quantum communications leap out of the lab. *Nat.*, 508(7497): 441–442, 2014.

[32] M. R. Ramya, P. Kumar, M. D. Dhanasekaran, M. R. S. Kumar, and S. A. Sharavan. A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques. *Franklin Open*, page 100223, 2025.

[33] M. Razavi. *Quantum networks at continental scales*, pages 4–1–4–17. Morgan & Claypool Publishers, 5 2018. doi: 10.1088/978-1-6817-4653-1ch4.

[34] J. Roffe. Quantum error correction: an introductory guide. *Contemporary Physics*, 60(3):226–245, 2019.

[35] M. Roughan, J. Tuke, and E. Parsonage. Estimating the parameters of the waxman random graph. In *Algorithms and Models for the Web Graph: 16th International Workshop, WAW 2019, Brisbane, QLD, Australia, July 6–7, 2019, Proceedings 16*, pages 71–86. Springer, 2019.

[36] Q. Ruihong and M. Ying. Research progress of quantum repeaters. In *Journal of Physics: Conference Series*, volume 1237, page 052032. IOP Publishing, 2019.

[37] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics express*, 19(11):10387–10409, 2011.

[38] B. Schumacher and M. Westmoreland. *Quantum Processes Systems, and Information*. Cambridge University Press, 3 2010. ISBN 9780521875349. doi: 10.1017/CBO9780511814006.

[39] R. Singh. Simulation of observations for the half-normal distribution. *Sankhyā: The Indian Journal of Statistics, Series B*, pages 137–139, 1994.

[40] S. K. Sood et al. Quantum computing review: A decade of research. *IEEE Transactions on Engineering Management*, 71:6662–6676, 2023.

[41] M. R. Spiegel, S. Lipschutz, and J. Liu. Mathematical handbook of formulas and tables, schaum's outline series mcgraw–hill. *International edition*, 1990.

[42] B. M. Waxman. Routing of multipoint connections. *IEEE journal on selected areas in communications*, 6(9):1617–1622, 1988.

[43] S. M. Zangi, C. Shukla, A. Ur Rahman, and B. Zheng. Entanglement swapping and swapped entanglement. *Entropy*, 25(3):415, 2023.

[44] R. Zhang, L.-Z. Liu, Z.-D. Li, Y.-Y. Fei, X.-F. Yin, L. Li, N.-L. Liu, Y. Mao, Y.-A. Chen, and J.-W. Pan. Loss-tolerant all-photonic quantum repeater with generalized shor code. *Optica*, 9(2):152, Feb. 2022. ISSN 2334-2536. doi: 10.1364/optica.439170. URL http://dx.doi.org/10.1364/OPTICA.439170.

[45] Q. Zhuang and B. Zhang. Quantum communication capacity transition of complex quantum networks. *Physical Review A*, 104(2):022608, 2021.