Anna Arikainen

Tor-verkon rakenne ja toiminta

Tietotekniikan kandidaatintutkielma

13. toukokuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Anna Arikainen

Yhteystiedot: anarikai@student.jyu.fi

Ohjaaja: Tytti Saksa

Työn nimi: Tor-verkon rakenne ja toiminta

Title in English: Structure and operation of the Tor network

Työ: Kandidaatintutkielma

Opintosuunta: All study lines

Sivumäärä: 24+0

Tiivistelmä: Tämä kirjallisuuskatsaus käsittelee Tor-verkon rakennetta ja toimintaa sekä siihen liittyviä ilmiöitä. Tutkielmassa käsitellään internetin eri kerroksia, Tor-verkon rakennetta ja sipulireitityksen kehitystä vuosien varrella, reititystä, Tor-verkon ja virtuaalisen erillisverkon (VPN) eroja, Tor-verkkojen laillisuutta ja sen käyttöä sorretuissa maissa.

Avainsanat: Tor-verkko, Tor, VPN, sipulireititys, reititys

Abstract: This literature review focuses on the structure and operation of the Tor-network and phenomenons related to it. The thesis focuses on the different layers of the internet, on the structure of the Tor network and on the evolution of the onion routing over the years. The thesis deals also with routing and the difference between Tor and VPN, the legality of the Tor network and its use in oppressed countries.

Keywords: Tor network, Tor, VPN, onion routing, routing

Kuviot

Sisältö

1 Johdanto

Nykypäivän hakukoneet eivät pysty löytämään kaikkea olemassa olevaa tietoa. Tiedonhaku on hyvin pitkälti verrattavissa sormien läpi valuvaan hiekkaan. On mahdotonta vahingossa päätyä pimeään verkkoon tavallisen verkkoselailun kautta, sillä pääsyn näihin syvempiin internet-kerroksiin mahdollistaa erillinen ohjelmisto.

Eräs keino, jonka avulla pääsy syvempiin kerroksiin on mahdollista, on Tor-verkko. Tor on tällä hetkellä suosituin ja eniten käytetyin ohjelmisto (Europol 2015). Tämän takia I2P- ja Freenet-ohjelmistot tässä tutkielmassa sivuutetaan ja keskitytään tutkimaan Tor-verkon rakennetta ja toimintaa.

Tutkielman tarkoituksena on selventää lukijalle mistä Tor-verkko koostuu, miten se toimii, miksi sitä tarvitaan pimeään verkkoon pääsyyn sekä miksi se helpottaa rikollisten toimintaa verkossa. Tutkielman tavoitteena on luoda yleiskuva Tor-verkosta ja sen toiminnasta sekä siihen liittyvistä ilmiöistä. Sivussa on tarkoitus tuoda lyhyesti esiin anonyymisyyden haittapuolet.

Tämä tutkielma koostuu kuudesta luvusta. Aluksi esitellään yleisesti internetin eri kerrokset ja niiden sisältö. Sen jälkeen käsitellään Tor-verkon rakennetta ja toimintaa sekä Tor-ohjelmiston käyttämää sipulireititystekniikkaa. Tutkielmassa käydään myös yleisesti läpi VPN-palveluiden roolia Tor-ohjelmiston rinnalla. Lopussa käsitellään piilopalveluita ja Tor-verkkojen laillisuutta.

2 Internetin eri kerrokset

Tämä luku käsittelee internetin eri kerroksia ja niiden sisältöä. Luku koostuu kolmesta alaluvusta. Aluksi käsitellään pintaverkkoa, joka sijaitsee muiden kerroksien yläpuolella ja on tavallisten hakukoneiden ulottuvissa. Sen jälkeen siirrytään käsittelemään syvää verkkoa, joka sijaitsee pintaverkon alapuolella. Lopuksi käsitellään vielä pimeä verkko, joka muodostaa internetin viimeisimmän ja syvimmän kerroksen.

2.1 Pintaverkko

Internetin kerrosmaista rakennetta havainnollistetaan usein jäävuorena. Pintaverkko (engl. surface web) muodostaa siten jäävuoren huipun. Pintaverkolla tarkoitetaan sitä kerrosta internetistä, joka on tavallisten hakukoneiden, kuten Googlen, ulottuvissa (Bergman 2001). Pintaverkkoon kuuluu esimerkiksi YouTube, Google, Facebook ja Twitter (Weimann 2016).

2.2 Syvä verkko

Syvä verkko (engl. deep web) oli tuotu käsitteenä ensimmäistä kertaa esiin vuonna 2001. Termin keksijä, tietojenkäsittelytieteilijä Michael K. Bergman, määrittelee sen osaksi maailmanlaajuista verkkoa (engl. world wide web), jonka sisältöjä ei tavalliset hakukoneet voi indeksoida (Bergman 2001). Syvä verkko muodostaa jäävuoren toiseksi alimman kerroksen.

Syvä verkko siis koostuu siitä datasta, joka on olemassa verkossa, mutta jota ei tekstihakukoneet pysty löytämään (Khare, An ja Song 2010). Syvään verkkoon kuuluvat esimerkiksi verkkopankki, yksityiset viestit, sähköpostiviestit ja OmaKanta-verkkopalvelu.

On useita syitä siihen, miksi hakukoneet eivät pysty löytämään kaikkea olemassa olevaa informaatiota. Suurin osa verkkosisällöstä on haudattu syvälle dynaamisesti tuotetuille verkkosivuille. Syvän verkon useimmat verkkosivut eivät ole olemassa, kunnes verkkosivu luodaan dynaamisesti tarkennetun haun seurauksena. Koska tavalliset hakukoneet, kuten Google ja Yahoo, käyttävät hakurobotteja (engl. web crawler) verkkosivujen indeksointiin, eivät hakurobotit näe olemassaolemattomia sivuja eikä näin pysty palauttamaan mitään sisältöä selai-

meen. (Bergman 2001)

Löydettävissä olevan verkkosivun tulee täyttää kaksi ehtoa (Bergman 2001):

1. Verkkosivun tulee olla staattinen.
2. Verkkosivun tulee olla linkitetty muihin verkkosivuihin.

Internetin sisältö on vuosien mittaan vain kasvanut ja tällä hetkellä on vaikea arvioida, kuinka monta prosenttia kaikesta olemassa olevasta tiedosta esimerkiksi Googlen hakukone käyttäjilleen tarjoaa. Elämme aikakautta, jolloin tietoa on saatavilla enemmän kuin koskaan ennen. Kuten Bergman (2001) huomauttaa: "Jos informaatioaikakauden halutuin hyödyke on tosiaan informaatio, syvän verkon sisällön arvo on mittaamaton."

2.3 Pimeä verkko

Pimeä verkko (engl. dark web) muodostaa jäävuoren alimman ja syvimmän keroksen (Bergman 2001). Pimeä verkko on joukko verkkosivuja, joiden löytäminen perinteisillä hakukoneilla on mahdotonta, ja joiden sisältö on tarkoituksella salattu (Weimann 2016). Erillinen ohjelmisto mahdollistaa pääsyn pimeään verkkoon (Jardine 2015).

Pimeän verkon kuuluisin kauppapaikka on vuonna 2011 avattu Silk Road, silkkitie (Europol 2015). Sivusto tuli tunnetuksi palkkamurhien, huumekaupan, terrorismin sekä lasten hyväksikäytön ansiosta (Jardine 2015). Vuonna 2013 FBI sulki kauppapaikan ensimmäisen version (Weimann 2016). Silkkitie, kuten monet muutkin pimeän verkon osista, on saavuttavissa vain Tor-ohjelmiston kautta.

On olemassa monia eri vaihtoehtoisia ohjelmistoja, jotka mahdollistavat pääsyn pimeään verkkoon. Yleisin niistä on kuitenkin Tor, jonka rakennetta ja toimintaa tässä tutkielmassa käsitellään. (Jardine 2015)

3 Tor-verkko

Tämä luku käsittelee Tor-verkon rakennetta ja toimintaa sekä sen kehitystä. Pääluku koostuu kahdesta alaluvusta: ensimmäinen alaluku käsittelee Tor-verkon rakennetta ja toimintaa ja toinen Tor-verkon kolmea eri sukupolvea.

Nimi Tor on akronyymi projektin englannin kielisestä nimestä The Onion Routing (*The Tor Project: History* 2020). Nykypäivän Tor-ohjelmisto on käytännössä kolmannen sukupolven sipulireititys (Syverson 2011). Maailmassa, jossa valtiot hyödyntävät omassa toiminnassaan tarkkailujärjestelmiä ja sensuuria, Tor mahdollistaa sen käyttäjille näiden toimien välttämisen tarjoamalla heille anonymiteetin (Casenove ja Miraglia 2014).

3.1 Tor-verkon rakenne ja toiminta

Tor on vapaaehtoisten muodostama verkosto, joka tarjoaa tuhansia reitittimiä verkkoliikenteen hajauttamiseen Tor-verkossa (Casenove ja Miraglia 2014). Tor-verkon toiminta perustuu verkkoliikenteen haajauttamiseen useiden eri solmujen (engl. node) kautta (McCoy ym. 2008). Nykypäivän Tor tarjoaa anonyymikerroksen TCP-protokollan päälle muodostaen Tor-verkossa reitin kolmen solmun kautta käyttäen monikerroksista salausmentelmää (McCoy ym. 2008). Tekniikka, jota Tor-verkko käyttää, sanotaan sipulireititykseksi (Casenove ja Miraglia 2014).

Kolmen satunnaisen solmun muodostamaa kokonaisuutta sanotaan piiriksi (engl. circuit), jonka Tor-reitittimet muodostavat. Tor tarjoaa anononyymikerroksen TCP:lle rakentamalla piirin Tor-reitittimistä käyttämällä kerroksittaista salaus menetelmää, joka muistuttaa sipulireititystä. Yleisesti yhden käyttäjän TCP-yhteydet tunneloidaan yhden piirin kautta, joka kiertää ajan myötä. (McCoy ym. 2008)

Piirin ensimmäistä solmua sanotaan sisääntulosolmuksi (engl. entrance Tor router) tai vartijasolmuksi (engl. guard). Koska piiri voi muodostua useammasta kuin kolmesta solmusta, sanotaan sisääntulosolmun ja ulostulosolmun välissäolevia solmuja keskisolmuiksi (engl. middle Tor router). Piirin sulkee viimeisenä oleva ulostulosolmu (engl. exit Tor router). (McCoy ym. 2008)

Piirin solmuista ainoastaan sisääntulosolmu kykenee tarkkailemaan pyynnön tekijää Tor-verkon kautta, ja vain ulostulosolmu voi suoraan tutkia salattua hyötykuormaa sekä tietää päämääräserverin. Tämä näkyy ulkopuolisille tahoille siten että käyttäjän yhteys tulee ulostulosolmun IP-osoitteista, joiden sijainti voi olla missä päin maailmaa tahansa. Käyttäjän oma IP-osoite pysyy salattuna Tor-ohjelmistoa käyttäessä. (McCoy ym. 2008)

Tor-verkon käyttäjä lataa ja asentaa Tor-asiakasohjelmiston, joka toimii SOCKS-välityspalvelimena liittämällä asiakasohjelmiston (tavallisesti nettiselaimen) ja Tor-verkon yhteen. Tämä ohjelmisto ensin muodostaa yhteyden yhteen hakemistoauktoriteeteistä (engl. directory authority), jota ohjaa Tor Project -yhtiön valtuutetut henkilöt. Valtuutetuilta henkilöiltä ohjelmisto lataa listan saatavilla olevista solmuista, jotka ovat vapaaehtoisten ylläpitämiä reitittimiä. (Loesing, Murdoch ja Dingledine 2010)

Kuvitellaan tilanne, jossa käyttäjä Alice haluaa kommunikoida anonyymisti käyttäjän Bob kanssa, kuten kuviossa 1 näkyy. Aluksi Alice valitsee satunnaisesti kolme eri solmua, jotka vastaavat sisääntulosomua (solmu A kuviossa 1), keskisolmua (solmu B kuviossa 1) sekä ulostulosolmua (solmu C kuviossa 1). Solmut muodostavat virtuaalisen piirin kommunikaation lähteestä sen määränpäähän. Asiakas neuvottelee jokaisen piirin solmun kanssa erillisen sarjan salausavaimista varmistaakseen piirin yksityisyyden. Kyseisessä tilanteessa kommunikaatio kehittyy seuraavasti: Alice lähettää viestin sisääntulosolmulle salatun väylän kautta. Kun viesti on saapunut Tor-verkon sisälle, se lähetetään eteenpäin solmujen kautta, kunnes se saavuttaa ulostulosolmun. Viesti lähetetään ulostulosolmusta avoimen väylän kautta päämäärään. (Casenove ja Miraglia 2014)

3.2 Sipulireitityksen kehitys

Nykypäivän Tor-verkosta löytyy paljon eroja verrattuna sipulireitityksen ensimmäisiin prototyyppeihin, joiden kehittäminen alkoi vuonna 1995 (*The Tor Project: History* 2020). Tämän luvun tarkoituksena on tarkastella sipulireitityksen kehitystä vuosien varrella ja sitä, kuinka se tuo meidät nykypäivän Tor-ohjelmiston ääreen.

3.2.1 Ensimmäinen sukupolvi

David Goldschlag, Michael Reed ja Paul Syverson aloittivat työt sipulireitityksen parissa vuonna 1995 (Syverson 2011). Heidän tarkoituksena oli toteuttaa keino, joka mahdollistaisi yhteyksien muodostamisen verkossa ilman sen osapuolien ilmiantamista muille (*The Tor Project: History* 2020). Tästä alkoi ensimmäisten sipulireitityksen prototyyppien kehitys.

Ensimmäinen sukupolvi eroaa kahdesta seuraajastaan monella tapaa. Ensimmäisen sukupolven sipulireitityksellä oli kiinteät, viiden solmun piirit. Jos reitit olisivat olleet kolmen solmun pituisia, kaapattu keskisolmu tietäisi heti sekä lähteen että päämäärän. Jos reitit koostuisivat neljästä solmusta, lähteen tai määränpään vieressä olevan solmun murtaminen kertoisi hyökkääjälle mikä solmu pitää vielä murtaa, jotta saadaan tietoon koko piiri ja kommunikaation osapuolet. Viiden solmun piireissä hyökkääjä ei saisi käsiinsä tätä tietoa ilman vielä yhden solmun murtamista. (Syverson 2011)

Toinen merkittävä ero ensimmäisessä sukupolvessa oli integroitu kokoonpano. Tällä tarkoitetaan asiakkaan ja sipulireititimen yhdistettyä kokoonpanoa. Kolmantena erona voidaan pitää staattista topologiaa. Ensimmäisen sukupolven mallissa ei ollut topologian muutosta tai verkon löytämistä koskevia säännöksiä. Oletettiin, että kyseessä olisi kohtuullisen kokoinen verkko solmuja (mahdollisesti 20-100 solmua), jotka olisivat vakaiden organisaatioiden johtamia. Organisaatiot eivät luottaisi toisiinsa ja kaikki tieto koskien verkkokokoonpanoa ja avaimia hoidettaisiin offline-tilassa. (Syverson 2011)

Löysä reititys on myös yksi ensimmäisen sukupolven eroavaisuus. Mikäli solmu ei pystynyt muodostamaan yhteyttä seuraavaan solmuun esimerkiksi taustalla olevien verkko-ongelmien vuoksi, se pystyi muodostamaan oman sipulireititimen. Näin solmu yritti saada piirin valmiiksi lisäämällä reittiin epäsuoraisuutta. (Syverson 2011)

3.2.2 Toinen sukupolvi

Toinen sipulireitityksen sukupolvi omaa monia eroja verrattuna ensimmäiseen ja kolmanteen sukupolveen. Merkintävin niistä liittyy kuitenkin ensimmäisen sukupolven integroituun kokoonpanoon. Toisessa sukupolvessa asiakas ja sipulireititin toimivat erillään. Tämä lisäsi joustavuutta asiakkaiden mahdollisuuksiin hallita luottamusta ja resursseja. Integroidussa

kokoonpanossa käyttäjien oli pakko joko antaa oman tietokoneen osallistua sipulireitityksen infrastruktuuriin tai luottaa johonkin toisen käyttäjän ylläpitämään etäreitittimeen. Nyt asiakkaiden oli mahdollista saada tietoa verkosta sekä muodostaa omia reittejä ilman muun verkkoliikenteen reitittämistä tai luottamusta toiseen reitittimeen, joka pystyisi hallitsemaan asiakkaalta tulevaa reititystä ja dataa. (Syverson 2011)

Toinen sukupolvi luopui myös kiinteistä, viiden solmun piireistä, jotka olivat käytössä sen edeltäjällä. Toisen sukupolven käytössä oli eripituisia piirejä (enintään 11 solmua yhdessä piirissä; enemmän kuin 11 solmun piirit olivat mahdollisia vain tunneloinnin avulla). (Syverson 2011)

Reaaliaikainen eri piirien solujen sekoittaminen on myös sipulireitityksen toisen sukupolven ominaisuus. Tämä mahdollisti esimerkiksi paremman ajoituksen tutkimisen. Tästä ominaisuudesta kuitenkin luovuttiin kolmannen sukupolven sipulireitityksessä. Syynä tähän on osittainen perustelujen puute sille, että tämä ominaisuus oli hyödyllinen mahdollisen hyökkäyksen varalta. (Syverson 2011)

3.2.3 Kolmas sukupolvi

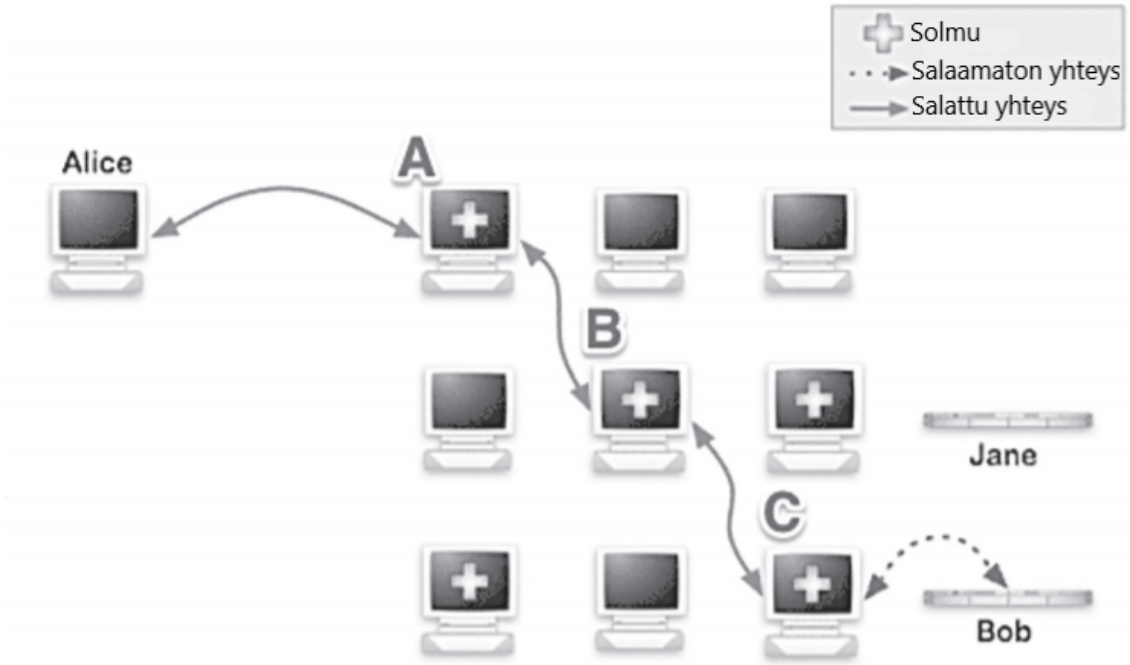
Sipulireitityksen kolmas sukupolvi on tällä hetkellä sen viimeisin versio. Nykypäivän Tor on kolmannen sukupolven sipulireititys. Mahdollisesti tärkein eroavaisuus kahteen muuhun sukupolveen on Diffie-Hellman-salausprotokollaan perustuva piirien muodostaminen. Kahdessa edellisessä sukupolvessa piirit muodostettiin jakamalla istuntoavaimia sipulirakennetta käyttäen. (Syverson 2011)

Diffie-Hellman-salausprotokolla mahdollistaa kommunikaatio-osapuolten vaihtaa lyhytaikaiset julkiset avaimet, jotka voi yhdistää toisen yksityisavaimeen luodakseen istuntoavaimen. Istuntoavainta ei lähetetä edes sen salatussa muodossa. Näin varmistetaan istuntoavainten turvallisuus, vaikka pitkäaikaiset avaimet saattaisivatkin vaarantua tulevaisuudessa. (Syverson 2011)

Toinen merkitsevä ero kahteen edelliseen sukupolveen oli hakemistopalveluiden lisäys. Ensimmäisen sukupolven sipulireitityksessä oletettiin verkkotietojen olevan staattisia tai offline-tilassa jaettuja. Toisen sukupolven sipulireititys oletti, että verkon perusjäsenyyden tiedot

luodaan offline-tilassa, mutta käytti tulvamekanismia (engl. flooding mechanism) tedennetun verkkolinkkitilan ja piirien muodostamiseen tarvittavien tietojen jakeluun. (Syverson 2011)

Sipulireitityksen kolmas sukupolvi otti hakemistopalvelut käyttöön niin verkon tilan kuin verkkojäsenyyden jakamista varten. Tämä on vähemmän monimutkainen, enemmän joustava ja paremmin skaalautuva tapa yhtenäisen verkkokuvan ylläpitämiseksi. Hakemistopalveluiden käyttöönotto paransi myös turvallisuutta mahdollistaen kaiken jaetun tiedon tarkastelun. (Syverson 2011)



Kuvio 1. Havainnollistava esimerkki Tor-verkon rakenteesta. (Casenove ja Miraglia 2014, 276, muokattu)

4 Reititys

Tämä luku käsittelee reititystä erityisesti reititysprotokollien ja Tor-verkon käyttämän sipulireititystekniikan avulla. Aluksi käsitellään reititysprotokollat ja niiden toiminta, jonka jälkeen siirrytään sipulireitityksen toimintaan ja rakenteeseen sekä lopuksi käsitellään Tor-verkon ja VPN-palveluiden ero.

4.1 Reititysprotokollat

Internettiin kytketyt tietokoneet voivat vaihtaa keskenään dataa (Moy 1998). Tiedonsiirrossa verkkosovellusten lähettämä data muuttuu paketeiksi (Otomo ym. 1978). Paketit koostuvat biteistä, jotka ryhmitellään usein tavuiksi (Anttila 2000).

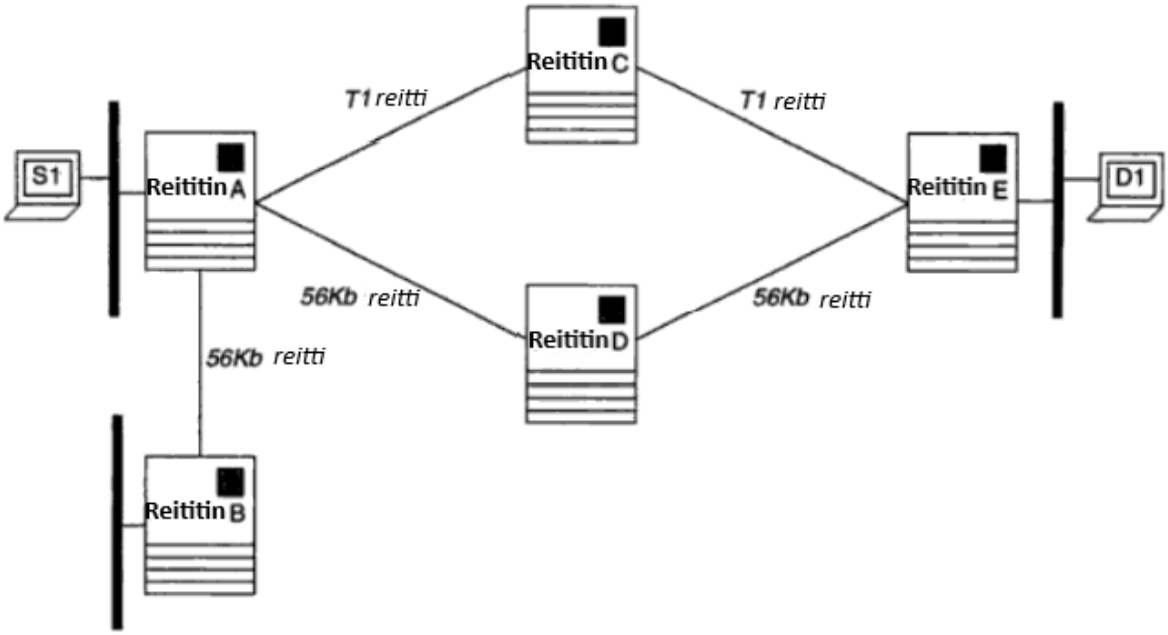
Paketit tulee lähettää oikealle laitteelle verkossa, joten pitää selvittää reitti. Laitteita, jotka vastaavat kyseisistä päätöksistä, kutsutaan reitittimiksi. Reitittimien välillä toimivia hajautettuja algoritmeja, joiden tehtävänä on oikeiden reittien määrittäminen, kutsutaan taas reititysprotokolliksi. (Moy 1998)

IP-protokolla vastaa pakettien kujetuksesta (Snoeren ym. 2002). Reititysprotokollat siten selvittävät reitin oikealle laitteelle kommunikoimalla muiden reitittimien kanssa jakaen samalla reititysinformaatiota. Reititysalgoritmi määrittää reitin ja reititin valitsee sopivimman reitin reititysprotokollien käyttämien metriikkojen avulla (Anttila 2000). Verkkojen välisen etäisyyden kuvaamiseen eli metriikkaan voivat vaikuttaa esimerkiksi luotettavuus, kuormitus tai pituus (Wendell 2010).

Reititysprotokollat voidaan jakaa kahteen pääryhmään: verkon sisäisiin ja verkkojen välisiin, ulkoisiin reititysprotokolliin (Anttila 2000). Autonomisessa järjestelmässä käytetään Interior Gateway Protocol -ryhmään kuuluvia protokollia, joita ovat: RIP, RIPv2, IGRP, EIGRP, OSPF sekä IS-IS. Exterior Gateway Protocol -ryhmän protokollia käytetään siinä tapauksessa, kun autonomisessa järjestelmässä on enemmän kuin yksi yhteys ulkomaailmaan. EGP-protokolliin kuuluvat seuraavat: EGP, BGP-1, BGP-2, BGP-3 ja BGP-4 (Anttila 2000).

Kuviossa 2 on esitetty yksinkertaistettu esimerkki reitityksestä ja reititysprotokollien toimin-

nasta. Reititysprotokolla valitsee nopeamman reitin reitittimen C (kuviossa 2) kautta. Kun reititysprotokollat huomaavat reitittimen C olevan poissa käytöstä, valitaan hitaampi reitti reitittimen D (kuviossa 2) kautta kohteeseen.



Kuvio 2. Esimerkki reitityksestä verkossa. (Moy 1998, 4, muokattu)

4.2 Sipulireititys

Sipulireitityksen historia juontaa juurensa vuoteen 1995, kun Yhdysvaltalainen Naval Research Laboratory aloitti rahoittamaan projektia, jonka päämääränä oli tunnistuksen erotus reitityksestä (Syverson 2011). Sovellusten pitää todentaa itsensä muille sovelluksille ja todennustiedot pitää pystyä kuljettamaan tietovirrassa, mutta julkisen verkon käytön ei tulisi automaattisesti paljastaa kommunikaation osapuolia. Tarkoituksena siten on anonyymireititys, ei anonymiteetti (Reed, Goldschlag ja Syverson 1996). Sipulireititystä käyttävistä ohjelmistoista tunnetuin ja käytetyin on Tor (Syverson 2011).

4.2.1 Sipulireitityksen toiminta

Sipulireititys on hajautettu kerrosverkko (engl. overlay network), joka on suunniteltu anonymisoimaan TCP-pohjaiset sovellukset, kuten web-selailun, secure shell:n ja pikaviestit. Asiakkaat valitsevat tien verkossa ja rakentavat piirin, jossa jokainen solmu (tai sipulireititin) tietää oman edeltäjäsolmun ja seuraajasolmun, mutta ei muita piirin solmuja. Verkkoliikenne virtaa piirissä kiinteän kokoisissa soluissa, jotka avataan symmetrisellä avaimella joka solmun kohdalla ja välitetään virrassa eteenpäin. (Syverson, Dingledine ja Mathewson 2004)

Sipulireitityksen nimi tulee reitittimien käyttämästä monikerrossalaustekniikasta (engl. multilayer encryption), joka rakenteeltaan muistuttaa sipulin kerroksia (Casenove ja Miraglia 2014). Sipuli rakentuu siten salatuista kerroksista; viestin reitin varrella olevat reitittimet kuorivat nämä kerrokset yksi kerrallaan viestin liikkuessa verkossa (Syverson, Dingledine ja Mathewson 2004). Saapuvat viestit noudattavat samaa reittiä, paitsi tällä kertaa reitittimet lisäävät sipuliin kerroksia, jotka sitten vastaanottava osapuoli purkaa (Syverson, Dingledine ja Mathewson 2004).

4.2.2 Tor-solut

Kuten edellä mainittiin, sipulipiirien sisällä solmujen välillä välitettäviä viestejä sanotaan soluiksi (engl. cells). Jokainen solu on 512 tavun kokoinen ja koostuu ylätunnisteesta (engl. header) sekä tietosisällöstä (engl. payload). Ylätunniste sisältää piiritunnisteen (circID), joka spesifioi mihin piiriin mikäkin solu viittaa, ja käskyn, joka kuvaa, mitä tehdä solun tietosisällölle (CMD). (Syverson, Dingledine ja Mathewson 2004)

Riippuen käskystä, solut voivat olla joko kontrollisoluja (engl. control cells) tai viestisoluja (engl. relay cells), jotka kuljettavat tietovirtaa päästä päähän (engl. end-to-end). Kontrollisolujen käskyjä ovat (Syverson, Dingledine ja Mathewson 2004):

1. CREATE / CREATED
2. DESTROY
3. PADDING

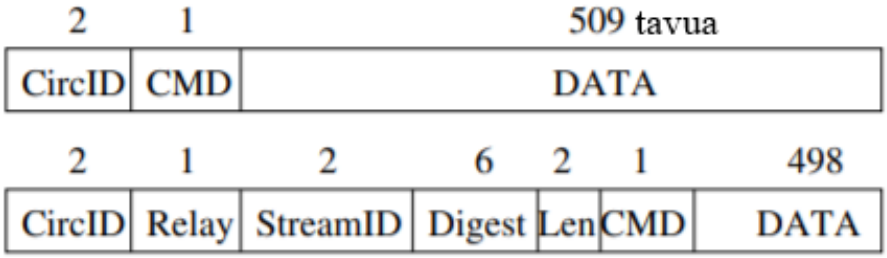
Create-käsky luo uuden piirin. Destroy-käsky vastaavasti tuhoaa olemassa olevan piirin.

Padding-käskyä käytetään yhteyden ylläpitämiseksi. (Syverson, Dingledine ja Mathewson 2004)

Viestisoluilla on kontrollisoluja enemmän informaatiota ylätunnisteessaan. Piiritunnisteen (cirID kuviossa 3) ja käskyn (CMD kuviossa 3) lisäksi määritellään streamID, koska useat tietovirrat voivat moninkertaistua piirin yli; tarkistussumma eheyden tarkistamiseksi sekä tietosisällön pituus. Viestisolujen käskyjä ovat (Syverson, Dingledine ja Mathewson 2004):

1. RELAY DATA
2. RELAY BEGIN
3. RELAY END
4. RELAY TEARDOWN

Relay data -käsky välittää dataa piirin sisällä. Relay begin -käsky avaa tietovirran ja relay end -käsky vastaavasti sulkee tietovirran. Relay teardown sulkee rikkinäisen tietovirran (Syverson, Dingledine ja Mathewson 2004). Kuvio 3 havainnollistaa kontrolli- ja viestisolujen rakennetta.



Kuvio 3. Tor-solujen rakenne. Ylhäältä alas: kontrollisolu (control cell), viestisolu (relay cell). (Syverson, Dingledine ja Mathewson 2004, muokattu)

4.3 Tor ja VPN

Tor (engl. The Onion Routing) ja VPN (engl. Virtual Private Network) eli virtuaalinen erillisverkko ovat esimerkkejä anonyymisestä viestinnästä. Kummallakin on sama tunnelimallikommunikaatio (engl. tunneling model communication) sekä molemmat käyttävät salaus-

tekniikkaa datan eheyden saavuttamiseksi. Erona on kuitenkin se, että kun VPN-palvelut ovat yritysten tarjoamia, Tor-verkko on vapaa ohjelmisto, jota käytetään yleensä internetin pimeällä puolella. (Ramadhani 2018)

VPN on verkkoteknologia viestinnän turvaamiseksi jäsenten tai ryhmien kesken, jotka yhdessä käyttävät julkista viestintäinfrastruktuuria, joka puolestaan tarjoaa tietosuojapalveluita viestintälinjoille käyttäen turva- ja tunnelointiprotokollia. VPN-teknologiaa kutsutaan yleensä VPN-tunneloinniksi. (Ramadhani 2018)

Tunnelointi on myös verkkoteknologia. Se kattaa yhden tyyppisen protokollan, joka sisältää paketteja ja datagrammeja eri protokollista. Esimerkiksi Windows VPN käyttää point-to-point (PPTP) tunnelointi -protokollapakettia yksityisen verkkoliikenteen täydentämiseksi ja lähettämiseksi TCP/IP julkisissa verkoissa, kuten internetissä. (Ramadhani 2018)

Virtuaalinen erillisverkko koostuu palvelinverkosta, jotka sijaitsevat yleensä useammassa eri maassa. Virtuaalista erillisverkkoa käyttäessä käyttäjän tietokoneelta lähetetty data menee yhden VPN-palvelun tarjoajan serverin läpi ennen kohteeseen saapumista. Tämä pätee myös toisinpäin: data, joka lähetetään käyttäjän koneelle lähiverkon ulkopuolelta menee yhden VPN-serverin läpi ennen käyttäjälle saapumista. Tuloksena on datan lähettäminen ja vastaanottaminen ilman käyttäjän sijainnin ilmiantoa. (Ramadhani 2018)

Erona kahden laajasti käytössä olevan teknologian välillä on niiden käyttötarkoitus. Tor-verkko on hidas verrattuna virtuaaliseen erillisverkkoon, mutta se takaa käyttäjälleen anonyymisyyden internetissä (Ramadhani 2018). Tor-verkko koostuu palvelimista, joiden kanssa käyttäjä anonyymisti kommunikoi. Sekä Tor-ohjelmisto käyttäjän koneella että Tor-verkossa olevat palvelimet eivät ole minkään tahon omistamia. Tor-verkko on maailmanlaajuinen, vapaaehtoisten ylläpitämä vapaa ohjelmisto. (*The Tor Project: Overview* 2019)

Virtuaalinen erillisverkko, VPN, koostuu myös palvelimista. Nämä palvelimet suojelevat käyttäjän yksityisyyttä salaamalla viestit ja piilottamalla käyttäjän koneen IP-osoitteen. IP-osoite, joka näkyy muille, on VPN-palvelimen osoite. Iso ero Tor-verkkoon on kuitenkin se, että VPN-palveluiden tarjoaja (yritys tai jokin muu taho) hallitsee niin käyttäjän koneella olevan VPN-ohjelmiston kuin myös verkossa olevat palvelimet. (Ramadhani 2018)

5 Tor-verkon laillisuus

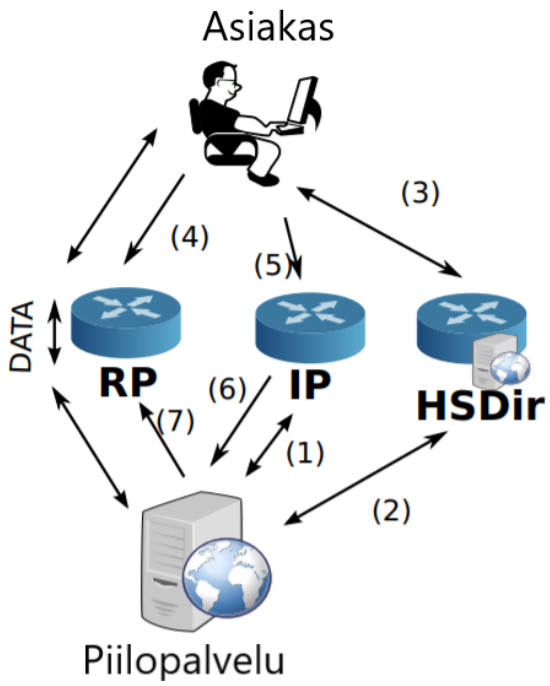
Tässä luvussa käsitellään Tor-verkon anonyymisyyden tuomat uhat ja Tor-verkon käyttöä Internet-sensuurin vastaisena työkaluna. Tämä luku jakautuu kahteen alalukuun: ensimmäinen alaluku käsittelee piilopalveluita, joita erityisesti rikolliset hyödyntävät kaupankäyntiä varten Tor-verkossa. Toinen alaluku käsittelee Tor-verkon merkitystä erityisesti internet-sensuurille altistuneille maille, kuten Kiinalle.

5.1 Piilopalvelut

Piilopalvelut (engl. hidden services) ovat olleet osana sipulireititystä jo vuodesta 1997, mutta niiden nykyisessä muodossa ovat otettu käyttöön vuonna 2004 (Øverlier ja Syverson 2007). Piilopalvelut sallivat Internet-palvelun, kuten esimerkiksi verkkosivun tai SSH-palvelimen, ylläpitämisen ilman sen IP-osoitteen ilmiantamista pavelun asiakkaille (Biryukov, Pustogarov ja Weinmann 2013). Tämä saavutetaan reitittämällä kaikki asiakkaan ja piilopalvelun välinen kommunikaatio kohtaamispaikan (engl. rendezvous point) kautta, joka yhdistää asiakkaan ja palvelimen anonyymit piirit (Biryukov, Pustogarov ja Weinmann 2013).

Kuviossa 4 on esitetty havainnollistava kuva piilopalveluiden eri osista. Tor-piilopalvelun arkkitehtuuri koostuu seuraavista komponenteista (Biryukov, Pustogarov ja Weinmann 2013):

- Internet-palvelu, joka on saatavilla Tor-verkon piilopalveluna;
- Asiakas, joka haluaa käyttää Internet-palvelua;
- Johdantokohdat (engl. introduction points (IP)): Piilopalvelun valitsemat solmut, joita käytetään hallintasolujen (engl. management cells) edelleenlähettämiseen, jotta voidaan yhdistää asiakas ja piilopalvelu kohtaamispaikassa;
- Piilopalvelun hakemistot (HSDir): Solmut, joissa piilopalvelu julkaisee deskriptoreita ja jotka kommunikoivat asiakkaiden kanssa saadakseen selville piilopalvelun johdantokohtien osoitteet;
- Kohtaamispaikka (engl. rendezvous point (RP)): Asiakkaan valitsema solmu, jota käytetään datan edelleenlähettämiseen asiakkaan ja piilopalvelun välillä;



Kuvio 4. Piilopalvelun komponentit. (Biryukov, Pustogarov ja Weinmann 2013, 82, muokattu)

Kuka tahansa voi perustaa Tor-verkkoon piilopalvelun. Piilopalveluiden osoitteet ovat muotoa XYZ.onion, missä XYZ on 16-merkkinen palvelun julkisesta avaimesta johdettu nimi. (*The Tor Project: Onion Services* 2019)

5.2 Tor-verkon käyttö sorretuissa maissa

Yhä useammat käyttäjät käyttävät Tor-ohjelmistoa sen sensuurin vastuskykyominaisuuksien vuoksi kuin sen tarjoaman anonyymisyyden takia. Jos Tor-verkkoa käytetään saadakseen pääsyn esimerkiksi Wikipedia- tai Blogspot-verkkosivulle, paikallinen sensuuri ja palomuurin säännöt eivät voi vaikuttaa siihen. Epävirallinen käyttäjätutkimus osoitti, että muutama sata tuhatta käyttäjää käyttää Tor-verkkoa päivittäin. Näistä käyttäjistä noin 20% on Kiinasta. (Dingledine ja Mathewson 2006)

Verkkoyhteyden määränpään salassapito on tehnyt Tor-verkosta houkuttelevan työkalun internet-

sensuurin kiertämiseksi. Tämä on johtanut Tor-ohjelmiston kehittäjät ja Kiinan sensuurilaitteen, suuren palomuuren (engl. Great Firewall of China), jatkuvaan kilpailuun. (Dunna, O'Brien ja Gill 2018)

Tor-kehitttäjien yksi merkittävä toimintasuunnitelma on ollut siltasolmujen (engl. bridge relays), tai siltojen, käyttö (Dunna, O'Brien ja Gill 2018). Siltasolmut ovat julkaisemattomia solmuja, joita Kiinassa olevat käyttäjät voivat käyttää muodostaakseen yhteyden Tor-verkoon (Dunna, O'Brien ja Gill 2018). Koska Tor-verkko käyttää lähteen reitittämistä (engl. source routing) saavuttaakseen viestinnän yksityisyyden ja kaikkien Tor-reitittimien tiedot ovat julkisesti listattuna internetissä, on Tor-verkkoon pääsyn rajoittaminen niin yksinkertaista kuin näille reitittimille muodostuvien yhteyksien estäminen (Ling ym. 2013).

Siltasolmu voi toimia ensimmäisenä hyppypaikkana Tor-verkon ytimeen. Siltojen tiedot eivät ole julkisesti saatavilla internetistä verrattuna Tor-reitittimiin (Ling ym. 2013). Vuonna 2011 Kiinan suuri palomuuri alkoi estämään julkaisemattomia Tor-verkon siltasolmuja (Dunna, O'Brien ja Gill 2018). Viimeisimmät tutkimukset ovat osoittaneet, että palomuuri toteuttaa niin pakettien syvätarkastuksen (engl. deep packet inspection) kuin myös aktiiviset verkon tutkimusmenetelmät voidakseen tunnistaa ja estää Tor-protokollan käyttö (Dunna, O'Brien ja Gill 2018). Kiinan suurta palomuuria on siten parannettu mahdollisuudella dynaamisesti estää Tor-verkon käyttö (Winter ja Lindskog 2012). Suunnitellaakseen tehokkaan sensuuria kiertävän työkalun tarvitaan kattava malli tavoitteista ja niiden sensoreiden resursseista, joita työkalun on tarkoitus kiertää. (Dingledine ja Mathewson 2006)

6 Yhteenveto

Tutkielmassa käsiteltiin Tor-verkon rakennetta ja toimintaa, sipulireitityksen kehitystä vuosien varrella, sipulireititystä, Tor-verkon ja virtuaalisen erillisverkon eroja, piilopalveluita sekä Tor-verkon käyttöä sorretuissa maissa, kuten Kiinassa.

Luvussa 2 kuvailtiin yleisellä tasolla internetin kerrosmaista rakenteesta ja sitä, että kaikkea olemassa olevaa tietoa ei tavalliset hakukoneet löydä. Samalla esiin tuotiin tarve erillisestä ohjelmistosta, joka mahdollistaa pääsyn syvään verkkoon. Luvussa 3 tarkennettiin Tor-verkon rakennetta ja toimintaa sekä sipulireitityksen kehitystä vuosien varrella.

Luku 4 käsitteli reitystä yleisellä tasolla pyrkien muodostamaan yleisen kuvan siitä, mitä reititysprotokollat on ja miten ne toimivat. Tämän jälkeen tuotiin esiin Tor-verkon käyttämä sipulireititystekniikka, jonka komponentteja ja toimintaa käsiteltiin tarkemmin. Lopuksi luvussa 4 käytiin läpi Tor-verkon ja virtuaalisen erillisverkon (engl. VPN) erot.

Luku 5 keskittyi Tor-verkon lailliseen puoleen. Siinä käytiin läpi piilopalveluiden toiminta ja niiden komponentit sekä miten Tor-verkko voi toimia sensuurin kiertämisen työkaluna.

Kirjallisuuskatsauksen tarkoituksena oli luoda lukijalle yhtenäinen kuva Tor-verkon tarkoituksesta ja toiminnasta sekä sen tuomista mahdollisuuksista erilaisia päämääriä tavoittelevien käyttäjien työkaluna. Lopulta Tor-verkko, kuten internetkin, on kaikkea sitä mitä käyttäjä haluaa sen olevan.

Jatkotutkimuksen aiheena voisi toimia miltei mikä tahansa tutkielmassa käsiteltävistä aiheista. Tutkielmassa ei juurikaan käsitelty Tor-verkon heikkouksia tai niiden vaikutuksia Tor-verkon korostamaan anonyymiteettiin. Tämä osa-alue on toki laaja, mutta tärkeä tutkimuskohde Tor-verkon kehittämisen ja sen luottamuksellisuuden kannalta.

Lähteet

Anttila, Aki. 2000. *TCP/IP tekniikka.* Helsinki Media.

Bergman, Michael K. 2001. “White paper: the deep web: surfacing hidden value”. *Journal of electronic publishing* 7 (1).

Biryukov, Alex, Ivan Pustogarov ja Ralf-Philipp Weinmann. 2013. “Trawling for tor hidden services: Detection, measurement, deanonymization”. Teoksessa *2013 IEEE Symposium on Security and Privacy,* 80–94. IEEE.

Casenove, Matteo, ja Armando Miraglia. 2014. “Botnet over Tor: The illusion of hiding”. Teoksessa *2014 6th International Conference On Cyber Conflict (CyCon 2014),* 273–282. IEEE.

Dingledine, Roger, ja Nick Mathewson. 2006. *Design of a blocking-resistant anonymity system Tor Project technical report, Nov 2006.*

Dunna, Arun, Ciarán O’Brien ja Phillipa Gill. 2018. “Analyzing China’s Blocking of Unpublished Tor Bridges”. Teoksessa *8th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 18).*

Europol. 2015. “The Internet Organised Crime Threat Assessment (IOCTA)”: TODO:sivut.

Jardine, Eric. 2015. *The Dark Web Dilemma: Tor, Anonymity and Online Policing.* Lontoo: Chatham house.

Khare, Ritu, Yuan An ja Il-Yeol Song. 2010. “Understanding deep web search interfaces: A survey”. *ACM SIGMOD Record* 39 (1): 33–40.

Ling, Zhen, Junzhou Luo, Wei Yu, Ming Yang ja Xinwen Fu. 2013. “Tor bridge discovery: extensive analysis and large-scale empirical evaluation”. *IEEE Transactions on Parallel and Distributed Systems* 26 (7): 1887–1899.

Loesing, Karsten, Steven J Murdoch ja Roger Dingledine. 2010. “A case study on measuring statistical data in the Tor anonymity network”. Teoksessa *International Conference on Financial Cryptography and Data Security,* 203–215. Springer.

McCoy, Damon, Kevin Bauer, Dirk Grunwald, Tadayoshi Kohno ja Douglas Sicker. 2008. “Shining light in dark places: Understanding the Tor network”. Teoksessa *International symposium on privacy enhancing technologies symposium,* 63–76. Springer.

Moy, John T. 1998. *OSPF: Anatomy of an Internet routing protocol.* Addison-Wesley Professional.

Otomo, Koju, Takeshi Itoh, Kazuyuki Hayashi, Hiroshi Omoto, Takayuki Yui, Makoto Suzuki ym. 1978. *Data sending and receiving system for packet switching network.* US Patent 4,074,232, helmikuu.

Ramadhani, E. 2018. “Anonymity communication VPN and Tor: a comparative study”. *Journal of Physics: Conference Series.*

Reed, Michael G., David M. Goldschlag ja Paul F. Syverson. 1996. “Hiding Routing Information”. *Naval Research Laboratory, Center For High Assurance Computer Systems* (Washington, D.C).

Snoeren, Alex C, Craig Partridge, Luis A Sanchez, Christine E Jones, Fabrice Tchakountio, Beverly Schwartz, Stephen T Kent ja W Timothy Strayer. 2002. “Single-packet IP traceback”. *IEEE/ACM Transactions on networking* 10 (6): 721–734.

Syverson, Paul. 2011. “A peel of onion”. Teoksessa *Proceedings of the 27th Annual Computer Security Applications Conference,* 123–137.

Syverson, Paul, Roger Dingledine ja Nick Mathewson. 2004. “Tor: The secondgeneration onion router”. Teoksessa *Usenix Security,* 303–320.

The Tor Project: History. 2020. Saatavilla WWW-muodossa, `https://www.torproject.org/about/history/`, viitattu 29.4.2020.

The Tor Project: Onion Services. 2019. Saatavilla WWW-muodossa, `https://2019.www.torproject.org/docs/onion-services`, viitattu 12.4.2020.

The Tor Project: Overview. 2019. Saatavilla WWW-muodossa, `https://2019.www.torproject.org/about/overview.html.en`, viitattu 7.4.2020.

Weimann, Gabriel. 2016. “Terrorist migration to the dark web”. *Perspectives on Terrorism* 10 (3): 40–44.

Wendell, Odom. 2010. *CCNP ROUTE 642-902 Official Certification Guide.* 800 East 96th Street Indianapolis, IN 46240: Cisco Press.

Winter, Philipp, ja Stefan Lindskog. 2012. “How china is blocking tor”. *arXiv preprint arXiv:1204.0447.*

Øverlier, Lasse, ja Paul Syverson. 2007. “Improving efficiency and simplicity of Tor circuit establishment and hidden services”. Teoksessa *International Workshop on Privacy Enhancing Technologies,* 134–152. Springer.