Henri Jussila

Keinot BGP:n tietoturvan parantamiseksi

Tietotekniikan pro gradu -tutkielma

28. helmikuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Henri Jussila

Yhteystiedot: henri.m.jussila@student.jyu.fi

Ohjaaja: Ari Viinikainen

Työn nimi: Keinot BGP:n tietoturvan parantamiseksi

Title in English: Methods for improving BGP security.

Työ: Pro gradu -tutkielma

Opintosuunta: Ohjelmisto- ja tietoliikennetekniikka

Sivumäärä: 51+3

Tiivistelmä: Tutkielmassa käsitellään BGP:n tietoturvaa ja sen sisältämiä heikkouksia. BGP:n tietoturvaan on esitetty useita erilaisia ratkaisuja, joita tarkastellaan tutkielmassa systemaattisen kirjallisuuskatsauksen keinoin. Tutkielman tarkoituksena on selvittää millaisia ratkaisuja on käyttöönotettu. Lisäksi tarkastellaan, kuinka nämä ratkaisut vertautuvat akateemisessa kirjallisuudessa esitettyihin ratkaisuihin. Tämän tiedon pohjalta on tarkoitus koostaa suosituksia siitä, mikä tekee ratkaisusta hyvän ja siten antaa pohja mahdolliselle jatkotutkimukselle.

Avainsanat: BGP, Tietoturva, Kaappaaminen, Kirjallisuuskatsaus

Abstract: The thesis is looking at BGP security and the weaknesses it has. There have been several proposed solutions to improve the security. In this work the solutions will be looked at through the lens of systematic literature review. The aim of the thesis is to find what solutions have actually been deployed and how they compare to the solutions proposed in academic literature. This information will be worked into a set of elements that are part of a "good"solution. Those elements could then be used as a basis for further research.

Keywords: BGP, Security, Hijacking, Literature Review

Kuviot

Taulukot

Sisällys

1 Johdanto

Border Gateway Protocol (BGP) (Rekhter, Li ja Harres 2006) on protokolla, jolla Internetin reititystä ylläpidetään. BGP:n tietoturva on kuitenkin hyvin paljon aikaansa jäljessä, ja Internetin jatkuvan toiminnan turvaamiseksi on tarpeellista tarkastella keinoja sen parantamiseksi.

Keskustelu BGP:n tietoturvan merkityksestä on jatkanut kasvuaan viimeisten vuosien aikana erilaisten kaappausten seurauksena, ja tarve ratkaisulle BGP:n tietoturvaongelmiin on ilmeinen. BGP:n tietoturvaa on tarkasteltu ennenkin kirjallisuuskatsauksen keinojen avulla, mutta uusin kirjallisuuskatsaus on vuodelta 2018 (Mitseva, Panchenko ja Engel 2018), ja viimeisen neljän vuoden aikana on julkaistu merkittävästi uutta kirjallisuutta, joka avaa uusia näkökulmia ongelmien ratkaisemiseksi.

Tutkielmassa tarkastellaan systemaattisen kirjallisuuskatsauksen menetelmin akateemisessa kirjallisuudessa esitettyjä keinoja BGP:n tietoturvan parantamiseksi. Tutkielman tarkoituksena on selvittää mitkä eri elementit, kuten esimerkiksi tehokkuuden eri osa-alueet ovat tärkeitä ratkaisulle, jotta sillä on mahdollisuus saavuttaa käyttöönotto tuotannossa. Tämän lisäksi tutkielma esittää näiden havaittujen elementtien pohjalta mahdollisia tulevia tutkimuskohteita.

Tutkielman rakenne muodostuu seuraavasti: Luvussa kaksi käsitellään tutkielman tavoitteita ja esitetään nämä tavoitteet tutkimuskysymysten muodossa. Luvussa kolme käsitellään tutkielman tutkimusmetodit. Luvuissa neljä ja viisi käsitellään BGP:n toiminta lyhyesti ja syvennytään sen sisältämiin tietoturvaongelmiin. Luvuissa kuusi ja seitsemän käsitellään kirjallisuuskatsauksen aineistoa ja sen antia. Luvussa kahdeksan tarkastellaan sitä, kuinka käytössä olevat ratkaisut vertautuvat kirjallisuuskatsauksen aineistoon. Luvuissa yhdeksän ja kymmenen käsitellään tutkielman antia ja tarkastellaan mahdollisia tulevia tutkimussuuntia.

2 Tutkimuskysymykset

Tutkielman tarkoituksena on tarkastella BGP:n tietoturvaa, sen heikkouksia ja akateemisessa kirjallisuudessa esitettyjä ratkaisuja näihin heikkouksiin. Tämän tarkastelun tavoitteena on saada vastauksia seuraaviin alla esiteltyihin tutkimuskysymyksiin.

- Mitä keinoja kirjallisuudessa on esitetty BGP:n tietoturvan parantamiseksi?
- Mitä keinoja on otettu käytäntöön BGP:n tietoturvan parantamiseksi?
- Kuinka nämä kaksi vastausjoukkoa kohtaavat, ja mitä niistä voidaan havaita?

Ensimmäiset kaksi tutkimuskysymystä muodostavat molemmat omat vastausjoukkonsa, joissa on todennäköisesti jonkin verran päällekkäisyyttä. Tätä päällekkäisyyttä tarkastelemalle tutkimuskysymyksessä kolme voidaan selvittää mahdollisia syitä sille, millaiset ratkaisut ja niiden sisältämät elementit vastaisivat parhaalla tavalla käytännön tarpeisiin. Näiden syiden ja elementtien pohjalta on mahdollista kohdentaa tulevaa tutkimusta sellaisiin kohteisiin, jotka antavat parhaat mahdolliset lähtökohdat onnistumiselle.

Seuraavassa luvussa tarkastellaan millaisilla keinoilla näihin yllä esitettyihin tutkimuskysymyksiin etsitään vastauksia.

3 Tutkimuksen metodi

Tutkielmassa käytetään metodina systemaattista kirjallisuuskatsausta ja tarkemmin Kitchenhamin ja Chartersin esittämää runkoa metodin käyttämiseen (Kitchenham ja Charters 2007).

Tietokantoina, joista kirjallisuuskatsauksen aineisto kerätään käytetään: Scopus, Web of Science, IEEE Xplore, ACM ja ProQuestin Telecommunications Database '&' Computer Science Database. Näillä saavutetaan hyvä, joskaan ei täydellinen kattavuus tutkittavaan alueeseen. Kuitenkin gradun resurrsien puitteissa rajaus on tehtävä johonkin. Toinen rajaus, joka tehdään kirjallisuuskartoituksen materiaaliin on, että kaikki muut tiedejulkaisuissa oleva materiaali tullaan rajaamaan pois.

Hakemiseen käytetään lähtökohtaisesti seuraavaa hakua: "BGP AND (Security OR Hijacking OR Validation OR Pathing OR Redirection OR Attack)". Tietokantojen käyttöliittymistä johtuen joissain tietokannoissa joudutaan muokkaamaan hakua, jotta sen tulokset vastaavat muita hakuja. Tarkat käytetyt hakuehdot löytyvät alla olevasta Taulukosta 1.

Annetuilla hakuehdoilla Scopus palauttaa 231 teosta, Web of Science 224, IEEE Xplore 42, ACM 290 ja ProQuest 466. Yhteensä 1253 teosta. 1253 teosta on gradun puitteissa liikaa. Kuitenkin haun tulokset palauttavat paljon teoksiksi, jotka eivät liity käsiteltävään aiheeseen. Näin dokumenttien määrä rajautuu alla esitetyillä kriteereillä noin 100-200 teokseen, jotka tulee tarkastella lähemmin. Noin 100 - 200 teosta on tutkielman puitteissa käsiteltävä määrä.

Artikkelien rajaamiseen liittyen tärkeä asia on kriteerit, jotka rajaavat artikkelit joko läpikäytäviin tai sen ulkopuolelle. Kriteerit ovat lähtökohtaisesti samat, kuin Kitchenham ja Charters esittävät luvuissa 6.2.* (Kitchenham ja Charters 2007). Eli kaikkien sisällyttämiskriteereiden (eng. inclusion) tulee täyttyä, kun samaan aikaan mikään poissulkemiskriteeri (eng. exclusion) ei saa täyttyä.

Scopus	TITLE-ABS-KEY (bgp AND (security OR hijacking OR validation OR pathing OR redirection OR attack)) AND (LIMIT-TO (SRCTYPE , "j"))
Web of Science	ALL=(BGP AND (Security OR Hijacking OR Validation OR patching OR Redirection OR Attack)) + Articles only
IEEE Xplore	BGP AND (Security OR Hijacking OR Validation OR patching OR Redirection OR Attack) + Journals only
ACM	BGP AND (security OR Hijacking OR Validation OR patching OR Redirection OR Attack) + Journals only
ProQuest	BGP AND (Security OR Hijacking OR validation OR Pathing OR Redirection OR Attack) + Scholarly journal Article only.

Taulukko 1. Hakuehdot

Sisällytyskriteerit:

- Kieli: englanti
- Julkaisu tutkimuskirjallisuudessa (peer reviewed journal)
- Käsittelee BGP-tietoliikenneprotokollaa
- Tarjoaa uuden ratkaisun BGP:n tietoturvaan liittyen (primary research)

Poissulkemiskriteerit:

- Vuosi < 1994 (ennen BGP:tä [RFC1654])
- Mahdolliset kaksoisjulkaisut (duplikaatit)
- Ei täyttä tekstiä saatavilla JYU:n / HY:n oikeuksilla

Kirjallisuuskatsauksen materiaalin käsittelyyn ja luokitteluun käytetään muokattuja kriteereitä Mitsevan, Panchenkon ja Engelin teoksesta (Mitseva, Panchenko ja Engel 2018, 46 - 48), koska pro gradu tutkielman puitteissa ei ole resursseja lähteä kehittämään uutta luokittelujakoa, sekä samalla tehdä systemaattista kirjallisuuskatsausta.

Mitsevan, Panchenkon ja Engelin luokittelusta kohdat Performance, Privacy ja Status otetaan käyttöön sellaisinaan. Attack coverage arvioidaan uuden kirjallisuuden valossa, että onko siihen tarvetta tehdä joitain lisäyksiä tai poistoja. Kuitenkaan teoksen julkaisusta ei ole kuin kolme vuotta, joten ei ole syytä olettaa tarvetta merkittäville muutoksille. Security eli control-/dataplane erottelu sivutetaan tutkielman käytettävien resurssien rajallisuuden takia kokonaan. Deployabilityn käsitettä muokataan hieman, sen tarkka määritelmä käsitellään myöhemmin, kun se on ajankohtaista.

Jokaisesta kirjallisuuskatsauksen materiaalin teoksesta otetaan ylös liitteessä A mainitut tiedot. Näin laaja materiaali saadaan koostettua helpommin analysoitavaan muotoon, josta voidaan etsiä yhdistäviä ja erottavia tekijöitä. Materiaalin koostamisen jälkeen näitä tekijöitä voidaan lähteä analysoimaan syvemmälle, ja etsimään vastauksia luvussa kaksi esitettyihin tutkimuskysymyksiin. Esimerkiksi tarkastelemalle käyttöönotettuja ratkaisuja ja niiden tehokkuuden kriteerejä voidaan löytää yhteisiä tekijöitä, jotka mahdollisesti selittävät teknologioiden käyttöönottoa.

3.1 Tutkimuksessa huomioitavat tekijät

Johtuen siitä, että tutkimusta tekee vain yksi ihminen, on työskentelyssä mahdotonta kokonaan välttää henkilökohtaisia vinoumia (eng. personal bias). Nämä vinoumat ovat merkittävimmillään, kun teoksia rajataan sisään ja ulos materiaalista rajauskriteereiden mukaan, sekä silloin kun materiaalia luokitellaan liitteen A mukaisilla kriteereillä. Vinoumien vaikutus on tarkoitus minimoida tarkoilla ja selkeillä kriteereillä, joiden avulla tutkimuksen materiaalin kerääminen voidaan näin haluttaessa toistaa. Lisäksi tutkimuksen koostettu materiaali on saatavilla halukkaille liitteessä B.

3.2 Aikaisempi tutkimus

BGP:n tietoturvaa on tutkittu aikaisemminkin kirjallisuuskatsauksen keinoin, mutta uusinkin löydetty kirjallisuuskatsaus on tässä vaiheessa jo useamman vuoden vanha (kesäkuulta 2018) (Mitseva, Panchenko ja Engel 2018). Toiseksi työssä on tarkoituksena toteuttaa kirjallisuuskatsaus systemaattisesti, joka tuo oman lisäarvon tutkimukselle, koska sillä katetaan edellisiä tutkimuksia laajempi osa tutkimuskirjallisuudesta. Näin ollen on uskottavaa olettaa, että tutkimuksen on mahdollista tuottaa uutta tieteellistä arvoa. Alla on listattu tiedossa olevat aikaisemmat kirjallisuuskatsaukset samasta aiheesta.

- (Nicholes ja Mukherjee 2009)
- (Butler ym. 2010)
- (Huston, Rossi ja Armitage 2011)
- (Bakkali, Benaboud ja Ben Mamoun 2013)
- (Sharma ja Sharma 2015)
- (N. Wang ym. 2017)
- (Mitseva, Panchenko ja Engel 2018)

Oman tieteellisen arvon tutkimukseen tuo myös kolmas tutkimuskysymys, jonka tarkoituksena on selvittää tekijöitä, jotka yhdistävät käyttöönotettuja ratkaisuja. Näihin tekijöihin voisi olla syytä keskittää mahdollista tulevaa tutkimusta, jotta voidaan selvittää miksi nämä tekijät erottuvat joukosta. Seuraavassa luvussa tarkastellaan BGP:tä ja sen toimintaa.

4 BGP:n toiminta ja käyttötarkoitus

BGP on TCP/IP:n mukaisesti sovelluskerroksen reititysprotokolla, jonka avulla Internetissä liikkuva liikenne ohjautuu oikeaan osoitteeseen. Protokollan nykyversio BGP-4 on vuodelta 2006 (Rekhter, Li ja Harres 2006), joskin protokollan ensimmäiset luonnokset johtavat juurensa aina 80- ja 90-luvun taitteeseen asti (Lougheed ja Rekhter 1990). Vaikka protokolla ei olekaan saanut varsinaista uutta versioitua standardia yli 15 vuoteen, on siihen esitetty joukko erilaisia parannuksia, joista osa on otettu aktiiviseen käyttöön.

BGP:n käyttäjien määrä on myös nähnyt merkittävää kasvua viimeisten vuosikymmenten aikana (Huston, Smith ja Bates 2021). BGP-reittejä ilmoittavien AS:ien (eng. Autonomous System) määrä on noussut vuosituhannen vaihteen noin 5000 AS:tä nykyhetken yli 70 000. Tämä johti myös siihen, että AS:n numerointi piti siirtää 16 bitistä 32 bittiin (Vohra ja Chen 2012). 16 bitin ylärajan ollessa 65 536, joka olisi tässä vaiheessa täyttynyt. BGP:n käyttäjäkunta on myös laaja.

BGP:n toiminta käytännössä on protokollatasolla melko yksinkertaista. Kuten Rekhter, Li ja Harres määrittävät RFC:ssä 4271 (Rekhter, Li ja Harres 2006), kahden BGP tahon välille avataan yhteys TCP-protokollan päälle. Tämän jälkeen tahot vaihtavat OPEN-viestit keskenään ja vahvistavat ne KEEPALIVE-viesteillä (Rekhter, Li ja Harres 2006, 4.2, 4.4). Tämän jälkeen tahot voivat lähettää UPDATE-viestejä (Rekhter, Li ja Harres 2006, 4.3), joilla he voivat ilmoittaa muutoksista reititykseen. UPDATE-viestit ovat OPEN- ja KEEPALIVE-viestejä monimutkaisempia siinä mielessä, että niiden sisältö saattaa vaihdella viestistä riippuen, koska yksittäisellä UPDATE-viestillä voidaan sekä ilmoittaa uusi reitti, että tarvittaessa poistaa vanhentuneita reittejä käytöstä.

Näistä kolmesta viestistä katsotaan tarkemmin UPDATE-viestin toimintaa, koska sillä tehdään muutokset reititykseen. Muiden viestien toimintaan ei tutustuta tässä teoksessa tarkemmin, mutta halukkaat löytävät ne protokollan dokumentaatiosta (Rekhter, Li ja Harres 2006). UPDATE-viesti koostuu kolmesta osasta: Poistetut reitit, reittiatribuutit ja verkkokerroksen saavutettavuusinformaatio (eng. Network Layer Reachability Information). Poistetut reitit ilmoitetaan IP-osoitteena ja maskina, reittipoistoja voi olla 0..n kappaletta yhdessä viestissä.

Seuraavaksi viestissä ilmoitetaan reittiatribuutit, joista pakollisia ovat (ORIGIN, AS_PATH ja NEXT_HOP). Näiden lisäksi vapaaehtoisia atribuutteja ovat (MULTI_EXIT_DISC, LOCAL _PRREF, ATOMIC_AGGREGATE JA AGGREGATOR). Viimeksi viestissä tulevat mahdolliset uudet reitit verkkokerroksen saavutettavuusinformaation osassa. Uudet reitit ilmoitetaan samalla tavalla, kuin poistot mutta tässä tulee huomata, että kaikki ilmoitettavat reitit jakavat samat reittiatribuutit. Uusia reittejä voi olla yhdessä viestissä myös 0..n kappaletta.

UPDATE-viestien sisältö säilytetään RIB:ssä (eng. Routing Information Base) (Rekhter, Li ja Harres 2006, 3.2). RIB voidaan jakaa kolmeen erilliseen osaan. Adj-RIBs-In, Loc-RIB ja adj-RIBs-Out. Adj-RIBs-In sisältää kaikki UPDATE-viesteissä tulleet reitti-ilmoitukset. Loc-RIB puolestaan sisältää Adj-RIBs-In hyväksytyksi valitut reitit, joita käytetään reitityksseen. Se kuinka reitit tulee hyväksyä Adj-RIBs-Instä Loc-RIBiin ei ole määritelty protokollatasolla, vaan se jätetään toimijoiden päätettäväksi. Adj-RIBs-Out puolestaan sisältää reitit, joita AS ilmoittaa (eng. announces) muille tahoille UPDATE-viesteissä.

Huomioksi, että BGP:stä saatetaan myös käyttää termejä IBGP (Internal-BGP) ja EBGP (External-BGP) (Rekhter, Li ja Harres 2006). IBGP:tä käytetään kuvaamaan yhden AS:n sisällä tapahtuvaa BGP:tä, kun taas EBGP:ssä "puhujina"on kaksi erillistä AS:ää. Tässä tutkimuksessa keskitytään lähinnä EBGP:hen ja niiden välillä kulkevaan liikenteeseen liittyviin riskeihin, joskin osa käsitellyistä ratkaisuista saattaa olla sovellettavissa myös IBGP:hen liittyviin ongelmiin. IBGP:n kohdalla ongelmat muodostuvat lähinnä inhimillisistä virheistä.

Mitä puolestaan BGP:n tulevaisuuteen tulee, niin BGP:lle ei näy ainakaan toistaiseksi yhtäkään realistista korvaavaa teknologiaa. Vaan parannukset Internetin reititykseen tullaan tekemään kehittämällä BGP:tä ja sitä ympäröiviä ratkaisuja eteenpäin vastaamaan nykyisiin tarpeisiin. Syitä sille, miksi ongelmaa ei yritetä ratkaista uudella protokollalla, vaan laajennuksella vanhaan on useita. Merkittävin näistä on kuitenkin se, että uusi protokolla vaatisi laajamittaisesti uutta teknologiaa, joko ohjelmistotasolla tai rautatasolla. Tämä teknologia vuorostaan vaatisi investointeja, joka puolestaan tulisi kohtaamaan muutosvastarintaa. Seuraavassa luvussa tarkastellaan, millaisiin ongelmiin mahdolliset päivitykset yrittävät vastata.

5 BGP:n Tietoturvaongelmat

Kuten edellisessä kappaleessa todettiin, on BGP nykyisessä vaiheessa elinkaartaan ikääntynyt protokolla, joka kehitettiin aikana jolloin tietoturva ei ollut tärkeänä osana protokollan suunnitteluvaihetta. Kuitenkin aika on edennyt tästä, ja nykyään tietoturva on asia, jonka merkitykseen on herätty ja siihen kiinnitetään enemmän huomiota ja sen parantamiseen keskitetään resursseja.

Kuten Huston, Rossi ja Armitage toteavat kirjallisuuskatsauksessaan (Huston, Rossi ja Armitage 2011) BGP:ssä ei ole protokollatasolle sisäänrakennettua varmennusta sille mitä osapuolet viestittävät, vaan protokollan toiminta perustuu osapuolien väliseen luottamukseen, että informaatio jota toinen osapuoli lähettää on oikeaa ja validia. Protokollan rakentamisesta luottamuksen päälle ongelmallisen tekee aiemmassa kappaleessa mainittu BGP:n massiivinen noin 1400% kasvu AS:ien määrässä viimeisen kahden vuosikymmenen aikana. Vaikka kaikki osapuolet toimisivatkin oikein ja huolellisesti. Tulee silti huomioida inhimillisten virheiden riski, joka kasvaa samassa suhteessa käyttäjien määrään kasvuun. Inhimillisen virheen tapahtumiseen ei tarvita muuta, kuin yksi väärä painallus numeroita syötettäessä, jota ei huomata ja virhe lähtee siitä leviämään.

Luottamuksesta teki ongelmallisen myös se, että BGP:ssä ei alkuperin ollut protokollatasolla todentamista (eng. authentication), jonka avulla voitaisiin varmistaa puhujien identiteetti. RFC-2385 (Heffernan 1998) esitti MD5 pohjautuvan toteutuksen, jolla BGP:tä voidaan suojata yksinkertaisilta hyökkäyksiltä. Tämä toteutus vahvistettiin osaksi BGP protokollan versio 4 RFC-4271ssä (Rekhter, Li ja Harres 2006). Kuitenkin MD5 on nykyään vanhentunut protokolla kryptografisiin tarkoituksiin kuten Stewens, Lenstra ja Weger havainnollistavat (Stewens, Lenstra ja Weger 2012).

MD5:n heikkouksiin on esitetty ratkaisuksi RFC-5925ssä (Touch, Mankin ja Bonica 2010) toteutus, joka korjaa MD5 toteutuksen ongelmia. Tätä toteutusta ei kuitenkaan toistaiseksi ole otettu pakolliseksi osaksi BGP-protokollaa, vaan MD5 pohjautuvat toteutukset ovat edelleen protokollan puolesta sallittuja. Kuitenkin mainittakoon, että nykyisten IETF:n RFC-7454:ssä / BCP-194 (Durand, Pepelnjak ja Doering 2015) annettujen vallitsevien parhaiden

käytäntöjen (eng. Current Best Practices) mukaan RFC5925:ssä esitettyä TCP-AO:ta TULISI (eng. SHOULD (Bradner 1997)) käyttää MD5 pohjautuvan toteutuksen sijaan. Protokollan salaamisen parantaminen toisi suojausta ulkoisia hyökkääjiä vastaan.

BGP:n protokollatason mahdollisia muita virheitä ja heikkouksia on käsitelty laajasti esimerkiksi Murphyn toimesta RFC-4272:ssä (Murphy 2006) ja reititysprotokollia uhkaavia uhkia on käsitelty yleisesti Barbirin, Murphyn ja Yangin toimesta RFC-4593:ssä (Barbir, Murphy ja Yang 2006). Lisäksi aiheesta on aikaisemmin kirjoitettu kirjallisuuskatsauksia, joissa on myös paneuduttu näihin ongelmiin. Näitä kirjallisuuskatsauksia on tarkasteltu tarkemmin luvussa 3.3 Aikaisempi tutkimus.

On myös mahdollista, että näitä yllä käsiteltyjä BGP:n heikkouksia käytetään tahojen toimesta tarkoituksellisesti jonkinlaisen hyödyn tavoittelemiseen. Tarkoituksellisien kaappausten todistaminen on kuitenkin vaikeaa, koska käytännössä täytyy todistaa, että kyseessä ei ollut tahaton kaappaus eli inhimillinen virhe tai vahinko.

Lopulta kaappauksen tahallisuudella ei kuitenkaan ole merkittävästi väliä lopputuloksen kannalta, koska kaappaus aiheuttaa joka tapauksessa haittaa taholle jonka IP-avaruus (eng. address space) kaapattiin, ja myös käyttäjille jotka käyttävät tämän tahon palveluita. Kaappauksien tapahtuminen on realiteetti, jota tapahtuu, kuten Ballani, Francis ja Zhang toteavat tutkimuksessaan (Ballani, Francis ja Zhang 2007).

Tällaisien tahallisten hyökkäyksen toteuttamista on teorisoitu esimerkiksi Apostolakin, Zoharin ja Vanbeverin toimesta Bitcoiniin kohdennettuna (Apostolaki, Zohar ja Vanbever 2017) tai vaihtoehtoisesti Ekparinya, Gramoli ja Jourjonin tutkimus Etherneumiin kohdistettuna (Ekparinya, Gramoli ja Jourjon 2018). Kuitenkaan tämän mittakaavaan hyökkäyksien toteuttamisen käytännöllisyydestä ei ole tarkkaa selvyyttä. Kuitenkin kryptovaluutat niiden täysin digitaalisesta luonteesta johtuen ovat mahdollisesti merkittävä kohde hyökkäyksille, joihin BGP:n tulisi kyetä tulevaisuudessa vastaamaan.

Viimeaikaisten tapahtumien johdosta BGP on noussut suuremman joukon tietoon, kun Facebook kärsi käyttökatkoksesta 2021.10.04 (Facebook 2021b). Käyttökatkoksen takana oli virheellinen komento, joka puolestaan aiheutti ketjureaktion, joka toi kaikki Facebookin palvelut alas useiden tuntien ajaksi (Facebook 2021a). Vaikka tässä tapauksessa ei ollutkaan kyse

suoraan BGP:hen liittyvästä virheestä, on tämä kuitenkin esimerkki siitä, kuinka suurta roolia Internetin toiminnasta BGP kantaa harteillaan, ja mikäli BGP:n toiminta jostain syystä estyy, on seurauksena yleensä laaja häiriö.

Puolestaan tapaus, jossa BGP oli selkeänä syynä Internetin toiminnan häiriössä on, kun Googlen palvelut olivat marraskuussa 2018 kaapattuna väärän BGP reitti-ilmoituksen (Prefix hijacking) takia yli tunnin ajan (Google 2018). Tarkemmin tämän kaappauksen takana oli konfiguraatiovirhe pienellä Internet operaattorilla, jonka seurauksena väärä reitti levisi ympäri Internetiä (ThousandEyes 2018). Tämän inhimillisen virheen seurauksena merkittävä osa Internet liikenteestä Pohjois-Amerikassa ohjautui väärään suuntaan, ja lopputulos oli verrannollinen palvelunestohyökkäykseen Googlen palveluita kohtaan. Tämä on jälleen vain yksi esimerkki siitä, kuinka herkkä kokonaisuus BGP lopulta on, ja kuinka suuria häiriöitä yksittäinenkin virhe voi lopulta aiheuttaa.

Kuitenkin BGP:ssä on mahdollisuus isompaankin vahinkoon, koska kuten Ballani, Francis ja Zhang havainnollistavat, liikenne voidaan yrittää kaapata kokonaan kaappaajien haluamaan kohteeseen (Ballani, Francis ja Zhang 2007, 267). Tai liikenne voidaan uudelleenohjata kaappaajan kautta lopulta alkuperäiseen kohteeseensa (eng. interception attack) (Ballani, Francis ja Zhang 2007, 268). Tämä mahdollistaa liikenteen tallentamisen mahdollista tulevaa käyttöä varten. Tuleva käyttö voi olla lähes reaaliaikaista salakuuntelua, mikäli liikennettä ei ole salattu. Liikenne voidaan myös tallentaa tulevaisuutta varten siltä varalta, että salaus pystytään murtamaan myöhemmin. Uudelleenohjaaminen on vaarallista myös siksi, että loppukäyttäjälle asti tilanne ei välttämättä näyttäydy millään muulla tavalla, kuin että palvelun käytössä on normaalia enemmän viivettä, liikenteen kulkeman pidemmän reitin seurauksena.

BGP:stä on selkeästi nykyään nähtävissä sen ikä ja tarve uudistuksille, jotka auttavat sitä vastaamaan 2000-luvun alati muuttuviin tarpeisiin. Uudistuksia on esitetty paljon erilaisia, joista kaikilla on hyötynsä ja heikkoutensa. Seuraavissa luvuissa tullaan tarkastelemaan näitä uudistuksia, ja sitä miten nämä uudistukset mahdollisesti auttaisivat BGP:tä ja Internetiä kokonaisuutena toimimaan paremmin tulevaisuudessa.

6 Kirjallisuuskatsauksen aineisto

Systemaattisen kirjallisuuskatsauksen aineisto kerättiin luvussa kolme valituista tietokannoista annettujen kriteerien perusteella. Aineiston kerääminen aloitettiin 02.11.2021, aineistonkeruu päättyi 04.11.2021. Aineistonkeruu onnistui ilman merkittäviä ongelmia.

Aineistonkeruu aloitettiin IEEEXplore tietokannasta (IEEE 2022). IEEEXploresta kerättiin 2.11. yhteensä 42 teosta tarkempaa tarkastelua varten. Seuraavaksi kerättiin Scopus (Scopus 2022) 3.11., josta saatiin kerättyä 84 teosta erilaisten maksumuuri ja saatavuusongelmien jälkeen. Seuraavaksi kerättiin Web of Sciencestä (Clarivate 2022) 112 teosta 4.11., ACM (Computing Machinery 2022) 78 teosta 4.11. ja viimeisenä ProQuest (ProQuest 2022) 37 teosta 4.11.

Yhteensä eri tietokannoista kerättiin 353 teosta. Kuitenkin moni tietokannoista indeksoi samoja julkaisuja. Tästä seuraa se, että tarkastamalla teokset duplikaattien osalta jää jäljelle 269 teosta. Aineistolle suoritettiin tämän jälkeen ensimmäinen alustava. Alustavassa läpikäynnissä tarkasteltiin teoksia tiivistelmien osalta läpikäynti luvussa kolme annettujen kriteerien perusteella. Tämä tiputti aineiston koon 81 teokseen. Tämän jälkeen suoritettiin toinen tarkempi läpikäynti. Tarkemmassa läpikäynnissä selattiin koko artikkeli, mikäli tiivistelmä ei riittänyt rajauksen tekemiseen, jossa aineisto tippui lopulliseen 42 teosta kattavaan kokoonsa.

Koko aineisto löytyy tutkielman liitteestä B. Seuraavissa luvuissa tarkastellaan tätä aineistoa, ja etsitään aineistosta mahdollisia suuntia, johon viedä BGP:n kehitystä tulevaisuudessa.

7 Kirjallisuuskatsauksen läpikäynti

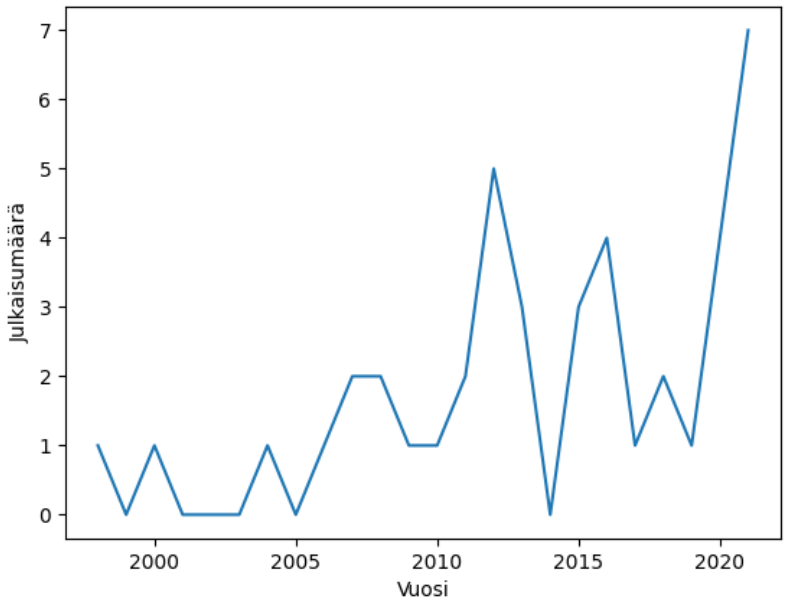
Aineisto käsittelee BGP:n tietoturvaa ja sen heikkouksia useista eri näkökulmista, samalla tarjoten paljon erilaisia ratkaisuja, joilla kaikilla on vahvuutensa ja heikkoutensa BGP:n tietoturvan parantamiseksi.

Aineistoa ajallisesti tarkastellessa voidaan huomata, että mitä lähemmäs nykyhetkeä alla olevassa kuviossa 1 edetään, sitä tiheämpi aineiston julkaisunopeus on ollut. Tarkkaa yksittäistä selitystä tälle ilmiölle on vaikea antaa. Kuitenkin esimerkiksi tietoturvan korostunut merkitys viime vuosien aikana voi olla yksi selittävä tekijä. Toinen mahdollinen tekijä voisi olla lohkoketjujen suosion kasvaminen viimeisen muutaman vuoden aikana. Materiaalin artikkeleista seitsemän (7) neljästäkymmenestä kahdesta (42) perustaa ratkaisunsa lohkoketjuihin.

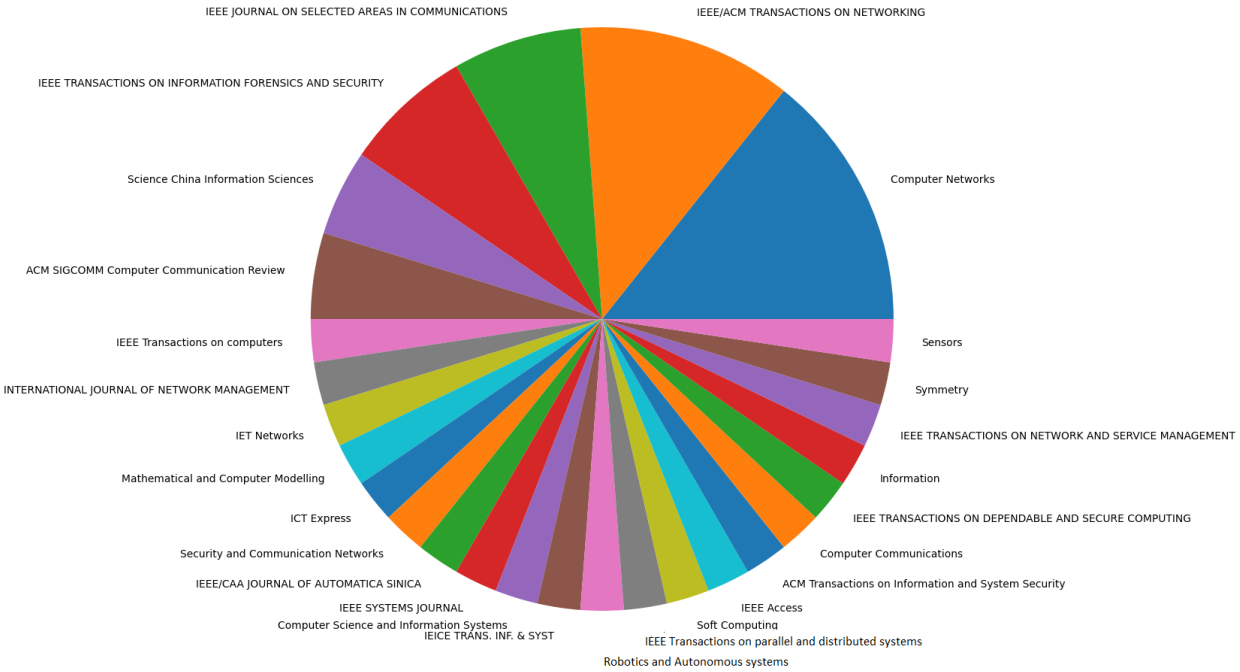
Toinen havainto, jonka aineistoista pystyy tekemään on se, kuinka laajaan joukkoon erilaisia akateemisia julkaisuja aineisto on hajautunut. Aineisto koostuu yhteensä 41 artikkelista, jotka ovat jakautuneet yhteensä 27 akateemiseen julkaisuun. Aineiston julkaisujen tarkempi erittely löytyy alla olevasta kuviosta 2 tai liittestä B. Käytännössä on nähtävissä, että tutkimusalueella ei ole yksittäistä johtavaa julkaisua vaan aineisto on hajautunut laajaan joukkoon julkaisuja.

Kolmas aineistosta tehtävissä oleva selkeä havainto on se, että siinä esitettyjä ratkaisuja ei ole otettu käyttöön. Syitä tälle on useita. Yksi niistä on aineiston painottuminen lähelle kirjoitushetkeä joka tarkoittaa, että mahdollinen aikaikkuna ratkaisujen toteuttamiseen on melko pieni. Toinen (osa)selitys tälle on se, että valtaosa Internetin teknologisista ratkaisuista ei tule suoraan akatemiasta, vaan niitä kehitetään esimerkiksi IETF:n toimesta RFC:eiksi, jotka vuorostaan otetaan käyttöön sovellettuna.

Seuraavassa alaluvussa käsitellään erilaisia ongelmia, joihin tutkimusartikkelit yrittävät löytää ratkaisuja. Tämän jälkeen tarkastellaan sitä, kuinka tehokkaita nämä ratkaisut mahdollisesti olisivat. Sen jälkeen tarkastellaan reitityksen yksityisyyttä. Luvun lopuksi tarkastellaan vielä, kuinka käytännöllisiä nämä ratkaisut olisivat ottaa käytäntöön, ja mitä käyttöönotettavuus merkitsee tässä kontekstissa.



Kuvio 1. Julkaisut vuosittain



Kuvio 2. Akateemiset julkaisut

7.1 BGP:n hyökkäyspinnat

Tulevat alaluvut on jäsennelty seuraavasti: ensimmäisenä tiivistetään lyhyesti kyseisessä alaluvussa käsiteltävä ongelma, seuraavaksi käydään läpi tähän ongelmaan ratkaisuja tarjoavat teokset, lopussa tarkastellaan materiaalista tehdyt havainnot ja pohjustetaan siirtymä seuraavaan ongelmaan / hyökkäyspintaan.

Ratkaisujen tehokkuutta ongelmien ratkaisussa on arvioitu seuraavalla asteikolla: Ratkaisu saa arvon 2, mikäli ratkaisu esittää kokonaisvaltaisen ratkaisun ongelmaan. Ratkaisu saa arvon 1, mikäli ratkaisu esittää osittaisen ratkaisun käsiteltävään ongelmaan. Arvo 0 saadaan silloin, mikäli ratkaisua ongelmaan ei esitetä teoksessa.

Huomiona, että valtaosa ratkaisuista ei kuulu vain yhteen kategoriaan. Vaan ne saattavat toimia ratkaisuna useampaankin ongelmakategoriaan, mutta kategoriat on lähtökohtaisesti valittu niin, että ongelma jota ratkaisu yrittää pääasiassa ratkaista on se, jonka alle ratkaisu on liitetty. Toinen huomio on, että alalukujen sisäinen järjestys on se, missä artikkelit ladattiin tietokannoista.

7.1.1 Osoitekaappaus

Aineiston valossa osoitekaappaus on yleisin ongelma, johon lähdemateriaalin kirjallisuudessa on lähdetty esittämään ratkaisuja. Osoitekaappaus on kenties klassisin hyökkäys BGP:tä vastaan. Hyökkäys on myös hyvin yksinkertainen toteuttaa, koska BGP ei protokollatasolla sisällä tietoturvaa tai keinoa varmistaa ilmoitettuja reittejä. Tarvitsee hyökkääjän vain ilmoittaa reitti halumaansa kohteeseen (osoitteeseen) (eng. prefix), ja mikäli hyökkääjä on lähempänä kuin alkuperäinen oikea kohde, kulkee liikenne tässä tilanteessa lähtökohtaisesti hyökkääjälle oikean kohteen sijaan. Seuraavaksi käydään lyhyesti läpi kirjallisuudessa esitetyt ratkaisut osoitekaappaukseen.

Kent, Lynn ja Seo kehittävät ratkaisun (Kent, Lynn ja Seo 2000) BGP:n tietoturvan parantamiseksi. Ratkaisu on kenties klassisin esimerkki esitetysti parannuksesta BGP:hen. Ratkaisu perustaa juurensa kryptografiaan ja PKI:hin, jolla turvataan BGP:n UPDATE-viestien oikeellisuus.

Moriano, Hill ja Camp tarkastelevat teoksessaan (Moriano, Hill ja Camp 2021) mahdollisuutta käyttää hyödyksi havaintoa, että BGP häiriön tapahtuessa BGP-UPDATE viestien määrässä on havaittavissa aaltoilua (eng. burstiness), jossa häiriötä aiheuttavat UPDATE-viestit tulevat usein yhdessä nopeassa aallossa. Tätä tietoa käyttämällä voidaan rakentaa julkisen tiedon pohjalta malli, joka arvioi milloin kyseessä saattaa olla häiriö / hyökkäys.

Schlamp ym. kehittävät teoksessaan (Schlamp ym. 2016) ratkaisun, jolla kyetään tunnistamaan mahdolliset osoitekaappaukset. Ratkaisu hyödyntää joukkoa erilaista tietoa kuten verkkotopologiaa ja reititysrekistereitä, joka vuorostaan syötetään matemaattiseen malliin, joka arvioi onko kyseessä osoitekaappaus vai normaali tilanne (eng. legitimate event).

Sermperzis ym. esittävät teoksessaan (Sermpezis ym. 2018) ratkaisun, jolla kyetään havaitsemaan ja neutralisoimaan osoitekaappaukset. Ratkaisu perustaa toimintansa siihen, että sitä käytetään lokaalisti, näin se tietää käyttäjän hallinnoimat osoitteet ja kykenee havaitsemaan väärennetyt reitit näihin osoitteisiin. Neutralisointi perustuu ennalta määriteltyjen toimenpiteiden automaattiseen aktivointiin, mikäli osoitekaappaus havaitaan.

Xiang ym. kehittävät teoksessaan (Xiang ym. 2013) kryptografiaan perustuvan ratkaisun, jossa tietty määrä BGP:n reitistä allekirjoitetaan kryptografisesti. Ratkaisun hyötynä on muun muassa se, että näin kyetään vähentämään tarvittavan kryptografian määrää. Tämä puolestaan myös nopeuttaa liikenteen käsittelyä. Ratkaisu kuitenkin varmistaa reitin olemassaolon, vaikka koko reittiä ei olekaan allekirjoitettu.

Zhang, Li, ja Zhao kehittävät teoksessaan (Zhang, Li ja Zhao 2019) immuunijärjestelmään perustuvan mallin, joka kykenee tunnistamaan osoitekaappaukset. Mallia hyödynnetään BGP:n UPDATE-viestien käsittelyssä, ja mikäli UPDATE-viesti havaitaan hyökkäykseksi, tiputetaan se ennen kuin sillä on mahdollisuus vaikuttaa reititykseen.

Guo ja Wang esittävät teoksessaan (Guo ja Wang 2012) immuunijärjestelmään perustuvan ratkaisun reitityksen suojaamiseen. Ratkaisu perustuu äärellisiin automaatteihin (eng. Finite State Machine [FSM]), sekä "immuunimuistiin"tapauksista, jotka ovat olleet haitallisia. Mikäli ratkaisu tunnistaa päivityksen "immuunimuistista"poistetaan se.

Pradeepa ja Pushpalatha esittävät teoksessaan (Pradeepa ja Pushpalatha 2020) SDN:ssä (Softwa-

re Defined Networking) toteuttavan ratkaisun, jolla seurataan ja analysoidaan BGP:ssä tapahtuneet epäilyttävät tapahtumat ja mikäli niin tapahtuma havaitaan hyökkäykseksi, siihen reagoidaan.

Hong, Ju ja Hong tarkastelevat teoksessaan (Hong, Ju ja Hong 2013) periaatteessa yksinkertaista, mutta kuitenkin hyvin tehokasta tapaa havaita osoitekaappaukset. Ratkaisu perustuu reitin varmistamiseen "sormenjäljillä"(eng. fingerprinting), joiden avulla voidaan varmistua siitä, että muuttunut reitti johtaa edelleen oikeaan kohteeseensa eikä kyseessä ole osoitekaappaus.

Chang ym. esittävät teoksessaan (Chang ym. 2012) maineeseen (eng. reputation) perustuvan ratkaisun BGP:n turvaamiseksi. Ratkaisu arvostelee historiallisen tiedon valossa AS:t erilaisiin luokkiin. Tämän tiedon avulla ratkaisu arvioi BGP:n UPDATE viestien sisältöä ja voi nostaa hälytyksen, mikäli ratkaisu arvioi, että kyseessä on osoitekaappaus.

Lu, Tang ja Sun, kehittävät teoksessaan (Lu, Tang ja Sun 2021) lohkoketjuihin perustuvan ratkaisun. Ratkaisussa hyödynnetään lohkoketjujen hajautettua luonnetta siihen, että ratkaisussa ei ole yhtä rikkoutumispistettä (eng. point of failure). Kaikilla toimijoilla on lohkoketjun ansiosta pääsy ajantasaiseen reititysinformaatioon, jonka ansiosta väärät reitit ja osoitekaappaukset voidaan tunnistaa ja neutralisoida.

Li ym. kehittävät teoksessaan (P. Li ym. 2021) myöskin lohkoketjuihin perustuvan ratkaisun. Tässäkin ratkaisussa lohkoketjuja esitetään ratkaisuksi keskitettyjen ratkaisujen ongelmiin. Ratkaisun hyötyinä voidaan nähdä PKI-ratkaisuja kevyempi kryptografia sekä tarvittaessa kevyt avainten poistaminen (eng. revocation).

Mastilak ym. esittävät myös teoksessaan (Mastilak ym. 2020) lohkoketjuun perustuvaa ratkaisua BGP:n tietoturvaongelmiin. Ratkaisu keskittyy lähtökohtaisesti siihen, että reitityksen oikeellisuus on varmistettu lohkoketjun toimesta, ennen kuin reititys edes siirrettään reitittimeen.

He ym. rakentavat teoksessaan (He ym. 2020) lohkoketjuihin perustuvan ratkaisun BGP:n turvaamiseksi. Ratkaisu perustuu reitityksen vahvistamiseen lohkoketjuun merkittyjen omistuksien kautta. Lohkoketjun muokkaaminen puolestaan on turvattu niin, että vain sallitut

(eng. whitelisted) tahot pystyvät tekemään uusia tapahtumia lohkoketjuun.

Yan ja Lee kehittävät teoksessaan (Yan ja Lee 2021) myös lohkoketjuihin perustuvan ratkaisun, jossa reititys tapahtuu älykkään sopimuksen (eng. smart contract) avulla. Asiakkaat tekevät sopimuksen lohkoketjuun, jonka reitittimet voivat hyväksyä ja näin sopia siirtävänsä liikennettä sopimuksen mukaisesti eteenpäin sopimuksen kohteeseen.

McDaniel ym. tarkastelevat teoksessaan (McDaniel ym. 2006) reititystä ja alkuperän vahvistamista (Origin authentication). Ratkaisussa kehitetään formaali tapa delegoida osoitteita ja seurata niiden delegaatiota. Teoksessa havaitaan myös, että Internetissä on joukko suuria toimijoita, jotka kattavat merkittävän osan Internetin osoiteavaruudesta (vuonna 2006), ja tätä voidaan käyttää hyödyksi ratkaisua optimoidessa.

Zhang ym. kehittävät teoksessaan (Zhang ym. 2008) ratkaisun, joka tunnistaa ja reagoi tapahtuviin osoitekaappauksiin. Ratkaisu erottuu muista siten, että se on tarkoitettu käytettäväksi (eng. deployed) paikallisesti. Tällöin järjestelmään syötetään käyttäjän hallinnoimat osoitteet (eng. prefix) ja järjestelmä tarkkailee havaitaanko näitä muualla, ja mikäli havaitaan on kyseessä kaappaus ja siihen voidaan reagoida.

Alkadi ym. esittävät teoksessaan (Alkadi ym. 2019) ratkaisun, jolla kyetään havaitsemaan epäilyttävät tapahtumat reititysverkosta, ja tarvittaessa reagoimaan niihin automaattisilla toimenpiteillä. Ratkaisu perustuu opetettuun malliin (eng. trained model), joka arvioi onko kyseessä epäilyttävä tapahtuma vai normaali tilanne.

Zheng ym. esittävät teoksessaan (Zheng ym. 2007) ratkaisun, jota voidaan myös käyttää BGP:n häiriöiden havaitsemiseen. Ratkaisu käyttää hyväkseen tietoa siitä, että mikäli reitti on normaali, ei siihen tapahdu yleensä merkittäviä muutoksia. Käyttämällä hyödyksi muun muassa tätä ja useita havainnointipisteitä (eng. vantage points), pystytään luotettavasti arvioimaan, onko kyseessä reittikaappaus vai ei.

Alaluvussa käsiteltiin paljon erilaisia ratkaisuja pitkältä aikaväliltä BGP:n tietoturvan parantamiseksi. Valtaosa ratkaisuista perustaa itsensä kryptografiaan, kuitenkin joukkoon mahtuu erilaisiakin ratkaisuja, kuten mallintaminen ja immuunipuolustus. Kryptografisista ratkaisuista voidaan havaita jako kahteen leiriin: niin kutsutut klassiset ratkaisut (esimerkiksi PKI)

ja uuden sukupolven lohkoketjuihin perustuvat ratkaisut. Seuraavassa alaluvussa käsitellään reittiväärennöksiä ja tarkastellaan ratkaisuja niiden vähentämiseen.

7.1.2 Reittiväärennös

Toisena ongelmana käsitellään reittiväärennöksiä (eng. AS-PATH Hijack / forgery), eli sitä kuinka taho ilmoittaa reitin oikeaan alkuperäiseen kohteeseen, kuitenkin muokaten reittiä niin, että väärennetty reitti on nopein mahdollinen kohteeseen. Lähtökohtaisesti väärennetyn reitin ilmoittajalla ei myöskään ole ilmoitetussa reitissä mainittua yhteyttä kohteeseen, jolloin liikenne ei kulje perille (eng. black hole).

Smith ja Aceves esittävät teoksessaan (Smith ja Garcia-Luna-Aceves 1998) ratkaisuksi reittiväärennökseen, että kaikki BGP:n UPDATE-viestin kentät allekirjoitetaan kryptografisesti. Näin toimiessa voidaan läpinäkyvästi varmistua siitä, että reitti on oikea ja muokkaamaton.

Li ym. esittävät teoksessaan (Q. Li ym. 2011) järjestelmän, joka pohjautuu myöskin kryptografiseen UPDATE-viestien allekirjoittamiseen. Eroa edellä mainittuun ratkaisuun tulee kuitenkin siitä, että koska allekirjoitukset on ketjutettu, riittää koko reitin varmistamiseen lähtökohtaisesti yhden reitillä olevan allekirjoituksen oikeellisuuden varmistaminen.

Oorschot, Wan ja Kranakis kehittävät teoksessaan (Oorschot, Wan ja Kranakis 2007) järjestelmän, joka myöskin perustuu kryptografiaan, mutta sen sijaan, että jokainen vaihe varmistettaisiin erillisellä allekirjoituksella, viestin luotettavuus arvioidaan siihen osallistuvien AS:n luottamuksen pohjalta.

Bruhadeshwar, Kulkarni ja Liu esittävät teoksessaan (Bruhadeshwar, Kulkarni ja Liu 2011) ratkaisun, joka myöskin perustuu kryptografiaan. Tässä ratkaisussa eroa edellisiin tuo se, että ratkaisu voidaan toteuttaa joko keskitetysti tai hajautetusti. Tämän lisäksi ratkaisu hyödyntää oletusta siitä, että N pitkältä reitillä on vähintään yksi luotettava taho. Näin ollen koko reitin varmistamisen sijaan riittää, että varmistetaan vain osa reitistä.

Zhu ym. esittävät teoksessaan (Zhu ym. 2012) ryhmittelyyn (eng. Alliance) perustuvan ratkaisun, jossa ryhmät koostuvat AS:stä. Ryhmästä vain tietyt keskuspisteinä (eng. Hub nodes) toimivat AS:t saavat muodostaa yhteyksiä ryhmän ulkopuolelle. Samalla voidaan rajoit-

taa tarvittavan kryptografian määrää, koska keskuspisteet vastaavat keskitetysti valtaosasta tarvittavaa kryptografiaa.

Kong ja Shen jatkokehittävät teoksessaan (Kong ja Shen 2015) Xiangjiangin, Peidongin ja Zhenghun työtä (Xiangjiang, Peidong ja Zhenghu 2007) sekä Zhun ym. työtä (Zhu ym. 2012), jossa keskitetyn mallin sijaan luodaan hajautettu ratkaisu, joka ei siten ole riippuvainen yhdestä rikkoutumispisteestä (eng. Single point of failure).

Yin ym. Kehittävät teoksessaan (Yin ym. 2010) kryptografiaan perustuvan ratkaisun, jossa voidaan hyödyntää erilaisia salaustekniikoita. Ratkaisun muina hyötyinä voidaan myös nähdä ketjutukseen (eng. keychain) perustuva allekirjoittaminen, joka vähentää laskentaan kuluvaa aikaa UPDATE-viestejä käsiteltäessä.

Comer, Singh ja Vasudevan esittävät teoksessaan (Comer, Singh ja Vasudevan 2012), että BGP:n turvaamisen voisi toteuttaa ilman julkisiin avaimiin (eng. Public key) perustuvaa raskasta infrastruktuuria. Comer, Singh ja Vasudevan puolestaan esittävät ratkaisuna mallin, jossa käytetään sekä historiallista tietoa vanhoista reiteistä, sekä dataa ulkoisista lähteistä varmentamaan BGP-ilmoitusten oikeellisuus.

Hu, Perrig ja Sirbu esittävät teoksessaan (Hu, Perrig ja Sirbu 2004) tehokkaamman kryptografisen ratkaisun reittiväärennösten ehkäisemiseen. Ratkaisu perustuu hajautusketjujen ja -puiden (eng. Hash chain / tree) käyttämiseen siten, että reittiä ei pystytä väärentämään jälkikäteen.

Valtaosa alaluvussa käsitellyistä ratkaisuista perustuu kryptografian hyödyntämiseen tavalla tai toisella reitityksen turvaamisessa. Kuitenkin joukkoon mahtuu muutama ratkaisu, jotka ovat yrittäneet selvittä ongelman ilman kryptografian vaatimia resursseja. Seuraavassa alaluvussa käsitelleen uudelleenohjaushyökkäystä. Lähtökohtaisesti uudelleenohjaushyökkäyksessä on pitkälti sama toimintalogiikka kuin reittiväärennöksessäkin, mutta siinä tapauksessa liikenne toimitetaan lopulta kuitenkin perille alkuperäiseen kohteeseen.

7.1.3 Uudelleenohjaushyökkäys

Kolmantena käsiteltävänä kategoriana on uudelleenohjaushyökkäys (eng. interception attack), jossa muokataan liikenteen reittiä niin, että se kulkee parempien (nopeampi tai tehokkaampi) reittien sijaan hyökkääjään tahtomaa reittiä pitkin. Tämä puolestaan mahdollistaa liikenteen mahdollisen tallentamisen tai salakuuntelun hyökkääjän toimesta. Uudelleenohjaushyökkäys on hankala havaita, koska se saattaa olla ulospäin näkymätön sen takia, että liikenne kulkee kuitenkin lopulta haluttuun kohteeseen asti.

Hiran, Carlsson ja Shahmehri esittävät teoksessaan (Hiran, Carlsson ja Shahmehri 2017) yhteistyöhön ja tiedon jakamiseen perustuvan hajautetun järjestelmän, jolla pidetään yllä tietokantaa eri AS:n ja osoitteiden (eng. prefix) toiminnasta historiallisesti. Mikäli reitin (eng. AS-PATH) muuttuessa havaitaan, että ilmoitettu reitti ei vastaa oletettua reittiä ilmoitetaan reitin kohteena olevalle AS:llee asiasta.

Shapira ja Shavitt kehittävät teoksessaan (Shapira ja Shavitt 2021) neuroverkkoihin ja IP-osoitteiden paikallistamiseen (eng. geolocation) perustuvan järjestelmän, jonka tarkoituksena on havaita poikkeukselliset ja siten mahdollisesti haitalliset muutokset reitityksessä.

Meng ym. tarkastelevat teoksessaan (Meng ym. 2020) mahdollisuutta rajoittaa uudelleenohjaushyökkäyksien toimintaa käyttämällä hyödyksi historiallista tietoa sekä mallinnusta. Tätä tietoa hyödyntämällä on tarkoitus valita "oikea"reitti kohteeseen.

7.1.4 Reittivuoto

Neljäntenä erillisenä kategoriana on reittivuoto (eng. Route leak) eli käytännössä yksinkertaisesti tapahtuma, jossa jokin taho ilmoittaa BGP-reitin tarkoitettua laajemmalla joukolle. Esimerkiksi kahden AS:n välillä oleva reitti vuotaa muille AS:lle ja siten liikennettä ohjautuu mahdollisesti hitaammalle ja pienemmälle reitille, joka saattaa mennä tästä liikenteestä tukkoon. Reittivuotoon on esitetty akateemisessa kirjallisuudessa erilaisia ratkaisuja, joihin tutustaan tarkemmin alla.

Deshpande ym. esittävät teoksessaan (Deshpande ym. 2009) ratkaisuna BGP:n UPDATE-viestien analysointiin perustuvan ratkaisun. Mikäli UPDATE-viestin analyysistä havaitaan

poikkeavuus normaalista, aktivoi järjestelmä toimenpiteet, joilla on tarkoitus rajoittaa poikkeavuuden aiheuttamia haittoja.

Xing, Wang ja Wang tarkastelevat teoksessaan (Xing, Wang ja Wang 2018) lohkoketjuihin (eng. blockchain) perustuvaa ratkaisua, jolla varmennetaan kryptografisesti BGP-liikenteen oikeellisuus. Eduksi ratkaisussa katsotaan se, että se ei keskitä valtaa vain muutamalle toimijalle, vaan lohkoketjujen avulla toiminta on hajautettu eikä yksittäinen taho pysty hallitsemaan BGP:tä mielivaltaisesti.

Siddiqui ym. kehittävät teoksessaan (Siddiqui ym. 2015) ratkaisun, joka pystyy havaitsemaan BGP:n reittivuoden pelkästään paikallisen verkon tieto- ja hallintakerroksen datan pohjalta. Esitetty ratkaisu kykenee kuitenkin havaitsemaan vain reittivuodon alun (eng. initiation) eikä leviämistä (eng. propagation).

Dai ym. tarkastelevat teoksessaan (Dai ym. 2012) näkökulmaa, jossa monipolkuisten (eng. multipath) reittien levittämistä on tarkoitus rajoittaa nykyistä paikallisemmalle (eng. regional) tasolle / alueelle. Käytännössä ratkaisu perustuu siihen, että AS:t jaetaan paikallisiksi alueiksi, joiden ulkopuolelle ei levitetä monipolkuisia reittejä.

Kim ym. tarkastelevat teoksessaan (Kim ym. 2008) reitititysrekistereitä (eng. Routing Registry) [IRR]. IRR:t ovat jo olemassa, kuitenkaan niitä ei pidetä kunnolla ajan tasalla, eikä niiden tiedon oikeellisuudesta ole takuita. Kim ym. esittävät teoksessaan ratkaisun siihen, kuinka niistä voitaisiin kehittää ajantasainen ja turvallinen (eng. secure) ratkaisu Internetin reitityksen turvaamiseksi.

Reittivuodon kohdalla voidaan havaita edellisiin alalukuihin verrattuna se, että ratkaisut perustuvat laajalti kryptografian sijaan johonkin muuhun vaihtoehtoiseen teknologiaan. Myöskin havaittavissa on se, että ratkaisuja on alaluvun sisällä vaikea ryhmitellä, joka puolestaan osittain kertoo siitä että kyseessä on laaja ongelma jota voi lähestyä monesta näkökulmasta. Seuraavassa alaluvussa käsitellään kirjallisuuskatsauksen ratkaisut, jotka eivät sopineet edellä käsiteltyihin neljään alalukuun.

7.1.5 Muut

Viimeisenä käsitellään viisi artikkelia, jotka keskittyvät muihin, kuin aikaisempaan neljään kategoriaan.

Guon ym. esittämä MAF-SAM (Guo ym. 2016) keskittyy tietokerroksen (eng. data plane) uhkiin hallintakerroksen (eng. control plane) sijaan. Erityisesti artikkeli keskittyy sellaisten hyökkäyksien havaitsemiseen, jotka yrittävät keskeyttää BGP session. Ratkaisuksi artikkelissa esitetään laskennallista mallia, joka vertaa nykyistä dataa historialliseen ja kykenee näin havaitsemaan virheet. Vaikka malli keskittyykin tietokerroksen uhkiin, on sen osoitettu olevan toimiva myös hallintakerroksen uhkia vastaan.

Li, Lu ja Li (Li, Lu ja Li 2021) esittävät ratkaisun, joka perustuu siihen, että virheiden havaitsemisen sijaan keskitytään arvioimaan naapurin luotettavuus erilaisten mittareiden avulla ennen yhteyden avaamista, sekä myöskin yhteyden ollessa auki. Mikäli naapurin arvioidaan olevan epäluotettava, reitit tiputetaan ja yhteys katkaistaan.

Wang ym. (A. Wang ym. 2012) esittävät työssään "työkalupakin"(eng. toolkit), jolla voidaan sekä analysoida, että luoda konfiguraatioita reititystä varten. "Työkalupakki"ei itsessään ratkaise ongelmia vaan havaitsee ne, jotta ne pystytään korjaamaan. Kiinnostava ja muista ratkaisuista poikkeava siinä, että kyseessä on algebraan pohjautuva malli.

Song, Venkataramani ja Gao (Song, Venkataramani ja Gao 2016) esittävät työssään uudenlaisen hyökkäyksen: "protokollan manipulaatio"(eng. protocol manipulation), jota soveltamalla taho kykenee häiritsemään kolmannen osapuolen reititystä käytännössä poistamalla täysin toimivan reitin käytöstä. Song, Venkataramani ja Gao. esittävät kaksi uutta mekanismia, joita hyödyntämällä esitetty hyökkäyspinta kyetään neutralisoimaan.

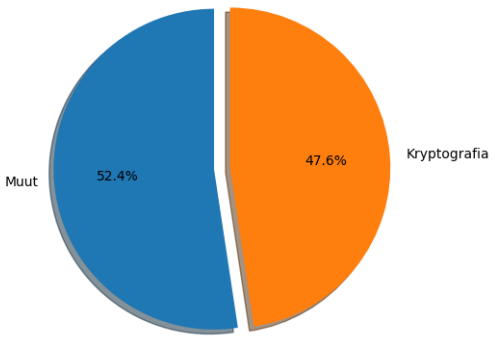
Li ym. (Q. Li ym. 2014) tarkastelevat työssään BGP:hen esitettyjä tietoturvaratkaisuja ja esittävät niissä olevan heikkouden, jonka he nimeävät TIGER:iksi. TIGER:ia hyödyntämällä esitetyt tietoturvaratkaisut kuten BGPsec tai S-BGP (Kent, Lynn ja Seo 2000) voidaan ohittaa. Työssä esitetään myös ratkaisu, jolla TIGER:iin pohjautuvat hyökkäykset pystytään havaitsemaan ja estämään.

Luvun esittämät aiheet kertovat siitä kuinka monimutkainen käsite BGP:n tietoturva lopulta

on. Näin ollen on hyvä myös mainita, että tässä työssä käytetty jako ei ole ainoa tapa luokitella BGP:n tietoturvaongelmia vaan muitakin tapoja jakaa BGP:n tietoturvaongelmat on olemassa.

7.1.6 Yhteenveto

Yllä olevissa alaluvuissa käsiteltiin laaja kirjo erilaisia ratkaisu BGP:n sisältämiin tietoturvaongelmiin. Lähes puolet käsitellyistä ratkaisuista, kaksikymmentä (20) neljästäkymmenestä kahdesta (42), perustuu jollain tavalla kryptografiaan. Kuitenkin ratkaisujen joukkoon mahtuu paljon ratkaisuja, jotka lähtivät ratkaisemaan ongelmaa muilla kuin kryptografian keinoilla.



Kuvio 3. kryptografian suhde muihin ratkaisuihin

Seuraavissa alaluvuissa käsitellään sitä, kuinka nämä yllä esitellyt ratkaisut vertautuvat joukolla erilaisia kriteereitä, kuten tehokkuus, käyttöönotettavuus ja reitityksen yksityisyys.

7.2 Tehokkuus

Tehokkuudesta keskusteltaessa on tärkeää määritellä tehokkuus, jota käsitellään. Tässä tapauksessa tehokkuus jaetaan seuraavaan viiteen alaluokkaan: yhdentymisen viive, laajennettavuus, laskennan-, kaistanleveyden- ja säilytyksen kustannukset.

Tietoa kerättäessä kerättiin myös arvot vakaudelle, mutta näiden arvojen luokittelu tutkiel-

man laajuuden asettamien rajoitteiden puitteissa ei ole mielekästä, koska käytännössä kaikki materiaalin teokset saivat arvon 2 erottelun vaikeuden takia.

Seuraavat alaluvut on jäsennelty seuraavasti: alaluvun alussa avataan lyhyesti käsitteen määritelmä, sekä kuinka materiaalin teoksien arviointiin käytetty asteikko on koostettu. Tämän jälkeen alaluvussa tarkastellaan mitä havaintoja ja ryhmittelyjä aineistosta kyetään tekemään.

7.2.1 Yhdentymisen viive

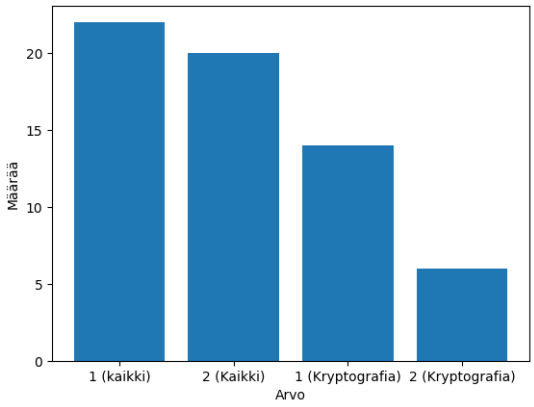
Yhdentymisen viiveellä (eng. Convergence delay) tarkoitetaan viivettä, joka kuluu, että verkko saavuttaa tilan jossa reitityksen muutokset ovat levinneet ympäri verkkoa (eng. network).

Tutkielman resurssien aiheuttamien rajoitteiden seurauksena yhdentymisen viive on luokiteltu materiaalissa seuraavasti: teokselle on annettu arvoksi 2, mikäli on arvioitu, että ratkaisulla ei ole vaikutusta yhdentymisen viiveeseen verrattuna BGP:n nykyiseen versioon. Teos on saanut arvoksi 1, mikäli on arvioitu, että ratkaisulla on vaikutusta yhdentymisen viiveeseen. Tarkempi arviointi viiveen määrän osalta olisi vaatinut resursseja, joita ei tämän tutkielman rajoissa ole.

Materiaalissa on havaittavissa selkeä jakaantuminen kahteen lähes yhtä suureen lohkoon. 22 teosta on saanut arvon 1 ja 20 teosta on puolestaan saanut arvon 2. Käytännössä jakolinjana voidaan nähdä kryptografiaa vaativat ratkaisut, joiden laskentaan kuluva aika hidastaa muutosten leviämistä verkossa. Alla olevasta kuviosta voidaan havaita, että kryptografiset ratkaisut ovat keskimääräistä ratkaisua heikompia yhdentymisen viiveen osalta.

Toinen havainto on se, että myös havainnointiin perustuvat järjestelmät ovat materiaalin perusteella yleisesti ottaen lievästi hitaampia, koska niiden täytyy havaita tapahtunut häiriö, ja vasta sen jälkeen pystytään reagoimaan tapahtumaan ja muokkaamaan reititystä.

Yhdentymisen viiveen pitäminen mahdollisimman pienenä on siitä tärkeää, että mikäli verkon jossain kohdassa on ongelmia, voidaan niihin reagoida mahdollisimman nopeasti esimerkiksi muuttamalla reititystä ja saamalla tämä muutos voimaan kaikkialla nopeasti. Seuraavaksi tarkastellaan ratkaisujen laajennettavuutta.



Kuvio 4. Yhdentymisen viive ja kryptografia

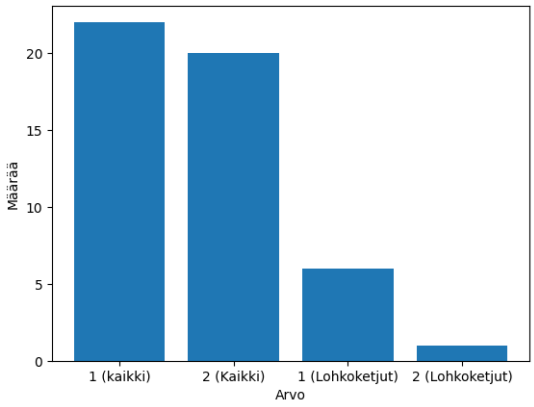
7.2.2 Laajennettavuus

Laajennettavuudella (eng. Scalability) tarkoitetaan sitä, kuinka suureen verkkoon ratkaisua kyetään käyttämään ilman, että ratkaisu alkaa esimerkiksi hidastua tai jostain muusta syystä ratkaisun tehokkuus kärsii.

Tutkielman resurssien seurakseni tässäkin kategoriassa joudutaan tyytymään karkeisiin arvioihin ratkaisujen laajennettavuuden osalta. Teokselle annetaan laajennettavuudesta arvo 2, mikäli ei ole nähtävissä syytä, joka aiheuttaisi ongelmia laajennettavuuteen. Muissa tapauksissa on annettu arvo 1.

Materiaali jakautuu tälläkin kertaa kahteen suureen joukkoon. 2 ovat kuitenkin tällä kertaa suurempi joukko 22 kappaleella, kun taas 1 on 20 kappaletta. Materiaalista on edellistä alalukua vaikeampaa löytää selkeitä ryhmittelyjä, jotka selittävät jakoa. Kuitenkin yksi ryhmittymä on havaittavissa materiaalista. Sen ollessa lohkoketjujen resurssien tarpeen kasvu, kun lohkoketjussa prosessoitavan tiedon määrä kasvaa. Resurssien tarpeen kasvaminen puolestaan nostaa mahdollisia kysymyksiä siitä, kuinka raskas ratkaisu on esimerkiksi ympäristölle. Lohoketjujen ja laajennettavuuden suhdetta on avattu tarkemmin alla olevassa kuviossa 5.

Laajennettavuus on hyvin tärkeä elementti toimivaa BGP:n ratkaisua, koska nykyään CIDR raportin (Huston, Smith ja Bates 2021) osoitteita (eng. prefix) on reitityksessä yli 900 000



Kuvio 5. Laajennettavuus ja lohkoketjut

kappaletta, ja AS:nkin määrä on ylittänyt 70 000 kappaletta. Seuraavaksi tarkasteluun otetaan ratkaisujen reititykseen vaatimat laskennalliset resurssit.

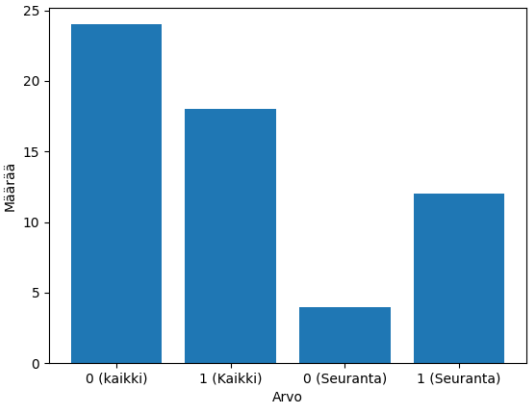
7.2.3 Laskennan kustannukset

Laskennan kustannuksilla (Eng. Computational overhead) tarkoitetaan tässä tapauksessa laskentatehoa, joka tarvitaan järjestelmän toimintojen ylläpitoon. Laskennan kustannuksia tarkastellaan sekä pelkästään reitittimien tasolla, että myös muut ratkaisuun tarvittavat elementit huomioiden.

Ratkaisu voi saada laskennan kustannuksista arvon 2, mikäli ratkaisu vastaa tai on nykyistä BGP:n toteutusta tehokkaampi. Ratkaisu saa arvon 1, mikäli ratkaisu vaatii lisää laskentatehoa reitittimien ulkopuolella. Ratkaisu saa arvon 0, mikäli ratkaisu vaatii lisää laskentatehoa itse reitittimissä.

Materiaalista voidaan havaita, että yksikään ratkaisu ei saanut arvoa 2. Tämä ei ole yllättävää, koska ratkaisu joka samanaikaisesti parantaa tietoturvaa ja tehokkuutta olisi hyvin haluttu, mutta samalla myös hyvin vaikea saavuttaa. Enemmistö ratkaisuista, 24 ratkaisua sai arvosanan 1. Loput ratkaisut, 18, saivat arvosanan 0.

Selkein erottelu, joka aineistosta voidaan havaita on se, että ratkaisut joiden tarkoituksena on kokonaan estää reitityksen häiriöt esimerkiksi kryptografialla saivat pääasiassa arvosanaksi



Kuvio 6. Laskenta ja seurantaratkaisut

0, kun taas ratkaisut jotka keskittyvät tilanteen seurantaan ja (nopeaan) reagointiin saivat enemmän arvosanaksi 1.

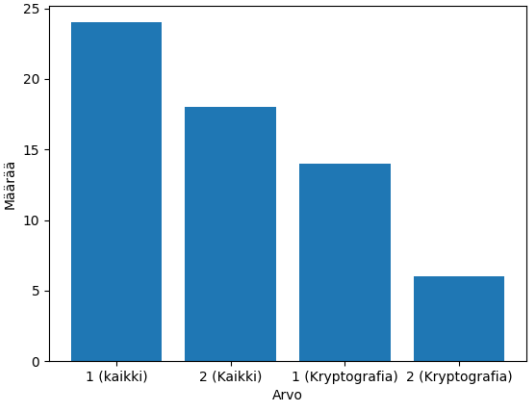
Kategorian arvioinnissa päätettiin painottaa reitittimien resursseja, koska niiden päivittäminen on lähtökohtaisesti vaikeampaa ja kalliimpaa, kuin yksinkertaisen laskentatehon, joka voidaan tarvittaessa hajauttaa esimerkiksi pilveen. Seuraavaksi tarkastellaan ratkaisujen kaistanleveyden kustannuksia.

7.2.4 Kaistanleveyden kustannukset

Kaistanleveyden kustannuksilla (eng. Bandwidth overhead) tarkoitetaan tässä tapauksessa suoraan BGP-liikenteeseen (esimerkiksi UPDATE-viestit) liittyvien viestien kokoa ja/tai määrää ja näiden kasvua.

Ratkaisu voi saada kaistanleveyden kustannuksista arvon 2, mikäli ratkaisu ei aiheuta ylimääräisiä kaistanleveyden kustannuksia. Ratkaisu saa arvon 1, mikäli sillä on vaikutuksia BGP-liikenteen vaatimaan kaistanleveyteen.

Materiaali jakautui jälleen kerran kahteen lähes saman kokoluokan lohkoon. 24 ratkaisua sai arvon 2, ja 18 ratkaisua sai puolestaan arvon 1. Vaikka jakauma vastaakin lukujen osalta edellisen osan arvoja, eivät arvot ole kuitenkaan identtiset näiden kahden välillä. Kaistanleveyden materiaalista on vaikea löytää selkeitä linjoja, jotka selittävät jakaumaa. Kuitenkin



Kuvio 7. Kaistanleveys ja kryptografia

lähtökohtaisesti kryptografiaa hyödyntävät ratkaisut joutuvat jollain tasolla varmentamaan kryptografian oikeellisuuden, joka puolestaan vaatii kasvanutta kaistanleveyttä, joka taas on nähtävissä yllä olevassa kuviossa 7.

Vaikka kaistanleveys ei olekaan niin merkittävä resurssi, kuin laskentateho, on kuitenkin tärkeää pitää huolta myös siitä, että vaadittu kaistanleveys ei pääse kasvamaan liikaa, koska vaikka viestintä onkin nopeaa, aiheuttaa kasvu väkisin hidastusta BGP-liikenteen käsittelyyn. Seuraavaksi otetaan käsittelyyn säilytyksen kustannukset.

7.2.5 Säilytyksen kustannukset

Säilytyksen kustannuksilla (eng. Storage overhead) tarkoitetaan reitittimiltä vaadittua muistia. Esimerkiksi jos reitittimen täytyy säilyttää muistissaan jotain tietoa reitityksen oikeellisuuden varmistamiseksi, säilytyksen kustannukset kasvavat.

Ratkaisu saa säilytyksen kustannuksista arvosanan 2, mikäli sillä ei ole vaikutusta reitittimeltä vaadittuun säilytystilaan. Ratkaisu saa puolestaan säilytyksen kustannuksista arvosanan 1, mikäli ratkaisu vaatii nykyistä BGP-toteutusta enemmän säilytystilaa reitittimestä.

Myös säilytyksen kustannukset jakautuivat kahteen melko lailla yhtä suureen lohkoon. Enemmistö, 25 ratkaisua, sai säilytyksestä arvosanan 1, kun vähemmistö, 17 ratkaisua, sai arvosanan 2. Materiaalista ei löydy selkeää jakolinjaa, jolla voitaisiin selittää miksi tietyt ratkaisut

ovat toisia parempia säilytyksen osalta.

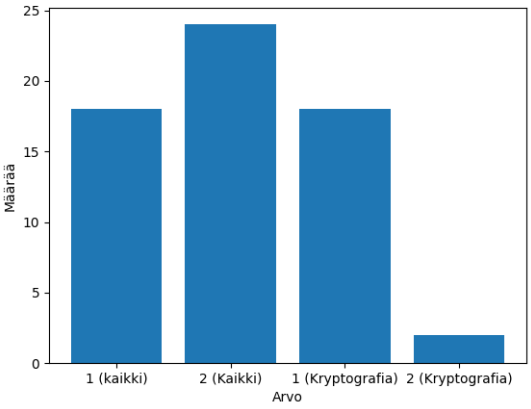
Säilytyksen kustannukset ovat merkittävä osa ratkaisua, koska mikäli esitetty ratkaisu tarvitsee merkittävästi nykytilannetta enemmän säilytystilaa. Se hidastaa BGP-liikenteen prosessointia ja se voi aiheuttaa tilanteen, jossa muuten täysin toimivia reitittimiä joudutaan vaihtamaan uusiin, koska ne eivät enää vastaa uusiin tarpeisiin. Laajemmin käyttöönotettavuutta käsitellään seuraavassa kappaleessa.

7.3 Käyttöönotettavuus

Käyttöönotettavuudella (eng. Deployability) tarkoitetaan sitä, että tarvitseeko ratkaisu ottaa käyttöön kerralla koko Internetin laajuudella, jotta ratkaisun hyödyt voidaan saavuttaa. Vai voidaanko ratkaisu ottaa käyttöön vain muutamassa AS:ssä kerallaan ja silti saavuttaa ratkaisun hyödyt näiden AS:n alueella.

Ratkaisu saa käyttöönotettavuudesta arvon 2, mikäli se voidaan ottaa käyttöön paikallisesti ja saavuttaa halutut hyödyt. Ratkaisu saa käyttöönotettavuudesta arvosanan 1, mikäli ratkaisu vaatii laajan käyttöönoton ennen sen hyötyjen realisoitumista.

Materiaalissa on jälleen havaittavissa jakautuminen kahteen lähes yhtä suureen lohkoon. 24 ratkaisua sai käyttöönotettavuudesta arvon 2, kun taas loput 18 ratkaisua saivat arvon 1. Materiaalissa voidaan havaita jakolinjana jälleen havaita seurantaratkaisut, jotka saivat lähtökohtaisesti paremmat arvosanat ja kryptografiset ratkaisut, jotka puolestaan vastasivat kaikista käyttöönotettavuuden heikommista arvosanoista, kuten kuviosta 8 on nähtävissä.



Kuvio 8. Käyttöönotettavuus ja kryptografia

Käyttöönotettavuuden alle kuuluu materiaalissa myös omaksuttavuuden (eng. adoptability) määritelmä. Omaksuttavuudella tarkoitetaan sitä, kuinka suuren osan AS:stä voidaan olettaa ottavan valittu ratkaisu käyttöön. Kuitenkin tutkielman resursseista johtuen omaksuttavuuden arviointi mielekkäällä tasolla on tutkielman mittakaavan ulkopuolella, ja siitä annetut arvot seuraavat tästä johtuen lähes yksi yhteen käyttöönotettavuuden arvoja. Tästä johtuen omaksuttavuutta ei käsitellä tarkemmin.

Käyttöönotettavuus on hyvin tärkeä tekijä toimivassa ratkaisussa BGP:n tietoturvan parantamiseksi, koska Internet on hyvin laaja ja monimuotoinen verkko täynnä erilaisia toimijoita erisuuruisilla resursseilla. Valitun ratkaisun täytyisi kuitenkin lähtökohtaisesti olla jotain, joka toimii jollain tasolla kaikille Internetin toimijoille.

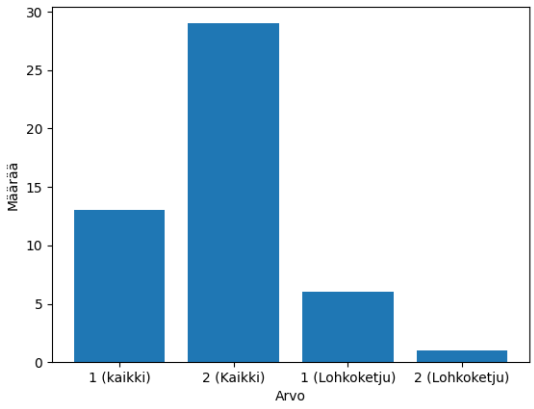
Jotkin isommat toimijat saattavat pystyä tarvittaessa uudistamaan kaikki reitittimensä kerralla, mutta pienemmille toimijoille tämä voi olla mahdollista vasta usean vuoden kuluttua. Tällaisessa tilanteessa ratkaisu, joka vaatii täyden käyttöönoton eikä ole jostain syystä otettavissa käyttöön vanhoissa reitittimissä on heikko ratkaisu Internetin toimivuuden kannalta. Seuraavassa kappaleessa käsitellään reitityksen yksityisyyttä ja sitä, kuinka esitetyt ratkaisut vaikuttavat siihen.

7.4 Reitityksen yksityisyys

Reitityksen yksityisyydellä tarkoitetaan sitä, kuinka paljon yksityistä tietoa tahot joutuvat ratkaisun toteutuksessa tekemään julkiseksi. Esimerkiksi valtaosa tahoista haluaa säilyttää tarkan reitityksen liikesalaisuutena.

Ratkaisu saa reitityksen yksityisyydestä arvon 2, mikäli ratkaisun ei nähdä heikentävän reitityksen yksityisyyttä nykytilaan verrattuna. Ratkaisu saa arvon 1, mikäli sen nähdään paljastavan elementtejä, jotka ovat nykyään yksityisiä.

Materiaalissa on havaittavissa edelliskertoja selkeämpi jakautuminen suurempaan arvon 2 saaneiden lohkoon, 29 kappaletta, ja pienempään 1 saaneiden lohkoon, 13 kappaletta. Pienemmästä lohkosta voidaan havaita, että lohkoketjut ovat ainoa sieltä selkeästi havaittavissa oleva ryhmittymä. Ja samalla lohkoketjut menevät muuta aineistoa vastaan kuten kuviosta 9 voidaan nähdä.



Kuvio 9. Yksityisyys ja lohkoketjut

Vaikka reitityksen yksityisyydellä ei olekaan suoranaista vaikutusta reitityksen tietoturvaan, on sillä kuitenkin merkittävä epäsuora vaikutus. Johtuen siitä että ratkaisut jotka heikentävät toimijoiden asemaa nykytilanteeseen verrattuna kohtaavat todennäköisesti enemmän muutosvastarintaa, kuin kilpailevat ratkaisut jotka eivät kärsi vastaavista ongelmista.

7.5 Käyttöönotto

Käyttöönotolla tarkoitetaan sitä, että onko ratkaisua otettu käytäntöön. Käyttöönotto on materiaalissa jaettu kolmeen kategoriaan: käytössä, standardisoitu ja vain akateeminen.

Ratkaisu saa arvon käytössä, mikäli se on otettu käyttöön. Ratkaisu saa arvon standardisoitu, mikäli se on otettu standardiksi esimerkiksi RFC:ssä. Ratkaisu saa puolestaan arvon vain akateeminen, mikäli sitä ei ole otettu käyttöön.

Materiaali on käyttöönoton osalta hyvin yksinkertainen, 42 kappaletta vain akateemisia ratkaisuja. 0 kpl muita ratkaisuja. Osittain tätä voi selittää se, kuinka paljon materiaalin ratkaisuista on uusia. Siten nämä ratkaisut eivät ole vielä ehtineet tulla käyttöön. Toinen selitys on myös se, että osa ratkaisuista saattaa olla käytössä pienessä mittakaavassa, mutta näitä ei tutkielman resurssien puitteissa pystytä huomioimaan. Seuraavassa alaluvussa tarkastellaan kuinka nämä yllä esitellyt teknologiat vertautuvat toisiinsa.

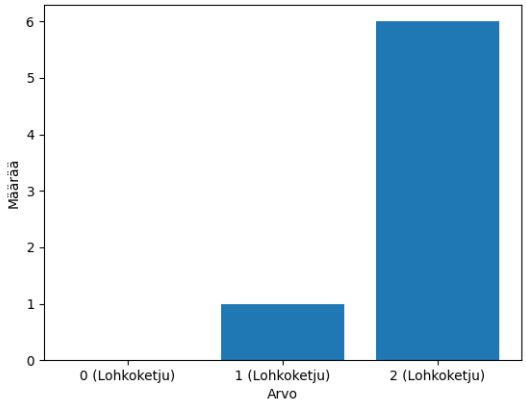
7.6 Kirjallisuuskatsauksen yhteenveto

Edeltävissä alaluvuissa on käsitelty ratkaisuja erilaisista tehokkuuden ja käyttöönotettavuuden näkökulmista. Kuitenkaan tehokkuus ja käyttöönotettavuus eivät yksinään aseta ratkaisuja järjestykseen, vaan vertailuun tarvitaan myös mukaan luvun alussa käsitellyt hyökkäyspinnat ja se, kuinka hyvin ratkaisut pystyvät vastaamaan näihin ongelmiin.

Seuraavaksi on hyvä antaa muutamalle käytettävälle termille tarkat määritelmät ennen kuin niitä käsitellään tämän luvun loppuosassa. Lohkoketjuihin perustuvia ratkaisuja ovat ne, joissa lohkoketju on kiinteä osa ratkaisua. Kryptografisilla ratkaisuilla tarkoitetaan puolestaan niitä ratkaisuja, jotka käyttävät esimerkiksi liikenteen vahvistamiseen kryptografiaa ja siten tarvitsevat lisää laskentatehoa. Lohkoketjuihin perustuvat ratkaisut ovat siten myös kryptografian osajoukko. Viimeinen termi on seurantaan perustuvat ratkaisut. Seurantaan perustuvissa ratkaisuissa ei käytetä absoluuttista tietoa kuten kryptografiaa, vaan ratkaisu perustuu esimerkiksi mallinnukseen tai historialliseen tietoon siitä, mikä on niin kutsuttu normaali.

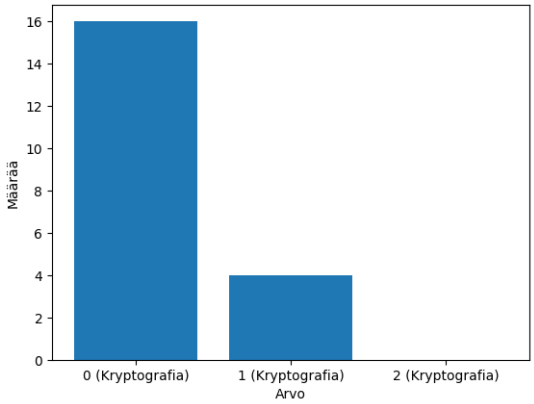
Lohkoketjuja käyttävät materiaalit tarjoavat aineiston tulosten perusteella vahvan suojan esimerkiksi osoitekaappauksilta (kuvio 10). Kuitenkin esimerkiksi tehokkuudessa on nähtävis-

sä selkeästi (kuvio 5), että lohkoketjut vaativat merkittäviä panostuksia esimerkiksi laskentatehoon, joka puolestaan voi vaikuttaa negatiivisesti siihen, kuinka innokkaasti ratkaisu halutaan ottaa käyttöön.



Kuvio 10. Osoitekaappaus ja lohkoketjut

Myös kryptografian osalta on nähtävissä pitkälti samat piireet. Ratkaisut tarjoavat pääasiassa tehokkaan suojan osoitekaappauksilta, ja osittain myös reittiväärennöksiltä. Kuitenkin kryptografiankin osalta on nähtävissä laajat vaatimukset esimerkiksi laskentatehon osalta valtaosassa ratkaisuja, kuten kuviossa 11 nähdään.

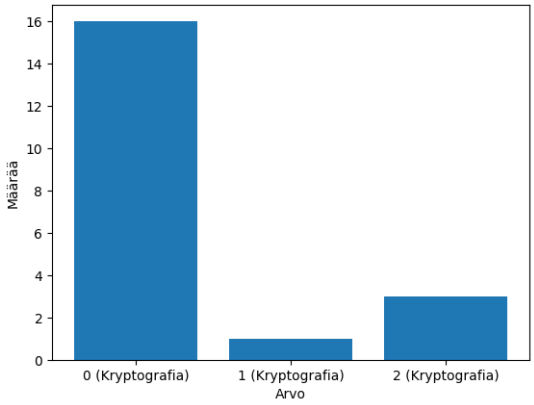


Kuvio 11. Laskenta ja kryptografia

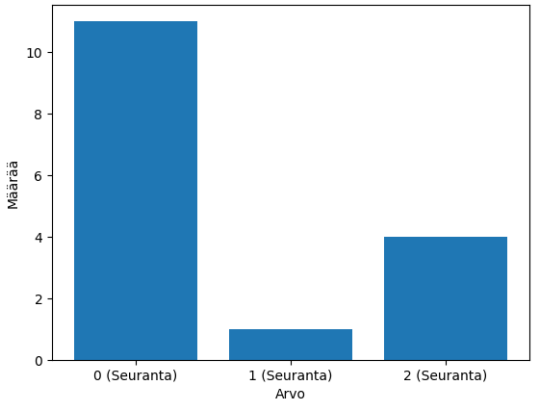
Toinen sekä kryptografiaan että lohkoketjuihin vaikuttava tekijä on myös käyttöönotettavuus. Erityisesti se, että lähes kaikki näistä ratkaisuista vaativat kattavan käyttöönoton ennen kuin

ratkaisujen tarjoamat hyödyt alkavat realisoitua. Kryptografian ja lohkoketjujen käyttöönotettavuus (kuvio 8).

Puolestaan seurantaan perustuvissa ratkaisuissa nähdään lievästi heikompaa suojausta osoitekaappauksien osalta, mutta samaan aikaan parempaa tehokkuutta kryptografiaan ja lohkoketjuihin verrattuna (kuviot 6 ja 11). Samalla seurantaratkaisut tarjoavat myös parempaa kattavuutta reittivuodon ja uudelleenohjaushyökkäysten osalta, kuin kryptografiaan ja lohkoketjuihin perustuvat ratkaisut (kuvio 13).



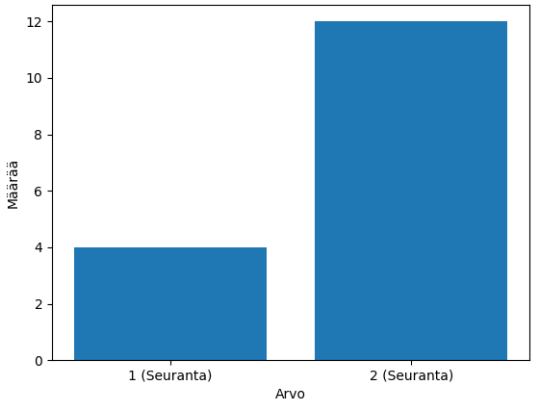
Kuvio 12. Uudelleenohjaushyökkäys ja kryptografia



Kuvio 13. Uudelleenohjaushyökkäys ja Seuranta

Toinen asia joka on nähtävissä seurantaratkaisuissa on se, kuinka ne voidaan lähtökohtaisesti ottaa käyttöön esimerkiksi yksittäisessä AS:n alueella ja silti saada kaikki tai lähes kaikki

ratkaisun tarjoamat hyödyt käyttöön. Tämä puolestaan näkyy kuviossa 14 parempina käyttöönotettavuuden arvoina.



Kuvio 14. Käyttöönotettavuus ja Seuranta

Materiaalia tarkasteltaessa on melko selkeästi havaittavissa, että ainakaan materiaalin puitteissa ei ole olemassa yksittäistä ratkaisua, jolla vastattaisiin kaikkiin BGP:n ongelmiin. Ja vaikka tällainen ratkaisu olisikin olemassa, tulee huomioida mahdolliset tämän teoreettisen ratkaisun mahdolliset ongelmat esimerkiksi tehokkuuden ja käyttöönotettavuuden osalta.

Tästä voidaan todeta, että mikäli BGP:n tietoturvan ongelmat halutaan ratkaista kokonaisuudessaan, tarvitaan todennäköisesti esitetyistä ratkaisuista ja niiden osista koottu hybridiratkaisu, jolla voitaisiin kattavasti vastata Internetin alati muuttuviin tietoturvan tarpeisiin.

Luvussa käsiteltiin materiaalia ja siinä esitettyjä ratkaisuja, sekä niiden vahvuuksia, että heikkouksia. Materiaalia voitaisiin käsitellä paljon laajemmin ja tarkemmilla menetelmillä kuten simulaatioilla. Kuitenkaan tutkielman asettamien resurssien rajoissa ei ole mahdollista suorittaa tällaista tarkastelua, vaan se jää tulevan tutkimuksen varaan.

Materiaalissa esitettyjen ratkaisujen tarkastelun jälkeen on syytä tarkastella teollisuudessa käytäntöön saatettuja ratkaisuja, ja kuinka nämä ratkaisut vastaavat ja mahdollisesti eroavat akateemisessa kirjallisuudessa esitetyistä ratkaisuista.

8 Käyttöönotetut ratkaisut

Käyttöönotettujen ratkaisujen osalta yksi merkittävä toimija on Mutually Agreed Norms for Routing Security (MANRS 2022a). MANRS:n tarkoituksena on kerätä yhteen joukko parhaita käytäntöjä, joiden avulla BGP:n ja yleisesti Internetin reititystä voidaan parantaa.

MANRS koostuu neljästä erillisestä elementistä. Ensimmäinen näistä elementeistä on BGP-liikenteen UPDATE-viestien suodattaminen (eng. filtering), jonka tarkoituksena on rajata virheelliset reitti-ilmoitukset pois BGP-liikenteestä. Toinen MANRS:n esittämä elementti on lähde-IP-osoitteiden (eng. source) väärentämisen estäminen (eng. Anti spoofing), joka auttaa esimerkiksi DoS (Denial of Service) hyökkäyksien torjunnassa. Kolmas elementti on yksinkertaisesti koordinaatio ja sen mahdollistaminen ajantasaisilla yhteystiedoilla. Viimeinen MANRS esittämä elementti ratkaisuun on globaali varmentaminen (eng. global validation), jonka tarkoituksena on säilyttää julkisesti informaatio, jonka avulla reititysinformaatio pystytään varmentamaan.

Näistä neljästä elementistä BGP:n kohdalla olemme lähinnä kiinnostuneita ensimmäisestä elementistä eli suodattamisesta (MANRS 2022b). MANRS ei esitä yksittäistä ratkaisua vaan tarjoaa useita erilaisia tapoja lähestyä ongelmaa. Tässä tapauksessa keskitymme tarkastelemaan RPKI:tä ja IRR:iä ratkaisuna.

Resource Public Key Infrastructure (RPKI) (Bush ja Austein 2013) on kryptografiaan perustuva ratkaisu, jonka avulla kyetään varmentamaan reitityksen oikeellisuus. Ratkaisulla on melko pitkälti samat vahvuudet ja heikkoudet, kuin muilla aiemmin tarkastelluilla akateemisilla kryptografiaan tukeutuvilla ratkaisuilla. Internet Routing Registry:t (IRR) ovat esimerkiksi ARIN:in (ARIN 2022) ylläpitämiä rekisterejä Internetin reitityksestä. Näiden rekisterien sisältämän tiedon avulla voidaan varmistua myös reitityksen oikeellisuudesta.

Tiivistetysti BGP:n tietoturvan parantamiseksi on otettu käyttöön muutamia erilaisia ratkaisuja. Kuitenkaan mikään ratkaisu ei ole ainakaan toistaiseksi ratkaissut BGP:n tietoturvaan liittyviä ongelmia kokonaan, vaan edelleen kaivataan parempaa/tehokkaampaa ratkaisua. Seuraavassa luvussa tarkastellaan millainen tämä mahdollisesti parempi ratkaisu voisi olla.

9 Johtopäätökset

Tutkielman aikana käsiteltiin laaja kirjo erilaisia mahdollisia ratkaisuja BGP:n tietoturvan parantamiseksi, kuitenkaan mitään näistä käsitellyistä ratkaisuista ei ole otettu käytäntöön. Syitä tälle on monia, ja näitäkin syitä tarkasteltiin aikaisemmissa tutkielman luvuissa.

Mitä tulee tutkielman alussa luvussa kaksi esitettyihin tutkimuskysymyksiin. Ensimmäiseen tutkimuskysymykseen vastattiin kattavasti systemaattisen kirjallisuuskatsauksen keinoin luvuissa kuusi ja seitsemän. Puolestaan tutkimuskysymykseen kaksi esitettiin ratkaisuja luvussa kahdeksan. Kiinnostavin tutkimuskysymys lienee kolmas, jonka vastauksia tullaan tarkastelemaan alla. Tutkimuskysymyksessä kolme kysyttiin sitä, kuinka teoreettisessa akateemisessa kirjallisuudessa esitettyjen ratkaisujen joukko vertautuu puolestaan käyttöönotettuihin ratkaisuihin.

Käyttöönotetuissa ratkaisuissa on hyödynnetty sekä kryptografiaa (Bush ja Austein 2013), että myös mallia jossa reitityksen oikeellisuus varmistetaan rekisteristä, esimerkiksi: (ARIN 2022). Johtuen käyttöönotettujen ratkaisujen määrän vähäisyydestä on tämän pohjalta vaikeaa tehdä yleistäviä lausuntoja siitä, että millainen ratkaisu olisi mahdollisesti paras.

Tämän pohjalta voidaan kuitenkin RPKI:n seurauksena havaita, että kryptografia ja sen vaatimat resurssit eivät poissulje ratkaisua mahdollisesti toteutettavien ratkaisujen listalta. Toinen havainto joka voidaan tehdä IRR:n pohjalta on se, että myös muut kuin kryptografiaan perustuvat ratkaisut voivat saavuttaa käyttöönoton.

Kokonaisuutena voidaan nähdä, että BGP:n tietoturvaan ei ole yhtä ratkaisua tai kaavaa, jolla tämä ratkaisu voitaisiin tuottaa, vaan BGP:n tietoturva koostuu erilaisista paloista, joiden muoto riippuu muista ratkaisun paloista. Yhdistämällä joukko erilaisten ratkaisujen parhaita paloja parannelluksi ratkaisuksi pystytään kattamaan mahdollisimman suuri joukko BGP:n heikkouksia ilman, että ratkaisun tehokkuus ja käytettävyys kärsivät liikaa.

Mitä tulee itse tutkimuksen onnistumiseen, niin systemaattinen kirjallisuuskatsaus oli melko pitkälti niin onnistunut, kuin yhden ihmisen gradun resurssien puitteissa voisi olettaa. Merkittävin heikkous on, että luokittelu jouduttiin tekemään yhden ihmisen toimesta, eikä

tällöin henkilökohtaisia vinoumia (eng. personal bias) pystytä välttämään. Tämä huomioitiin kuitenkin mahdollisena ongelmana jo ennen tutkimuksen aloittamista ja keinot tämän rajaamiseksi on esitetty luvussa 3.1.

Mitä taas tulee tutkimuskysymyksiin kaksi ja kolme, rajoittaa käytössä olevien ratkaisujen määrä mahdollisten johtopäätösten tekemistä, kuitenkin näissäkin kohdissa onnistuttiin kokoamaan joukko näkökulmia, joista voi olla hyötyä tulevaisuuden tutkimuksen kohdalla.

Kokonaisuutena tutkielma voidaan nähdä onnistuneena työnä. Mikäli olisi mahdollisuus aloittaa koko gradu uudestaan ja hyödyntää tämän prosessin aikana kerättyjä oppeja. Näkisin kenties suurimpana parannuskohteena sen, että materiaalin osalta olisi voinut tehdä tiukemmat rajaukset ja siten keskittyä siten pienempään joukkoon materiaalia ja syvemmin, mutta toisaalta tämäkin on lähinnä näkemysero siitä, että halutaanko laaja materiaali vai tiiviimpi materiaali, jota käsitellään tarkemmin.

10 Yhteenveto

BGP on vanha protokolla, joka kuitenkin kantaa hartioillaan merkittävä osaa Internetin toiminnasta. BGP kehitettiin aikana, jolloin tietoturvaan ei kiinnitetty paljoa huomiota tai käytetty resursseja sen parantamiseksi. Tämän seurauksena BGP ei kykene vastaamaan nykyajan tietoturvan tarpeisiin. Tämä ongelma on tiedostettu akateemisessa kirjallisuudessa ja tämän ratkaisemiseksi on esitetty joukko ratkaisuja, joita tutkielmassa tarkasteltiin ja vertailtiin keskenään. Myös käyttöönotettuja ratkaisuja tarkasteltiin. Teoreettiset ja käyttöönotetut ratkaisut yhdistämällä havaittiin, että ei ole yksittäistä ratkaisua, joka ratkaisee BGP:n tietoturvaan liittyvät ongelmat, vaan mahdollinen ratkaisu on todennäköisesti yhdistelmä useista esitetyistä ratkaisuista ja niiden elementeistä.

Puolestaan jatkotutkimuksen osalta BGP jättää paljon mahdollisia suuntia viedä tutkimusta ja tietoturvaa eteenpäin. Yksi mahdollinen suunta, johon tutkimuksen voisi viedä, olisi tutkia materiaalissa esitettyjä ratkaisuja esimerkiksi simulaation keinoin. Toinen mahdollinen tutkimussuunta olisi lähteä selvittämään esimerkiksi kyselytutkimuksen keinoin, että millaisia ominaisuuksia teollisuudessa arvostetaan mahdolliselta ratkaisulta. Nämä ovat vain muutamia mahdollisuuksia, ja BGP:n osalta on paljon muitakin suuntia, johon tutkimusta voi tulevaisuudessa viedä.

Lähteet

Alkadi, Osama S, Nour Moustafa, Benjamin Turnbull ja Kim-Kwang Raymond Choo. 2019. "An ontological graph identification method for improving localization of ip prefix hijacking in network systems". *IEEE Transactions on Information Forensics and Security* 15:1164–1174.

Apostolaki, Maria, Aviv Zohar ja Laurent Vanbever. 2017. "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies". Teoksessa *2017 IEEE Symposium on Security and Privacy (SP),* 375–392. https://doi.org/10.1109/SP.2017.29.

ARIN. 2022. "Internet Routing Registry (IRR)". Viitattu 28. tammikuuta 2022. https://www.arin.net/resources/manage/irr/.

Bakkali, Sara, Hafssa Benaboud ja Mouad Ben Mamoun. 2013. "Security problems in BGP: An overview". Teoksessa *2013 National Security Days (JNS3),* 1–5. https://doi.org/10.1109/JNS3.2013.6595458.

Ballani, Hitesh, Paul Francis ja Xinyang Zhang. 2007. "A Study of Prefix Hijacking and Interception in the Internet". *SIGCOMM Comput. Commun. Rev.* (New York, NY, USA) 37, numero 4 (elokuu): 265–276. ISSN: 0146-4833. https://doi.org/10.1145/1282427.1282411.

Barbir, A., S. Murphy ja Y. Yang. 2006. "Generic Threats to Routing Protocols, RFC 4593". https://datatracker.ietf.org/doc/html/rfc4593.

Bradner, S. 1997. "Key words for use in RFCs to Indicate Requirement Levels, RFC 2119". https://datatracker.ietf.org/doc/html/rfc2119.

Bruhadeshwar, Bezawada, Sandeep S Kulkarni ja Alex X Liu. 2011. "Symmetric key approaches to securing BGP—a little bit trust is enough". *IEEE Transactions on Parallel and Distributed Systems* 22 (9): 1536–1549.

Bush, R., ja R. Austein. 2013. "The Resource Public Key Infrastructure (RPKI) to Router Protocol, RFC 6810". Viitattu 6. helmikuuta 2022. https://tools.ietf.org/html/rfc6810.

Butler, Kevin, Toni R. Farley, Patrick McDaniel ja Jennifer Rexford. 2010. “A Survey of BGP Security Issues and Solutions”. *Proceedings of the IEEE* 98 (1): 100–122. https://doi.org/10.1109/JPROC.2009.2034031.

Chang, Jian, Krishna K Venkatasubramanian, Andrew G West, Sampath Kannan, Insup Lee, Boon Thau Loo ja Oleg Sokolsky. 2012. “As-cred: Reputation and alert service for interdomain routing”. *IEEE Systems Journal* 7 (3): 396–409.

Clarivate. 2022. “Web of Science”, tammikuu. Viitattu 6. helmikuuta 2022. https://clarivate.com/webofsciencegroup/solutions/web-of-science/.

Comer, Douglas, Parmjeet Singh ja Subramanian Vasudevan. 2012. “Effective border gateway protocol protection that does not require universal adoption of a public key infrastructure”. *IET networks* 1 (4): 217–228.

Computing Machinery, Association for. 2022. “ACM Digital Library”, tammikuu. Viitattu 6. helmikuuta 2022. https://dl.acm.org/.

Dai, Bin, Feng Wang, Baokang Zhao ja Jinshu Su. 2012. “Using regional routing to improve the scalability and security of inter-domain multipath routing”. *IEICE TRANSACTIONS on Information and Systems* 95 (1): 94–107.

Deshpande, Shivani, Marina Thottan, Tin Kam Ho ja Biplab Sikdar. 2009. “An online mechanism for BGP instability detection and analysis”. *IEEE transactions on Computers* 58 (11): 1470–1484.

Durand, J., I. Pepelnjak ja G. Doering. 2015. “BGP Operations and Security, RFC 7454”. https://datatracker.ietf.org/doc/html/rfc7454.

Ekparinya, Parinya, Vincent Gramoli ja Guillaume Jourjon. 2018. “Impact of Man-In-The-Middle Attacks on Ethereum”. Teoksessa *2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS),* 11–20. https://doi.org/10.1109/SRDS.2018.00012.

Facebook. 2021a. “More details about the October 4 outage”, lokakuu. Viitattu 11. lokakuuta 2021. https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/.

———. 2021b. “Update about the October 4th outage”, lokakuu. Viitattu 11. lokakuuta 2021. https://engineering.fb.com/2021/10/04/networking-traffic/outage/.

Google. 2018. “Google Cloud Networking Incident #18018”, joulukuu. Viitattu 11. lokakuuta 2021. https://status.cloud.google.com/incident/cloud-networking/18018#18018002.

Guo, Yi, Haixin Duan, Jikun Chen ja Fu Miao. 2016. “MAF-SAM: An effective method to perceive data plane threats of inter domain routing system”. *Computer Networks* 110:69–78.

Guo, Yi, ja ZhenXing Wang. 2012. “An immune-theory-based model for monitoring inter-domain routing system”. *Science China Information Sciences* 55 (10): 2358–2368.

He, Guobiao, Wei Su, Shuai Gao, Jiarui Yue ja Sajal K Das. 2020. “Roachain: Securing route origin authorization with blockchain for inter-domain routing”. *IEEE Transactions on Network and Service Management.*

Heffernan, A. 1998. “Protection of BGP Sessions via the TCP MD5 Signature Option, RFC 2385”. https://datatracker.ietf.org/doc/html/rfc2385.

Hiran, Rahul, Niklas Carlsson ja Nahid Shahmehri. 2017. “Collaborative framework for protection against attacks targeting BGP and edge networks”. *Computer Networks* 122:120–137.

Hong, Seong-Cheol, Hongtaek Ju ja James Won-Ki Hong. 2013. “Network reachability-based IP prefix hijacking detection”. *International Journal of Network Management* 23 (1): 1–15.

Hu, Yih-Chun, Adrian Perrig ja Marvin Sirbu. 2004. “SPV: Secure Path Vector Routing for Securing BGP”. *SIGCOMM Comput. Commun. Rev.* (New York, NY, USA) 34, numero 4 (elokuu): 179–192. ISSN: 0146-4833. https://doi.org/10.1145/1030194.1015488.

Huston, G., M. Rossi ja G. Armitage. 2011. “Securing BGP — A Literature Survey”. *IEEE Communications Surveys Tutorials* 13, numero 2 (helmikuu): 199–222. ISSN: 2373-745X. https://doi.org/10.1109/SURV.2011.041010.00041.

Huston, G., P. Smith ja T. Bates. 2021. “CIDR REPORT for 13 Sep 21”, syyskuu. Viitattu 13. syyskuuta 2021. https://www.cidr-report.org/as2.0/.

IEEE. 2022. “IEEE Xplore digital library”, tammikuu. Viitattu 6. helmikuuta 2022. https://ieeexplore.ieee.org/Xplore/home.jsp.

Kent, S., C. Lynn ja K. Seo. 2000. “Secure Border Gateway Protocol (S-BGP)”. *IEEE Journal on Selected Areas in Communications* 18, numero 4 (huhtikuu): 582–592. ISSN: 1558-0008. https://doi.org/10.1109/49.839934.

Kim, E-yong, Li Xiao, Klara Nahrstedt ja Kunsoo Park. 2008. “Secure interdomain routing registry”. *IEEE Transactions on Information Forensics and Security* 3 (2): 304–316.

Kitchenham, B., ja S. Charters. 2007. “Guidelines for performing Systematic Literature Reviews in Software Engineering”. Teoksessa *EBSE Technical Report,* nide 1.

Kong, Lingjing, ja Hong Shen. 2015. “Achieving inter-domain routing security based on distributed translator trust model”. *Computer Science and Information Systems* 12 (4): 1327–1344.

Li, Peipei, Bin Lu ja Daofeng Li. 2021. “BGP Neighbor Trust Establishment Mechanism Based on the Bargaining Game”. *Information* 12 (3): 110.

Li, Pengkun, Jinshu Su, Xiaofeng Wang ja Qianqian Xing. 2021. “DIIA: Blockchain-Based Decentralized Infrastructure for Internet Accountability”. *Security and Communication Networks* 2021.

Li, Qi, Mingwei Xu, Jianping Wu, Xinwen Zhang, Patrick PC Lee ja Ke Xu. 2011. “Enhancing the trust of internet routing with lightweight route attestation”. *IEEE Transactions on Information Forensics and Security* 7 (2): 691–703.

Li, Qi, Xinwen Zhang, Xin Zhang ja Purui Su. 2014. “Invalidating idealized BGP security proposals and countermeasures”. *IEEE Transactions on Dependable and Secure Computing* 12 (3): 298–311.

Lougheed, K., ja Y. Rekhter. 1990. “A Border Gateway Protocol (BGP), RFC 1163”. Viitattu 6. helmikuuta 2022. https://tools.ietf.org/html/rfc1163.

Lu, Huimin, Yu Tang ja Yi Sun. 2021. “DRRS-BC: Decentralized routing registration system based on blockchain”. *IEEE/CAA Journal of Automatica Sinica* 8 (12): 1868–1876.

MANRS. 2022a. “Mutually Agreed Norms for Routing Security”. Viitattu 27. tammikuuta 2022. https://www.manrs.org/.

MANRS. 2022b. “Mutually Agreed Norms for Routing Security”. Viitattu 27. tammikuuta 2022. https://www.manrs.org/isps/guide/filtering/.

Mastilak, Lukas, Marek Galinski, Pavol Helebrandt, Ivan Kotuliak ja Michal Ries. 2020. “Enhancing Border Gateway Protocol Security Using Public Blockchain”. *Sensors* 20 (16): 4482.

McDaniel, Patrick, William Aiello, Kevin Butler ja John Ioannidis. 2006. “Origin authentication in interdomain routing”. *Computer Networks* 50 (16): 2953–2980.

Meng, Meng, Ruijuan Zheng, Ruxi Peng, Junlong Zhu, Mingchuan Zhang ja Qingtao Wu. 2020. “Safeguarding against prefix interception attacks via online learning”. *Robotics and Autonomous Systems* 131:103556.

Mitseva, A., A. Panchenko ja T. Engel. 2018. “The state of affairs in BGP security: A survey of attacks and defenses”. Cited By 22, *Computer Communications* 124:45–60. https://doi.org/10.1016/j.comcom.2018.04.013. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046355671&doi=10.1016%2fj.comcom.2018.04.013&partnerID=40&md5=2f49b9befb4222cf49ba565e9679c638.

Moriano, Pablo, Raquel Hill ja L Jean Camp. 2021. “Using bursty announcements for detecting BGP routing anomalies”. *Computer Networks* 188:107835.

Murphy, S. 2006. “BGP Security Vulnerabilities Analysis, RFC 4272”, tammikuu. Viitattu 6. helmikuuta 2022. https://tools.ietf.org/html/rfc4272.

Nicholes, Martin O., ja Biswanath Mukherjee. 2009. “A survey of security techniques for the border gateway protocol (BGP)”. *IEEE Communications Surveys Tutorials* 11 (1): 52–65. https://doi.org/10.1109/SURV.2009.090105.

Oorschot, PC van, Tao Wan ja Evangelos Kranakis. 2007. “On interdomain routing security and pretty secure BGP (psBGP)”. *ACM Transactions on Information and System Security (TISSEC)* 10 (3): 11–es.

Pradeepa, R, ja M Pushpalatha. 2020. “A hybrid OpenFlow with intelligent detection and prediction models for preventing BGP path hijack on SDN”. *Soft Computing* 24 (13): 10205–10214.

ProQuest. 2022. “ProQuest”, tammikuu. Viitattu 6. helmikuuta 2022. https://www.proquest.com/.

Rekhter, Y., T. Li ja S. Harres. 2006. “A Border Gateway Protocol 4 (BGP-4), RFC 4271”, tammikuu. Viitattu 24. tammikuuta 2022. https://tools.ietf.org/html/rfc4271.

Schlamp, J., R. Holz, Q. Jacquemart, G. Carle ja E. W. Biersack. 2016. “HEAP: Reliable Assessment of BGP Hijacking Attacks”. *IEEE Journal on Selected Areas in Communications* 34 (6): 1849–1861.

Scopus. 2022. “Scopus - Abstract and citation database | Elsevier”, tammikuu. Viitattu 6. helmikuuta 2022. https://www.scopus.com/.

Sermpezis, P., V. Kotronis, P. Gigis, X. Dimitropoulos, D. Cicalese, A. King ja A. Dainotti. 2018. “ARTEMIS: Neutralizing BGP Hijacking Within a Minute”. *IEEE/ACM Transactions on Networking* 26 (6): 2471–2486.

Shapira, Tal, ja Yuval Shavitt. 2021. “SASA: Source-Aware Self-Attention for IP Hijack Detection”. *IEEE/ACM Transactions on Networking*.

Sharma, Priyanka, ja Vishnu Sharma. 2015. “Security enhancement on BGP protocol: A literature survey”. Teoksessa *International Conference on Computing, Communication Automation,* 859–864. https://doi.org/10.1109/CCAA.2015.7148495.

Siddiqui, MS, Diego Montero, René Serral-Gracià ja Marcelo Yannuzzi. 2015. “Self-reliant detection of route leaks in inter-domain routing”. *Computer Networks* 82:135–155.

Smith, Bradley R, ja JJ Garcia-Luna-Aceves. 1998. “Efficient security mechanisms for the border gateway routing protocol”. *Computer Communications* 21 (3): 203–210.

Song, Yang, Arun Venkataramani ja Lixin Gao. 2016. “Identifying and Addressing Reachability and Policy Attacks in “Secure” BGP”. *IEEE/ACM Transactions on Networking* 24 (5): 2969–2982.

Stewens, Marc., Arjen K. Lenstra ja Benne de. Weger. 2012. “Chosen-prefix collisions for MD5 and applications”. Viitattu 25. maaliskuuta 2020. https://infoscience.epfl.ch/record/164548/files/IJACT020403%5C%20STEVENS.pdf.

ThousandEyes. 2018. “Internet Vulnerability Takes Down Google”, joulukuu. Viitattu 11. lokakuuta 2021. https://www.thousandeyes.com/blog/internet-vulnerability-takes-down-google/.

Touch, J., A. Mankin ja R. Bonica. 2010. “The TCP Authentication Option, RFC 5925”. https://datatracker.ietf.org/doc/html/rfc5925.

Wang, Anduo, Limin Jia, Wenchao Zhou, Yiqing Ren, Boon Thau Loo, Jennifer Rexford, Vivek Nigam, Andre Scedrov ja Carolyn Talcott. 2012. “FSR: Formal analysis and implementation toolkit for safe interdomain routing”. *IEEE/ACM Transactions on Networking* 20 (6): 1814–1827.

Wang, N., X.-H. Du, W.-J. Wang ja A.-D. Liu. 2017. “A Survey of the Border Gateway Protocol Security”. Cited By 3, *Jisuanji Xuebao/Chinese Journal of Computers* 40 (7): 1626–1648. https://doi.org/10.11897/SP.J.1016.2017.01626. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85031813936&doi=10.11897%2fSP.J.1016.2017.01626&partnerID=40&md5=00ee07427ccba9670dbbeda928ac5dc5.

Vohra, Q., ja E. Chen. 2012. “BGP Support for Four-Octet Autonomous System (AS) Number Space, RFC 6793”. Viitattu 13. syyskuuta 2021. https://datatracker.ietf.org/doc/html/rfc6793.

Xiang, Yang, Xingang Shi, Jianping Wu, Zhiliang Wang ja Xia Yin. 2013. “Sign what you really care about–Secure BGP AS-paths efficiently”. *Computer Networks* 57 (10): 2250–2265.

Xiangjiang, Hu, Zhu Peidong ja Gong Zhenghu. 2007. “Translator Trust for the Internet Inter-domain Routing”. Teoksessa *Future Generation Communication and Networking (FGCN 2007),* 1:453–458. https://doi.org/10.1109/FGCN.2007.221.

Xing, Qianqian, Baosheng Wang ja Xiaofeng Wang. 2018. “Bgpcoin: Blockchain-based internet number resource authority and bgp security solution”. *Symmetry* 10 (9): 408.

Yan, Zhiwei, ja Jong-Hyouk Lee. 2021. “BGPChain: Constructing a secure, smart, and agile routing infrastructure based on blockchain”. *ICT Express.*

Yin, Heng, Bo Sheng, Haining Wang ja Jianping Pan. 2010. “Keychain-based signatures for securing BGP”. *IEEE Journal on Selected Areas in Communications* 28 (8): 1308–1318.

Zhang, Jian, Daofeng Li ja Bowen Zhao. 2019. “A prefix hijacking detection model based on the immune network theory”. *IEEE Access* 7:132384–132394.

Zhang, Zheng, Ying Zhang, Y Charlie Hu, Z Morley Mao ja Randy Bush. 2008. “iSPY: Detecting IP prefix hijacking on my own”. Teoksessa *Proceedings of the ACM SIGCOMM 2008 conference on Data Communication,* 327–338.

Zheng, Changxi, Lusheng Ji, Dan Pei, Jia Wang ja Paul Francis. 2007. “A light-weight distributed scheme for detecting IP prefix hijacks in real-time”. *ACM SIGCOMM Computer Communication Review* 37 (4): 277–288.

Zhu, Peidong, Huayang Cao, Laurence T Yang ja Kan Chen. 2012. “AS Alliance based security enhancement for inter-domain routing protocol”. *Mathematical and computer modelling* 55 (1-2): 241–255.

Liitteet

A Tiedon keräyslomake

- Tekijä(t)
- Otsikko
- Vuosi
- Julkaisu
- Vastatut heikkoudet (Attacks covered)
  - Osoitekaappaus (Prefix Hijacking)
  - Reittiväärennös (AS path forgery)
  - Uudelleenohjaushyökkäys (Interception attack)
  - Reittivuoto (Route Leak)
  - Muu (Other)
- Tehokkuus (Performance)
  - Yhdentymisen viive (covergence delay)
  - Vakaus (Stability)
  - Laajennettavuus (Scalability)
  - Laskennan kustannukset (Computational overhead)
  - Kaistanleveyden kustannukset (Bandwidth overhead)
  - Säilytyksen kustannukset (Storage overhead)
- Reitityksen yksityisyys (Routing Privacy)
- Käyttöönotettavuus (Deployability)
  - Käyttöönotettavuus (Deployability)
  - Omaksittavuus (Adoptability)
- Käyttöönoton tila (Status)
  - Käytössä (Adopted)
  - Standardisoitu (Standardized)
  - Vain akateeminen (Academic paper only)

B Aineisto

Tekijät	Otsikko	Vuosi	Julkaisu	OsoiteKauppaus	Reittiäiäremmis	Uudelleenohjaushyökkäys	Reititvuoto	Convergence	Vakaus	Laajennettavuus	Laskennan kustannukset	Kaistankeveyden kustannukset	Säilytyksen kustannukset	Reitityksen yksityisyys	Käyttöönotettavuus	Omaksittavuus	Käytössä	Standardisoitu	Vain Akateeminen	Kryptografia	Lohkoketju	Seuranta
Shivani Deshpande, Marina Thottan,Tin Kam Ho, Biplab Sikdar	An Online Mechanism for BGP Instability Detection and Analysis	2009	IEEE Transactions on computers	1	0	0	1	1	2	2	1	2	1	2	2	1	0	0	2	0	0	1
Rahul Hiran,Niklas Carlsson,Nahid Shahmehri	Collaborative framework for protection against attacks targeting BGP and edge networks	2017	Computer Networks	2	0	2	0	1	2	1	1	2	2	1	1	1	0	0	2	1	0	1
Pablo Morianoa,Raquel Hillb,L. Jean Camp	Using bursty announcements for detecting BGP routing anomalies	2021	Computer Networks	2	0	0	0	1	2	2	1	2	1	2	2	2	0	0	2	0	0	1
Johann Schlamp, Ralph Holz, Quentin Jacquemart, Georg Carle, Ernst W. Biersack	HEAP: Reliable Assessment of BGP Hijacking Attacks	2016	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS	2	0	0	0	2	2	2	1	2	1	2	1	1	0	0	2	0	0	1
Pavlos Sermpezis,Vasileios Kotronis,Petros Gigis,Xenofontas Dimitropoulos,Danilo Cicalese, Alistair King, and Alberto Dainotti	ARTEMIS: Neutralizing BGP Hijacking Within a Minute	2018	IEEE/ACM TRANSACTIONS ON NETWORKING	2	0	0	0	2	2	2	1	2	1	2	2	2	0	0	2	0	0	1
Qianqian Xing, Baosheng Wang, Xiaofeng Wang	BGPcoin: Blockchain-Based Internet Number Resource Authority and BGP Security Solution	2018	Symmetry	2	1	0	1	2	2	1	0	2	2	1	1	1	0	0	2	1	1	0
Tal Shapira, Yuval Shavitt	SASA: Source-Aware Self-Attention for IP Hijack Detection	2021	IEEE/ACM TRANSACTIONS ON NETWORKING	0	0	2	0	2	2	2	1	2	1	2	2	2	0	0	2	0	0	1
M.S. Siddiqui, D. Montero, R. Serral-Gracià, M. Yannuzzi	Self-reliant detection of route leaks in inter-domain routing	2015	Computer Networks	0	0	0	1	2	2	2	1	2	1	2	2	2	0	0	2	0	0	1
Guobiao He, Wei Su, Shuai Gao, Jiarui Yue, Sajal K. Das	ROAchain: Securing Route Origin Authorization With Blockchain for Inter-Domain Routing	2021	IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT	2	1	0	0	1	2	2	0	2	1	1	1	1	0	0	2	1	1	0
Yi Guo, Haixin Duan, Jikun Chen, Fu Miao	MAF-SAM: An effective method to perceive data plane threats of inter domain routing system	2016	Computer Networks	0	0	0	2	2	2	2	1	2	2	2	2	2	0	0	2	0	0	0
Peipei Li, Bin Lu, Daofeng Li	BGP Neighbor Trust Establishment Mechanism Based on the Bargaining Game	2021	Information	0	0	0	0	2	2	1	0	1	2	2	1	1	0	0	2	0	0	0
Anduo Wang Limin Jia, Wenchao Zhou, Yiqing Ren, Boon Thau Loo, Jennifer Rexford, Vivek Nigam, Andre Scedrov, and Carolyn Talcott	FSR: Formal Analysis and Implementation Toolkit for Safe Interdomain Routing	2012	IEEE/ACM TRANSACTIONS ON NETWORKING	0	0	0	0	2	2	2	1	2	1	2	2	2	0	0	2	0	0	0
Yang Song, Arun Venkataramani, Lixin Gao	Identifying and Addressing Reachability and Policy Attacks in “Secure” BGP	2016	IEEE/ACM TRANSACTIONS ON NETWORKING	0	0	0	0	1	2	2	1	1	2	2	2	2	0	0	2	1	0	0
Qi Li, Xinwen Zhang, Xin Zhang, Purui Su	Invalidating Idealized BGP Security Proposals and Countermeasures	2015	IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	0	0	0	0	2	2	2	0	1	2	2	2	2	0	0	2	0	0	0
Yang Xiang, Xingang Shi, Jianping Wu, Zhiliang Wang, Xia Yin	Sign what you really care about – Secure BGP AS-paths efficiently	2013	Computer Networks	2	0	2	0	2	2	2	0	2	2	2	1	2	0	0	2	1	0	0
Osama S. Alkadi, Nour Moustafa, Benjamin Turnbull, Kim-Kwang Raymond Choo	An Ontological Graph Identification Method for Improving Localization of IP Prefix Hijacking in Network Systems	2020	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	2	0	0	0	2	2	2	1	2	2	2	2	2	0	0	2	0	0	1
Bradley R. Smith, J.J. Garcia-Luna-Aceves	Efficient security mechanisms for the border gateway routing protocol	1998	Computer Communications	0	2	0	0	2	2	1	1	1	2	2	1	1	0	0	2	1	0	0
P. C. VAN OORSCHOT, TAO WAN, EVANGELOS KRANAKIS	On Interdomain Routing Security and Pretty Secure BGP (psBGP)	2007	ACM Transactions on Information and System Security	1	1	0	0	2	2	1	0	1	1	2	1	1	0	0	2	1	0	0
Qi Li, Mingwei Xu, Jianping Wu, Xinwen Zhang, Patrick P. C. Lee, Ke Xu	Enhancing the Trust of Internet Routing With Lightweight Route Attestation	2011	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	2	1	0	0	2	2	2	1	1	2	2	1	1	0	0	2	1	0	0
JIAN ZHANG, DAOFENG LI, OWEN ZHAO	A Prefix Hijacking Detection Model Based on the Immune Network Theory	2019	IEEE Access	2	0	0	0	2	2	2	1	2	1	2	2	2	0	0	2	0	0	0
R. Pradeepa, M. Pushpalatha	A hybrid OpenFlow with intelligent detection and prediction models for preventing BGP path hijack on SDN	2020	Soft Computing	2	0	0	0	1	2	2	1	2	1	2	2	2	0	0	2	0	0	1
Bin DAI,Feng WANG, Baokang ZHAO, Jinshu SU	Using Regional Routing to Improve the Scalability and Security of Inter-Domain Multipath Routing	2012	IEICE TRANS. INF. & SYST	1	0	0	1	2	2	1	1	1	1	1	1	1	0	0	2	0	0	0
Bezawada Bruhadeshwar, Sandeep S. Kulkarni, Alex X. Liu	Symmetric Key Approaches to Securing BGP—A Little Bit Trust Is Enough	2011	IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS	2	2	0	0	1	2	1	0	1	1	2	1	1	0	0	2	1	0	0
Meng Meng,Ruijuan Zheng,Ruxi Peng,Junlong Zhu,Mingchuan Zhang, Qingtao Wu	Safeguarding against prefix interception attacks via online learning	2020	Robotics and Autonomous Systems	0	0	2	0	2	2	2	1	2	2	2	2	2	0	0	2	0	0	1
E-yong Kim, Li Xiao, Klara Nahrstedt, Kunsoo Park	Secure Interdomain Routing Registry	2008	IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY	2	2	2	1	1	1	1	0	1	2	1	1	1	0	0	2	1	0	0
Zheng Zhang, Ying Zhang, Y. Charlie Hu, Z. Morley Mao, Randy Bush	iSPY: Detecting IP Prefix Hijacking on My Own	2010	IEEE/ACM TRANSACTIONS ON NETWORKING	2	1	0	0	1	2	2	1	2	2	2	2	2	0	0	2	0	0	1
Seong-Cheol Hong, Hongtaek Ju, James Won-Ki Hong	Network reachability-based IP prefix hijacking detection	2013	INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT	2	0	0	0	2	2	1	1	1	1	2	2	2	0	0	2	0	0	1
Changxi Zheng, Lusheng Ji, Dan Pei , Jia Wang, Paul Francis	A Light-Weight Distributed Scheme for Detecting IP Prefix Hijacks in Real-Time	2007	ACM SIGCOMM Computer Communication Review	2	1	1	1	2	2	2	1	2	1	2	2	2	0	0	2	0	0	1
Lingjing Kong, Hong Shen	Achieving Inter-domain Routing Security Based on Distributed Translator Trust Model	2015	Computer Science and Information Systems	1	1	0	0	1	2	1	1	2	1	2	1	1	0	0	2	0	0	0
Heng Yin, Bo Sheng, Haining Wang, Jianping Pan	Keychain-Based Signatures for Securing BGP	2010	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS	1	1	0	0	2	2	1	0	1	1	2	1	2	0	0	2	1	1	0
Jian Chang, Krishna K. Venkatasubramanian, Andrew G. West, Sampath Kannan, Insup Lee, Boon Thau Loo, Oleg Sokolsky	AS-CRED: Reputation and Alert Service for Interdomain Routing	2013	IEEE SYSTEMS JOURNAL	2	0	0	0	1	2	1	0	2	2	1	1	1	0	0	2	1	0	1
Huimin Lu, Yu Tang, Yi Sun	DRRS-BC: Decentralized Routing Registration System Based on Blockchain	2021	IEEE/CAA JOURNAL OF AUTOMATICA SINICA	2	0	0	0	1	1	1	0	1	1	1	1	1	0	0	2	1	1	0
Pengkun Li, Jinshu Su, Xiaofeng Wang, Qianqian Xing	DIIA: Blockchain-Based Decentralized Infrastructure for Internet Accountability	2021	Security and Communication Networks	2	0	0	0	1	2	1	0	1	1	1	1	1	0	0	2	1	1	0
Song LI, Haixin DUAN, Zhiliang WANG, Jinjin LIANG, Xing LI	An accurate distributed scheme for detection of prefix interception	2016	Science China Information Sciences	0	0	2	0	1	2	2	1	2	2	2	2	2	0	0	2	0	0	1
Zhiwei Yan, Jong-Hyouk Lee	BGPChain: Constructing a secure, smart, and agile routing infrastructure based on blockchain	2021	ICT Express	2	2	0	0	1	2	1	0	1	1	1	1	1	0	0	2	1	1	0
Peidong Zhu, Huayang Cao,Laurence T.Yang, Kan Chen	AS Alliance based security enhancement for inter-domain routing protocol	2012	Mathematical and Computer Modelling	2	1	0	0	1	2	1	1	2	1	1	1	1	0	0	2	0	0	0
D. Comer P. Singh S. Vasudevan	Effective border gateway protocol protection that does not require universal adoption of a public key infrastructure	2012	IET Networks	2	2	0	0	1	2	2	0	2	1	2	2	2	0	0	2	1	0	0
GUO Yi, WANG ZhenXing	An immune-theory-based model for monitoring inter-domain routing system	2012	Science China Information Sciences	2	0	0	0	1	2	1	1	2	1	2	1	1	0	0	2	0	0	1
Lukas Mastilak, Marek Galinski, Pavol Helebrandt, Ivan Kotuliak, Michal Ries	Enhancing Border Gateway Protocol Security Using Public Blockchain	2020	Sensors	2	0	0	0	1	1	1	0	1	1	1	1	2	0	0	2	1	1	0
Patrick McDaniel, William Aiello, Kevin Butler, John Ioannidis	Origin authentication in interdomain routing	2006	Computer Networks	2	0	0	0	1	1	2	0	1	2	1	1	1	0	0	2	1	0	0
Yih-Chun Hu, Adrian Perrig, Marvin Sirbu	SPV: Secure Path Vector Routing for Securing BGP	2004	ACM SIGCOMM Computer Communication Review	2	2	0	0	1	2	2	0	1	2	2	1	1	0	0	2	1	0	0
Stephen Kent, Charles Lynn, Karen Seo	Secure Border Gateway Protocol (S-BGP)	2000	IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS	2	2	1	0	1	2	1	0	1	1	1	1	1	1	0	2	1	0	0