**Juha Moisio**

# Palvelunestohyökkäysten havainnointi ja torjuminen tilastollisilla menetelmillä

Tietotekniikan kandidaatintutkielma

25. huhtikuuta 2015

Jyväskylän yliopisto

Tietotekniikan laitos

**Tekijä:** Juha Moisio

**Yhteystiedot:** juha.pa.moisio@student.jyu.fi

**Ohjaaja:** Anneli Heimbürger

**Työn nimi:** Palvelunestohyökkäysten havainnointi ja torjuminen tilastollisilla menetelmillä

**Title in English:** Denial-of-service attack detection and prevention with statistical methods

**Työ:** Kandidaatintutkielma

**Sivumäärä:** 22+0

**Tiivistelmä:** Palvelunestohyökkäykset ovat ajankohtaisena ongelmana tärkeä tutkimuksen kohde. Palvelunestohyökkäysten torjumiseen tarvitaan menetelmiä, joilla palvelua kuormittava hyökkäysliikenne voidaan erottaa tavallisesta verkkoliikenteestä. Tämän tutkimuksen tavoitteena on perehtyä palvelunestohyökkäysten toimintaan ja selvittää, mitä tilastollisia torjumismenetelmiä hyökkäysten torjumiseen käytetään. Tutkimuksessa selvitettiin palvelunestohyökkäysten yleiset pääpiirteet ja luokiteltiin hyökkäykset kahteen pääluokkaan. Lisäksi tutkimuksessa tunnistettiin neljä eri tilastollista torjumismenetelmää. Palvelunestohyökkäysten torjuminen on haasteellista, eikä yleiskäyttöistä torjumismenetelmää ole kehitetty. Siksi uusien menetelmien jatkotutkimukselle on tarvetta.

**Avainsanat:** palvelunestohyökkäys, tilastollinen

**Abstract:** Denial-of-service attacks are important area of research. Methods that can separate normal network traffic from the overloading traffic coming from the attack source are needed. The object of this research is to study about denial-of-service attacks and to survey what statistical methods are used for the detection and prevention of such attacks. This study summarises general main aspects of denial-of-service attacks and categorises attacks to two main groups. Furthermore, in this study, four statistical methods were found. The prevention of denial-of-service attacks is a challenging problem. An universal prevention method is not known. Therefore, there is ongoing need for research for new prevention methods.

**Keywords:** denial-of-service attack, statistical

# Kuviot

# Sisältö

# 1 Johdanto

Internetpohjaisten palveluiden suosio on kasvanut. Asioimme internetin kautta yhä useammin. Maksamme laskuja, varaamme matkalippuja ja teemme muita hyvin aika kriittisiä tehtäviä. Näiden toimintojen onnistumisen edellytyksenä on palveluiden täsmällinen toimintavarmuus. Kuitenkin internetin avoimuus ja kontrolloimattomuus mahdollistavat sen, että melkeinpä kuka tahansa voi toimillaan yrittää estää minkä tahansa palvelun toiminnan. Paketit välitetään eteenpäin mahdollisimman tehokkaasti, mitä väärinkäyttämällä voidaan hyökätä palvelua vastaan.

Tutkimusaiheena on palvelunestohyökkäyksen havainnointiin ja torjumiseen käytettävien menetelmien kartoitus. Palvelunestohyökkäys on verkkohyökkäys, joka pyrkii estämään palvelun toiminnan sen käyttäjiltä (Mirkovic ym. 2004). Hyökkäys on onnistunut, jos se lamauttaa kohteen siten, että se ei kykene palvelemaan käyttäjiään toivotusti (Mirkovic ym. 2004). Tutkimuskysymyksenä on kuinka hyökkäykset havaitaan tavallisesta palveluun kohdistuvasta verkkoliikenteestä ja mitä tilastollisia menetelmiä käytetään niiden torjumisessa.

Palvelunestohyökkäykset ovat ajankohtainen ja siten tärkeä tutkimuksen kohde. Viime vuodenvaihteessa palvelunestohyökkäyksiä kohdistui suomalaisten pankkien verkkopalveluihin, minkä vaikutukset ulottuivat korttimaksu- ja pankkiautomaattipalvelujen toimintaan (Viestintävirasto 2014). Hyökkäykset eivät kuitenkaan ole uhka verkkopalvelun tiedoille (Viestintävirasto 2015). Toisaalta palvelunestohyökkäys tietoturvakriittistä palvelua vastaan voisi edesauttaa tietomurtohyökkäysten tekemistä. Lisäksi niiden avulla voitaisiin viedä huomiota pois muilta hyökkäysyrityksiltä.

Palvelunestohyökkäyksiä on helppo toteuttaa ja ne voidaan käytännössä kohdistaa mitä tahansa palvelua vastaan (Freiling 2005). Siten kohteina voivat olla suuryritysten, pankkien ja valtioiden lisäksi myös pienet yritykset, joilla ei ole välttämättä käytettävissä tarvittavia resursseja ja osaamista hyökkäysten torjumiseen. Maailmalla tapahtuu kuukausittain voimakkaita hyökkäyksiä, jotka Suomessa aiheuttaisivat runkoverkkotason ongelmia (Viestintävirasto 2014). Palveluntarjoajien on varauduttava hyökkäyksiltä ja mietittävä, miten palveluiden toiminta voidaan taata. Palvelun toiminnan estyminen tarkoittaa taloudellisia tappioita

sekä hyökkäyksen kohteena olevalle yritykselle että sen palvelua käyttäville asiakkaille. Siksi palvelunestohyökkäysten tutkimukseen on aihetta, jotta tunnistetaan toimivia ja tehokkaita menetelmiä hyökkäyksien havaitsemiseen ja torjumiseen.

Palvelunestohyökkäysten ongelmana on hyökkäystapojen yhteisten tekijöiden puuttuminen, mikä tekee niiden torjumisesta haasteellista (Tariq 2006). Tässä tutkimuksessa kuvataan hyökkäystyyppien yleiset pääpiirteet, joihin havainnointi- ja torjumismenetelmät nojautuvat. Tutkimusaihetta on rajattu palvelunestohyökkäysten torjumismenetelmien osalta tilastollisiin menetelmiin.

Tilastolliset menetelmät palvelunestohyökkäysten torjumisessa ovat saaneet suosiota. Tavoitteena on löytää menetelmiä, joilla pystytään erottamaan hyökkäysliikenne tavallisesta palveluun kohdistuvasta verkkoliikenteestä. Tutkimuksessa käydään läpi neljä eri teoreettista poikkeavuuteen perustuvaa tilastollista torjumismenetelmää.

Tutkimus on toteutettu kirjallisuuskatsauksena, joka on teoreettinen tutkimusstrategia. Luonteeltaan tutkimus on toteava tutkimus, jossa kerätään tietoa tutkittavasta kohteesta ja analysoidaan tietojen luotettavuutta. Tutkimusmetodiksi valittiin systemaattinen kirjallisuuskatsaus, jonka päämääränä on antaa vastaukset tutkimuskysymykseen, mikä toteutetaan tekemällä analyyttistä ja objektiivista tiivistelmää aiempien tutkimusten perusteella. Menetelmässä painotetaan hakutekniikoita ja lähteiden keskinäistä yhteyttä.

Tutkimuksen toisessa osiossa kuvataan palvelunestohyökkäyksien yleiset pääpiirteet ja luokitellaan palvelunestohyökkäykset kahteen pääluokkaan. Kolmannessa osiossa käsitellään palvelunestohyökkäysten torjumiseen käytettyjä tilastollisia menetelmiä ja esitellään neljä eri teoreettista poikkeavuuteen perustuvaa tilastollista torjumismenetelmää. Neljännessä osiossa on koottu tutkimuksen keskeiset johtopäätökset.

# 2 Palvelunestohyökkäysten luokittelu

Palvelunestohyökkäyksiä voidaan luokitella hyvin perusteellisesti (Tariq 2006). Yleistäen ne voidaan jakaa kahteen pääluokkaan, joita ovat haavoittuvuuksia hyödyntävät hyökkäykset ja tulvahyökkäykset (Carl ym. 2006). Haavoittuvuuksia hyödyntävät hyökkäykset aiheuttavat ongelmia huonosti ylläpidetyille palveluille (Carl ym. 2006). Tulvahyökkäykset väärinkäyttävät internetin perusrakenteita, kuten internetprotokollia (Carl ym. 2006). Seuraavissa alaluvuissa esitellään hyökkäystyypit tarkemmin.

## 2.1 Haavoittuvuuksia hyödyntävät hyökkäykset

Haavoittuvuuksia hyödyntävät hyökkäykset kohdistavat hyökkäykset kohdekoneesta löytynyttä haavoittuvuutta vastaan (Carl ym. 2006). Hyökkääjä toteuttaa hyökkäyksen lähettämällä kohdekoneelle haavoittuvuutta hyödyntävän internetpaketin, joka voi aiheuttaa toiminnan häiriöitä kohdekoneessa sen vastaanotettuaan (Carl ym. 2006). Hyökkääjän täytyy siten olla tietoinen kohdekoneen ominaisuuksista ja tunnistaa siinä oleva haavoittuvuus. Historiallinen esimerkki haavoittuvuutta hyödyntävästä hyökkäyksestä on ICMP-protokollalla lähetetty ylipitkä IP-paketti (ping-of-death), joka protokollasta poikkeavana lähetteenä aiheutti järjestelmien kaatumista (Carnegie Mellon University 1996).

Haavoittuvuudet, joita vastaan hyökkäyksiä tehdään ovat usein kuljetus- ja ohjelmistokerroksella (Carl ym. 2006). Ohjelmistokerroksella hyökkäyksen kohteena ovat kohdekoneen ohjelmiston haavoittuvuudet protokollien haavoittuvuuksien sijasta (Durcekova, Schwartz ja Shahmehri 2012). Ohjelmistokerroksella hyökkäykset hyödyntävät ohjelmistovirheitä ja -haavoittuvuuksia, jotka voivat aiheuttaa järjestelmän kaatumisen, muistin käytön kuormitusta, prosessoritehon kuluttamista tai yleistä järjestelmän hitautta (Carl ym. 2006). Yleisimmät ohjelmistotason haavoittuvuudet kohdistuvat väärään syötteseen, joka saa ohjelman epätoivottuun tilaan (Chen 2007).

Haavoittuvuuksia vastaan tehdyt hyökkäykset voidaan torjua suoraviivaisesti tunnettujen haavoittuvuuksien paikkaamisella (Carl ym. 2006). Siten haavoittuvuuksia hyödyntävien hyökkäysten torjumiseen ei tarvita yhteydenaikaisia torjumismenetelmiä. Tarpeeksi voimakkaina

hyökkäykset voivat kuitenkin aiheuttaa ongelmia haavoittuvuuden paikkaamisenkin jälkeen palvelua kuormittavina hyökkäyksinä (Carl ym. 2006). Seuraavassa luvussa esitellään toinen palvelunestohyökkäysten pääluokka, tulvahyökkäykset.

## 2.2 Tulvahyökkäykset

Internetin perusrakenteita väärinkäyttäviä palvelunestohyökkäyksiä kutsutaan tulvahyökkäyksiksi (Beitollahi ja Deconinck 2012). Tulvahyökkäykset väärinkäyttävät verkko- ja kuljetuskerrosta hyökkäysten tekoon (Beitollahi ja Deconinck 2012). Yleisimmät kuljetuskerroksen protokollat, joita tulvahyökkäyksissä väärinkäytetään, ovat ICMP-, UDP- ja TCP-protokollat (Carl ym. 2006).

Tulvahyökkäyksiä on mahdollisia toteuttaa silloinkin, kun kohdekoneessa ei ole mitään tunnistettavissa olevia haavoittuvuuksia (Carl ym. 2006). Tulvahyökkäyksen toteuttamiseen hyökkääjän tarvitsee tietää vain kohdekoneen IP-osoite (Beitollahi ja Deconinck 2012). Sen takia tulvahyökkäykset ovat uhka myös hyvin ylläpidetyille palveluille (Carl ym. 2006).

Tulvahyökkäykset perustuvat palvelun ylikuormittamiseen, joka tapahtuu kohdekoneen resurssien tai siirtonopeuden kuluttamisella (Carl ym. 2006). Hyökkääjä lähettää yhtäaikaista kuormittavaa liikennettä kohdekoneelle kuormittaen sitä niin, että se ei kykene palvelemaan muiden käyttäjien pyyntöjä (Carl ym. 2006). Tällöin palvelun toiminta estyy ja hyökkäys on onnistunut.

Esimerkki TCP-prokollaa väärinkäyttävästä tulvahyökkäyksestä on TCP-SYN-tulvahyökkäys, joka hyväksikäyttää TCP-protokollan yhteydenavaamisen kolmitiekättelyä (Siris ja Papagalou 2004). Hyökkäyksen kohteena voi olla mikä tahansa palvelin, joka tarjoaa TCP-prokollalla käytettäviä palveluja. TCP-SYN-tulvahyökkäyksessä hyökkääjä lähettää kohdekoneelle lukuisia SYN-viestejä yhteyden avaamiseen. Kohdekone vastaanottaa SYN-viestit varaamalla jokaiselle muistipaikan ja lähettämällä SYN/ACK-viestin vastauksena SYN-viestin lähdeosoitteeseen. Hyökkääjä joko jättää vastaamatta kolmitiekättelyn vaaditun hyväksymisviestin tai käyttää lähettämässään SYN-viestissään väärennettyä IP-osoitetta. Tällöin kohdekoneen muistiin jää keskenjääneitä puoliavoimia yhteyksiä. Koska koneiden resurssit ovat rajallisia, tarpeeksi voimakkaana hyökkäys aiheuttaa sen, että kohdekone ei kykene avaamaan uusia

yhteyksiä muille käyttäjille. (Siris ja Papagalou 2004)

Koska tulvahyökkäykset perustuvat palvelun ylikuormittamiseen, on niiden kuormittava vaikutus suoraan verrannollinen yhteyskuorman määrään (Carl ym. 2006). Siten tulvahyökkäysten yhteyskuormaa voidaan lisätä kasvattamalla hyökkäyslähteiden lukumäärää (Durcekova, Schwartz ja Shahmehri 2012). Tällöin myös hyökkäysten torjuminen on hankalampaa, koska hyökkäys ei enää tapahdu yhdestä helposti tunnistettavasta ja torjuttavasta lähteestä (Durcekova, Schwartz ja Shahmehri 2012).

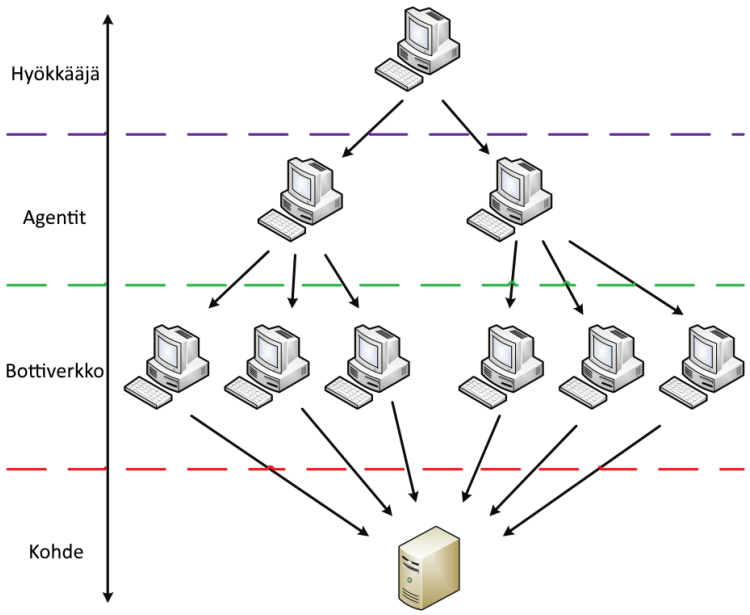
Seuraavissa alaluvuissa esitellään tulvahyökkäyksinä toteutettujen palvelunestohyökkäysten kaksi yleistä ilmentymää, jotka nojaavat edellä mainittuihin olettamuksiin yhteyskuorman kasvattamisesta ja hyökkäyslähteen tunnistamisen hankaloittamisesta. Ensimmäisenä kerrotaan hajautetusta palvelunestohyökkäyksestä ja toisena peilaavasta palvelunestohyökkäyksestä.

### 2.2.1 Hajautettu palvelunestohyökkäys

Palvelunestohyökkäystä, joka tapahtuu useasta hyökkäyslähteestä yhtäaikaisesti, kutsutaan hajautetuksi palvelunestohyökkäykseksi (Freiling, Holz ja Wicherski 2005). Hajautetun palvelunestohyökkäyksen tavoitteena on kasvattaa kuormittavan hyökkäyksen voimakkuutta (Freiling, Holz ja Wicherski 2005). Hajautetun palvelunestohyökkäyksen rakenne on kuvattu kuviossa 1.

Hajautettu palvelunestohyökkäys koostuu suuresta kaapattujen koneiden ryhmittymästä, jota kutsutaan bottiverkoksi (Freiling, Holz ja Wicherski 2005). Bottiverkon koneet ovat hyökkääjän kaappaamia laitteita hyökkäyksen tekoa varten (Freiling, Holz ja Wicherski 2005). Yksittäistä bottiverkon kaapattua konetta kutsutaan orja- (Paxson 2001) tai zombikoneeksi (Beitollahi ja Deconinck 2012). Kaapattuja laitteita voivat olla tavallisten kotikoneiden lisäksi mitkä tahansa hyökkäykseen kelpaavat verkkoon kytketyt laitteet, kuten huonosti suojatut reitittimet ja verkkotulostimet (Brenner 2014). Näitä kaapattuja koneita hallitsee usein yksi isäntäkone, joko suoraan tai erillisten agenttikoneiden avulla, jolloin hyökkäyksen lähdettä on vaikeampaa selvittää (Durcekova, Schwartz ja Shahmehri 2012).

Tuhansien koneiden bottiverkko mahdollistaa voimakkaiden tulvahyökkäysten tekemisen (Frei-

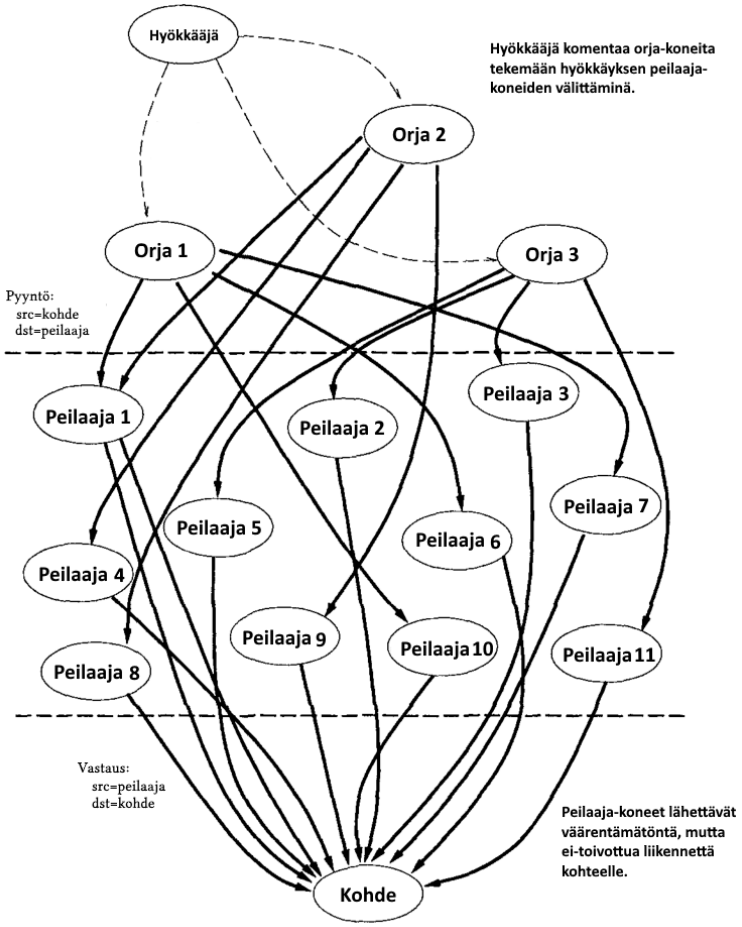



Kuvio 1. Hajautetun palvelunestohyökkäyksen rakenne (Durcekova, Schwartz ja Shahmehri 2012).

ling, Holz ja Wicherski 2005). Hajautettujen palvelunestohyökkäysten voimakkuutta voidaan yhä maksimoida huolellisella hyökkäyksen suunnittelulla kohdistamalla hyökkäys kohteen heikkouksiin (Carl ym. 2006). Hyökkäyksen kasvaessa myös sen torjumiseen tarvittava laskennallinen vaativuus kasvaa (Durcekova, Schwartz ja Shahmehri 2012). Suurien hajautettujen tulvahyökkäysten torjuminen on siten haasteellista. Torjumisen ongelmana on myös hyökkäyslähteen erottamisen vaikeus johtuen yhteyksien hajautuksesta (Durcekova, Schwartz ja Shahmehri 2012). Tulvahyökkäysten alkuperäisen lähteen tunnistamista voidaan yhä hankaloittaa yhteyksien peilaamisella, mistä kerrotaan seuraavassa alaluvussa.

### 2.2.2 Peilaava palvelunestohyökkäys

Palvelunestohyökkääjän tavoitteena on pyrkiä olemaan mahdollisimman tunnistamattomissa, jotta hyökkäyksen lähdettä ei voida jäljittää ja jotta hyökkäys olisi mahdollisimman hankalaa torjua (Durcekova, Schwartz ja Shahmehri 2012). Tällöin palvelunestohyökkäys onnistuu varmemmin ja saavuttaa tavoitteensa. Luvussa 2.2.1 kerrottiin, kuinka yhteyksien hajauttamisella voidaan hankaloittaa hyökkäyslähteen tunnistamista. Toinen hyökkäysmenetel-




Kuvio 2. Peilaavan hajautetun palvelunestohyökkäyksen rakenne (Paxson 2001).

mä, joka pyrkii piilottamaan hyökkäyksen lähdettä, on yhteyksien peilaaminen (Durcekova, Schwartz ja Shahmehri 2012).

Palvelunestohyökkäystä, jossa hyökkäys tehdään muiden järjestelmien välityksellä, kutsutaan peilaavaksi (reflective) palvelunestohyökkäykseksi (Beitollahi ja Deconinck 2012). Peilaavan hajautetun palvelunestohyökkäyksen rakenne on kuvattu kuviossa 2.

Peilaavassa palvelunestohyökkäyksessä hyökkäysliikenteen välitykseen käytettyjä koneita kutsutaan peilaajiksi (reflectors) (Paxson 2001). Peilaajat ovat internetiin kytkettyjä laitteita, jotka toimivat internetin pakettien välittäjinä, kuten reitittimet ja muut palvelimet (Durcekova, Schwartz ja Shahmehri 2012).

Peilaava hajautettu palvelinestohyökkäys tapahtuu käytännössä siten, että hyökkääjä komen-

taa bottiverkon orjakoneita lähettämään peilaaville koneille hyökkäyspaketit, joiden lähettäjäksi on väärennetty kohdekoneen IP-osoite. Vastaanottaessaan paketin, peilaavat koneet vastaavat kohdekoneelle eikä takaisin hyökkääjälle. Kohdekoneelle hyökkäys näkyy tulevan välittäjäkoneilta, jolloin hyökkäysliikennettä on vaikea erottaa palveluun kohdistuvasta tavallisesta verkkoliikenteestä. Tämän ansiosta hyökkääjä pysyy varmemmin tunnistamattomissa. kohteelle hyökkäys näyttäytyy yhä enemmän hajautetulta verrattuna tavalliseen hajautettuun palvelunestohyökkäykseen, mikä hankaloittaa hyökkäyksen torjumista. (Durcekova, Schwartz ja Shahmehri 2012)

Esimerkki peilaavasta palvelunestohyökkäyksestä on ICMP-prokollaa hyväksikäyttävä tulvahyökkäys (Beitollahi ja Deconinck 2012), joka tunnetaan nimeltä SMURF-hyökkäys (Guerid ym. 2011). SMURF-hyökkäys hyödyntää ICMP-prokollan ECHO-kyselyä hyökkäysliikenteen peilaamisessa (Beitollahi ja Deconinck 2012). Hyökkäys tapahtuu lähettämällä peilaaville koneille ICMP-paketteja, joihin lähettäjäksi on väärennetty kohdekoneen IP-osoite. Tällöin peilaavat koneet lähettävät ICMP-prokollan vaatiman vastausviestin kohdekoneelle. Riittävän suurena määränä peilaavien koneiden vastausviestit kuormittavat kohdekonetta niin, että sen palvelun toiminta häiriintyy ylikuormituksen seurauksena. SMURF-hyökkäys on yksi helpoimmista palvelunestohyökkäyksistä toteuttaa ollen samalla hankala torjuttava. Hyökkääjän ei tarvitse hallita suuria määriä hyökkäyskoneita, vaan hän voi hyväksikäyttää internetin tarjoamia kolmannen osapuolen koneita hyökkäyksen tekoon. (Guerid ym. 2011)

Hajautettujen ja peilaavien tulvahyökkäysten torjuminen on haasteellista, ja tehokkaiden torjumismenetelmien tutkiminen on ajankohtaista. Seuraavassa luvussa esitellään hajautettujen palvelunestohyökkäysten torjumiseen käytettyjä menetelmiä ja esitellään neljä eri poikkeavuuteen perustuvaa tilastollista torjumismenetelmää.

# 3 Poikkeavuuteen perustuvat tilastolliset torjumismenetelmät

Yleisesti palvelunestohyökkäysten torjumismenetelmät voidaan jakaa tunnusmerkkeihin perustuviin ja poikkeavuuteen perustuviin menetelmiin (Ozcelik, Fu ja Brooks 2013). Tunnusmerkkeihin perustuvat menetelmät vertaavat verkkoliikennettä entuudestaan tunnettuihin hyökkäysmalleihin (Ozcelik, Fu ja Brooks 2013). Poikkeavuuteen perustuvissa menetelmissä käytetään verkkoliikenteen tilastollisia ominaisuuksia hyökkäyksien tunnistamisessa (Li, Chang ja Chan 2005). Poikkeavuuteen perustuvat menetelmät pystyvät torjumaan uudenlaisia ja mukautuvia hyökkäysmenetelmiä, mutta ne aiheuttavat myös vääriä havaintoja (Ozcelik, Fu ja Brooks 2013).

Tutkijoiden haasteena on löytää tehokkaita hyvin palvelunestohyökkäyksiä havaitsevia menetelmiä, jotka samalla tuottaisivat vähän vääriä havaintoja ja jotka eivät olisi liian monimutkaisia tai kalliita toteuttaa. Lisähaasteena tutkijoille uusien torjumismenetelmien kehittämisessä on, että menetelmien testaaminen oikeassa ympäristössä on harvoin mahdollista. Usein menetelmien testaaminen joudutaan tekemään simuloiduissa ympäristöissä, miksi uusien menetelmien testituloksiin tulee suhtautua aina kriittisesti. (Ozcelik, Fu ja Brooks 2013)

Poikkeavuuteen perustuvat tilastolliset torjumismenetelmät ovat saaneet suosiota palvelunestohyökkäysten torjumisessa. Tavoitteena on löytää menetelmiä, joilla hyökkäykset voidaan erottaa palveluun kohdistuvasta tavallisesta verkkoliikenteestä. (Li, Chang ja Chan 2005) Verkkoliikenteen tilastolliset ominaisuudet ovat osoittautuneet hyväksi ja tehokkaaksi lähestymistavaksi palvelunestohyökkäysten torjumisessa (Feinstein ym. 2003).

Tilastolliset torjumismenetelmät pohjautuvat oletukseen, että verkkoliikenteelle on löydettävissä tekijöitä, jotka pysyvät stabiilina tavallisen liikenteen aikana. (Li, Chang ja Chan 2005) Lisäksi menetelmien toimivuuden kannalta täytyy olettaa, että palvelunestohyökkäys ei voi täydellisesti mallintaa tavallista palveluun kohdistuvaa verkkoliikennettä (Feinstein ym. 2003). Näiden kahden olettamusten nojalla voidaan verkkoliikenteen tilastollisia ominaisuuksia käyttää hyökkäysliikenteen poikkeavuuden tunnistamisessa. Poikkeavuuden ha-

vaittua, voidaan palveluun kohdistuvasta verkkoliikenteestä pudottaa pois ne paketit, jotka poikkeavat tavallisesta liikenteestä merkittävästi. Poikkeavuuden tunnistamiseen voidaan käyttää muun muassa IP-pakettien lähetystiheyttä ja otsikkotietoja, joista voidaan analysoida esimerkiksi lähettäjän IP-osoite ja käytetty protokolla. (Li, Chang ja Chan 2005)

Tunnettuja tilastollisen poikkeavuuden mittaamiseen käytettyjä algoritmeja ovat muun muassa khii toiseen -testiin perustuva algoritmi ja entropiaan perustuvat algoritmit (Feinstein ym. 2003). Näiden lisäksi yleisesti käytetään kumulatiivisen summan algoritmia (Ozcelik, Fu ja Brooks 2013). Jin ja Yeung (2004) ovat myös tutkineet kovarianssianalyysin soveltuvuutta palvelunestohyökkäysten torjumisessa. Seuraavissa alaluvuissa kerrotaan menetelmistä yksitellen.

## 3.1 Kumulatiiviseen summaan perustuva menetelmä

Kumulatiiviseen summan algoritmi (Cusum) on yleisesti käytetty poikkeamaan perustuva palvelunestohyökkäysten havainnointimenetelmä. Menetelmässä lasketaan poikkeavuutta nykyhetken ja mitatun keskiarvon välillä. Jos nykyhetken arvon muutos on kasvunopeudeltaan suurempi mitä mitatussa keskiarvoissa, algoritmin kerroin kasvaa. Kerroin lähestyy nollaa, kun etäisyys verrattujen pisteiden välillä pienenee. Kertoimelle voidaan siten määritellä rajaarvo, jonka ylitettyä voidaan epäillä syyksi palvelunestohyökkäystä. (Ozcelik, Fu ja Brooks 2013)

Kumulatiivisen summan algoritmi on yksi muutos-pisteen havaitsemisen (Change-point detection) algoritmeista. Niiden avulla voidaan verkkoliikenteestä erottaa hyökkäyksestä johtuvia tilastollisia muutoksia. Yleisesti menetelmissä tallennetaan aikasarjaan IP-pakettien osoite-, portti- ja protokollatietoja. Ajallisen muutoksen seuraamisesta johtuen, menetelmien hyökkäyksien havaitsemisessa on aina viiveettä. (Carl ym. 2006)

Kumulatiivisen summan algoritmia käytetään muun muassa UDP-, TCP- ja ICMP-protokollilla tapahtuvia tulvahyökkäyksiä vastaan (Carl ym. 2006). Ozcelik, Fu ja Brooks (2013) testasivat algoritmin toimintaa käyttämällä algoritmin muuttujana saapuvien pakettien lukumäärää. Kumulatiivisen summan kertoimen laskukaavan Ozcelik, Fu ja Brooks (2013) muodostivat seuraavasti:

$$S_0 = 0$$
$$S_i = max\{0, (S_{i-1} + N_i - avg_i)\},$$

missä $S_{i-1}$ on vanha laskettu kerroin, $N_i$ on saapuneiden pakettien lukumäärä ajanhetkellä $i$ ja $avg_i$ on kaikkien ajanhetkillä $i$ saapuneiden pakettien lukumäärien keskiarvo.

Kumulatiiviseen summan algoritmia pidetään tehokkaana torjumismenetelmänä, eikä se vaadi paljon laskentatehoa tai muistia hyökkäysten torjumisessa (Carl ym. 2006). Alhaisen muistinkäytön ja laskentatehon voidaan pitää olennaisina ominaisuuksina torjumismenetelmiltä, jotta niistä itsessään ei muodostuisi kuormittavaa lähdettä, jota hyökkääjä voisi hyödyntää palvelunestohyökkäyksessä.

## 3.2 Entropiaan perustuva menetelmä

Palvelunestohyökkäysten torjumiseen voidaan käyttää informaatioteorian suureita (Bhuyan, Bhattacharyya ja Kalita 2015). Entropia on informaatioteorian suure, joka mittaa epäjärjestyksen määrää (Bhuyan, Bhattacharyya ja Kalita 2015). Sitä voidaan pitää myös satunnaisuuden mittana (Carl ym. 2006). Nissinen (2008) määrittelee entropian hajontalukuna, joka mittaa muuttujan hajonnan tasaisuutta eri luokkiin. Entropia on sitä suurempi, mitä tasaisemmin havainnot ovat jakautuneet eri luokkiin (Nissinen 2008).

Entropian määritteli Shannon (1948) seuraavasti:

$$H(X) = \sum_{i=1}^{n} -p_i \log p_i,$$

missä $X$ on äärellinen joukko symboleita luvusta 1 lukuun $n$, $x_1, x_2, ..., x_n$ ja $p$ on lukujen $X$ todennäköisyydet, $p_1, p_2, ..., p_n$. (Özçelik ja Brooks 2015)

Joukolle $X$ lasketun entropian lukuarvo on suurin, kun $X$ on tasaisesti jakautunut. Entropia on 0, jos jokin joukon $X$ symboleiden todennäköisyys on 1. Kaikille muille joukon $X$ jakaan-

tumille entropia vaihtelee luvun 0 ja luvun $\log n$ välillä. Entropia voidaan normalisoida siten, että arvojen vaihteluväli on lukujen 0 ja 1 välillä, seuraavasti:

$$H_N(X) = \frac{H(X)}{\log n},$$

missä $n$ on symboleiden lukumäärä joukossa $X$. (Özçelik ja Brooks 2015)

Palvelunestohyökkäysten torjumiseen entropian laskemista voidaan käyttää hyökkäyksestä aiheutuvan poikkeaman mittaamiseen (Özçelik ja Brooks 2015). Entropian voi laskea IP-pakettien otsikkotiedoille, joiden entropiat muuttuvat palvelunestohyökkäyksen aikana merkittävästi(Özçelik ja Brooks 2015). Tällöin, kuten luvussa 3.1 kerrotulle kumulatiivisen summaan perustuvalle menetelmälle, voidaan asettaa raja-arvo, jonka ylittymisen syynä voidaan epäillä palvelunestohyökkäystä (Carl ym. 2006).

Entropiaan perustuvien menetelmien katsotaan auttavan hyökkäysliikenteen erottamisessa tavallisesta verkkoliikenteestä ja vaativan vähän laskentatehoa (Bhuyan, Bhattacharyya ja Kalita 2015). Özçelik ja Brooks (2015) kuitenkin osoittivat kuinka entropiaan perustuvia menetelmiä voidaan kiertää. Uusia hyökkäysmenetelmiä voi siis syntyä tehokkaina pidettyjen torjumisemenetelmien kiertämiseen.

## 3.3 Khii toiseen -testiin perustuva menetelmä

Pearsonin khii toiseen -testiä käytetään muuttujien välisessä riippuvuuden merkitsevyyden mittaamisessa (Nissinen 2008). Palvelunestohyökkäysten torjumisessa sillä voidaan mitata IP-pakettien otsikkotietojen jakautumaa. Mitattuja otsikkotietoja voivat olla muun muassa saapuneiden IP-pakettien käytettyjen porttien numeroita, pakettien pituuksia ja lukumääriä. (Feinstein ym. 2003)

Khii toiseen -testi toimii parhaiten, kun lukuarvot ovat pieniä ja vähintään suurempia kuin viisi. Testin toimivuuden kannalta lukuarvot voidaan muuntaa osittamalla niiden lukuväli väleiksi, joihin arvot osuvat, ja käyttämällä välien järjestyslukuja testin muuttujina. Hyvin suurten vaihteluvälin muuttujille, kuten IP-osoitteet, voidaan lisäksi laskea tiivisteet (hash)

ennen ositusta. (Feinstein ym. 2003)

Feinstein ym. (2003) määrittelivät khii toiseen -testin seuraavasti:

$$\chi^2 = \sum_{i=1}^{B} \frac{(N_i - n_i)^2}{n_i},$$

missä $B$ on ositusten lukumäärä, $N_i$ pakettien lukumäärä $i$:nnessä osituksessa ja $n_i$ odotettu pakettien lukumäärä $i$:nnessä osituksessa. Laskettu arvo noudattaa khii toiseen -jakaumaa vapausasteella $B-1$, kun otoksen lukuarvot ovat odotetusta jakautumasta. (Feinstein ym. 2003)

Feinstein ym. (2003) totesivat menetelmän toimivan hyvin silloisia palvelunestohöykkäysten tekoon tarkoitettuja työkaluja vastaan. Oshima, Nakashima ja Sueyoshi (2012) ovat edelleen tutkineet khii toiseen -testin tarkkuuden parantamista laajentamalla menetelmää yhden muuttujan mittaamismenetelmästä monimuuttujamenetelmäksi. Torjumismenetelmien tulisikin siten kyetä mittaamaan useita eri muuttujia yhtäaikaisesti.

## 3.4 Kovarianssianalyysiin perustuva menetelmä

Jin ja Yeung (2004) tutkivat kovarianssianalyysin soveltuvuutta palvelunestohyökkäysten torjumismenetelmäksi. Kovarianssianalyysiä käyttäen he mittasivat tavallisen ja hyökkäysliikenteen ominaisuuksien korrelaatiota. Menetelmä kykeni tunnistamaan hyökkäyksestä aiheutuvan poikkeavuuden. Jin ja Yeung (2004) mukaan menetelmän etu muihin tilastollisiin menetelmiin verrattuna on se, että menetelmä ei ole riippuvainen normaalin verkkoliikenteen pakettien jakautumasta. Lisäksi he osoittivat menetelmän olevan laskennalliselta vaativuudeltaan lineaarinen, luokkaa $O(n)$. (Jin ja Yeung 2004)

Kovarianssi on tilastotieteen tunnusluku, joka mittaa kahden muuttujan välistä lineaarista riippuvuutta (Nissinen 2008). Kovarianssi määritellään seuraavasti:

$$S_{xy} = \frac{1}{n-1} \sum_{i=1}^{n} (x_i - \bar{x})(y_i - \bar{y}),$$

missä $\bar{x}$ ja $\bar{y}$ ovat havaintojen $x_i$ ja $y_i$ keskiarvot. (Nissinen 2008)

Jin ja Yeung (2004) käyttivät kovarianssianalyysiä TCP-protokollalla tapahtuvaan SYN-tulvahyökkäysten tunnistamiseen. SYN-tulvahyökkäyksessä saapuneiden SYN- ja FIN-pakettien lukumäärät eivät vastaa (Jin ja Yeung 2004). Käyttämällä tätä olettamusta, Jin ja Yeung (2004) laskivat kovarianssin pareittain jokaiselle kuudelle TCP-paketin otsaketietojen kontrollilipulle. Simuloidussa testissä menetelmä tunnisti SYN-tulvahyökkäykset tarkasti (Jin ja Yeung 2004).

Jin ja Yeung (2004) kuitenkin epäilivät menetelmässä käytetyn kuuden kontrollilipun riittävyyttä palvelunestohyökkäysten torjumisessa. Tutkimuksessa ei myöskään testattu sitä, miten menetelmä toimisi muiden kuin SYN-tulvahyökkäysten torjumisessa. Torjumismenetelmiltä tulisikin vaatia yleiskäyttöisyyttä.

# 4 Yhteenveto

Tässä tutkimuksessa käytiin läpi palvelunestohyökkäysten yleiset pääpiirteet ja luokiteltiin hyökkäystyypit kahteen pääluokkaan, joita olivat haavoittuvuuksia hyödyntävät hyökkäykset ja tulvahyökkäykset. Tämän jälkeen tutkimuksessa esiteltiin palvelunestohyökkäysten torjumiseen käytettyjä menetelmiä ja tunnistettiin neljä eri poikkeavuuteen perustuvaa tilastollista torjumismenetelmää.

Johtopäätöksinä neljästä eri tutkielmassa esitetystä menetelmästä voidaan sanoa, että palvelunestohyökkäysten torjumismenetelmien tulisi olla muistinkäytöltä ja laskentavaativuudelta tehokkaita, jotta torjumismenetelmistä itsessään ei muodostuisi hyökkäyskohdetta. Torjumismenetelmät ovat myös alttiita kiertämiselle. Uusia hyökkäysmenetelmiä voi syntyä kehitettyjen torjumismenetelmien kiertämiseen. Lisäksi torjumismenetelmien tulisi olla monimuuttujamenetelmiä ja yleiskäyttöisiä.

Tutkielmasta on hyötyä jatkotutkimukseen, jota voidaan tehdä kirjallisuuskatsauksen pohjalta. Esimerkkinä jatkotutkimuksesta on uusien torjumis- tai havainnointimenetelmien kehittäminen. Lisätutkimusta vaativat myös tutkielmassa esitettyjen neljän eri torjumismenetelmän tarkempi testaaminen ja vertailu.

Palvelunestohyökkäykset ovat yleinen ja ajankohtainen ongelma, johon palveluntarjoajien tulee varautua. Tilastolliset poikkeavuuteen perustuvat torjumismenetelmät ovat yleisiä tulvahyökkäysten torjumisessa. Kuitenkaan läpimurtoa torjumismenetelmien kehityksessä ei ole tehty. Uusien tehokkaiden ja yleiskäyttöisten menetelmien kehittämiselle on tarvetta.

# Lähteet


Beitollahi, Hakem, ja Geert Deconinck. 2012. “Analyzing well-known countermeasures against distributed denial of service attacks”. *Computer Communications* 35 (11): 1312–1332. ISSN: 0140-3664. http://www.sciencedirect.com/science/article/pii/S0140366412001211.

Bhuyan, Monowar H., D.K. Bhattacharyya ja J.K. Kalita. 2015. “An empirical evaluation of information metrics for low-rate and high-rate {DDoS} attack detection”. *Pattern Recognition Letters* 51:1–7. ISSN: 0167-8655. http://www.sciencedirect.com/science/article/pii/S016786551400244X.

Brenner, Bill. 2014. *UPnP Devices Used in DDoS Attacks.* Saatavilla WWW-muodossa, https://blogs.akamai.com/2014/10/upnp-devices-used-in-ddos-attacks.html, viitattu 15.3.2015.

Carl, Glenn, George Kesidis, Richard R. Brooks ja Suresh Rai. 2006. “Denial-of-Service Attack-Detection Techniques”. *IEEE Internet Computing* (Los Alamitos, CA, USA) 10 (1): 82–89. ISSN: 1089-7801. doi:http://doi.ieeecomputersociety.org/10.1109/MIC.2006.5.

Carnegie Mellon University. 1996. *Denial-of-Service Attack via ping.* Saatavilla WWW-muodossa, http://www.cert.org/historical/advisories/CA-1996-26.cfm, viitattu 5.3.2015.

Chen, Shay. 2007. *Application Denial of Service - Is it Really That Easy?* Saatavilla WWW-muodossa, https://www.owasp.org/images/d/da/OWASP_IL_7_Application_DOS.pdf, viitattu 5.3.2015.

Durcekova, V., L. Schwartz ja N. Shahmehri. 2012. “Sophisticated Denial of Service attacks aimed at application layer”. Teoksessa *ELEKTRO, 2012,* 55–60.

Feinstein, L., D. Schnackenberg, R. Balupari ja D. Kindred. 2003. “Statistical approaches to DDoS attack detection and response”. Teoksessa *DARPA Information Survivability Conference and Exposition, 2003. Proceedings,* 303–314 vol.1. Volyymi 1. doi:10.1109/DISCEX.2003.1194894.

Freiling, Felix C. 2005. “Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks”. *Computer Security ESORICS 2005.* http://link.springer.com/chapter/10.1007/11555827_19.

Freiling, FelixC, Thorsten Holz ja Georg Wicherski. 2005. “Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks”. 3679:319–335. http://dx.doi.org/10.1007/11555827_19.

Guerid, H., A. Serhrouchni, M. Achemlal ja K. Mittig. 2011. “A Novel Traceback Approach for Direct and Reflected ICMP Attacks”. Teoksessa *Network and Information Systems Security (SAR-SSI), 2011 Conference on,* 1–5. doi:10.1109/SAR-SSI.2011.5931380.

Jin, Shuyuan, ja D.S. Yeung. 2004. “A covariance analysis model for DDoS attack detection”. Teoksessa *Communications, 2004 IEEE International Conference on,* 1882–1886 Vol.4. Volyymi 4. doi:10.1109/ICC.2004.1312847.

Li, Q., E.-C. Chang ja Mun Choon Chan. 2005. “On the effectiveness of DDoS attacks on statistical filtering”. Teoksessa *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE,* 1373–1383 vol. 2. Volyymi 2. doi:10.1109/INFCOM.2005.1498362.

Mirkovic, Jelena, Sven Dietrich, David Dittrich ja Peter Reiher. 2004. *Internet Denial of Service: Attack and Defense Mechanisms (Radia Perlman Computer Networking and Security).* Upper Saddle River, NJ, USA: Prentice Hall PTR. ISBN: 0131475738.

Nissinen, Kari. 2008. *Tilastotieteen peruskurssi 1.*

Oshima, S., T. Nakashima ja T. Sueyoshi. 2012. “The Evaluation of an Anomaly Detection System Based on Chi-square Method”. Teoksessa *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on,* 708–713. doi:10.1109/WAINA.2012.166.

Ozcelik, I., Yu Fu ja R.R. Brooks. 2013. “DoS Detection is Easier Now”. Teoksessa *Research and Educational Experiment Workshop (GREE), 2013 Second GENI,* 50–55.

Paxson, Vern. 2001. “An Analysis of Using Reflectors for Distributed Denial-of-service Attacks”. *SIGCOMM Comput. Commun. Rev.* (New York, NY, USA) 31, numero 3 (): 38–47. ISSN: 0146-4833. doi:10.1145/505659.505664. http://doi.acm.org/10.1145/505659.505664.

Shannon, C. E. 1948. “A Mathematical Theory of Communication”. *SIGMOBILE Mob. Comput. Commun. Rev.* (New York, NY, USA) 5, numero 1 (): 3–55. ISSN: 1559-1662. http://doi.acm.org/10.1145/584091.584093.

Siris, V.A., ja F. Papagalou. 2004. “Application of anomaly detection algorithms for detecting SYN flooding attacks”. Teoksessa *Global Telecommunications Conference, 2004. GLOBECOM ’04. IEEE,* 2050–2054 Vol.4. Volyymi 4. doi:10.1109/GLOCOM.2004.1378372.

Tariq, Usman. 2006. “A Comprehensive Categorization of DDoS Attack and DDoS Defense Techniques”. *Advanced Data Mining and Applications.* http://link.springer.com/chapter/10.1007/11811305_112.

Viestintävirasto. 2014. *Kyberturvallisuuskeskuksen vuosikatsaus.* Saatavilla PDF-muodossa, https://www.viestintavirasto.fi/attachments/tietoturva/Kyberturvallisuusvuosikatsaus_2014.pdf.

———. 2015. *Palvelunestohyökkäys ei vaikuta verkkopalvelun sisältämiin tietoihin.* Saatavilla WWW-muodossa, https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2015/01/ttn201501051856.html, viitattu 4.3.2015.

Özçelik, İlker, ja Richard R. Brooks. 2015. “Deceiving entropy based DoS detection”. *Computers and Security* 48:234–245. ISSN: 0167-4048. http://www.sciencedirect.com/science/article/pii/S016740481400159X.