Samuli Toppi

Kone- ja syväoppiminen IoT-laitteiden DDoS-hyökkäyksissä

Tieto- ja ohjelmistotekniikan kandidaatintutkielma

29. huhtikuuta 2024

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Samuli Toppi

Yhteystiedot: samuli.e.j.toppi@student.jyu.fi

Ohjaaja: Antti-Jussi Lakanen

Työn nimi: Kone- ja syväoppiminen IoT-laitteiden DDoS-hyökkäyksissä

Title in English: Machine and deep learning in DDoS attacks on IoT devices

Työ: Kandidaatintutkielma

Sivumäärä: 30+0

Tiivistelmä: DDoS-hyökkäykset estävät käyttäjien pääsyn jaettuihin palveluihin, ja ne toteutetaan useasti hajautetun IoT-laiteverkon avulla. IoT-laitteiden tietoturva on puutteellinen, joten hyökkääjät hyödyntävät niitä DDoS-hyökkäysten toteuttamiseen. Tutkielmassa tarkastellaan kone- ja syväoppimisen käyttöä DDoS-hyökkäysten havaitsemisessa ja torjunnassa IoT-ympäristössä. Kone- ja syväoppimismenetelmiä käytetään tunkeutumisen havaitsemisjärjestelmien rakentamisessa.

Avainsanat: kandidaatintutkielmat, DoS, DDoS, IoT, koneoppiminen, syväoppiminen, kyberturvallisuus, bottiverkko, IDS

Abstract: DDoS attacks deny users access to shared services and are often carried out using a distributed network of IoT devices. The security of IoT devices is inadequate, so attackers exploit them to carry out DDoS attacks. The thesis examines the use of machine- and deep learning in detecting and mitigating DDoS attacks in an IoT environment. Machine- and deep learning methods are used to build intrusion detection systems.

Keywords: Bachelor's Theses, DoS, DDoS, IoT, machine learning, deep learning, cyber security, botnet, IDS

29. huhtikuuta 2024

Samuli Toppi

Kuviot

Kuvio 1. OSI-malli CloudFlare (2024) kuvaamana. 5
Kuvio 2. TCP-protokollan kolmisuuntainen kätteleminen. 6
Kuvio 3. DDoS-hyökkäys IoT-verkossa (Gupta ym. 2022). 9
Kuvio 4. Sumulaskentaa hyödyntävä IoT arkkitehtuuri (Roopak, Yun Tian ja Chambers 2019). 11
Kuvio 5. Koneoppimista hyödyntävän IDS-järjestelmän arkkitehtuuri (Gupta ym. 2022). . 18

Taulukot

Taulukko 1. IoT-verkon ominaisuuksia, jotka on johdettu verkon virtaustiedoista (Gupta ym. 2022). 14
Taulukko 2. Kone- ja syväoppimismallien suorituskyvyn arviointiin käytettäviä mittareita. 15
Taulukko 3. Perinteisten koneoppimismenetelmien tuloksia (Gupta ym. 2022). 16
Taulukko 4. Hybridi CNN + LSTM-syväoppimismallin tuloksia (Roopak, Tian ja Chambers 2020). 16

Sisällys

1 JOHDANTO 1

2 PALVELUNESTOHYÖKKÄYKSET 3
2.1 Hajautetut palvelunestohyökkäykset 3
2.2 DDoS-hyökkäysten tavoitteet ja hyökkäystyyppejä 4
2.3 Volyymipohjaiset DDoS-hyökkäykset 5
2.4 Protokollapohjaiset DDoS-hyökkäykset 6
2.5 Sovellustason DDoS-hyökkäykset 6

3 IOT-LAITTEET DDOS-HYÖKKÄYKSISSÄ 8

4 KONE- JA SYVÄOPPIMINEN IOT-LAITTEIDEN DDOS-HYÖKKÄYKSISSÄ 10
4.1 Pilvipalveluun ja sumulaskentaan pohjautuvat IDS-järjestelmät 10
4.2 Paikalliseen verkkoon pohjautuvat IDS-järjestelmät 11
4.3 DDoS-hyökkäysten havaitseminen 12
4.4 Mallin kouluttaminen ja käyttöönotto 13
4.4.1 Kouluttamiseen tarvittava syöttödata 13
4.4.2 Mallin kouluttaminen 14
4.4.3 Mallin suorituskyvyn arviointi 15
4.5 Mallin hyödyntäminen käytännössä 17
4.6 Kone- ja syväoppimismenetelmien hyödyt ja haasteet 18

5 JOHTOPÄÄTÖKSET 20

LÄHTEET 22

1 Johdanto

Palvelunestohyökkäyksillä (engl. denial of service, DoS) tarkoitetaan hyökkäyksiä, joilla pyritään estämään todellisten käyttäjien pääsy jaettuihin palveluihin tai resursseihin (Gligor 1984). Hajautetuilla palvelunestohyökkäyksillä (engl. distributed denial of service, DDoS) tarkoitetaan suurta joukkoa DoS-hyökkäyksiä, joita toteutetaan koordinoidusti hajautetun laiteverkon eli bottiverkon (engl. botnet) avulla. Vuonna 2020 kyberturvallisuuskeskus ilmoitti, että hajautettuja palvelunestohyökkäyksiä tapahtui Suomessa noin 10 000 kappaletta vuodessa (Kyberturvallisuuskeskus 2020). Tämän jälkeen hyökkäysten määrä on edelleen kasvanut, erityisesti sen jälkeen, kun Venäjä aloitti hyökkäyssodan Ukrainaa vastaan vuonna 2022 (Willett 2022; Kyberturvallisuuskeskus 2024). Venäläismieliset kyberaktivistit ovat olleet aktiivisia tekijöitä näissä hyökkäyksissä (Kyberturvallisuuskeskus 2024). DDoS-hyökkäykset ovat yleisiä myös globaalisti. Esimerkiksi NetScout raportoi, että vuoden 2023 ensimmäisen puoliskon aikana havaittiin 7,8 miljoonaa DDoS-hyökkäystä (NetScout 2023). Voidaan siis todeta, että DDoS-hyökkäykset muodostavat jatkuvan haasteen kyberturvallisuudelle.

DDoS-hyökkäyksille on kehitetty lukuisia erilaisia torjuntamekanismeja, kuten algoritmipohjaisia DDoS-hyökkäyksen havaitsemisjärjestelmiä ja eri tavoin toteutettuja tunkeutumisen havaitsemisjärjestelmiä (engl. intrusion detection system, IDS) (Roopak, Tian ja Chambers 2020; Salim, Rathore ja Park 2020). Kone- ja syväoppimisen alalla on tapahtunut nopeaa kehitystä, mikä on nostanut koneoppimismenetelmien suosiota käytettyinä menetelminä DDoS-hyökkäysten havaitsemiseen ja torjumiseen. Koneoppimismenetelmin voidaan automatisoida DDoS-hyökkäysten havaitsemista, sekä mahdollisesti myös torjua ennalta tuntemattomia hyökkäyksiä.

DDoS-hyökkäykset liittyvät vahvasti IoT-laitteisiin (engl. internet of things, IoT), sillä hyökkääjät käyttävät IoT-laitteita bottiverkkojen luomiseen ja toteuttavat näin DDoS-hyökkäyksiä. Bottiverkko koostuu joukosta haittaohjelmalla tartutettuja laitteita, joita kutsutaan boteiksi tai zombeiksi. Tässä tapauksessa hyökkääjä, eli niin kutsuttu bottimestari voi komentaa näitä laitteita tekemään haitallisia tehtäviä, kuten DDoS-hyökkäyksiä (Hoque, Bhattacharyya ja Kalita 2015).

Tässä kandidaatintyössä tarkastellaan mitä hyötyjä kone- ja syväoppiminen voivat tuoda DDoS-hyökkäysten havaitsemiseen ja torjumiseen IoT-ympäristössä. Tutkielma suoritetaan kirjallisuuskatsauksena. Työssä katselmoidaan erityisesti tieteellisiä artikkeleita ja konferenssijulkaisuja, jotka esittelevät uusia menetelmiä DDoS-hyökkäysten havaitsemiseen ja torjuntaan. Lisäksi aineistoon kuuluu vertailua uusien menetelmien ja aiempien lähestymistapojen välillä. Työn tavoitteena on syventää ymmärrystä DDoS-hyökkäyksistä sekä niiden torjumismekanismeista. Erityisesti keskittyen kone- ja syväoppimisen rooliin DDoS-hyökkäysten havaitsemisessa ja torjunnassa IoT-ympäristössä.

Tutkielmassa tarkastellaan aluksi DoS- ja DDoS-hyökkäyksiä, niiden eri muotoja ja vaikutuksia. Sen jälkeen keskitytään IoT-laitteiden osuuteen DDoS-hyökkäyksissä. Lopuksi syvennytään kone- ja syväoppimisen merkitykseen DDoS-hyökkäysten havaitsemisessa ja torjunnassa IoT-ympäristössä.

2 Palvelunestohyökkäykset

Palvelunestohyökkäyksellä pyritään estämään todellisten käyttäjien pääsy jaettuihin palveluihin tai resursseihin (Gligor 1984). Tutkimuksia DoS-hyökkäyksistä on tehty pitkään. Gligor (1984) tarkastelee DoS-hyökkäyksiä, jotka kohdistuvat käyttöjärjestelmätasolle. Yksi esimerkki tällaisesta hyökkäyksestä on, kun valtuutettu käyttäjä tai joukko käyttäjiä rajoittaa muiden käyttäjien pääsyä jaettuun palveluun enimmäisodotusajan ylittävän ajanjakson ajaksi. DoS-hyökkäyksiä tapahtuu myös verkkotasolla, jossa tavoitteena on aiheuttaa liiallista liikennettä, niin että todellinen liikenne estyy, katoaa tai jää kokonaan käsittelemättä ylikuormittuneen palvelimen vuoksi (Needham 1994).

Käyttöjärjestelmätasolla on mahdollista estää hyökkäyksiä paikkaamalla tunnettuja tietoturva-aukkoja, mutta verkkotasolla hyökkäyksiä on vaikeampi torjua (Peng, Leckie ja Ramamohanarao 2007). Nykyään verkkotason hyökkäykset ovat myös yleisin tapa toteuttaa DoS-hyökkäyksiä (Mirkovic ja Reiher 2004; Peng, Leckie ja Ramamohanarao 2007).

Palvelimen tietoturvamekanismit, kuten palomuurit ovat hyödyllisiä hyökkäysten estämisessä. Ne eivät silti riitä yksinään, koska haitallista verkkoliikennettä on hankala erottaa todellisesta verkkoliikenteestä. Lisäksi hyökkääjät pyrkivät matkimaan äkillisiä väkijoukkoja (Yuan, Li ja Li 2017). Näistä hyökkäyksistä aiheutuu palveluntarjoajalle haittoja, kuten asiakastyytyväisyyden laskua ja taloudellisia menetyksiä (Peng, Leckie ja Ramamohanarao 2007; Salim, Rathore ja Park 2020). Seuraavaksi siirrymme tarkastelemaan hajautettuja palvelunestohyökkäyksiä, jotka ovat edistyneempiä ja monimutkaisempia kuin perinteiset DoS-hyökkäykset.

2.1 Hajautetut palvelunestohyökkäykset

Hajautetut palvelunestohyökkäykset tai DDoS-hyökkäykset eroavat perinteisistä DoS-hyökkäyksistä. Niiden toteuttamiseen käytetään hajautettua laiteverkkoa. Tällä verkolla voidaan toteuttaa koordinoituja DoS-hyökkäyksiä yhteen tai useampaan kohteeseen (Yuan, Li ja Li 2017). Tällaista verkkoa kutsutaan bottiverkoksi.

Ensimmäinen DDoS-hyökkäys toteutettiin Minnesotan yliopistoa vastaan vuonna 1999 (Salim, Rathore ja Park 2020). Hyökkäystyyppinä käytettiin kahden päivän pituista UDP-tulvaa (engl. UDP-flood), jolla palvelimen kaistanleveys kulutettiin loppuun. UDP-tulva on kuvattu luvussa 2.3. Nykypäivänä DDoS-hyökkäykset ovat yleistyneet, sillä niiden toteuttamiseen ei tarvita enää syvällistä tietoteknistä osaamista. Internetistä löytyy laaja valikoima valmiita sovelluksia, jotka on suunniteltu toteuttamaan DDoS-hyökkäyksiä. Esimerkkinä tästä on tunnetun Mirai-bottiverkon lähdekoodin vuotaminen julkisuuteen (jgamblin 2016).

Smithin verkkojulkaisun mukaan DDoS-hyökkäysten määrä vuonna 2018 oli 7,9 miljoonaa kappaletta (Smith 2024). NetScoutin tekemän analyysin perusteella vuonna 2022 havaittiin noin 13 miljoonaa DDoS-hyökkäystä (NetScout 2022). Vuoden 2023 ensimmäisen puoliskon aikana DDoS-hyökkäyksiä havaittiin 7,8 miljoonaa kappaletta (NetScout 2023). Tämän perusteella voidaan todeta, että DDoS-hyökkäysten määrä on kasvanut jatkuvasti, mikä tekee niistä jatkuvan haasteen kyberturvallisuudelle.

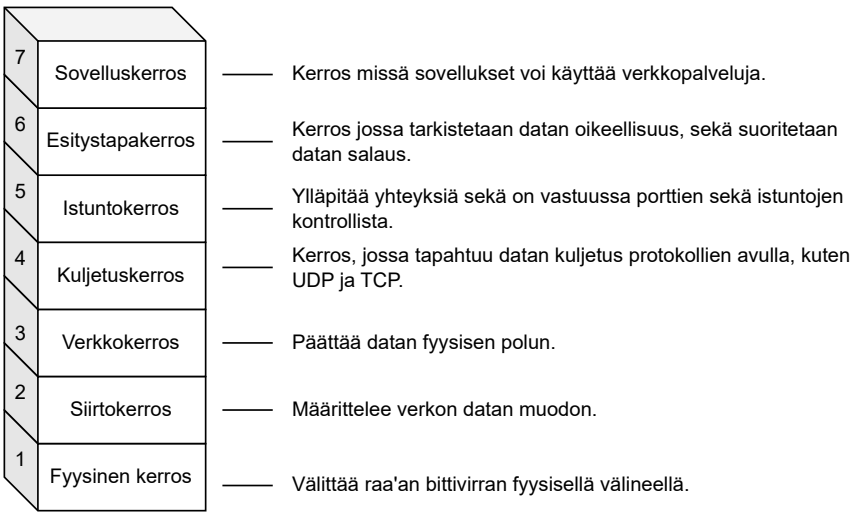
DDoS-hyökkäykset voidaan yleisesti jakaa useaa eri hyökkäysmuotoa käyttäviin hyökkäyksiin ja yhtä hyökkäysmuotoa käyttäviin hyökkäyksiin (Abrams 2018). Näitä kutsutaan monivektorihyökkäyksiksi (engl. multi-vector attack) ja yhden vektorin hyökkäyksiksi (engl. single-vector attack). Erilaisia hyökkäystyyppejä käsitellään tarkemmin seuraavassa luvussa. Kaikista vuoden 2018 toisella neljänneksellä tehdyistä DDoS-hyökkäyksistä noin 52 % oli yhden vektorin hyökkäyksiä, kun taas noin 48 % koostui monivektorihyökkäyksistä (Abrams 2018).

2.2 DDoS-hyökkäysten tavoitteet ja hyökkäystyyppejä

Ymmärtääksemme DDoS-hyökkäysten merkitystä ja vaikutuksia, on tärkeää tarkastella niiden tavoitteita ja hyökkäystyyppejä. DDoS-hyökkäysten pääasiallisena kohteena ovat järjestelmän resurssit sekä verkon kaistanleveys. DDoS-hyökkäykset vaihtelevat OSI-mallin tasoilla verkkotasolta sovellustasolle (Yuan, Li ja Li 2017). Hyökkäysten kohteina on yleensä esimerkiksi reitittimet, palomuurit tai uhrin tietokone ja verkkopalvelin (Hoque, Bhattacharyya ja Kalita 2015).

DDoS-hyökkäykset voidaan luokitella volyymipohjaisiin- ja protokollapohjaisiin hyökkäyk-

siin, sekä sovellustason hyökkäyksiin (Peng, Leckie ja Ramamohanarao 2007; Gaur ja Kumar 2022). Tällaiset hyökkäykset voidaan toteuttaa useilla eri tavoilla, jotka vaikuttavat eri OSI-mallin 1 tasoilla (Salim, Rathore ja Park 2020; Peng, Leckie ja Ramamohanarao 2007).



Kuvio 1. OSI-malli CloudFlare (2024) kuvaamana.

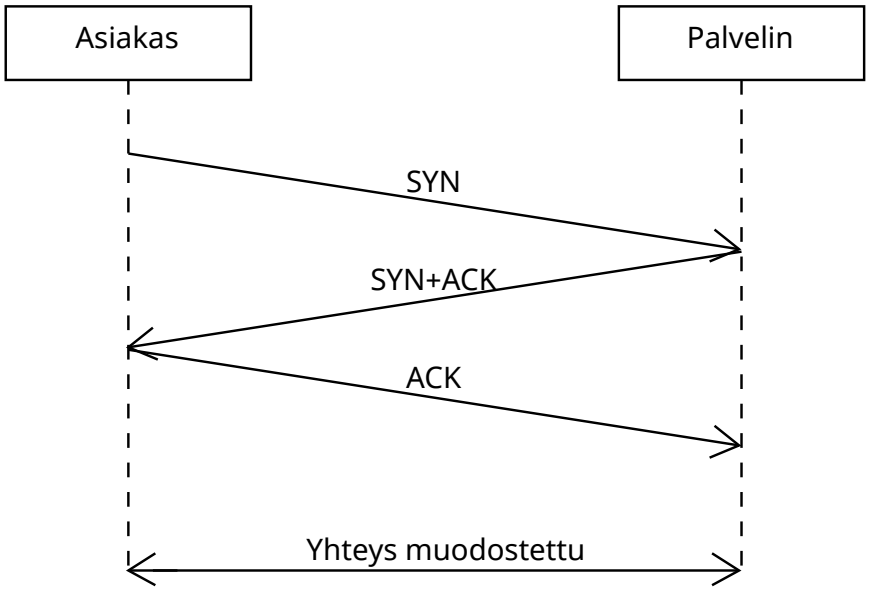
2.3 Volyymipohjaiset DDoS-hyökkäykset

Volyymipohjaiset DDoS-hyökkäykset riippuvat sisääntulevan liikenteen määrästä. UDP- ja ICMP-tulvat ovat hyviä esimerkkejä volyymipohjaisista hyökkäyksistä (Gaur ja Kumar 2022). UDP-tulvissa hyökkääjä lähettää suuria määriä väärennettyjä UDP-paketteja kohteelle. Kun kohde vastaanottaa nämä paketit, se yrittää vastata niihin ICMP-paketeilla, joihin ei tietenkään tule vastausta. Suurten pakettimäärien vastaanottaminen ja vastauksen puuttuminen saavat kohteen tietokoneen hidastumaan ja lopulta kaatumaan (Salim, Rathore ja Park 2020).

ICMP-tulvassa hyökkääjä lähettää suojaamattomalle lähetysasemalle (engl. broadcast station) useita ICMP-kaikupaketteja, jotka sisältävät uhrin tietokoneen väärennetyn lähdeosoitteen. Lähetysasema lisää kaikuviestien määrää ja lähettää ne kohteeseen, joka tulvii vastaanotetuista kaikupaketeista. Tämän seurauksena uhrin tietokone hukutetaan suurella määrällä kaikupaketteja, mikä hidastaa sen toimintaa ja lopulta tekee sen käytön mahdottomaksi (Salim, Rathore ja Park 2020). UDP- ja ICMP-tulvat vaikuttavat OSI-mallissa verkkokerrokseen (Bhuyan, Bhattacharyya ja Kalita 2015; Gaur ja Kumar 2022).

2.4 Protokollapohjaiset DDoS-hyökkäykset

Protokollapohjaiset DDoS-hyökkäykset vaikuttavat taas kuljetuskerroksella. Esimerkkinä protokollapohjaisesta DDoS-hyökkäyksestä on TCP SYN-tulva (engl. TCP SYN-flood) (Gaur ja Kumar 2022). TCP SYN-tulvassa hyökkääjä käyttää hyväksi haavoittuvuutta TCP-protokollan kolmisuuntaisessa kättelyssä 2. Hyökkääjä lähettää kohdejärjestelmälle suuren määrän väärennettyjä SYN-paketteja, joihin kohde vastaa lähettämällä SYN + ACK-vastauksen. Normaalisti asiakasohjelmisto lähettäisi tämän jälkeen vielä viimeisen ACK-paketin yhteyden vahvistamiseksi, mutta hyökkääjä jättää tämän paketin lähettämättä. Seurauksena kohteen muistipino täyttyy näistä vahvistamattomista yhteyksistä, jonka seurauksena kohteen palvelin ei pysty muodostamaan uusia yhteyksiä (Peng, Leckie ja Ramamohanarao 2007). Protokollapohjaiset DDoS-hyökkäykset, kuten TCP SYN-tulva, kohdistuvat enemmän OSI-mallin kuljetuskerrokseen (Gaur ja Kumar 2022).



Kuvio 2. TCP-protokollan kolmisuuntainen kätteleminen.

2.5 Sovellustason DDoS-hyökkäykset

Sovellustason DDoS-hyökkäykset hidastavat palvelinta lähettämällä suuria määriä väärennettyjä HTTP GET-pyyntöjä palvelimelle. Palvelin käsittelee näitä vahvistettuina pyyntöi-

nä ja vastaa kaikkiin pyyntöihin HTTP:n POST metodia käyttäen. Tämän seurauksena palvelimen resurssit loppuvat, mikä lopulta kaataa palvelimen (Gaur ja Kumar 2022). HTTP GET-hyökkäys on yksi tapa toteuttaa HTTP-tulvahyökkäyksiä (engl. HTTP-flood) (Salim, Rathore ja Park 2020).

DDoS-hyökkäyksiä voidaan toteuttaa useilla eri tavoilla, jotka vaikuttavat eri OSI-mallin tasoilla. Koska hyökkäykset vaikuttavat eri tasoilla, jokainen hyökkäystyyppi vaatii erilaisia torjuntamekanismeja (Salim, Rathore ja Park 2020). Tilannetta monimutkaistaa entisestään se, että hyökkääjät toteuttavat aiemmin mainittuja monivektorihyökkäyksiä, joissa käytetään samanaikaisesti useita eri hyökkäystyyppejä.

Volyymipohjaiset hyökkäykset pyrkivät ylikuormittamaan verkon kaistanleveyttä, kun taas protokollapohjaiset hyökkäykset hyödyntävät heikkouksia verkkoprotokollissa ja kuormittavat palvelinta. Sovellustason hyökkäyksillä pyritään hidastamaan ja kaatamaan kohteena oleva palvelin.

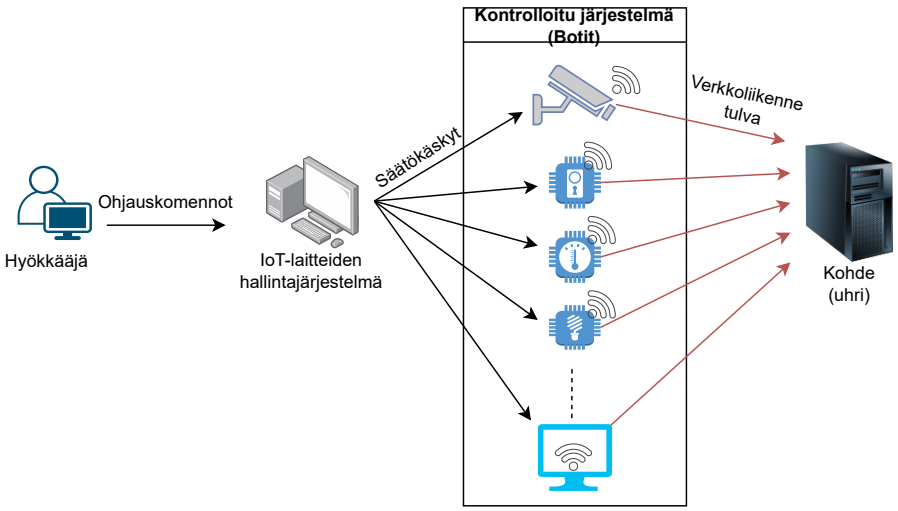
3 IoT-laitteet DDoS-hyökkäyksissä

Asioiden internet eli IoT käsittää laitteet, jotka kykenevät havainnoimaan, oppimaan ja reagoimaan ympäröivään ympäristöönsä verkkoprotokollien avulla (Gupta ym. 2022).
IoT-laitteita on monia erilaisia, kuten esimerkiksi termostaatteja, valvontakameroita ja sydänmonitorilaitteita. IoT-laitteita on alettu käyttämään myös laajemmassa skaalassa, kuten älykaupungeissa tai älykkäissä sähköverkoissa (De La Torre Parra ym. 2020; Risteska Stojkoska ja Trivodaliev 2017). IoT-verkot yleisesti koostuvat radiotaajuustunnisteista (engl. radio-frequency identification, RFID) ja langattomista sensoriverkoista (engl. wireless sensor network, WSN) (Risteska Stojkoska ja Trivodaliev 2017). IoT-laitteilla pyritään parantamaan ja auttamaan ihmisten arkipäiväistä- ja ammatillista elämää, sekä yhteiskuntaa (Xiao ym. 2018).

IoT-laitteet ovat alttiita lukuisille haavoittuvuuksille, kuten heikoille salasanoille ja päivittämättömille ohjelmistoille. IoT-laitteet ovat myös usein pienikokoisia ja niiden laskentateho on rajallinen, minkä vuoksi niiden tietoturvaominaisuudet ovat puutteellisia (Salim, Rathore ja Park 2020; Soe, Santosa ja Hartanto 2019). Tämän vuoksi on syytä kehittää menetelmiä, jotka ovat keveitä, mutta tehokkaita. Lisäksi tietoturvaominaisuuksia voidaan ulkoistaa laitteen ulkopuolisiin järjestelmiin. IoT-laitteet ylläpitävät jatkuvaa yhteyttä Internettiin, mikä tekee niistä helpon kohteen hyökkääjille (Salim, Rathore ja Park 2020). Tämän vuoksi hyökkääjälle on helppoa kaapata IoT-laitteita kontrolliinsa ja käyttää niitä DDoS-hyökkäyksissä.

Kuten aikaisemmin luvussa 2.1 mainittiin, IoT-laitteita voi käyttää DDoS-hyökkäyksiin bottiverkkojen avulla. Hyökkääjän saadessa lukuisia botteja kontrolliinsa, niistä muodostuu verkko, joita hyökkääjä voi käyttää koordinoitujen ja monipuolisten DDoS-hyökkäysten toteuttamiseen. Tämän perusteella on tarpeellista kehittää mekanismeja, joilla voidaan puolustautua IoT-laitteiden DDoS-hyökkäyksiä vastaan. Kuviossa 3 on esitetty DDoS-hyökkäys IoT-verkossa.

Salim, Rathore ja Park (2020) käsittelevät laajalti tunnettua Mirai-bottiverkkoa. Vuonna 2016 Mirai-bottiverkon avulla suoritettiin merkittävä DDoS-hyökkäys, jonka aikana haitallisen verkkoliikenteen määrä nousi jopa 1,1 terabittiin sekunnissa. Tämä hyökkäys toteutettiin



Kuvio 3. DDoS-hyökkäys IoT-verkossa (Gupta ym. 2022).

käyttämällä 148,000 IoT-laitetta, kuten valvontakameroita ja reitittimiä. Kyseinen hyökkäys kohdistui Dyn-nimiseen yritykseen, joka tarjoaa DNS-palveluita. Hyökkäyksen seurauksena useat suuret internet-sivustot, kuten GitHub, Netflix ja Reddit olivat saavuttamattomissa useiden tuntien ajan. Myöhemmin Mirai-haittaohjelman lähdekoodi vuosi julkisuuteen, minkä jälkeen Mirai-bottiverkkoa on hyödynnetty useissa erilaisissa hyökkäyksissä.

On tärkeää huomioida, että on olemassa muitakin haittaohjelmia, joita voidaan käyttää bottiverkkojen rakentamiseen (Hoque, Bhattacharyya ja Kalita 2015). Ongelmana on, että näihin haitallisiin ohjelmiin on usein helppo päästä käsiksi ja niitä voidaan käyttää hyökkäysten toteuttamiseen ilman suurta tietoteknistä osaamista. Positiivisena puolena tässä tilanteessa on se, että tutkijat ja kyberturvallisuuden asiantuntijat voivat hyödyntää näitä haittaohjelmia torjuntamekanismien kehittämisen välineinä.

IoT-laitteiden määrä on kasvanut jatkuvasti, ja niiden määrän odotetaan kasvavan edelleen tulevaisuudessa. Ericsson ennusti vuonna 2023 että yhdistettyjen IoT-laitteiden määrä saavuttaisi 15,7 miljardia vuoden 2023 loppuun mennessä. Tämä ennustettu määrä tulisi nousemaan 38,9 miljardiin laitteeseen vuoteen 2029 mennessä (Ericsson 2023). IoT-laitteet ovat keskeinen osa DDoS-hyökkäyksiä, sillä hyökkääjät käyttävät niitä välineenä hyökkäyksiensä toteuttamiseen.

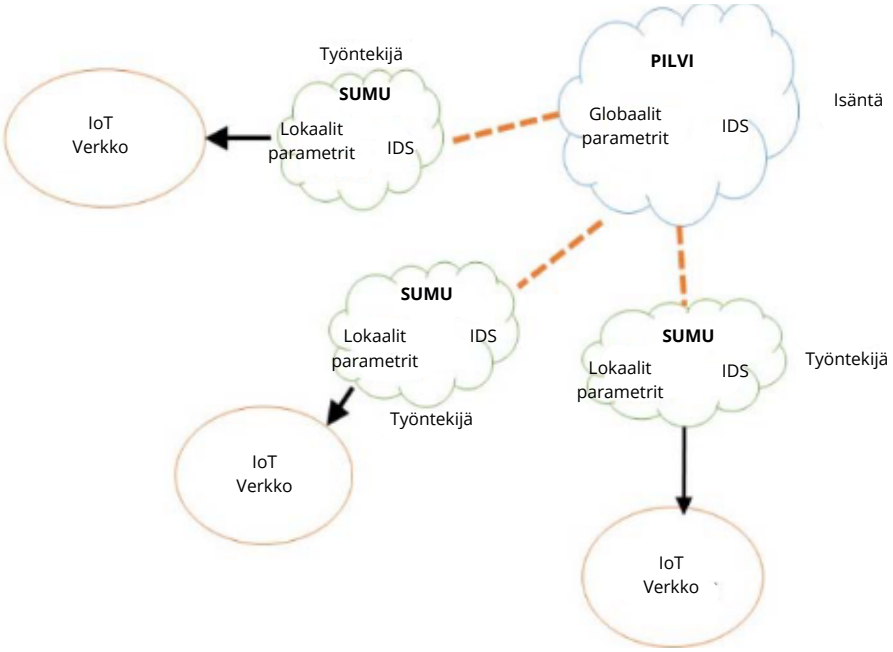
4 Kone- ja syväoppiminen IoT-laitteiden DDoS-hyökkäyksissä

Kone- ja syväoppimista voidaan hyödyntää DDoS-hyökkäysten havaitsemisessa ja torjumisessa luomalla tunkeutumisen havaitsemisjärjestelmiä. Lyhyesti näistä käytetään myös nimitystä IDS-järjestelmä.

Tässä kandidaatintyössä katselmoidaan kone- ja syväoppimismenetelmien avulla kehitettyjä IDS-järjestelmiä, joilla voidaan seurata IoT-laitteiden käyttäytymistä sekä niiden tuottamaa verkkoliikennettä. Tavoitteena on tunnistaa haitalliset ja normaalit verkkoliikennemallit. Tämän perusteella voidaan havaita laitteet, jotka saattavat olla osallisina kyberhyökkäyksessä, ja hyökkäysliikenne voidaan suodattaa pois (Gupta ym. 2022). Järjestelmä voi myös antaa hälytyksen ja luoda raportin, jotta verkon haltija voi tehdä halutut suojaustoimenpiteet (Labiod, Amara Korba ja Ghoualmi 2022). Tällaisia IDS-järjestelmiä voidaan rakentaa lokaaliin verkkoon tai pilvipalvelun yhteyteen.

4.1 Pilvipalveluun ja sumulaskentaan pohjautuvat IDS-järjestelmät

Pilvipalvelun yhteydessä IoT-laitteet hyödyntävät niin kutsuttua sumulaskentaa (engl. fog computing), jossa laskentaa ja ohjausta voidaan suorittaa verkon reunoissa, lähempänä IoT-laitteita (Roopak, Yun Tian ja Chambers 2019; Diro ja Chilamkurti 2018; Salim, Rathore ja Park 2020). Tästä on se hyöty, että ottaen huomioon IoT-laitteiden rajallinen laskentateho ja muisti, laskenta ja laitteen käytöksen seuranta voidaan suorittaa ulkoisessa IDS-järjestelmässä, joka sijaitsee lähellä itse IoT-laitetta. IDS-järjestelmä otetaan käyttöön verkon solmussa, jonka alla sijaitsevat tarkasteltavat IoT-laitteet 4.



Kuvio 4. Sumulaskentaa hyödyntävä IoT arkkitehtuuri (Roopak, Yun Tian ja Chambers 2019).

4.2 Paikalliseen verkkoon pohjautuvat IDS-järjestelmät

Paikalliseen verkkoon pohjautuva IDS-järjestelmä voidaan toteuttaa esimerkiksi paikallisessa reitittimessä (Gupta ym. 2022). DDoS-hyökkäyksen havaitseminen paikallisessa verkossa tuo sen edun, että haitallinen verkkoliikenne voidaan suodattaa pois ennen sen siirtymistä julkiseen verkkoon. Perusperiaatteeltaan kummatkin menetelmät toimivat samalla tavalla, mutta pilvipalveluun ja sumulaskentaan pohjautuvaa IDS-järjestelmää voidaan hyödyntää paljon laajemmalla skaalalla, kuten yhtiön tai kaupungin IoT-verkossa.

Yleisesti DDoS-hyökkäysten torjumisessa koneoppimisen avulla on kaksi vaihetta, jotka ovat havaitsemis- ja torjumisvaihe (Gupta ym. 2022). Havaitsemisvaiheessa IDS-järjestelmä analysoi verkkoliikennettä ja tunnistaa haitallisen verkkoliikenteen. Vastaavasti torjumisvaiheessa IDS-järjestelmä suodattaa haitallisen verkkoliikenteen ja estää sen pääsyn verkkoon.

4.3 DDoS-hyökkäysten havaitseminen

Kun halutaan havaita IoT-laitteilta lähteviä DDoS-hyökkäyksiä, on oleellista tunnistaa IoT-laitteen haitallinen, tai epäilyttävä käytös. Keskeiset vaiheet havainnoinnissa sisältävät verkkoliikenteen muodostamisen ja keräämisen, sekä attribuuttien valinnan ja luokittelun (Gupta ym. 2022).

Tunkeutumisen havaitseminen perustuu yleensä allekirjoituspohjaiseen havaitsemiseen (engl. signature based) tai poikkeavuuksien havaitsemiseen (engl. anomaly based). Allekirjoituspohjainen tunkeutumisen havaitseminen perustuu aiemmin tunnistettuihin hyökkäysmalleihin, kun taas poikkeamiin perustuva tunkeutumisen havaitseminen perustuu poikkeamien tunnistamiseen normaalista käyttäytymisestä (Diro ja Chilamkurti 2018).

IoT-laitteet keskustelevat vain vakioidun lukumäärän yhteyspisteiden kanssa, sekä laitteiden ei pitäisi muodostaa uusia yhteyksiä. Laitteen käyttäytymistä voidaan seurata esimerkiksi tarkkailemalla laitteen muodostamia yhteyksiä ja niiden määrää. Tämän lisäksi voidaan myös tarkkailla laitteen verkkoliikennettä, kuten lähetetyn datan määrää, sekä pakettien kokoa, jotta voidaan havaita poikkeamia normaalista käyttäytymisestä. Tämän perusteella voidaan valita ominaisuuksia, joista koostetaan syöttödata koneoppimismallin kouluttamiseen. Gupta ym. (2022) jakavat ominaisuudet kahteen eri luokkaan, jotka ovat virtauksesta riippuvat ja virtauksesta riippumattomat ominaisuudet. Virtauksesta riippuvat ominaisuudet ovat ominaisuuksia, jotka riippuvat IoT-laitteen verkkoliikennevirrasta, kuten laitteen käyttämä kaistanleveys. Virtauksesta riippumattomat ominaisuudet taas eivät riipu verkkoliikennevirrasta, kuten paketin koko tai paketissa käytetty protokolla.

Koneoppimismalli tarvitsee kerättyä ja jäsenneltyä verkkoliikennettä tunnistaakseen IoT-laitteen haitallisen käytöksen. Kerätystä verkkoliikenteestä luodaan syöttödata mallin kouluttamista varten. Havaitsemista helpottaa se, että IoT-laitteiden käytös on hyvin vakioitunut ja muutokset laitteen käyttäytymisessä voidaan havaita helposti.

4.4 Mallin kouluttaminen ja käyttöönotto

Seuraavaksi käsitellään mallin kouluttamisen ja käyttöönoton vaiheita. Ensin tarkastellaan mallin kouluttamiseen tarvittavaa syöttödataa. Sen jälkeen tarkastellaan itse koulutusprosessia, joka sisältää datan jakamisen koulutus- ja testidataan sekä mallin kouluttamisen. Lopuksi käsitellään mallin käyttöönottoa ja sen toiminnan arviointia käytännön sovelluksissa.

4.4.1 Kouluttamiseen tarvittava syöttödata

Mallin kouluttamiseen tarvitaan syöttödataa, joka koostuu verkkoliikenteestä johdetuista attribuuteista. Attribuutit tulee valita huolella, jotta malli pystyy erottamaan haitallisen ja normaalin verkkoliikenteen. Syöttödata voidaan tuottaa itse ja jäsentää se haluttuun muotoon. Vaihtoehtoisesti voidaan käyttää valmiita verkkoliikennetiedostoja (Brunswick 2017, 2012). Verkkoliikennetiedostot sisältävät valmiiksi jäsennettyä ja luokiteltua DDoS-hyökkäysdataa, joka muistuttaa reaalimaailman verkkoliikennettä. Verkkoliikenne on kerätty simuloimalla erilaisia DDoS-hyökkäyksiä.

Tiettyjen datasarjojen tapauksessa havaintojen määrä eri luokissa ei välttämättä ole tasapainossa. Tällöin saattaa olla tarpeen muokata datasarjaa niin, että eri luokkien havaintomäärät tulevat tasapuolisemmiksi (Roopak, Tian ja Chambers 2020). Kun syöttödata on saatu valmiiksi, data yleensä jaetaan kahteen osaan: koulutusdataan ja testidataan. Koulutusdata yleensä sisältää suurimman osan datasta, ja sitä käytetään mallin kouluttamiseen. Testidataa käytetään testaamaan koulutetun mallin tehokkuutta ja yleistettävyyttä. Taulukossa 1 on esimerkkejä syöttödatasta johdetuista attribuuteista. Syöttödata kerättiin simuloimalla yleisiä DDoS-hyökkäyksiä, kuten SYN-, UDP- ja HTTP-tulvia (Gupta ym. 2022).

Taulukko 1. IoT-verkon ominaisuuksia, jotka on johdettu verkon virtaustiedoista (Gupta ym. 2022).

Ominaisuuden kategoria	Ominaisuus	Kuvaus
Virtauksesta riippuva (Tilallinen)	DIP	Kohteen IP-osoite
	SIP	Lähteen IP-osoite
	S_Port	Lähteen porttinumero
	D_Port	Kohteen porttinumero
	BW	Kaistanleveys
	DIP_Count	Kunkin laitteen kiinteiden kohteiden määrä
	New_DIP	Istunnon aikana lähestyttyjen uusien kohteiden määrä
	SIP_AvgTCP	TCP protokollan keskimääräinen siirtonopeus SIP:tä kohti
	SIP_AvgUDP	UDP protokollan keskimääräinen siirtonopeus SIP:tä kohti
	SIP_AvgHTTP	HTTP protokollan keskimääräinen siirtonopeus SIP:tä kohti
	Pkt_Size	Paketin koko
	β	Pakettien välinen aikaero
	$\frac{d\beta}{dt}$ $\frac{d^2\beta}{dt^2}$	1. ja 2. derivaatta, jotta saadaan selville verkkoliikenteen purskeisuus
Virtauksesta riippumaton (Tilaton)	Is_TCP	Paketin hyödyntämä protokolla
	Is_UDP	
	Is_HTTP	
	Is_ICMP	
	Is_Other	
	Pkt_TCP	Toimitettujen TCP pakettien määrä
	Pkt_UDP	Toimitettujen UDP pakettien määrä
	Pkt_HTTP	Toimitettujen HTTP pakettien määrä
	Pkt_ICMP	Toimitettujen ICMP pakettien määrä
	Pkt_Other	Toimitettujen pakettien määrä muille protokollille

4.4.2 Mallin kouluttaminen

Kun syöttödata on valmiina, siirrytään mallin kouluttamiseen. Tähän vaiheeseen voidaan valita erilaisia kone- tai syväoppimismenetelmiä. Esimerkkejä perinteisistä koneoppimisen luokittelijoista ovat tukivektorikone (engl. support vector machine, SVM), lähimmän naapurin algoritmi (engl. k-nearest neighbors, k-NN) ja satunnaismetsä (engl. random forest, RF). Toisaalta voidaan hyödyntää myös syväoppimismenetelmiä, kuten monikerroksisia perseptroniverkkoja (engl. multilayer perceptron, MLP), konvoluutioneuroverkkoja (engl. convolutional neural network, CNN) ja pitkä- ja lyhytaikaiseen muistiin perustuvia verkkoja (engl. long short-term memory, LSTM). Voidaan myös käyttää näiden yhdistelmää, kuten CNN +

LSTM (Roopak, Yun Tian ja Chambers 2019). Mallin kouluttamisessa täytyy myös muistaa perusteellinen testaus, että saadaan valittua sopiva malli, jolla varmistetaan mallin tehokkuus ja yleistettävyys. Mallin testaus voidaan suorittaa tekemällä ennusteita testidatalla ja havainnoimalla kykeneekö malli tekemään oikeita ennusteita. Testidata voi sisältää esimerkiksi 10–30 % koko datasarjasta. Testidatan jakaminen riippuu käytetystä menetelmästä ja koulutusdatasta. Roopak, Tian ja Chambers (2020) jakoivat opetus- ja testidatan suhteessa 90:10.

4.4.3 Mallin suorituskyvyn arviointi

Kone- ja syväoppimismallien suorituskykyä arvioidaan testidatan avulla, käyttäen erilaisia mittareita, kuten tarkkuutta, herkkyyttä ja F1-arvoa. Näitä mittareita käytetään mallin suorituskyvyn ymmärtämiseen eri näkökulmista. Kuvattujen mittareiden kaavat on esitetty taulukossa 2.

Kaava	**Kuvaus**
$Tarkkuus = \frac{OP+ON}{OP+ON+VN+VP}$	Tarkkuus kuvaa kuinka suuren osan havainnoista malli luokitteli oikein.
$Herkkyys = \frac{OP}{OP+VN}$	Herkkyys kuvaa kuinka usein malli tunnistaa oikein todelliset positiiviset tapaukset kaikista datasarjan todellisista positiivisista näytteistä.
$F1 = \frac{2 \cdot Tarkkuus \cdot Herkkyys}{Tarkkuus+Herkkyys}$	F1-arvo on tarkkuuden ja herkkyyden harmoninen keskiarvo.

Taulukko 2. Kone- ja syväoppimismallien suorituskyvyn arviointiin käytettäviä mittareita.

.

Alla esitetään taulukon 2 kaavojen lyhenteiden selitykset:

- Oikea positiivinen (OP) tarkoittaa, että malli ennusti positiivisen tapauksen oikein.
- Oikea negatiivinen (ON) tarkoittaa, että malli ennusti negatiivisen tapauksen oikein.
- Väärä negatiivinen (VN) tarkoittaa, että malli ennusti negatiivisen tapauksen positiiviseksi.
- Väärä positiivinen (VP) tarkoittaa, että malli ennusti positiivisen tapauksen negatiivi-

seksi.

Gupta ym. (2022) kehittivät paikalliseen verkkoon pohjautuvan IDS-järjestelmän käyttämällä ohjattua koneoppimista. Kyseiseen IDS-järjestelmään koulutettiin erilaisia malleja perinteisillä koneoppimisen luokittelumenetelmillä. Tuloksia ja käytettyjä koneoppimismenetelmiä on listattu taulukossa 3. Tutkimuksessa käytetty datasarja koostui 241,289 paketista, joista 31,233 pakettia sisälsivät normaalia verkkoliikennettä ja loput sisälsivät haitallista verkkoliikennettä. Virhemäärä on myös tärkeä mittari, joka havainnollistaa kuinka usein malli tekee virheellisiä luokitteluja. Gupta ym. (2022) mittasivat virhemäärää laskemalla väärien positiivisten (engl. false positive rate, FPR) ja väärien negatiivisten (engl. false negative rate, FNR) havaintojen määrää. Väärien positiivisten määrä on merkitty taulukkoon 3 lyhenteellä VPM ja väärien negatiivisten määrä on merkitty lyhenteellä VNM.

Taulukko 3. Perinteisten koneoppimismenetelmien tuloksia (Gupta ym. 2022).

Luokitin	Tarkkuus	Herkkyys	F1-arvo	VPM	VNM
RF	99,2 %	98,9 %	97,8 %	0,08 %	1,1 %
k-NN	98,6 %	95,4 %	96,1 %	0,7 %	4,6 %
SVM	98,1 %	97,8 %	94,9 %	1,9 %	2,2 %

Roopak, Tian ja Chambers (2020) puolestaan kehittivät IDS-järjestelmän hyödyntäen syväoppimista. Heidän tutkimuksessaan käytettiin aiemmin mainittuja CNN- ja LSTM-menetelmiä. Tuloksia heidän tutkimuksesta on esitelty taulukossa 4. Heidän tutkimuksensa datasarja koostui 225,742 tapauksesta, mikä tasapainotettiin sisältämään 39 % DDoS-hyökkäysdataa ja 61 % normaalia verkkoliikennettä. Virhemäärää ei ilmoitettu. Kehitetty IDS-järjestelmä on suunniteltu toimimaan pilvipalvelussa, jossa se voi havaita IoT-laitteiden DDoS-hyökkäyksiä.

Taulukko 4. Hybridi CNN + LSTM-syväoppimismallin tuloksia (Roopak, Tian ja Chambers 2020).

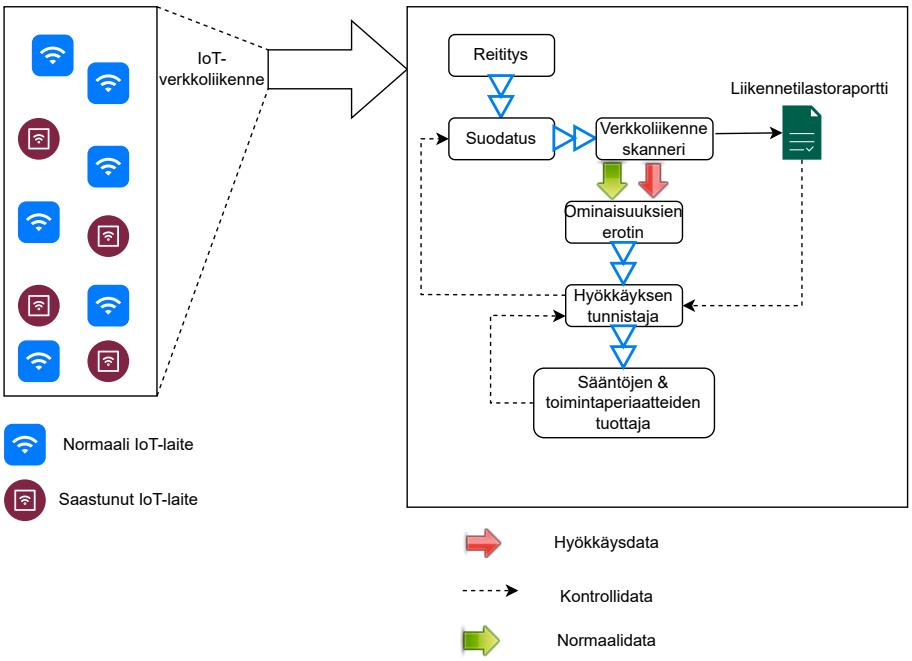
Syväoppimismalli	Tarkkuus	Herkkyys	F1-arvo
CNN + LSTM	99,03 %	99,35 %	99,36 %

4.5 Mallin hyödyntäminen käytännössä

Koulutetun mallin avulla voidaan torjua IoT-laitteiden DDoS-hyökkäyksiä integroimalla se IDS-järjestelmään. Tämä järjestelmä voi toimia sumuverkon solmuissa tai lokaalissa verkossa kuten aikaisemmin mainittiin. Kuviossa 5 esitetään Gupta ym. (2022) toteuttaman IDS-järjestelmän korkean tason arkkitehtuuri. Järjestelmä arvioi samaan verkkoon yhdistettyjen IoT-laitteiden käytöstä tarkkailemalla näiden laitteiden verkkoliikennettä. Seuraavaksi esitellään paikallisessa reitittimessä toimivan IDS-järjestelmän toimintalogiikka. Hyökkäyksen havaitseminen tapahtuu siinä vaiheessa, kun hyökkäysliikenne on lähdössä lähiverkosta uhria kohti.

Ensiksi IoT-laitteiden verkkoliikenne reititetään suodattimen läpi. Suodatinta koulutetaan jatkuvasti ominaisuuksien erottelijan antaman syötteen avulla. Kun hyökkäys tunnistetaan, suodatin pudottaa hyökkäysliikenteeksi arvioidut paketit ominaisuuksien erottelijan antamien tietojen perusteella. Suodattimen jälkeen, verkkoliikenne etenee verkkoskanneriin, joka kerää liikenteestä tietoja, kuten lähteen ja kohteen IP-osoitteet, paketin koon ja liikennevirran määrän. Skanneri myös esikäsittelee kerätyt tiedot hyökkäysten havaitsemiseen käytettävän mallin vaatimuksiin. Lisäksi se välittää saapuvan liikenteen ominaisuuksien erottelijalle, joka valitsee hyökkäysten havaitsemiseen tarvittavat ominaisuudet.

Ominaisuuksien erottelijan luomaa informaatiota käytetään eri koneoppimismallien kouluttamiseen ja hyökkäysten tunnistamiseen. Seuraavaksi verkkoliikenne kulkeutuu hyökkäyksen tunnistimen läpi, jonka tehtävänä on ennustaa, käyttäytyvätkö IoT-laitteet haitallisesti vai eivät. Se tehdään erottamalla hyökkäysliikenne normaalista liikenteestä luokittelijoiden avulla. Hyökkäyksen tunnistamisen jälkeen luodaan raportti, joka sisältää tietoja hyökkäystilastoista, kuten käytetystä protokollasta ja mahdollisista tavoista puolustautua hyökkäystä vastaan. Lisäksi raporttiin sisällytetään myös merkittävien ominaisuuksien tiedot, ja ne toimitetaan ominaisuuksien erottelijalle, joka poimii olennaisimmat piirteet luokittelijoiden havaitsemistarkkuuden parantamiseksi, ja niitä käytetään myös suodatusprosessissa (Gupta ym. 2022).



Kuvio 5. Koneoppimista hyödyntävän IDS-järjestelmän arkkitehtuuri (Gupta ym. 2022).

4.6 Kone- ja syväoppimismenetelmien hyödyt ja haasteet

Kone- ja syväoppimismenetelmillä saadaan tehokkaasti havaittua ja torjuttua DDoS-hyökkäyksiä IoT-ympäristössä. Perinteisten koneoppimismallien käytössä on haasteita. Yksi niistä on tarve laajalle verkkoasiantuntemukselle ja kokeiluille, jotta osataan valita oikeat tilastolliset menetelmät ja ominaisuudet. Lisäksi perinteiset koneoppimismallit voivat olla rajoittuneita tunnistamaan lukuisia DDoS-hyökkäysvektoreita (Yuan, Li ja Li 2017; Mirkovic ja Reiher 2004). Lisäksi jos mallilla halutaan tunnistaa uusia hyökkäyksiä, se vaatii mallin uudelleen kouluttamisen (Mirkovic ja Reiher 2004).

Syväoppimismalleilla saavutetaan lisäetuja perinteisiin koneoppimismalleihin verrattuna. Näihin etuihin kuuluu kyky mukautua uuteen dataan, mikä tarkoittaa, että mallin tehokkuus ei ole riippuvainen syöttödatasta (Yuan, Li ja Li 2017). Tämän lisäksi syväoppimismallit pystyvät löytämään piileviä rakenteita datasta, joten mallit pystyvät helpommin tunnistamaan myös uusia ja tuntemattomia hyökkäyksiä.

Jotta syväoppimismallit ovat tarpeeksi tehokkaita, niiden kouluttamiseen tarvitaan paljon da-

taa. Tämä on yksi ongelma syväoppimismalleissa, koska datamäärän kasvaessa myös mallin kouluttamiseen kuluva aika kasvaa. Roopak, Tian ja Chambers (2020) hakevat ratkaisua tähän ongelmaan. He syöttävät normalisoidun koulutusdatan ei-dominoivan lajittelualgoritmin läpi (engl. non-dominated sorting algorithm, NSGA), joka on monitavoitteellinen optimointialgoritmi, jonka avulla voidaan pienentää datan ulottuvuuksia (Kumar ja Guria 2017). Lisäksi he käyttävät mallina CNN + LSTM-yhdistelmää, jotta he saavat hyödyt alueellisen (engl. spatial) ja ajallisen (engl. temporal) datan analysoinnista. LSTM-mallin avulla saadaan myös se hyöty, että mallia pystyy käyttämään suoraan raakaan dataan, eikä tarvitse toteuttaa ominaisuuksien erottelua (Roopak, Yun Tian ja Chambers 2019). LSTM-malli pystyy myös tallettamaan tietoa kuin tietokoneen muisti ja pystyy lukemaan ja kirjoittamaan tietoa solmuissa (Roopak, Tian ja Chambers 2020). Näiden avulla he saavat koulutusajan pienennettyä 11 kertaa pienemmäksi kuin muissa syväoppimismenetelmissä.

On otettava huomioon, että eri menetelmät ovat tuottaneet eri tuloksia eri datasarjoilla, joten on tärkeää valita oikea menetelmä oikeaan käyttötarkoitukseen. Esimerkiksi Roopakin, Tianin ja Chambersin (2020) julkaisussa MLP-mallin tarkkuus oli vain 88,74 %, kun taas Gaurin ja Kumarin (2022) julkaisemassa analyysissä mainitut kaksi tutkimusta olivat saaneet parhaimmat tulokset hyödyntäen MLP-mallia eri datasarjoilla (Wang, Lu ja Qin 2020; Alkasassbeh ym. 2016).

5 Johtopäätökset

Tässä kandidaatintutkielmassa käsiteltiin DoS- ja DDoS-hyökkäyksiä, niiden kohteita ja tavoitteita. Lisäksi tarkasteltiin erilaisia DDoS-hyökkäysten toteuttamistapoja, sekä IoT-laitteiden roolia näissä hyökkäyksissä. Lopuksi pohdittiin kone- ja syväoppimismenetelmien tuomia hyötyjä DDoS-hyökkäysten havaitsemiseen ja torjuntaan IoT-ympäristössä.

IoT-laitteet mahdollistavat DDoS-hyökkäysten toteuttamisen, koska nämä laitteet ovat usein huonosti suojattuja, mikä mahdollistaa helpon haltuunoton hyökkääjälle. Hyökkääjä voi luoda vaarantuneista IoT-laitteista bottiverkon, jonka avulla voidaan toteuttaa koordinoituja DDoS-hyökkäyksiä yhteen tai useampaan kohteeseen. IoT-laitteiden yleistyessä DDoS-hyökkäykset ovat jatkuvassa kasvussa, ja ne ovat nykyään yksi suurimmista kyberuhkista. Tästä syystä on tärkeää kehittää uusia menetelmiä DDoS-hyökkäysten havaitsemiseen ja torjumiseen IoT-ympäristössä.

Kone- ja syväoppimismenetelmät ovat tehokkaita DDoS-hyökkäysten havaitsemis- ja torjuntatyökaluja. IoT-laitteiden vakioitunut käytös mahdollistaa sen, että kone- ja syväoppimismenetelmät pystyvät tunnistamaan helposti poikkeavuuksia normaalista IoT-laitteen käyttäytymisestä. Näin ollen voidaan kehittää kone- ja syväoppimismenetelmiä hyödyntäviä IDS-järjestelmiä, jotka havaitsevat ja torjuvat DDoS-hyökkäyksiä IoT-ympäristössä. Oikein koulutettu malli tunnistaa haitallisen verkkoliikenteen ja se voidaan suodattaa pois ennen sen leviämistä verkkoon. Tämän lisäksi syväoppimismallit kykenevät oppimaan uusia hyökkäysmalleja ja tunnistamaan tuntemattomia hyökkäyksiä.

Vaikka syväoppimismenetelmät tuottavat parempia tuloksia kuin perinteiset koneoppimismenetelmät, ne vaativat enemmän dataa ja laskentatehoa. Siksi on tärkeää valita oikea menetelmä kunkin käyttötarkoituksen mukaan. Lisäksi syväoppimismalleja voidaan yleistää paremmin, joten ne eivät ole riippuvaisia opetusdatasta, ja ne pystyvät mukautumaan uuteen dataan.

Tutkielmassa katselmoidut artikkelit tarjosivat simuloituja tuloksia eri kone- ja syväoppimismenetelmien tehokkuudesta DDoS-hyökkäysten havaitsemisessa ja torjumisessa. Tulevaisuuden tutkimuksissa olisi kiinnostavaa arvioida näiden menetelmien suorituskykyä to-

dellisissa IoT-ympäristöissä. Erityisesti olisi hyödyllistä tutkia niiden kykyä tunnistaa uusia ja tuntemattomia hyökkäyksiä. Lisäksi olisi olennaista arvioida näiden menetelmien suorituskykyä suurissa IoT-verkoissa, kuten yritysten tai kaupunkien verkoissa. Näissä verkoissa on runsaasti verkkoliikennettä ja kohtaamme myös odottamatonta verkkoliikennettä ihmisten toimesta. Koska käytetyt datasarjat katselmoiduissa artikkeleissa ovat vanhoja, uudet tutkimukset uusilla datasarjoilla ovat tärkeitä jatkotutkimuksen kannalta.

Lähteet

Abrams, Bleeping Computer - Lawrence. 2018. “Dramatic Increase of DDoS Attack Sizes Attributed to IoT Devices”. Viitattu 5. maaliskuuta 2024. https://www.bleepingcomputer.com/news/security/dramatic-increase-of-ddos-attack-sizes-attributed-to-iot-devices/.

Alkasassbeh, Mouhammd, Ghazi Al-Naymat, Ahmad B. A. Hassanat ja Mohammad Almseidin. 2016. “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques”. Number: 1 Publisher: The Science and Information (SAI) Organization Limited, *International Journal of Advanced Computer Science and Applications (ijacsa)* 7, numero 1 (1. kesäkuuta 2016). ISSN: 2156-5570, viitattu 11. maaliskuuta 2024. https://doi.org/10.14569/IJACSA.2016.070159.

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. tammikuuta 2015): 1–7. ISSN: 0167-8655, viitattu 26. helmikuuta 2024. https://doi.org/10.1016/j.patrec.2014.07.019.

Brunswick, University Of New. 2012. “Intrusion detection evaluation dataset (ISCXIDS2012)”. Viitattu 7. maaliskuuta 2024. https://www.unb.ca/cic/datasets/ids.html.

———. 2017. “Intrusion detection evaluation dataset (CIC-IDS2017)”. Viitattu 7. maaliskuuta 2024. https://www.unb.ca/cic/datasets/ids-2017.html.

CloudFlare. 2024. “What is the OSI Model?” Viitattu 7. maaliskuuta 2024. https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/.

De La Torre Parra, Gonzalo, Paul Rad, Kim-Kwang Raymond Choo ja Nicole Beebe. 2020. “Detecting Internet of Things attacks using distributed deep learning”. *Journal of Network and Computer Applications* 163 (1. elokuuta 2020): 102662. ISSN: 1084-8045, viitattu 21. helmikuuta 2024. https://doi.org/10.1016/j.jnca.2020.102662.

Diro, A.A., ja N. Chilamkurti. 2018. “Distributed attack detection scheme using deep learning approach for Internet of Things”. *Future Generation Computer Systems* 82:761–768. ISSN: 0167-739X. https://doi.org/10.1016/j.future.2017.08.043.

Ericsson. 2023. “IoT connections outlook”. Viitattu 11. maaliskuuta 2024. https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook.

Gaur, V., ja R. Kumar. 2022. “Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices”. *Arabian Journal for Science and Engineering* 47 (2): 1353–1374. ISSN: 2193-567X. https://doi.org/10.1007/s13369-021-05947-3.

Gligor, V.D. 1984. “A Note on Denial-of-Service in Operating Systems”. *IEEE Transactions on Software Engineering* SE-10 (3): 320–324. ISSN: 0098-5589. https://doi.org/10.1109/TSE.1984.5010241.

Gupta, B.B., P. Chaudhary, X. Chang ja N. Nedjah. 2022. “Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers”. *Computers and Electrical Engineering* 98. ISSN: 0045-7906. https://doi.org/10.1016/j.compeleceng.2022.107726.

Hoque, N., D.K. Bhattacharyya ja J.K. Kalita. 2015. “Botnet in DDoS Attacks: Trends and Challenges”. *IEEE Communications Surveys and Tutorials* 17 (4): 2242–2270. ISSN: 1553-877X. https://doi.org/10.1109/COMST.2015.2457491.

jgamblin, Github -. 2016. “Mirai-Source-Code”. Viitattu 28. helmikuuta 2024. https://github.com/jgamblin/Mirai-Source-Code.

Kumar, Mithilesh, ja Chandan Guria. 2017. “The elitist non-dominated sorting genetic algorithm with inheritance (i-NSGA-II) and its jumping gene adaptations for multi-objective optimization”. *Information Sciences* 382-383 (1. maaliskuuta 2017): 15–37. ISSN: 0020-0255, viitattu 9. maaliskuuta 2024. https://doi.org/10.1016/j.ins.2016.12.003.

Kyberturvallisuuskeskus. 2020. “Palvelunestohyökkäykset ovat arkipäivää Suomessa”. Viitattu 27. helmikuuta 2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa.

———. 2024. “Palvelunestohyökkäykset jatkuvat myös vuonna 2024”. Viitattu 27. helmikuuta 2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-jatkuvat-myos-vuonna-2024.

Labiod, Y., A. Amara Korba ja N. Ghoualmi. 2022. “Fog Computing-Based Intrusion Detection Architecture to Protect IoT Networks”. *Wireless Personal Communications* 125 (1): 231–259. ISSN: 0929-6212. https://doi.org/10.1007/s11277-022-09548-7.

Mirkovic, Jelena, ja Peter Reiher. 2004. “A taxonomy of DDoS attack and DDoS defense mechanisms”. *ACM SIGCOMM Computer Communication Review* 34, numero 2 (1. huhtikuuta 2004): 39–53. ISSN: 0146-4833, viitattu 12. maaliskuuta 2024. https://doi.org/10.1145/997150.997156.

Needham, Roger M. 1994. “Denial of service: an example”. *Communications of the ACM* 37, numero 11 (1. marraskuuta 1994): 42–46. ISSN: 0001-0782, viitattu 13. helmikuuta 2024. https://doi.org/10.1145/188280.188294.

NetScout. 2022. “Netscout DDoS Threat Intelligence Report / 5th anniversary edition”. Viitattu 7. maaliskuuta 2024. https://www.netscout.com/threatreport/2h2022/ddos-threat-intelligence-report/.

———. 2023. “Netscout DDoS Threat Intelligence Report / Findings from 1st half of 2023”. Viitattu 7. maaliskuuta 2024. https://www.netscout.com/threatreport/global-highlights/.

Peng, Tao, Christopher Leckie ja Kotagiri Ramamohanarao. 2007. “Survey of network-based defense mechanisms countering the DoS and DDoS problems”. *ACM Computing Surveys* 39, numero 1 (12. huhtikuuta 2007): 3–es. ISSN: 0360-0300, viitattu 13. helmikuuta 2024. https://doi.org/10.1145/1216370.1216373.

Risteska Stojkoska, B.L., ja K.V. Trivodaliev. 2017. “A review of Internet of Things for smart home: Challenges and solutions”. *Journal of Cleaner Production* 140:1454–1464. ISSN: 0959-6526. https://doi.org/10.1016/j.jclepro.2016.10.006.

Roopak, Monika, Gui Yun Tian ja Jonathon Chambers. 2020. “An Intrusion Detection System Against DDoS Attacks in IoT Networks”. Teoksessa *2020 10th Annual Computing and Communication Workshop and Conference (CCWC),* 0562–0567. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). Tammikuu. Viitattu 6. helmikuuta 2024. https://doi.org/10.1109/CCWC47524.2020.9031206.

Roopak, Monika, Gui Yun Tian ja Jonathon Chambers. 2019. “Deep Learning Models for Cyber Security in IoT Networks”. Teoksessa *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC),* 0452–0457. 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). Tammikuu. Viitattu 6. helmikuuta 2024. https://doi.org/10.1109/CCWC.2019.8666588.

Salim, Mikail Mohammed, Shailendra Rathore ja Jong Hyuk Park. 2020. “Distributed denial of service attacks and its defenses in IoT: a survey”. *The Journal of Supercomputing* 76, numero 7 (1. heinäkuuta 2020): 5320–5363. ISSN: 1573-0484, viitattu 23. tammikuuta 2024. https://doi.org/10.1007/s11227-019-02945-z.

Smith, StationX - Gary. 2024. “DDoS Statistics: How Large a Threat Are DDoS Attacks? (2024)”. Viitattu 5. maaliskuuta 2024. https://stationx.net/ddos-statistics/.

Soe, Yan Naung, Paulus Insap Santosa ja Rudy Hartanto. 2019. “DDoS Attack Detection Based on Simple ANN with SMOTE for IoT Environment”. Teoksessa *2019 Fourth International Conference on Informatics and Computing (ICIC),* 1–5. 2019 Fourth International Conference on Informatics and Computing (ICIC). Lokakuu. Viitattu 6. helmikuuta 2024. https://doi.org/10.1109/ICIC47613.2019.8985853.

Wang, Meng, Yiqin Lu ja Jiancheng Qin. 2020. “A dynamic MLP-based DDoS attack detection method using feature selection and feedback”. *Computers & Security* 88 (1. tammikuuta 2020): 101645. ISSN: 0167-4048, viitattu 11. maaliskuuta 2024. https://doi.org/10.1016/j.cose.2019.101645.

Willett, M. 2022. “The Cyber Dimension of the Russia–Ukraine War”. *Survival* 64 (5): 7–26. ISSN: 0039-6338. https://doi.org/10.1080/00396338.2022.2126193.

Xiao, L., X. Wan, X. Lu, Y. Zhang ja D. Wu. 2018. “IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?” *IEEE Signal Processing Magazine* 35 (5): 41–49. ISSN: 1053-5888. https://doi.org/10.1109/MSP.2018.2825478.

Yuan, Xiaoyong, Chuanhuang Li ja Xiaolin Li. 2017. “DeepDefense: Identifying DDoS Attack via Deep Learning”. Teoksessa *2017 IEEE International Conference on Smart Computing (SMARTCOMP),* 1–8. 2017 IEEE International Conference on Smart Computing (SMARTCOMP). Toukokuu. Viitattu 14. helmikuuta 2024. https://doi.org/10.1109/SMARTCOMP.2017.7946998.