Tampereen yliopisto

Elias Ihalainen

IP-TUNNELOINTI

Kandidaatintyö
Informaatioteknologian ja viestinnän tiedekunta (ITC)
Tarkastaja: Lehtori Juha Vihervaara
Joulukuu 2023

TIIVISTELMÄ

Elias Ihalainen: IP-tunnelointi
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaattiohjelma
Joulukuu 2023

Internetin kehittyessä ja sen käyttäjämäärän kasvaessa siltä vaaditaan joustavuutta ja turvallisuutta. IP-tunnelointi on monipuolinen teknologia internetin verkkokerroksella, jonka sovelluksia voidaan käyttää tuomaan verkkoihin joustavuutta ja suojaa hyökkäyksiä vastaan. Verkkokerroksella tietoa välitetään datagrammeina, jotka koostuvat IP-otsikoista ja ylempien kerroksien datasta. Datagrammeja välitetään verkkolaitteiden kautta internetverkon läpi IP-otsikossa sijaitsevan IP-osoitteen perusteella.

Verkkoon voidaan luoda IP-tunneleita kahden laitteen välillä siten, että tunnelin lähtöpiste enkapsuloi datagrammit ja tunnelin päätepiste purkaa enkapsuloinnin. Enkapsulointi toteutetaan yksinkertaisimmillaan asettamalla alkuperäisen IP-otsikon eteen uusi IP-otsikko. Tämän jälkeen datagrammi reititetään uuden IP-otsikon osoitteen mukaan ja alkuperäistä otsikkoa käsitellään osana datakenttää tunnelin päätepisteiden välissä. Yleisimpiä tunnelointimenetelmiä ovat IP-in-IP, minimaalinen enkapsulointi ja GRE. Niiden toteutukset ja sovelluskohteet eroavat toisistaan, mutta ne kaikki noudattavat aiempaa tunneloinnin määritelmää.

Mobile IP on tekniikka, jonka tarkoituksena on säästää verkon resursseja ja tarjota käyttäjille sujuvampia liikkuvuuden palveluja. Mobile IP:n avulla käyttäjälle määritetään kotiverkko, johon verkon muut käyttäjät osaavat reitittää sille tarkoitetut datagrammit. Käyttäjän poistuessa kotiverkostaan vierasverkkoon, sille määritetään väliaikainen IP-osoite vierasverkon osoiteavaruudesta. Kotiverkossa oleva, määrätty verkkolaite toteuttaa tunnelin internetin läpi vierasverkkoon ja siten verkon muut laitteet voivat lähettää datagrammit käyttäjän alkuperäiseen IP-osoitteeseen, vaikka käyttäjä olisi liikkeellä. Mobile IP -tekniikkaa sovelletaan esimerkiksi WLAN- ja IoT-verkoissa.

VPN-teknologia mahdollistaa yksityisten, suojattujen verkkojen luomisen julkisen internetin resursseja hyödyntäen. VPN-verkkoja voidaan toteuttaa eri tekniikoilla, jotka hyödyntävät internetin eri kerroksia. Tässä työssä käsitellään VPN-teknologiaa, joka on toteutettu IPsec:illä. IPsec toimii verkkokerroksella ja hyödyntää tunnelointia ja datan salausalgoritmeja.

TuCP on protokolla, jota käytetään vähentämään tunneloinnin ylimääräistä tiedonsiirtoa kompressoimalla tunneloinnissa käyttämättömiä otsikoita. TuCP-protokollaa voidaan soveltaa useisiin eri tunnelointimenetelmiin. GTP on langattomissa mobiiliverkoissa käytössä oleva protokolla, joka hyödyntää tunnelointia reitittääkseen dataa internetverkosta mobiililaitteiden hyödyntämään radioverkkoon. GTP toimii mobiiliverkkojen runkoverkoissa, jotka toimivat datan välittäjinä radioverkon antenneista internetin pakettikytkentäiseen verkkoon.

Avainsanat: IP-protokolla, IP-tunnelointi, Mobile IP, VPN, GTP

ABSTRACT

Elias Ihalainen: IP tunneling
Bachelor’s thesis
Tampere University
Bachelor’s degree in Computing and Electrical Engineering
December 2023

As the internet evolves and its user base grows, flexibility and security become essential. IP tunneling is a versatile technology at the internet network layer, and its applications can provide flexibility and protection against attacks. At the network layer, information is transmitted as datagrams, consisting of IP headers and higher layer data. Datagrams are forwarded through network devices across the internet based on the IP address in the IP header.

IP tunnels can be established between two network devices, where the tunnel's starting point encapsulates datagrams, and the tunnel's endpoint decapsulates them. The simplest form of encapsulation is adding a new IP header in front of the original IP header. Subsequently, the datagram is routed based on the address in the new IP header, and the original header is processed as part of the data field between the tunnel's endpoints. Common tunneling methods include IP-in-IP, minimal encapsulation, and GRE. While their implementations and applications differ, they all follow to the general definition of tunneling.

Mobile IP is a technology designed to conserve network resources and provide users with smoother mobility services. Mobile IP assigns a home network to the user. Other networks users route the user’s data into this home network. When the user moves from their home network to a foreign network, a temporary IP address is assigned from the foreign network's address space. A specified network device in the home network establishes a tunnel through the internet to the foreign network, enabling other network devices to send datagrams to the user's original IP address, even when the user is on the move. Mobile IP technology is applied in, for example WLAN and IoT networks.

VPN technology enables the creation of private, secure networks using the resources of the public internet. VPN networks can be implemented using various techniques that leverage different layers of the internet. This thesis discusses VPN technology implemented with IPsec, which operates at the network layer and utilizes tunneling techniques and data encryption algorithms.

TuCP is a protocol used to reduce unnecessary data transfer in tunneling by compressing unused headers. TuCP can be applied to various tunneling methods. GTP is a protocol used in wireless mobile networks, taking advantage of tunneling to route data from the internet to the radio network utilized by mobile devices. GTP operates in the core networks of mobile networks, serving as intermediaries for data transmission from the radio network's antennas to the internet's packet-switched network.

Keywords: IP protocol, IP tunneling, Mobile IP, VPN, GTP

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

3GPP	3rd Generation Partnership Project
AS	Autonomous System
CCoA	Colocated Care of Address
CoA	Care of Address
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
GGRE	Generic Routing Encapsulation
GGNS	Gateway GNS
GNS	GPRS Support Node
GRE	Generic Routing Encapsulation
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IRDP	ICMP Router Discovery Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IOT	Internet Of Things
IP	Internet Protocol
IPsec	IP security
ISP	Internet Service Provider
LTE	Long-Term Evolution
NR	New Radio
QoS	Quality of Service
RFC	Request For Comment
RRP	Registration Reply
RRQ	Registration Request
SA	Security Association
SGNS	Serving GNS

TCP	Transmission Control Protocol
TuCP	Tunneling Header Compression Protocol
TTL	Time To Live
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

1. JOHDANTO

Verkkoteknologian kehitys on muuttanut tapaa, jolla tieto liikkuu verkossa, ja tässä murroksessa on noussut tarve joustaville tietoturvallisuuden palveluille. IP-tunnelointi tarjoaa internetin käyttäjille tiedon turvallisen siirron eri verkoissa ja yhteyksissä, tarjoten samalla joustavuutta ja tehokkuutta verkkoliikenteen hallintaan.

IP-tunneloinnin kehittäminen on aloitettu jo internetin alkuvaiheissa, ja se pysyy keskeisenä teknologiana vielä tänäkin päivänä. Se voi näennäisestä yksinkertaisuudestaan huolimatta tarjota erittäin kehittyneitä palveluja mahdollistamaan turvallisen ja tehokkaan tietoliikenteen eri verkkojen välillä. Sen sovelluskohteita löytyy niin verkkotekniikasta ja tietoturvasta, kuin myös langattomien mobiiliverkkojen teknologioista.

Tässä kirjallisuuskatsauksessa esitellään IP-tunnelointiteknologian erilaisia toteutuksia ja yleisessä käytössä olevia sovelluskohteita. Työssä hyödynnetään aiheesta kirjoitettua kirjallisuutta, tutkimusjulkaisuja ja teknologioiden määrittelydokumentteja ja standardeja. Työn tavoitteena on tutustuttaa lukija IP-tunneloinnin perusteisiin ja tarjota kattava katsaus myös sen sovelluskohteisiin ja turvallisuusnäkökohtiin.

Aiheen käsittely aloitetaan perusasioista. Luvussa 2 käsitellään internetin protokollakerrokset ja IP-otsikko. Lukija saa pohjustuksen niistä tekniikoista, joiden päälle IP-tunnelointi rakentuu. Yksinkertaisimmillaan IP-tunnelointi tarkoittaa uuden IP-otsikon asettamista IP-paketin oman otsikon eteen. Luvussa 3 esitellään IP-tunneloinnin yleisessä käytössä olevia tekniikoita: IP-in-IP, minimaalinen enkapsulointi ja GRE. Lisäksi luvussa tuodaan esiin myös tietoturvaa tunneloinnin näkökulmasta.

Teknologian esittelyn jälkeen työssä käsitellään IP-tunneloinnin sovelluskohteita. Luvussa 4 esitellään Mobile IP-tekniikka, joka mahdollistaa käyttäjän liikkumisen verkoissa ilman IP-osoitteen vaihtumista. Luvussa 5 käsitellään VPN-teknologiaa, joka on myös monella yksityisellä kuluttajalla käytössä oleva tietoturvapalvelu. Lopuksi luvussa 6 käydään läpi kaksi muuta IP-tunneloinnin sovellusta: TuCP ja GTP. TuCP tehostaa tunneloinnin tiedonsiirtoa tarjoamalla otsikon kompressoinnin palveluja. GTP on langattomissa mobiiliverkoissa käytössä oleva tunnelointitekniikka.

2. VERKKOKERROS JA IP-PROTOKOLLA

2.1 Protokollapino

Internetiä käsitellessä keskeinen termi on protokollapino. Protokollapino kuvaa verkkoa kerrosmaisena rakenteena, jossa eri verkon toimintoja käsitellään eri tasoilla, kukin täydentäen edellistä. Kurose ja Ross (2009) pyrkivät kuvaamaan internetin kerrosmaista rakennetta käyttämällä vertausta lentoliikenteeseen. Lentoliikenteessä päätepisteinä ovat lentokentät. Lentokentällä matkustaja ensin ostaa lipun, luovuttaa matkatavarat, nousee lentokoneeseen, joka viimein lähtee lentoon. Lentokone lentää tiettyä reittiä kohdekentälle, jossa edelliset toimenpiteet toteutetaan vastakkaisessa järjestyksessä. [1]

2.1.1 Motivaatio kerrosmaiseen ajatteluun

Kun jokaisen toimenpiteen ajatellaan toteutuvan yhdessä kerroksessa, saadaan hyvä käsitys siitä, mitä tarkoitetaan verkon kerrosmaisella rakenteella. Vasta, kun matkustaja on hankkinut matkalipun, hän voi luovuttaa matkatavaransa ja vasta matkatavaransa luovutettuaan, hän voi nousta koneeseen. [1]

Samoin verkossa kulkeva viesti tarvitsee alemmilta kerroksilta saatavat palvelut, jotta sille voidaan tarjota palveluita seuraavalta kerrokselta. Kukin kerros kommunikoi vain toisessa päädyssä olevan saman kerroksen kanssa. Muiden kerrosten viestintä on sille käytännössä merkityksetöntä bittivirtaa. Kerrosmainen rakenne helpottaa verkon jakamista osiin ja siten mahdollistaa sen käsittelemisen ja päivittämisen pienemmissä osissa. [1]

2.1.2 Viisi protokollakerrosta

Internetin protokollapino koostuu viidestä kerroksesta: fyysisestä kerroksesta, siirtoyhteyskerroksesta, verkkokerroksesta, kuljetuskerroksesta ja sovelluskerroksesta. Yksinkertaisesti ajateltuna kerroksien voidaan ajatella kulkevan alhaalta ylös tässä järjestyksessä alkaen fyysisestä kerroksesta. Fyysisellä kerroksella määritetään, miten yksittäiset bitit liikkuvat käytettävässä tiedonsiirtokanavassa. Esimerkiksi tiedonsiirtokanavan vaihtuessa kuparijohdosta valokaapeliin, fyysisen kerroksen protokollat määrittävät, millaista signaalia käytetään bittivirran siirtämiseen. Siirtoyhteyskerroksella lisätään palveluja liittyen verkon eri linkkien välillä. Viestien siirtyminen tällä kerroksella käsitellään pisteestä pisteeseen. Esimerkkejä siirtoyhteyskerroksen protokollista ovat Ethernet- ja WiFi-protokollat. [1]

Verkkokerroksella käsitellään viestien reitittämistä isommalla mittakaavalla. Löytääkseen tiensä monimutkaisen verkon läpi viestit tarvitsevat reitin, ja verkkokerroksen protokollat tarjoavat tämän palvelun. Tätä palvelua voidaan verrata esimerkiksi fyysisen postin lähettämiseen tarvittavien osoitteiden antamiseen. Verkkokerroksella sijaitsee IP-protokolla, joka on internetverkossa kaikista tärkein verkkokerroksen protokolla, ja se on myös tämän työn kannalta oleellisin protokolla. [1]

Kuljetuskerros tarjoaa tiedonsiirtoon tärkeitä luotettavuuteen vaikuttavia protokollia. Tällä tasolla valitulla protokollalla on suuri vaikutus tiedonsiirron tehokkuuteen ja virheettömyyteen. Riippuen ylemmän kerroksen tarpeista, käyttäjä voi karkeasti haluta kuljetuskerrokselta nopeaa, mutta ei-luotettavaa tiedonsiirtoa (esim. UDP-protokolla), tai luotettavaa, mutta hitaampaa tiedonsiirtoa (esim. TCP-protokolla). Sovelluskerroksella esiintyy paljon vaihtelevia protokollia, ja niiden valinta on aina sovelluskohtaista. Esimerkkinä sovelluskerroksen protokollasta on HTTP-protokolla, jota käytetään hakemaan tiedostoja verkosta. Tämän kerroksen käyttökohteet ovat laajoja ja protokollia käytetään pääasiassa tiettyä tarkoitusta varten. [1]

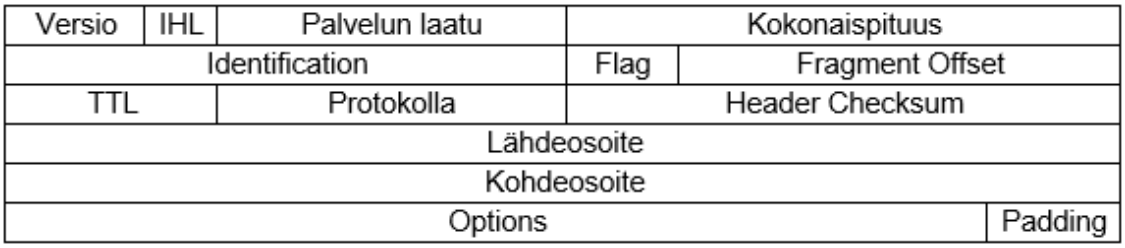
Protokollapino mahdollistaa internetin jakamisen osiin, joita voidaan käsitellä erikseen. Siten yhdellä kerroksella tehdyt valinnat eivät välttämättä määritä koko tiedonsiirron prosessia. Protokollien kerrostaminen ei kuitenkaan ole täydellinen tapa määrittää verkkoja, ja tällaisessa rakenteessa on haittapuoliakin. Eri kerroksien protokollat voivat esimerkiksi tarjota samoja palveluja liittyen esimerkiksi luotettavuuteen ja virheettömyyteen, mikä ei ole tehokasta. Koska kerrokset ovat käytännössä sokeita toistensa käyttämään informaatioon, protokollat eivät voi hyödyntää toisella kerroksella saatavana olevaa informaatiota, vaikka se olisi tälle protokollalle hyödyllistä. [1]

2.2 IP-otsikko

Verkkokerroksen IP-protokollan tarjoama palvelu on pakettien reitittäminen lähteeltä kohteelle osoitteiden perusteella. IP-protokollassa paketteja kutsutaan datagrammeiksi ja osoitteita IP-lähde- ja IP-kohdeosoitteiksi. IP-protokollassa on laajassa käytössä kaksi versiota: IPv4 ja IPv6, joista jälkimmäinen on uudempi, joka on syrjäyttämässä aikaisempaa. Tällä hetkellä protokollan versioita käytetään rinnakkain, ja Googlen ylläpitämän tilaston mukaan lokakuussa 2023 noin 40–45 % käyttäjistään käyttää IPv6-protokollaa. [2]

IP-paketti eli datagrammi koostuu otsikkokentästä ja datakentästä. IP-protokollalle olennaista informaatiota sijaitsee vain otsikkokentässä. Otsikkokenttä eroaa protokollan

version mukaan. Tarkastellaan ensin IPv4-otsikkoa, joka määritellään RFC-dokumentissa 791 ja esitellään kuvassa 1.



Kuva 1: *IPv4-paketin otsikkokenttä*

Otsikon eri kentät lyhyesti:

- Versio (4 bittiä): Protokollan versio, tässä tapauksessa 4.
- IHL (4 bittiä): Otsikkokentän pituus, eli kuinka monta 32:n bitin sanaa datakentän alkuun.
- Palvelun laatu (8 bittiä): Tätä kenttää voidaan käyttää määrittämään datagrammin reitittämiseen käytettäviä parametrejä, kuten viive ja luotettavuus.
- Kokonaispituus (16 bittiä): Koko datagrammin pituus 8:n bitin oktetteina mitattuna.
- Identification (16 bittiä): Tunnistusarvo, jota käytetään kokoamaan fragmentoitu datagrammi.
- Flag (3 bittiä): Käytetään määrittämään datagrammin fragmentoitumista.
- Fragment offset (13 bittiä): Kertoo missä kohtaa datagrammia tämä palanen sijaitsee, mikäli datagrammi on fragmentoitunut.
- TTL (8 bittiä): Aika, mitattuna hyppyjen määränä, jonka loputtua datagrammi tuhotaan.
- Protokolla (8 bittiä): Kertoo käytetyn ylemmän kerroksen protokollan datakentässä.
- Header Checksum (16 bittiä): Käytetään havaitsemaan bittivirheitä datagrammissa.

- Lähde- ja kohdeosoite (molemmat 16 bittiä): IPv4-osoitteet, joiden perusteella datagrammi reititetään.
- Options (Vaihteleva määrä bittejä): Käytetään määrittämään lisäasetuksia datagrammille, tätä kenttää ei välttämättä esiinny jokaisessa datagrammissa.
- Padding (Vaihteleva määrä bittejä): Käytetään varmistamaan, että otsikkokenttä pysyy oikean mittaisena, eli on jaollinen 32:lla bitillä.

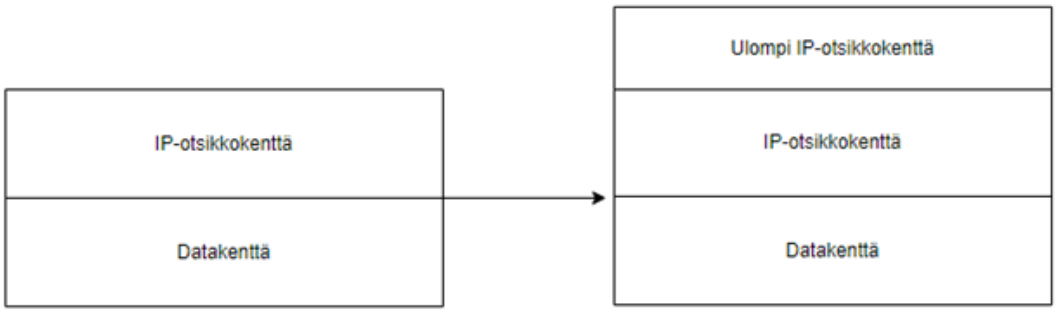
[3]

3. IP-TUNNELOINTITEKNOLOGIAT

IP-tunneloinnilla tarkoitetaan tekniikkaa, jossa IP-paketti kuljetetaan toisen IP-paketin sisällä. Lähetettävän datagrammin päälle luodaan tai muokataan uusi IP-otsikkokenttä, jossa on omat lähde- ja kohdeosoitteensa. Nämä osoitteet kuuluvat niin sanotun tunnelin päätepisteissä sijaiseville gateway-reitittimille. Tunnelointitekniikkaa voidaan käyttää monipuolisesti verkkojen yhteensovittamiseen, tietoturvan parantamiseen ja mobiiliverkkojen toteuttamiseen. Tässä osiossa esitellään IP-tunneloinnin eri teknologioita. [4]

3.1 IP-in-IP

Yksi IP-tunneloinnin toteuttamiseen käytetyistä tekniikoista on IP-in-IP-enkapsulointi. Tässä tekniikassa datagrammin eteen asetetaan uusi IP-otsikko. Tunnelin alkupisteessä datagrammia ei muuteta, pois lukien TTL-arvon laskemista yhdellä. Tunnelissa alkuperäinen datagrammi pysyy muuttumattomana ja reitittäminen tapahtuu ulomman otsikkokentän perusteella. Saavutettuaan ulomman IP-otsikon kohdeosoitteen ulompi otsikko hylätään ja alkuperäinen datagrammi reititetään alkuperäisten osoitteiden mukaan, mikäli tarpeellista. [5]. Kuvassa 2 esitetään miten alkuperäinen datagrammi asetetaan tunnelointipakettiin. Alkuperäisestä datagrammista muodostuu uuden datagrammin datakenttä.



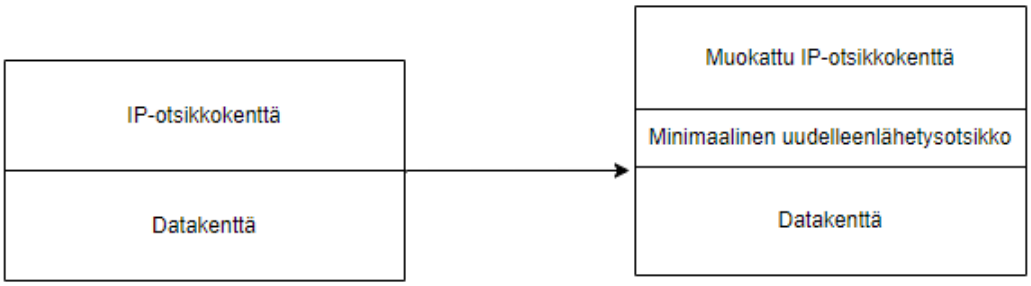
Kuva 2: *Datagrammi tunnelin sisällä*

IP-in-IP-tunnelointia hyödynnetään esimerkiksi IPv4- ja IPv6-verkkojen yhteensovittamisessa. Koska IPv4-reitittimet eivät pysty tulkitsemaan IPv6 otsikoita, IPv6-datagrammin päälle asetetaan IPv4-otsikko, jolloin IPv6-datagrammi pystytään reitittämään niiden verkon osien läpi, joissa ei ole IPv6-reitittimiä. [6]

3.2 Minimaalinen enkapsulointi

Toinen IP-tunnelointimenetelmä on RFC 2004:ssä määritelty minimaalinen enkapsulointi (engl. Minimal Encapsulation). Minimaalinen enkapsulointi vaatii vähemmän ylimääräistä tiedonsiirtoa kuin IP-in-IP-enkapsulointi, koska uuden IP-otsikon luomisen sijaan, alkuperäistä otsikkoa muokataan. Tunnelin alkupisteessä IP-otsikon lähde- ja kohdeosoitteet vaihdetaan tunnelin alku- ja päätepisteen osoitteisiin. Lisäksi protokolla-, kokonaispituus- ja header checksum -kentät päivitetään vastaamaan muokattua datagrammia. [7]

Jotta datagrammi voidaan reitittää tunnelin jälkeen oikein, IP-otsikon taakse lisätään minimaalinen uudelleenlähetysotsikko (engl. Minimal Forwarding Header). Tämä otsikko sisältää alkuperäiset lähde- ja kohdeosoitteet sekä toteutukseen liittyviä kenttiä. Datagrammin datakenttä enkapsuloidaan muuttumattomana tämän uudelleenlähetysotsikon taakse. [7]. Kuvassa 3 esitellään, miten minimaalinen enkapsulointi toteutetaan datagrammille.



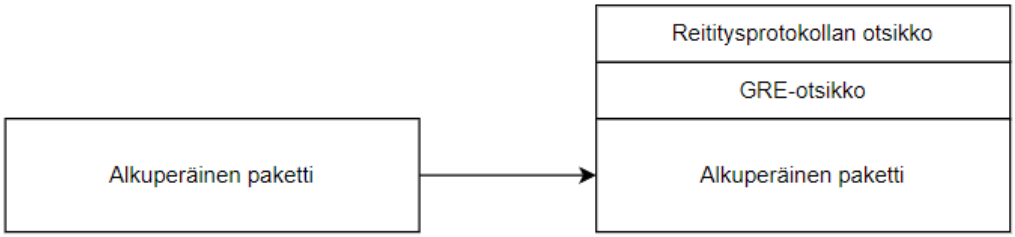
Kuva 3: *Minimaalinen enkapsulointi*

Tunnelin päätepisteessä alkuperäinen IP-otsikko muokataan alkuperäiseen muotoonsa palauttamalla lähde- ja kohdeosoitteet uudelleenlähetysotsikosta ja muokkaamalla IP-otsikon muut kentät vastaamaan alkuperäistä datagrammia. Tämän jälkeen datagrammi reititetään normaalisti kohdeosoitteeseen, mikäli se eroaa tunnelin päätepisteestä. Minimaalista enkapsulointia voidaan hyödyntää esimerkiksi myöhemmin esitellyssä Mobile IP -tekniikassa. [7]

3.3 GRE

Monenlaisten verkkojen yli tunnelointia varten voidaan käyttää RFC 2784:ssä määriteltyä GRE-tunnelointia (Generic Routing Encapsulation). GRE on määritelty

yleisemmällä tasolla kuin aiemmin esitellyt menetelmät, koska sen on tarkoitus sovittaa erilaisia reititysprotokollia yhteen. Se ei siis ole ainoastaan IP-tunnelointimenetelmä. GRE-menetelmä on esitelty kuvassa 4. Paketin saapuessa GRE-tunnelin alkupisteeseen se enkapsuloidaan muuttumattomana GRE-otsikon taakse. GRE-otsikon eteen asetetaan kuljetusotsikko, joka vastaa sen verkon reititysprotokollaa, jossa tunneli sijaitsee. GRE-otsikko sisältää alkuperäisessä paketissa käytetyn protokollan sekä toteutukseen liittyviä kenttiä. [8]



Kuva 4: *GRE*

Paketti reitite tään ulomman otsikon mukaan tunnelin läpi muuttumattoman. Paketin saavuttua tunnelin päätepisteeseen sen enkapsulointi puretaan ja se reitite tään alkuperäisen otsikon mukaan kohteeseen. [8]

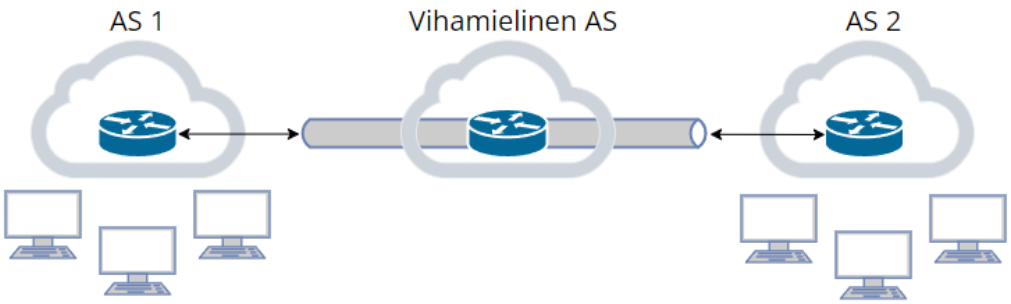
3.4 Tunnelointiteknologioiden tietoturva

Tunnelointi ei yleisesti tarjoa datan salauksen palveluja, mutta enkapsulointia voidaan käyttää suojaamaan viestintää autonomisten systeemien välillä. Abu-Amara, Asif, Sqalli, Mahmoud ja Azzedin esittelevät tutkimuksessaan (2011) [8] internetin palveluntarjoajien (ISP) aiheuttamia vaaroja ja tunneloinnin tuomia ratkaisuja. Autonomisella systeemillä (AS) tarkoitetaan verkkoa, jota ohjaa itsenäinen hallinnollinen jäsen. [8]

Tutkimuksen mukaan on tärkeää pystyä suojaamaan tiedonsiirto myös niiltä tahoilta, jotka hallinnoivat verkkoa. Internetin palveluntarjoajilla voi olla poliittisia tai sotilaallisia syitä tarkkailla ja vaikuttaa ihmisten väliseen viestintään esimerkiksi konfliktialueilla. Internetin palveluntarjoaja pystyy tarkkailemaan ja estämään viestintää, joka kulkee sen hallinnoiman autonomisen systeemin läpi, jos minkäänlaisia suojaamistoimenpiteitä ei käytetä. [8]

Tutkimuksessa esitellään keino ohittaa vihamieliset autonomiset systeemit tunneloinnin avulla. Verkon arkkitehtuurin täytyy olla sellainen, että tunnelin lähtö- ja päätepisteet sijaitsevat reitillä vihamielisen autonomisen systeemin molemmin puolin, jotta tunnelointi

voidaan tehdä suoraan vihamielisen systeemin läpi. Tutkimuksessa simuloitiin tällaista tilannetta ja käytettiin tunnelointiin IP-in-IP- ja GRE-tunnelointia ja tutkittiin niiden vaikutusta verkon suorituskykyyn. Kuvassa 5 esitellään verkon arkkitehtuuri, johon tällaista tekniikkaa voidaan soveltaa. [8]



Kuva 5: *Tunnelointi vihamielisen AS:n läpi*

Tutkimuksen mukaan viestinnän tunnelointi ei merkittävästi vaikuttanut verkon suorituskykyyn. Viestinnän viive lähteestä kohteeseen kasvoi, mutta vaikutus oli lähes merkityksetön. Erot tekniikoiden välillä olivat pieniä, mutta parhaiten suoriutui IP-in-IP-tekniikka. Tällainen ratkaisu voisi siis auttaa turvaamaan viestintää vihamielisiltä internetin palveluntarjoajilta vaikuttamatta kuitenkaan merkittävästi verkon suorituskykyyn. [8]

4. MOBILE IP

Nykypäivän langattomissa mobiiliverkoissa käytetty IP-tunneloinnin sovellus on Mobile IP. Mobile IP tarjoaa käyttäjilleen mahdollisuuden liikkua autonomisten systeemien välillä joutumatta vaihtamaan IP-osoitettaan. Mobile IP:n avulla esimerkiksi mobiililaitteen käyttäjä pystyy liikkumaan niin verkkojen kuin maantieteellisten sijaintienkin läpi tehokkaasti, koska käyttäjä pystytään aina tavoittamaan samasta IP-osoitteesta. [9]

4.1 Toiminta

Mobile IP toimii IPv4- ja IPv6-verkoissa hieman eri tavalla. Molemmissa verkoissa tekniikkaan liittyy olennaisesti termit kotiverkko, vierasverkko, kotiagentti, vierasagentti ja mobiilisolmu. Kotiverkolla tarkoitetaan verkkoa, jossa käyttäjä on saanut IP-osoitteensa, ja vierasverkko on verkko sen ulkopuolella. Mobiilisolmu (”mobile node”) on mobile IP:n käyttäjä, joka liikkuu kotiverkkonsa ulkopuolella [9]. Kotiagentti (”home agent”) on reititin, joka tunneloi datagrammeja mobiilisolmulle, kun se on poistunut kotiverkostaan. Vierasagentti (”foreign agent”) on reititin vierasverkossa, joka toimii tunnelin päätepisteenä ja reitittää kotiagentilta saadut datagrammit mobiilisolmulle. [10]

Kun mobiilisolmu on lähtenyt kotiverkostaan, sille lähetetyt datagrammit eivät luonnollisesti pääse perille normaalien reittien kautta. Jotta reititys voidaan toteuttaa, mobiilisolmun on tiedettävä olevansa vieraassa verkossa, ja mitkä verkon solmut ovat niin sanottuja mobiiliagentteja eli verkon käyttäjiä, jotka voivat tarjota Mobile IP -palveluja. Mobiilisolmu tarkkailee jatkuvasti saatavilla olevia reittejä verkossa ja tunnistaa reittien ilmaantumista ja katoamista, mikä auttaa mobiilisolmua määrittämään sijaintinsa [9]. Todellisuudessa sijainnin määrittäminen on monimutkaisempaa ja hyödyntää myös muiden kerroksien protokollia. Sen syvempi tarkasteleminen ylittää tämän työn rajat.

Kun mobiilisolmu saa tiedon sijainnistaan vierasverkossa, sen täytyy saada selville verkossa saatavilla olevat Mobile IP -resurssit. Verkossa olevat vierasagentit voivat mainostaa omia palvelujaan itse ”router advertisement” -viesteillä, joissa reitittimet kertovat olevansa vierasagentteja ja ilmoittavat tarjoamistaan palveluista. Reitittimet lähettävät näitä viestejä tasaisin väliajoin. Jos mobiilisolmu ei halua odottaa reitittimien lähettämiä viestejä, se voi tiedustella verkolta ”router solicitation” -viesteillä. Näihin viesteihin vierasagentit vastaavat ”router advertisement” -viestien tapaisesti. Sekä

advertisement- että solicitation -viestit käyttävät verkkokerroksen ICMP Router Discovery Protocol -protokollaa (IRDP). [9]

Mobiilisolmun ollessa vierasverkossa sille lähetetyt datagrammit reititetään sen saamaan CoA:an (Care of Address). CoA on mobiilisolmulle määritetty väliaikainen IP-osoite tietyssä vierasverkossa. Mobiilisolmu voi saada CoA:n kahdella eri tavalla. Vierasagentit lähettävät IRDP-viesteissään yhden tai useamman IP-osoitteen oman verkkonsa saatavilla olevista IP-osoitteista, jolloin on kyseessä FA CoA (Foreign Agent Care of Address). Mobiilisolmu voi myös itse hakea itselleen CoA:n DHCP:n tai muun osoitteiden hallintaprotokollan kautta, jolloin on kyseessä CCoA (Colocated Care of Address). Näistä kahdesta tavasta FA CoA on tehokkaampi, mutta CCoA on laajemmassa käytössä, koska se on yksinkertaisempi. [9]

Saatuaan CoA:n mobiilisolmu siirtyy rekisteröintivaiheeseen. Mobiilisolmu lähettää kotiagentilleen RRQ-viestin, jossa se ilmoittaa olevansa vierasverkossa ja antaa kotiagentille CoA:nsa. Kotiagentti vastaa RRP-viestillä, jolla se hyväksyy rekisteröinnin ja antaa sille elinajan. Elinajan sisällä mobiiliagentin on lähetettävä uusi RRQ-viesti tai muuten rekisteröinti täytyy suorittaa uudestaan. [9]

Rekisteröimisen jälkeen datagrammit voidaan reitittää tunneloimalla mobiilisolmulle sen ollessa vierasverkossa. Oletuksena Mobile IP:ssä käytetään aikaisemmin esiteltyä IP-in-IP-tunnelointia, mutta käyttäjät voivat pyytää myös eri tunnelointimenetelmiä, kuten Minimal Encapsulation ja GRE-enkapsulointi. Tunnelointimenetelmän valinta tapahtuu RRQ-viestin kautta. [9]

Tunnelointi tapahtuu lähtökohtaisesti viestinnässä verkon käyttäjältä (kutsutaan myös engl. correspondent node) mobiilisolmulle. Mobiilisolmulta käyttäjälle lähtevät viestit reititetään sen sijaan suoraan käyttäjän IP-osoitteeseen. Se voi kuitenkin aiheuttaa ongelmia, koska käyttäjä lähettää datagrammeja eri osoitteeseen kuin se, josta se vastaanottaa niitä. Käyttäjä lähettää datagrammin, jonka kohdeosoitteena on mobiilisolmun kotiosoite ja saa vastauksen, jossa lähdeosoitteena on mobiilisolmun CoA. Järjestelmälle on tietoturvan kannalta turvallisempaa, jos tällainen pystytään välttämään, ja siksi on mahdollista tunneloida viestintä myös mobiilisolmulta käyttäjälle käänteistunneloinnin avulla. [9]

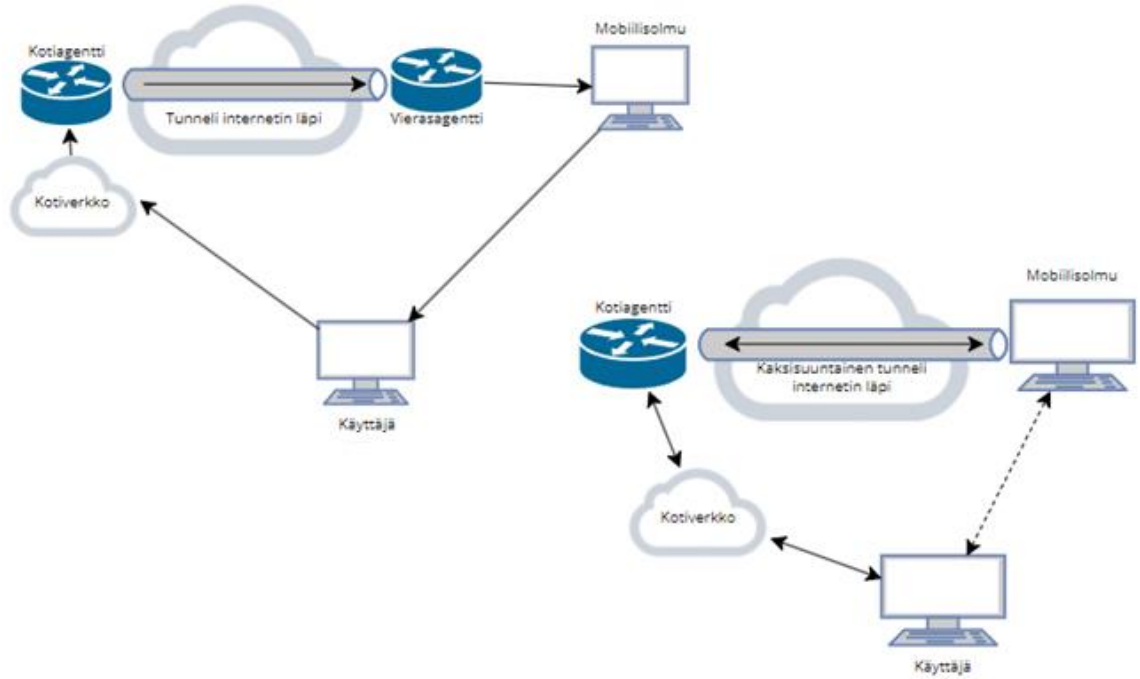
Käänteistunnelointi (engl. reverse tunneling) aloitetaan pyynnöllä, joka voidaan sisällyttää RRQ-viestiin. Rekisteröinti tapahtuu samankaltaisesti normaalin rekisteröinnin kanssa. Käänteistunnelointia käytettäessä kaikki viestintä tapahtuu vieras- ja kotiagentin kautta, jolloin lähde- ja kohdeosoitteet vastaavat toisiaan. [11]

4.2 Erot IPv4 ja IPv6 välillä

IPv6-protokolla tarjoaa Mobile IP:n toteuttamiseen palveluja, jotka tekevät toteutuksesta suoraviivaisempaa. Laajemman ja monipuolisemman otsikkokentän lisäksi Mobile IP on myös otettu huomioon IPv6:n suunnittelussa. Suurimpia eroja Mobile IPv4:n ja IPv6:n välillä ovat vierasagentin puuttuminen, uudenlaiset tavat reitittää viestejä mobiiliagentin ja käyttäjän välillä sekä lisätyt turvallisuusominaisuudet. [9]

Mobile IPv6 ei vaadi toimintaansa vierasagenttia. Rajoitetun IPv4-osoiteavaruuden takia Mobile IPv4 vaati vierasagenttien käyttöä. Vierasagentit pystyivät tarjoamaa usealle mobiilisolmulle saman CoA-osoitteen omassa verkossaan, mikä säästi käytettyjen osoitteiden määrää. IPv6 osoitteiden määrä on niin suuri, että samanlaista ongelmaa ei tarvitse ratkaista Mobile IPv6:ssa. [9]

Viestintä tapahtuu kaksisuuntaisella tunneloinnilla (engl. bidirectional tunneling) tai reitin optimoinnilla (engl. route optimization). Kaksisuuntainen tunnelointi vastaa Mobile IPv4:ssä tehtyä käänteistunnelointia, ilman vierasagenttia [9]. Kuvassa 6 esitetään yksinkertaistettuna, miten datagrammien kulkeutuminen eroaa Mobile IPv4:n ja IPv6:n välillä. Katkoviiva kuvaa reitin optimointia.



Kuva 6: *Viestinnän ero IPv4 ja IPv6 välillä. Kuvassa vasemmalla on IPv4-toteutus ja oikealla IPv6-toteutus*

Reitin optimointi vaatii molempien osapuolien käyttävän Mobile IPv6:ta. Mobiilisolmu aloittaa reitin optimoinnin viestimällä käyttäjälle samanaikaisesti kahta reittiä pitkin. Toinen reitti kulkee kaksisuuntaisen tunnelin kautta kotiagentille, joka reitittää edelleen käyttäjälle. Toinen reitti kulkee suoraan mobiiliagentilta käyttäjälle. Saatuaan molemmat viestit käyttäjä viestittää mobiilisolmulle samoja reittejä pitkin. Tätä prosessia kutsutaan Return Routability -testiksi. [9]

Mikäli viestintä on onnistunut, käyttäjä voi jatkossa käyttää kohdeosoitteenaan mobiilisolmun CoA-osoitetta ja mobiilisolmu käyttäjän normaalia IP-osoitetta. Reitin optimoinnin mahdollistaa IPv6-otsikon ominaisuus, jonka avulla mobiilisolmu lähettää oman kotiosoitteensa käyttäjälle otsikon sisällä. Reitin optimointi mahdollistaa viestien kulkemisen tehokkaammin käyttäjän ja mobiilisolmun välillä, koska niiden väliltä on usein löydettävissä tunnelia tehokkaampi reitti. [9]

4.3 Mobile IP:n sovelluskohteita

Mobile IP -teknologiaa on ehdotettu täydentämään IEEE 802.11 WiFi -teknologiaa. Mobile IP:n ja WiFi:n välinen siirtymä ei ole saumaton. Mobile IP-käyttäjän liittyessä WiFi-lähiverkkoon tämän verkon ”WLAN access point” -reititin voi estää pakettien saapumisen ja lähettämisen käyttäjältä, kunnes WiFi-yhteys on muodostettu. Yhteyden muodostaminen vaatii ylempien kerroksien protokollia, joista Mobile IP ei ole tietoinen. WiFi-yhteyden luominen voi siten estää Mobile IP -rekisteröintivaiheen. [9].

WiFi-yhteyden vahvistaminen voitaisiin toteuttaa siirtoyhteyskerroksella toimivalla EAP-protokollalla (Extensible Authentication Protocol). Se hyödyntää GSM SIM -teknologiaa vahvistaakseen WiFi-käyttäjiä yhteyden muodostuksessa. EAP-protokolla ei vaadi käyttäjän syötettä, joten verkkoon liittyminen olisi saumattomampaa, ja koska se on siirtoyhteyskerroksen protokolla, Mobile IP-rekisteröinti tapahtuisi normaalisti myös WiFi-verkossa. [9].

Pries, Mäder, Staehle ja Wiesen (2006) esittelevät konferenssijulkaisussa Mobile IP:n käyttöä liikuttaessa IEEE 802.11 WLAN-lähiverkon aliverkosta toiseen. Käsiteltävänä olivat tilanteet, joissa WLAN-lähiverkko sisältää useita aliverkkoja, joiden välillä liikutaan nopeasti. Tulosten mukaan normaalin Mobile IP:n rekisteröintivaiheen viive on liian suuri tällaiseen sovelluskohteeseen. Kuitenkin, ”Fast Mobile IPv6” -teknologia voisi mahdollistaa tämän sovelluskohteen. [12]. Fast Mobile IP on teknologia, joka vähentää verkon vaihtumisesta aiheutuvaa viivettä mobiilisolmun ollessa liikkeellä [9].

Yassein, Aljawarneh ja Al-sarayrah (2017) käsittelevät konferenssijulkaisussa eri mobiliteettiprotokollien käyttöä IoT-teknologiassa. IoT-laitteet ovat usein mobiilisolmuja,

jotka vaativat Mobile IP:n tarjoamia palveluja saumattomuuden takaamiseksi verkkojen välillä. Julkaisussa vertaillaan eri mobiliteettiprotokollien tuomia ratkaisuja IoT:n ongelmiin, kuten skaalautuminen ja QoS. Mobile IPv6:n päälle kehitetyt protokollat, kuten Fast Mobile IPv6 ja ”Clustered Mobile IPv6”, vähentävät verkon vaihtumiseen liittyvää viivettä, pakettien katoamista ja energiankulutusta IoT-systeemeissä. [13]

5. VPN JA TIETOTURVA

VPN (Virtual Private Network) -teknologia on laajasti yritys- ja yksityiskäytössä oleva IP-tunneloinnin sovelluskohde. VPN-verkot tarjoavat käyttäjilleen yksityisyyttä ja tietoturvaa hyödyntämällä samalla laajan internetverkon tarjoamia resursseja. Niiden avulla laajemman tietoverkon sisälle voidaan luoda yksityinen verkko, jonka viestintä on verkon ulkopuolisille käyttäjille käytännössä näkymätöntä. VPN-teknologiaa toteutetaan siirtoyhteys-, verkko- ja kuljetuskerroksilla. Tässä työssä keskitytään pääasiassa VPN:n toimintaan verkkokerroksella.

5.1 VPN-verkkojen toteutus

Yksityisten, tietoturvallisten verkkojen toteutus ennen VPN-teknologiaa oli mahdollista alemmilla protokollakerroksilla. Siirtoyhteyskerroksella se tarkoitti esimerkiksi Frame Relay -teknologiaa, joka perustui ethernet-kehysten enkapsulointiin ja kytkinten väliseen ”reitittämiseen”. Fyysisellä kerroksella tällaisia verkkoja voidaan toteuttaa asentamalla fyysisiä kaapeleita verkon laitteiden välillä, jolloin voidaan täysin estää ulkopuolisten pääsy verkkoon. Molemmat näistä toteutustavoista ovat kuitenkin huonosti skaalautuvia ja kustannuksiltaan tehottomia. [14]

VPN-teknologialla voidaan tarkoittaa monenlaisia erilaisia käytännön toteutuksia. Toteutukset koostuvat kuitenkin aina laitteista ja yksityisistä verkoista, jotka yhdistetään internetin yli tunnelointimenetelmillä. Verkon eri osia yhdistetään toisiinsa ”VPN Gateway” -reitittimillä, joiden välinen tietoliikenne on kyseisen toteutuksen mukaan salattua ja enkapsuloitua. [15]

VPN-verkon toteutukseen voidaan käyttää useita eri teknologioita riippuen vaadittavista tietoturvan palveluista. Yksi esimerkki tästä on edellä esitelty GRE-protokolla, joka tarjoaa pelkästään pakettien enkapsulointiin liittyviä palveluja. Tässä työssä keskitytään verkkokerroksen IPsec VPN -toteutukseen, joka tarjoaa käyttäjilleen datan luottamuksellisuuden, eheyden ja todennuksen takaavia palveluja. [15]

5.2 IPsec

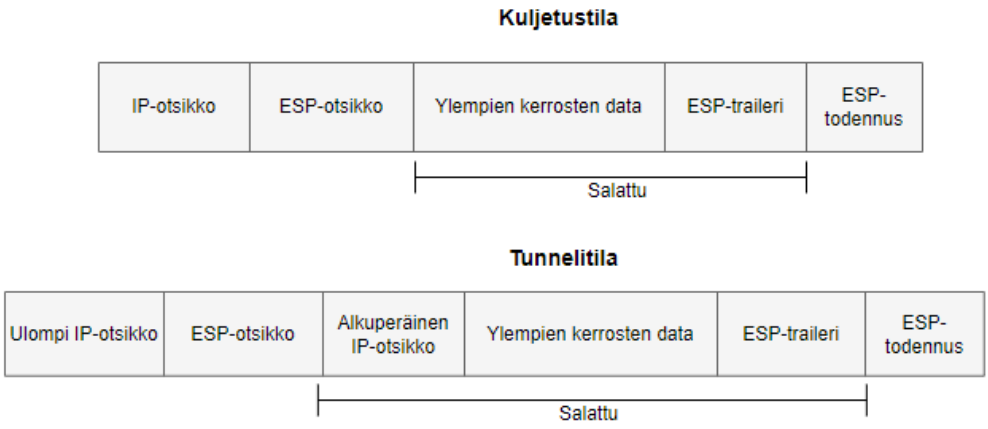
VPN-teknologiassa hyödynnetään laajasti verkkokerroksella toimivaa IPsec:iä (IP security). IPsec sisältää useita protokollia, joiden tarkoituksena on tarjota turvallista IP-viestintää epäluotettavien verkkojen läpi. IPsec tarjoaa käyttäjilleen kaksi mahdollista käyttötilaa: kuljetustila (transport mode) ja tunnelitila (tunnel mode), jotka muokkaavat

alkuperäistä IP-kehystä eri tarkoituksia varten. IP-kehys tunneli- ja kuljetustilassa on esitelty kuvassa 7. [16]

5.2.1 Tunneli- ja kuljetustila

IPsec-kuljetus- ja tunnelitilat käyttävät ESP-protokollaa datan salaamiseen. ESP (Encapsulating Security Payload) tarjoaa käyttäjilleen datan luottamuksellisuuden, alkuperän varmistamisen, eheyden ja datavirran luottamuksellisuuden takaavia palveluja. ESP:n tarjoamat palvelut riippuvat IPsec-yhteyden luomisessa sovituista parametreista ja IPsec-tilasta. ESP lisää IP-kehykseen ESP-otsikon, -trailerin ja -todennusosan. ESP-otsikon jälkeen tuleva data salataan aina ESP-trailerin loppuun asti, jonka jälkeen todennusosan avulla varmistetaan datan autenttisuus ja muuttumattomuus. [16]

Kuljetustilassa IP-datagrammista salataan ylempien protokollakerrosten käyttämän datan. ESP-otsikko luodaan alkuperäisen IP-otsikon taakse, ja traileri sekä todennusosa luodaan IP-datagrammin perään. Tunnelitilassa IP-datagrammi salataan kokonaisuudessaan. Alkuperäisen IP-otsikon eteen luodaan ESP-otsikko, jonka eteen luodaan uusi, ulompi IP-otsikko, joka eroaa alkuperäisestä. Traileri ja todennusosa luodaan kehyksen perään samoin kuin kuljetustilassa. Tunnelitila siis salaa myös alkuperäisen IP-otsikon, joten IP-paketin lähde- ja kohdeosoitteet ovat myös näkymättömiä ulkopuolisille. [16]



Kuva 7: *IPsec-kuljetus- ja tunnelitila*

Molemmilla IPsec-tilalla on omat käyttökohteensa. Kuljetustila on tehokkaampi ja sen toteuttaminen vaatii vähemmän toimenpiteitä. Datan salaamista voidaan myös toteuttaa ylemmillä protokollakerroksilla, joten mikäli alkuperäisen IP-otsikon salaaminen ei ole

käyttäjille olennaista, kuljetustila tarjoaa tehokkaamman palvelun. Tunnelitilaa käytetään, kun paketteja reititetään laajemman epäluotettavan verkon läpi. Tunnelitilaa käytetään myös, jos turvallisuuspalvelut toteutetaan pakettien lähettäjän tai vastaanottajan ulkopuolella. Esimerkiksi VPN-verkossa IP-paketti voidaan ensin lähettää salaamattomana reitittimelle, joka enkapsuloi paketin tunnelitilaan ja lähettää sen internetin kautta kohdeverkkoon. Kohdeverkossa vastaava reititin voi purkaa salauksen ja lähettää alkuperäisen paketin salaamattomana alkuperäiselle paketin vastaanottajalle. [17]

5.2.2 SA ja IKE

SA (Security Association) on tietoturvallisuudessa olennainen termi, joka määrittää parametrejä, joiden pohjalta tietoturvapalveluja määritetään. SA on uniikki, ja se luodaan jokaiselle IPsec-yhteyden päätepisteelle erikseen. SA:n tarjoamat tietoturvapalvelut riippuvat valitusta turvallisuusprotokollasta (esim. ESP), SA-tilasta (esim. kuljetus- tai tunnelitila), yhteyden päätepisteistä ja mahdollisista lisäpalveluista. [18]

SA:n luominen sisältää datan salaamiseen tarvittavat salausavaimet ja niiden vaihtamisen osapuolten välillä. Salausavainten avulla IPsec-yhteyden laitteet pystyvät salaamaan ja jälleen purkamaan salauksen lähetetystä datasta. Nämä avaimet voidaan asettaa manuaalisesti tai automaattisesti. Avainten manuaalinen asettaminen ei skaalaudu tehokkaasti laitteiden määrän kasvaessa, joten IPsec käyttää usein automaattista IKE-protokollaa (Internet Key Exchange). [16]

IKE-protokollan avulla osapuolet pystyvät neuvottelemaan SA-parametreistä turvallisen yhteyden yli. IKE koostuu kahdesta vaiheesta: neuvotteluyhteyden muodostaminen ja varsinaisten IPsec SA-parametrien vaihtaminen. Ensimmäisen vaiheen neuvotteluyhteydellä tarkoitetaan IKE-protokollan määrittämää SA-yhteyttä, jolla on protokollan määrittelemät parametrit. IKE SA -yhteys mahdollistaa IPsec SA-parametrien vaihtamisen turvallisen yhteyden yli. Toisessa vaiheessa osapuolet luovat ja vaihtavat SA-parametrit, kuten salaus- ja todentamisalgoritmit. [17]

5.3 IPsec yhdistettynä GRE-enkapsulointiin

Ogudo analysoi tutkimuksessaan (2019) [19] GRE-menetelmän tietoturvallisuutta. Aiemmin esitelty GRE tarjoaa pelkästään enkapsuloinnin palveluja, joten se ei tarjoa täydellistä tietoturvaa esimerkiksi VPN-toteutuksiin. Aikaisemmin todettiin tunneloinnin GRE- tai IP-in-IP-enkapsuloinnilla olevan tehokas tapa suojata tietoliikennettä kuormittamatta verkkoa. Tutkimuksessaan Ogudo yhdistää IPsec:in ja GRE:n ja vertailee niiden yhteisvaikutusta pelkkään GRE-enkapsulointiin [19].

Tutkimuksessa simuloitiin verkkoa, johon luotiin kaksi tunnelia. Molempien tunneleiden lähtöpisteissä paketit GRE-enkapsuloitiin ja toisessa enkapsuloitu paketti salattiin IPsec-tekniikalla. Paketteja kaapattiin tunnelista, jotta voitiin simuloida hyökkäystä, jossa vihamielinen tekijä yrittää saada selville sen läpi kulkevien pakettien tietoja. Pelkkien GRE-enkapsuloitujen pakettien sisältö saatiin selville, koska GRE ei tarjoa datan salaamisen palveluja. IPsec-tekniikalla salatut paketit sen sijaan pysyivät salattuina. [19]

Aikaisemmin esitelty tutkimus osoitti GRE:n suojaavan tietoliikennettä hyökkäyksiltä, joissa tarkoituksena on häiritä verkkoa ja vaikeuttaa tiedonsiirtoa. Tässä tutkimuksessa simuloitiin hyökkäystä, jossa tarkoituksena on sen sijaan saada selville lähetettyjen pakettien sisältö. Tutkimuksessa osoitettiin, että GRE-enkapsulointiin lisätty IPsec-salaus on tehokas tapa suojautua tällaista hyökkäystä vastaan esimerkiksi VPN-toteutuksissa [19].

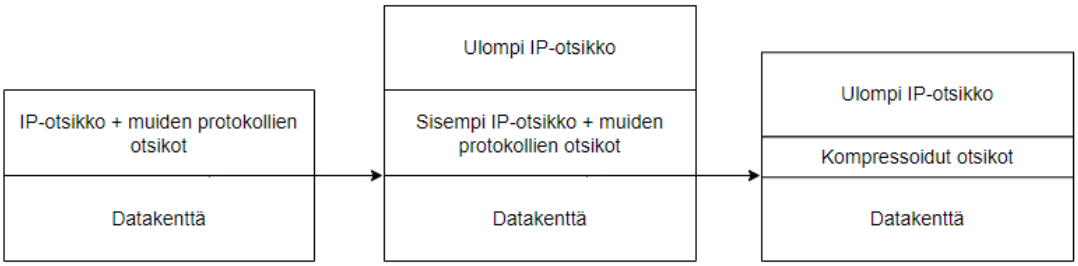
6. IP-TUNNELOINNIN MUITA SOVELLUKSIA

6.1 TuCP

IP-tunnelissa pakettia reititetään uloimman otsikon perusteella ja alkuperäinen datagrammi säilyy muuttumattomana eikä sen sisältämiä tietoja tarvita ennen tunnelin päätepistettä. Siitä syystä tunnelointiin sisältyy paljon ylimääräistä tiedonsiirtoa. Eri protokollakerroksilla ylimääräistä tiedonsiirtoa voidaan vähentää kompressoinnilla. Ylimääräisen tiedonsiirron vähentäminen on tärkeää erityisesti langattomissa järjestelmissä ja esimerkiksi IoT-teknologiassa. Konferenssijulkaisussaan Rawat ja Bonnin (2010) esittelevät TuCP-protokollan (Tunneling Header Compression Protocol), joka tarjoaa kompressoinnin palvelua IP-tunnelointiin. [20]

TuCP-protokolla toimii normaalin tunneloinnin ohessa. Reitittämiseen IP-tunnelissa vaaditaan vain ulompi IP-otsikko, joten TuCP kompressoi alkuperäisen IP-otsikon sekä mahdolliset muiden protokollien otsikot. Kompressointi tapahtuu enkapsuloinnin jälkeen, mutta ennen paketin lähettämistä verkkoon. Protokolla asettaa kompressoija ja dekompressoija -yksiköt tunnelin lähtö- ja päätepisteisiin, joiden välissä kompressointi tapahtuu. [20]

Tunnelin lähtö- ja päätepisteet neuvottelevat yhteyden alustusvaiheessa kompressointiin vaadittavat parametrit. Näitä ovat esimerkiksi kompression tyyppi ja lähetettävien otsikoiden staattiset ja dynaamiset osat. Kompressointi aloitetaan, kun TuCP-kompressoijayksikkö vastaanottaa enkapsuloidun IP-datagrammin. Sen jälkeen se kompressoi kaikki otsikot lukuun ottamatta ulompaa IP-otsikkoa ja lähettää datagrammin tunneliin. Tunnelissa datagrammi reititetään normaalisti uloimman otsikon mukaan. Dekompressoijayksikkö vastaanottaa datagrammin ja purkaa kompressoinnin. Sen jälkeen tunnelin päätepisteessä enkapsulointi poistetaan ja datagrammi reititetään normaalisti. Paketin kompressointi on esitelty yksinkertaisesti kuvassa 8. [20]



Kuva 8: *TuCP IP-in-IP-enkapsuloinnille*

TuCP ei vaadi toimintaansa tiettyä enkapsulointimenetelmää. Kuvan 8 esimerkissä enkapsulointi tehdään IP-in-IP-menetelmällä. Konferenssijulkaisun tarjoamien tutkimustulosten mukaan TuCP:ta kuvaillaan tehokkaana ja robustina palveluna otsikoiden kompressointiin. TuCP tarjoaa myös pakettien järjestyksen takaavan palvelun. [20]

6.2 GTP

GTP (GPRS Tunneling Protocol) on IP-tunnelointiprotokolla, joka käyttää IP-datagrammeja pakettikytkentäisen datan tunnelointiin mobiiliverkoissa, kuten GSM (2G), UMTS (3G), LTE (4G) ja NR (5G). GPRS (General Packet Radio Service) viittaa mobiiliverkkojen pakettikytkentäiseen osa-alueeseen. Sanastokeskus määrittelee pakettikytkentäisen verkon näin: ” televerkko, jossa siirrettävä data jaetaan määrämuotoisiksi jaksoiksi eli paketeiksi ja lähetetään pakettiin liitetyn osoitteen perusteella halutulle vastaanottajalle” [21]. Tässä kontekstissa sillä tarkoitetaan mobiiliverkkojen osa-aluetta, joka siirtää tietoa IP-datagrammeina mahdollistaen esimerkiksi internet-pohjaisten palveluiden käytön matkapuhelimilla. [22]

6.2.1 GTP-C ja GTP-U

GTP tunneloi käyttäjien dataa ja verkon toimintaan vaadittavaa signalointidataa GSN-solmujen (GPRS Support Node) välillä. GSN-solmuja ovat SGNS (Serving GNS) ja GGNS (Gateway GNS). SGNS yhdistää radioverkon GPRS-verkkoon. Radioverkko sisältää fyysiset antennit, jotka tarjoavat matkapuhelimille langattoman yhteyden. GGNS sovittaa internetin GPRS-verkkoon. [23]

GTP sisällyttää kaksi aliprotokollaa GTP-C (Control Plane) ja GTP-U (User Plane). GTP-C:tä käytetään tunneleiden hallitsemiseen. Se viestii GSN-solmuille informaatiota, jonka perusteella solmut luovat, muokkaavat ja lopettavat tunneleita solmujen välillä. GTP-C-viestit koostuvat GTP-otsikosta ja vaihtelevasta määrästä informaatiobittejä. [24]

GTP-U toteuttaa protokollan tarjoaman enkapsuloinnin palvelut. Datagrammin saapuessa internetistä GGSN-solmulle, GTP-C luo tarvittavat tunnelit datagrammin kohdeosoitteen mukaan. Tämän jälkeen GTP-U enkapsuloi datagrammin asettamalla GTP-otsikon datagrammin eteen. Otsikon TEID-kentän (Tunnel Endpoint Identifier) perusteella paketti reititetään GPRS-verkon läpi tunnelin päätepisteeseen, joka on SGNS-solmu. SGNS-solmussa paketin enkapsulointi puretaan, ja radioverkko välittää paketin lopulliseen kohteeseen. [24]

6.2.2 GTP-otsikko

GTP-otsikko on vaihtelevan mittainen otsikko, jota käytetään GTP-C:ssä ja GTP-U:ssa. Taulukko 1 on 3GPP:n standardi GTP-otsikolle GTP-protokollan määrittelydokumentista. 3GPP (3rd Generation Partnership Project) on yhteistyöorganisaatio, joka kehittää ja määrittelee mobiiliverkkojen teknologioita. [25]

Taulukko 1: *GTP-otsikon määrittely 3GPP:n dokumentissa. Muokattu lähteestä* ***[24]***

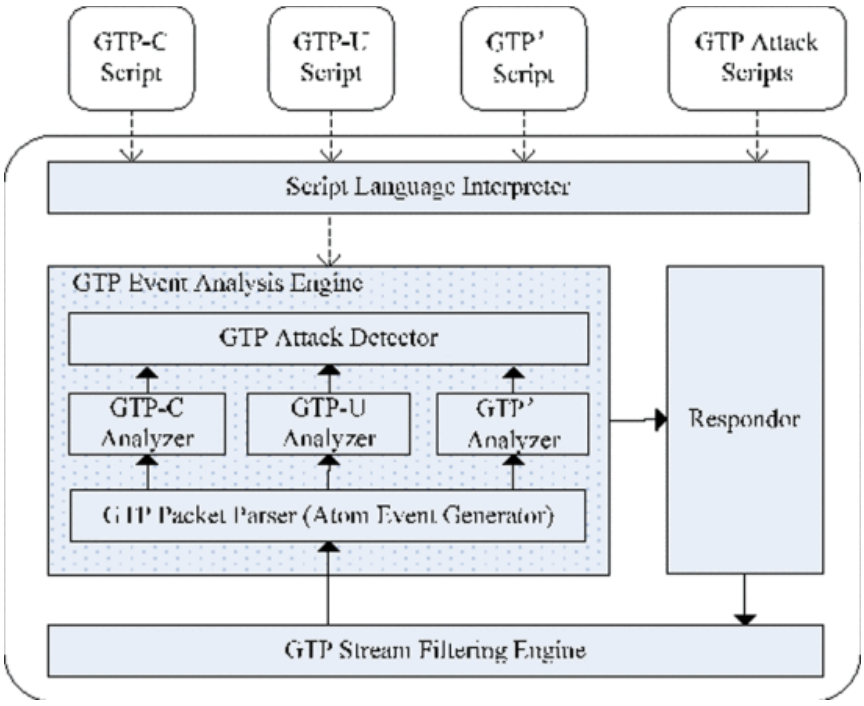
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	Version			PT	(*)	E	S	PN
2	Message Type							
3	Length (1st Octet)							
4	Length (2nd Octet)							
5	Tunnel Endpoint Identifier (1st Octet)							
6	Tunnel Endpoint Identifier (2nd Octet)							
7	Tunnel Endpoint Identifier (3rd Octet)							
8	Tunnel Endpoint Identifier (4th Octet)							
9	Sequence Number (1st Octet)							
10	Sequence Number (2nd Octet)							
11	N-PDU Number							
12	Next Extension Header Type							

Kaikkien otsikon kenttien esitteleminen ei ole oleellista tämän työn kannalta. GTP-C ja GTP-U käyttävät otsikkoa eri tavoilla hyödyntäen eri kenttiä. Ensimmäisen rivin kentät kertovat käytettävästä protokollasta ja kyseisen otsikon kenttien tulkinnasta. Message Type -kenttä kertoo, mikä viesti on kyseessä ja erottaa GTP-C ja GTP-U viestit toisistaan. TEID (Tunnel Endpoint Identifier) kertoo ne GSN-solmut, jotka toimivat tunnelin päätepisteinä. GTP-C käyttää näitä kenttiä hallinnoidakseen tunneleita ja GTP-U käyttää niitä enkapsuloitujen pakettien reitittämiseen. [24]

6.2.3 GTP:n turvallisuus

GTP on tärkeä protokolla pakettikytkentäisten mobiiliverkkojen toiminnalle. Peng, Yingyou, Dazhe ja Hong tutkivat julkaisussaan (2010) [26] GTP:n turvallisuuden riskejä UMTS-verkossa (yleisnimitykseltään 3G). GTP ei tarjoa tunneloinnin lisäksi turvallisuuden palveluja, joten se on riskialtis hyökkäyksille. GPRS yhdistää radioverkon internetverkkoon, mikä luo kahdenlaisia uhkia. Perinteisen radioverkon heikkouksia voidaan käyttää hyväksi IP-tekniikoilla, ja internetverkon heikkouksia voidaan käyttää hyväksi radioverkon avulla. GTP:n määrittelyssä ei oteta huomioon näitä turvallisuusuhkia, joten tutkimuksessa esitetään, että turvallisuuden palvelut toteutetaan erikseen. [26]

Tutkimuksessa esitetään GPRS-verkon arkkitehtuurin muuttamista siten, että siihen lisätään hyökkäyksien tunnistamisen ja estämisen toteuttavia yksiköitä. Hyökkäyksien tunnistamista varten esitetään koodikieli, jonka avulla mahdollistetaan GTP-tapahtumien analysoiminen. Tapahtumalla tarkoitetaan GTP-viestiä, joka voi olla normaali protokollan toimintaan liittyvä viesti tai datapaketti, tai hyökkäys. Kuvassa 9 nähdään tutkimuksessa esitetty GPRS arkkitehtuuri.



*Kuva 9: GPRS-arkkitehtuuri tutkimuksessa. Lähteestä **[26]***

”Script Language Interpreter” -yksikkö tulkitsee GTP-viestejä ja muuttaa ne tapahtumiksi esitetylle koodikielelle. ”GTP Stream Filtering Engine” suodattaa dataa ja mahdollistaa

turvallisten pakettien pääsyn systeemin läpi nopeasti. ”GTP Event Analysis Engine” jakaa paketit viestin tyypin mukaan GTP-C-, GTP-U- ja GTP’-analysointiyksiköille. ”GTP Attack Detector” tunnistaa analysointiyksiköiltä saadut tapahtumat ja erottaa hyökkäykset normaalista viestinnästä. ”Respondor” toteuttaa hyökkäyksen sattuessa tarvittavat toimenpiteet, jotka voivat olla esimerkiksi paketin tuhoaminen ja hyökkäyksen ilmoittaminen. [26]

Tutkimus toteutettiin laboratorio-olosuhteissa. Näissä olosuhteissa esitetty järjestely toimi hyvin, ja tutkimusta toivotaan jatkettavan todellisissa olosuhteissa UMTS-mobiiliverkossa. [26]

7. YHTEENVETO

Tässä työssä tutustuttiin IP-tunnelointiin ja siihen, miten IP-tunnelointi mahdollistaa turvallisen ja tehokkaan tietoliikenteen eri verkkojen välillä. Työn tavoitteena oli tarjota lukijalle kattava käsitys IP-tunneloinnin toiminnasta, toteutuksista ja sovelluskohteista sekä turvallisuusnäkökohdista.

Jotta IP-tunnelointia pystyttiin käsittelemään, oli ensin määriteltävä tärkeitä käsitteitä ja internetin rakenteita. IP-tunnelointi toteutetaan internetin kolmannella protokollakerroksella, verkkokerroksella. Verkkokerroksella käsitellään IP-datagrammeja, joita reititetään IP-otsikon perusteella. IP-tunnelointi perustuu juuri näiden datagrammien reitittämisen hallitsemiseen IP-otsikoiden avulla. Luvussa 3 esiteltiin kolme yleistä tunnelointitekniikkaa: IP-in-IP, minimaalinen enkapsulointi ja GRE. Jokaisella niistä on omat hyötynsä ja käyttökohteensa. Luvussa esiteltiin myös tutkimus, jossa tunnelointitekniikoita käytettiin sellaisenaan suojaamaan verkkoa hyökkäyksiltä.

Seuraavaksi, luvussa 4 käsiteltiin ensimmäistä sovelluskohdetta: Mobile IP -tekniikkaa. Mobile IP pyrkii tehostamaan internetin osoiteavaruuden käyttöä ja sujuvoittamaan käyttäjien liikkuvuutta. Se perustuu väliaikaisten IP-osoitteiden luovuttamiseen käyttäjälaitteille, jotta ne voivat pitää alkuperäisen osoitteensa. IP-tunnelointia hyödynnetään Mobile IP:ssä reitittämään datagrammeja internetin läpi käyttäen tätä väliaikaista osoitetta. Luvussa esiteltiin Mobile IP:n sovelluskohteita WLAN- ja IoT-teknologioissa.

Luvussa 5 käsiteltiin VPN-teknologiaa. VPN-verkoilla pystytään luomaan yksityisiä, suojattuja verkkoja käyttäen julkisen internetin resursseja. VPN-verkkoja voidaan toteuttaa eri tavoilla, mutta tässä työssä esiteltiin IPsec:iin perustuvaa toteutusta. Luvussa käsiteltiin IPsec:in toimintaa liittyen tiedon salaamiseen ja VPN-verkkojen toteuttamiseen sen avulla. Lisäksi esiteltiin toteutustapa, jossa IPsec yhdistetään aiemmin esiteltyyn GRE-enkapsulointiin.

Lopuksi työssä esiteltiin kaksi muuta IP-tunneloinnin sovellusta: TuCP ja GTP. TuCP-tekniikan avulla tunnelointia tehostetaan kompressoimalla eli tiivistämällä tunneloinnin otsikoita ja siten vähentämällä ylimääräistä tiedonsiirtoa. GTP on olennainen osa langattomia mobiiliverkkoja, joka yhdistää internetin radioverkkoihin, joita mobiililaitteet, kuten matkapuhelimet, käyttävät yhdistääkseen internetiin. Työn avulla lukijalle jää kattava käsitys monipuolisesta IP-tunnelointitekniikasta ja siitä, miten laajasti sitä voidaan soveltaa eri aloilla.

LÄHTEET

[1] J. F. Kurose and K. W. Ross, Computer Networking: A Top-down Approach, Viides painos ed., Pearson, 2009.

[2] Google, “IPv6 Adoption,” 2023. [Online]. Available: https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption. [Accessed 2 Lokakuu 2023].

[3] Information Sciences Institute, “RFC 791,” 1981.

[4] T. Anttalainen and V. Jaaskelainen, Introduction to Communication Networks, Ensimmäinen painos ed., Norwood: Artech House, 2014.

[5] C. Perkins, “RFC 2003,” 1996.

[6] S. Steffann, “RFC 7059,” 2013.

[7] C. Perkins, “RFC 2004,” IBM, 1996.

[8] M. Abu-Amara, M. A. K. Asif, M. H. Sqalli, A. Mahmoud and F. Azzedin, “Resilient Internet access using tunnel-based solution for malicious ISP blocking,” in *2011 IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, 2011.

[9] S. Raab, Mobile IP Technology and Applications, Ensimmäinen painos ed., Indianapolis: Cisco Press, 2005.

[10] C. Perkins, “RFC 3344,” Nokia Research Center, 2002.

[11] G. Montenegro, “RFC 3024,” 2001.

[12] R. Pries, A. Mäder, D. Staehle and M. Wiesen, “On the Performance of Mobile IP in Wireless LAN Environments,” in *Wireless Systems and Mobility in Next Generation Internet*, 2006.

[13] M. B. Yassein, S. Aljawarneh and W. Al-Sarayrah, “Mobility management of Internet of Things: Protocols, challenges and open issues,” in *2017 International Conference on Engineering & MIS (ICEMIS)*, 2017.

[14] J. S. Tiller, A Technical Guide to IPSec Virtual Private Networks, London: Auerbach Publishers, Incorporated, 2000.

[15] R. Deal, The complete cisco vpn configuration guide, Indianapolis: Cisco Press, 2005.

[16] J. H. Carmouche, IPsec virtual private network fundamentals, Cisco Press, 2007.

[17] N. Doraswamy, IPSec, Prentice Hall PTR, 2003.

[18] S. Kent and K. Seo, “RFC 4301,” BBN Technologies, 2005.

[19] K. A. Ogudo, “Analyzing Generic Routing Encapsulation (GRE) and IP Security (IPSec) Tunneling Protocols for Secured Communication over Public Networks,” in *2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, Winterton, 2019.

[20] P. Rawat and J.-M. Bonnin, “Designing a Header Compression Mechanism for Efficient Use of IP Tunneling in Wireless Networks,” in *2010 7th IEEE Consumer Communications and Networking Conference*, Las Vegas, 2010.

[21] T. sanastokeskus, “Matkaviestintäsanasto,” 2001. [Online]. Available: https://sanastokeskus.fi/tiedostot/pdf/Matkaviestinsanasto.pdf?file=pdf/Matkaviestinsanasto.pdf. [Accessed 10 Marraskuu 2023].

[22] 3rd Generation Partnership Project, “3G TS 29.060 version 3.0.0,” 10 Toukokuu 1999. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/29_series/29.060/. [Accessed 10 Marraskuu 2023].

[23] Y.-B. Lin and H. C. C. I. Rao, “General Packet Radio Service (GPRS): architecture, interfaces, and deployment,” in *Wireless communications and mobile computing*, Chichester, 2001.

[24] 3rd Generation Partnership Project, “3GPP TS 29.060,” 23 Syyskuu 2022. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/29_series/29.060/. [Accessed 11 Marraskuu 2023].

[25] 3rd Generation Partnership Project, “3GPP,” 3rd Generation Partnership Project, 13 Marraskuu 2023. [Online]. Available: https://www.3gpp.org/. [Accessed 13 Marraskuu 2023].

[26] X. Peng, W. Yingyou, Z. Dazhe and Z. Hong, “GTP Security in 3G Core Network,” in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, Wuhan, 2010.